МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА ДРАГОМАНОВА

Кваліфікаційна наукова праця на правах рукопису

МІНЕНКО ЄГОР СЕРГІЙОВИЧ

УДК 321:[351.746:007:004:056]:
[316:32]-021.387(477)(043.3)

ДИСЕРТАЦІЯ

РОЗВИТОК ІНСТИТУТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНОЇ УКРАЇНИ ЯК ЧИННИК СУСПІЛЬНО-ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ

Спеціальність 052 Політологія

Галузь знань 05 Соціальні та поведінкові науки

Подається на здобуття наукового ступеня доктора філософії. Дисертація містить результати власних досліджень. Використання чужих ідей, результатів і текстів мають посилання на відповідне джерело.

_____Є. С. Міненко

Науковий керівник:

Захаренко Костянтин Володимирович

доктор політичних наук, доцент

КИЇВ-2024

АНОТАЦІЯ

Міненко Є. С. Розвиток інститутів інформаційної безпеки сучасної України як чинник суспільно-політичної стабільності. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 052 - Політологія – Український державний університет імені Михайла Драгоманова, Київ, 2024.

Дисертація присвячена глибокому аналізу розвитку інститутів інформаційної безпеки в Україні з огляду на їх роль у забезпеченні суспільно-політичної стабільності. В умовах стрімкого розвитку інформаційних технологій та зростаючої глобалізації, тема інформаційної безпеки набуває ключового значення, особливо для держави, що зазнає міжнародної напруженості та інформаційно-психологічного впливу.

Дисертаційна робота побудована на трьох основних розділах, кожен з яких розглядає різні аспекти інформаційної безпеки.

В першому розділі дисертації здійснено теоретико-методологічний аналіз ролі інформаційної безпеки у забезпеченні суспільно-політичної стабільності. Подано фундаментальний підхід до визначення сутності інформаційної безпеки, акцентуючи увагу на міждисциплінарних та політологічних аспектах. Основна увага приділяється розгляду інформаційної безпеки як складової частини суспільно-політичної стабільності, що вимагає комплексного підходу до її аналізу та оцінки.

Висвітлено теоретичні основи дослідження суспільно-політичної стабільності через неоінституційний підхід, що дозволяє глибше розуміти механізми взаємодії між різними суб'єктами в контексті інформаційного простору. Це включає аналіз правових, соціальних та економічних аспектів, які формують умови для забезпечення інформаційної безпеки на національному та міжнародному рівнях.

Визначено роль і місце системи інформаційної безпеки в структурі суспільно-політичної стабільності, надаючи аналіз методів вивчення інформаційних загроз та механізмів їх нейтралізації, що дозволяє оцінити ефективність наявних інструментів інформаційної безпеки та визначити напрямки для подальшого розвитку інституційної бази.

Розкрито взаємозв'язок між глобалізаційними процесами, стрімким розвитком інформаційних технологій і забезпеченням інформаційної безпеки. Зазначено, що зростання міжнародної напруженості та активізація гібридних воєн вимагають нових підходів до захисту інформаційного простору.

Описано методологію дослідження, яка об'єднує аналітичний та порівняльний методи, що дозволяє здійснити глибокий аналіз діяльності інституцій, залучених до забезпечення інформаційної безпеки, та оцінити їх вплив на суспільно-політичну стабільність.

Вказано на наукову новизну дослідження, яка полягає у формуванні комплексного підходу до аналізу інформаційної безпеки як фактора суспільно-політичної стабільності. Зазначено, що робота робить внесок у розробку теоретичних основ інформаційної безпеки, а також розширює розуміння механізмів її забезпечення в сучасних умовах.

У розділі закладено фундамент для подальшого дослідження впливу інститутів інформаційної безпеки на забезпечення стабільності держави, а також визначено ключові напрямки для аналізу та розробки рекомендацій. Результати цього розділу слугують основою для глибшого розуміння взаємозв'язків між інформаційною безпекою і суспільно-політичною стабільністю в контексті сучасних викликів.

У другому розділі дисертації зосереджено увагу на суспільно-політичній стабільності як основі національної та міжнародної безпеки в умовах інформаційних викликів сучасності. Розглядаються чинники та критерії суспільно-політичної стабільності, зокрема роль інформаційного компонента у їх формуванні. Аналізується, як інформаційні виклики впливають на здатність держави підтримувати внутрішню та зовнішню стабільність.

Детально вивчено механізми забезпечення та виклики політичної стабільності в інформаційному суспільстві. Подано аналіз сучасних загроз інформаційній безпеці та їх впливу на суспільно-політичне життя країни, зокрема на прикладі гібридних війн та інформаційно-психологічного впливу.

Висвітлено розвиток суспільно-політичної стабільності в умовах інформаційно-психологічної війни, з акцентом на необхідність формування ефективної системи протидії інформаційним загрозам. Обговорюються стратегії захисту інформаційного простору та підвищення інформаційної стійкості суспільства до зовнішнього впливу.

Представлено огляд існуючих підходів до вимірювання та оцінки суспільно-політичної стабільності, з урахуванням інформаційної безпеки як одного з ключових її компонентів. Аналізуються індикатори стабільності та методи їх застосування в сучасних умовах.

Проаналізовано вплив міжнародних інформаційних конфліктів на суспільно-політичну стабільність країн, в тому числі через призму міжнародного права та міждержавних відносин. Показано, як глобальні інформаційні потоки та медійні кампанії можуть використовуватись для дестабілізації ситуації в окремих державах.

Оцінено роль і значення інформаційної культури та медіаграмотності населення у забезпеченні суспільно-політичної стабільності. Акцентується на важливості освітніх програм та ініціатив, спрямованих на підвищення критичного сприйняття інформації.

Розроблено рекомендації щодо зміцнення інформаційної безпеки як засобу підтримки суспільно-політичної стабільності, включаючи правові, технічні та соціальні аспекти. Обговорюється потреба в удосконаленні національного законодавства та міжнародної координації у сфері інформаційної безпеки.

Наголошено на необхідності комплексного підходу до забезпечення суспільно-політичної стабільності через зміцнення інформаційної безпеки. Висвітлено стратегії і тактики протидії інформаційним загрозам та акцентовано

на необхідності постійного моніторингу і адаптації до змінюваних умов інформаційного середовища.

У третьому розділі дисертації проведено аналіз інституційного розвитку інформаційної стійкості України, з акцентом на гібридні загрози та механізми протидії. Висвітлено сучасний стан інституційної бази інформаційної безпеки в Україні, визначено ключові виклики та загрози, що стоять перед державою в інформаційному просторі.

Проаналізовано безпековий аспект ключових агентів і каналів пропаганди, які використовувались під час російсько-української війни. Особлива увага приділена методам інформаційного впливу Російської Федерації на суспільно-політичну стабільність в Україні, в тому числі через мережеві операції та маніпуляції громадською думкою.

Представлено рекомендації щодо протидії інформаційному впливу Росії, зокрема розроблено стратегії посилення медіаграмотності населення, вдосконалення законодавчої бази та підвищення ефективності державної комунікаційної політики.

Досліджено перспективи розвитку інститутів і механізмів забезпечення суспільно-політичної стабільності в публічному інформаційному просторі України. Оцінено потенціал розвитку кібербезпеки як інструментів захисту національних інтересів у глобальному інформаційному середовищі.

Здійснено огляд міжнародного досвіду в сфері інформаційної безпеки, з акцентом на успішні практики інших країн, які можуть бути адаптовані та впроваджені в Україні. Аналіз включає вивчення моделей регулювання інформаційного простору, методів боротьби з фейковими новинами та забезпечення кібербезпеки.

Обговорено роль громадянського суспільства та медіа у формуванні стійкої інформаційної політики держави. Наголошено на необхідності активної участі громадянського суспільства в процесі вироблення та імплементації політик інформаційної безпеки, а також на важливості незалежних медіа як контролюючого фактора влади.

Визначено пріоритетні напрямки подальших досліджень в галузі інформаційної безпеки та розроблено конкретні пропозиції щодо покращення інформаційного середовища в Україні. Зокрема, акцентовано на необхідності розробки комплексних програм з підвищення рівня інформаційної безпеки, розвитку цифрової економіки та захисту інформаційного простору від зовнішнього впливу.

У третьому розділі підкреслено значення інтегрованого підходу до забезпечення інформаційної безпеки, що охоплює посилення правової бази, розвиток технологічної інфраструктури та активізацію участі громадськості у формуванні безпечного інформаційного простору. Наголошено на необхідності адаптації до постійно змінюваних умов глобалізованого інформаційного середовища для захисту національних інтересів України.

Наукова новизна дослідження полягає в комплексному теоретичному та емпіричному аналізі ролі інститутів інформаційної безпеки у забезпеченні стабільності держави, дослідженні тенденцій розвитку політичних інститутів інформаційної безпеки, що враховує взаємодію між різними рівнями управління та секторами суспільства. Дослідження також робить внесок у розробку нових стратегій та програм зміцнення інформаційної стійкості держави перед сучасними загрозами.

Практичне значення дослідження полягає у розробці рекомендацій для удосконалення державної політики в галузі інформаційної безпеки, які можуть сприяти підвищенню ефективності інституційного забезпечення інформаційної безпеки на національному рівні. Результати дослідження надають нові методологічні інструменти для оцінки стану та ефективності політичних інститутів інформаційної безпеки, що можуть бути використані державними органами, науковцями та експертами у сфері безпеки.

Ключові слова: Інформаційна безпека, суспільно-політична стабільність, гібридна війна, війна, інформаційний вплив, соціальна напруженість, інформаційна стійкість, громадсько-політична ідентичність, інформаційні операції, пропаганда, дезінформація, медіа, медіакратія, громадянське

суспільство, інформаційна політика, стратегічні комунікації, російська агресія, російсько-українська війна, національна безпека.

Список публікацій здобувача**:**

1. Суспільно-політична стабільність як складова системи інформаційної безпеки: виклики в умовах воєнного стану / Є. Міненко та ін. *Міждисциплінарні дослідження складних систем*. 2024. № 23 (2024). С. 41–54. URL: http://iscs-journal.npu.edu.ua/article/view/306847/298220

2. Міненко Є. С. Сутність політичної стабільності в умовах інформаційного суспільства. Науковий журнал «Politicus». 2023. № 5. С. 155–160. URL: http://politicus.od.ua/5_2023/24.pdf.

3. Міненко, Є. Організаційно-правовий аналіз забезпечення інформаційної безпеки як фактор суспільно-політичної стабільності. Науковий часопис НПУ імені М.П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін, 22(33), 76–84. URL: https://sj.udu.edu.ua/index.php/pnspd/article/view/1446/1183

4. Міненко Є. Вплив російської пропаганди на суспільно-державну стабільність України: аналіз методів та наслідків. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2023. Т. 3, № 69. URL: http://journals.maup.com.ua/index.php/political/article/view/2827/3286.

5. Міненко, Є., Захаренко К. Інститут медіа як суб’єкт інформаційної безпеки. Науковий часопис НПУ імені М.П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін, 22(34). URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/44664/Zakharenko-29-36.pdf?sequence=1&isAllowed=y

6. Міненко Є. С., Борсук А. С. Вплив російської пропаганди на інформаційний суверенітет країн Європи. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2024. Т. 1, № 73. С. 61–66. URL: https://journals.maup.com.ua/index.php/political/article/view/3124/3567

7. Міненко Є.С. Основні засади формування та реалізації державної політики інформаційної безпеки в умовах вітчизняної війни. Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні : матеріали Всеукр. наук.-практ. конф. у трьох томах, м. Київ, ДЗВО «Університет менеджменту освіти» НАПН України, 15-28 квітня 2022 р.; ред. колегія : І.О. Дегтярьова, В.С. Куйбіда, П.М. Петровський та ін., уклад. Т.О. Мельник. Т. 1. К. : ДЗВО «УМО» НАПН України, 2022. 213 с. URL: https://www.researchgate.net/profile/Vitalij-Kruglov/publication/361262262_PUBLICNE_UPRAVLINNA_TA_ADMINISTRUVANNA_V_UMOVAH_VIJNI_I_V_POSTVOENNIJ_PERIOD_V_UKRAINI_MATERIALI_VSEUKRAINSKOI_NAUKOVO-PRAKTICNOI_KONFERENCII/links/62a74e49416ec50bdb22cb5e/PUBLICNE-UPRAVLINNA-TA-ADMINISTRUVANNA-V-UMOVAH-VIJNI-I-V-POSTVOENNIJ-PERIOD-V-UKRAINI-MATERIALI-VSEUKRAINSKOI-NAUKOVO-PRAKTICNOI-KONFERENCII.pdf#page=38

8. Міненко Є. С., Любак Л. В., Логінов О. Ю., Ожегова Г. О. Основні засади реформування сектора безпеки і оборони України в контексті забезпечення інформаційної безпеки. The 6th International scientific and practical conference “Modern scientific research: achievements, innovations and development prospects” (November 21-23, 2021) MDPC Publishing, Berlin, Germany. 2021. 937 p. URL: https://sci-conf.com.ua/wp-content/uploads/2021/11/MODERN-SCIENTIFIC-RESEARCH-ACHIEVEMENTS-INNOVATIONS...-21-23.11.21.pdf

9. Міненко Є. С. Вплив сучасних інформаційних технологій на психологічний стан особистості. The 4 th International scientific and practical conference ―Modern research in world science‖ (July 10-12, 2022) SPC ―Sci-conf.com.ua‖, Lviv, Ukraine. 2022. 1161 p. URL: https://sci-conf.com.ua/wp-content/uploads/2022/07/MODERN-RESEARCH-IN-WORLD-SCIENCE-10-12.07.22.pdf

10. Міненко Є.С. Основні засади формування та реалізації державної політики інформаційної безпеки. Міжнародна наукова інтернет-конференція

"Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 55)" / Збірник тез доповідей: випуск 55 (м. Тернопіль, 9 лютого 2021 р.). – Тернопіль. – 2021. – 90 с. URL: https://drive.google.com/file/d/1TeaiQWRCWwxcrhSX_k6sCXCCv4KFMRYk/view?usp=sharing

11. Міненко, Є. С. Виклики інформаційній безпеці людини в умовах гібридної війни проти України. Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи тези доп. учасників міжн. наук.-практ. конф. (Анн-Арбор - Харків, 12-13 груд. 2023 р.) , 252-254. URL: https://doi.org/10.32782/PPSS.2023.1.66

ANNOTATION

Minenko Y. S. Development of Information Security Institutions of Modern Ukraine as a Factor of Socio-Political Stability. - Qualifying scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in speciality 052 - Political Science - Mykhailo Drahomanov Ukrainian State University, Kyiv, 2024.

The dissertation is devoted to an in-depth analysis of the development of information security institutions in Ukraine in terms of their role in ensuring socio-political stability. In the context of rapid development of information technologies and growing globalisation, the topic of information security is becoming of key importance, especially for a state that is subject to international tensions and information and psychological influence.

The thesis is organised into three main chapters, each of which deals with different aspects of information security.

The first chapter of the thesis provides a theoretical and methodological analysis of the role of information security in ensuring socio-political stability. It presents a fundamental approach to defining the essence of information security, focusing on interdisciplinary and political science aspects. The main attention is paid to the consideration of information security as an integral part of socio-political stability, which requires an integrated approach to its analysis and evaluation.

The theoretical foundations of the study of socio-political stability through a neo-institutional approach are highlighted, which allows for a deeper understanding of the mechanisms of interaction between different actors in the context of the information space. This includes an analysis of the legal, social and economic aspects that form the conditions for ensuring information security at the national and international levels.

The role and place of the information security system in the structure of socio-political stability is determined, providing an analysis of methods for studying information threats and mechanisms for their neutralisation, which allows assessing

the effectiveness of existing information security tools and identifying areas for further development of the institutional framework.

The article reveals the relationship between globalisation processes, rapid development of information technologies and information security. It is noted that the growth of international tensions and the intensification of hybrid wars require new approaches to the protection of the information space.

The research methodology combining analytical and comparative methods is described, which allows for an in-depth analysis of the activities of institutions involved in ensuring information security and assessing their impact on socio-political stability.

The scientific novelty of the study is indicated, which consists in the formation of an integrated approach to the analysis of information security as a factor of socio-political stability. It is noted that the work contributes to the development of the theoretical foundations of information security and expands the understanding of the mechanisms of its provision in modern conditions.

The chapter lays the foundation for further study of the impact of information security institutions on ensuring the stability of the state, and identifies key areas for analysis and development of recommendations. The results of this chapter serve as a basis for a deeper understanding of the relationship between information security and socio-political stability in the context of current challenges.

The second chapter of the thesis focuses on socio-political stability as the basis of national and international security in the context of modern information challenges. The factors and criteria of socio-political stability, in particular the role of the information component in their formation, are considered. The author analyses how information challenges affect the ability of the state to maintain internal and external stability.

The mechanisms of ensuring and challenges to political stability in the information society are studied in detail. The author analyses modern threats to information security and their impact on the socio-political life of the country, in

particular, on the example of hybrid wars and information and psychological influence.

The development of socio-political stability in the context of information and psychological warfare is highlighted, with an emphasis on the need to form an effective system of countering information threats. The strategies for protecting the information space and increasing the information resilience of society to external influence are discussed.

An overview of existing approaches to measuring and assessing socio-political stability is presented, taking into account information security as one of its key components. The stability indicators and methods of their application in modern conditions are analysed.

The article analyses the impact of international information conflicts on the socio-political stability of countries, including through the prism of international law and interstate relations. It is shown how global information flows and media campaigns can be used to destabilise the situation in individual countries.

The role and importance of information culture and media literacy in ensuring socio-political stability is assessed. The author emphasises the importance of educational programmes and initiatives aimed at increasing critical perception of information.

Recommendations are developed to strengthen information security as a means of maintaining socio-political stability, including legal, technical and social aspects. The need to improve national legislation and international coordination in the field of information security is discussed.

The need for a comprehensive approach to ensuring socio-political stability through strengthening information security is emphasised. The strategies and tactics of countering information threats are highlighted and the need for constant monitoring and adaptation to changing conditions of the information environment is emphasised.

The third chapter of the thesis analyses the institutional development of Ukraine's information resilience, with a focus on hybrid threats and countermeasures.

The current state of the institutional framework for information security in Ukraine is highlighted, and the key challenges and threats facing the state in the information space are identified.

The security aspect of key agents and propaganda channels used during the Russian-Ukrainian war is analysed. Particular attention is paid to the methods of information influence of the Russian Federation on socio-political stability in Ukraine, including through network operations and manipulation of public opinion.

The author presents recommendations for countering Russia's information influence, including strategies for enhancing media literacy, improving the legislative framework and increasing the effectiveness of the state communication policy.

The prospects for the development of institutions and mechanisms to ensure socio-political stability in the public information space of Ukraine are investigated. The potential for the development of cybersecurity as a tool for protecting national interests in the global information environment is assessed.

An overview of international experience in the field of information security is provided, with a focus on successful practices of other countries that can be adapted and implemented in Ukraine. The analysis includes the study of models of information space regulation, methods of combating fake news and ensuring cybersecurity.

The role of civil society and media in shaping a sustainable information policy of the state is discussed. The necessity of active participation of civil society in the process of developing and implementing information security policies, as well as the importance of independent media as a controlling factor of the government is emphasised.

Priority areas for further research in the field of information security are identified and specific proposals for improving the information environment in Ukraine are developed. In particular, the author emphasises the need to develop comprehensive programmes to improve information security, develop the digital economy and protect the information space from external influence.

The third section emphasises the importance of an integrated approach to ensuring information security, which includes strengthening the legal framework, developing technological infrastructure and enhancing public participation in the formation of a secure information space. The author emphasises the need to adapt to the ever-changing conditions of the globalised information environment in order to protect Ukraine's national interests.

The scientific novelty of the study lies in a comprehensive theoretical and empirical analysis of the role of information security institutions in ensuring the stability of the state, the study of trends in the development of political institutions of information security, taking into account the interaction between different levels of government and sectors of society. The study also contributes to the development of new strategies and programmes for strengthening the information resilience of the state in the face of modern threats.

The practical significance of the study lies in the development of recommendations for improving the state policy in the field of information security, which can contribute to improving the effectiveness of institutional support for information security at the national level. The results of the study provide new methodological tools for assessing the status and effectiveness of political institutions of information security, which can be used by government agencies, academics and security experts.

Keywords: Information security, socio-political stability, hybrid warfare, war, information influence, social tension, information resilience, socio-political identity, information operations, propaganda, disinformation, media, mediaocracy, civil society, information policy, strategic communications, Russian aggression, Russian-Ukrainian war, national security.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Вибір теми обумовлений низкою ключових чинників, що відображають актуальність і значущість цієї проблематики в сучасному світі.

Перш за все, глобалізаційні процеси та стрімкий розвиток інформаційних технологій зумовили значне зростання обсягів, швидкості обігу і доступності інформації, що, з одного боку, відкриває нові можливості для розвитку суспільства, а з іншого - створює додаткові загрози інформаційній безпеці як окремих осіб, так і державних структур.

Крім того, в умовах збільшення міжнародної напруженості, активізації конфліктів та гібридних воєн, інформаційний простір стає ареною для протистоянь, де інформація використовується як засіб досягнення політичних, економічних та військових цілей. Це вимагає від держав розробки та впровадження ефективних механізмів забезпечення інформаційної безпеки, адаптованих до сучасних викликів.

Зазначена тема дослідження також відповідає потребам розробки новітніх підходів до аналізу, оцінки та управління ризиками в інформаційній сфері. Активна інтеграція інформаційних технологій в усі сфери суспільного життя збільшує вразливість до кіберзагроз, що змушує шукати нові способи захисту інформації.

Окрему увагу слід звернути на соціально-політичну динаміку сучасного світу, яка характеризується швидкими змінами, непередбачуваністю подій та їх високим впливом на інформаційну безпеку. Дослідження в цій сфері допоможе краще розуміти механізми впливу соціально-політичних процесів на інформаційне середовище, виявляти нові загрози та розробляти стратегії їх нейтралізації.

У контексті глобалізації та стрімкого розвитку цифрових технологій інформаційна безпека стала однією з ключових складових національної безпеки держав. Інформаційні загрози, такі як кібератаки, інформаційна війна,

поширення фейкових новин та втручання у внутрішні справи через інформаційний простір, вимагають від держави розвитку ефективних політичних інститутів інформаційної безпеки.

Здатність держави забезпечити інформаційну безпеку безпосередньо впливає на її стабільність. Інформаційні атаки можуть підірвати довіру до державних інституцій, спричинити соціальну напруженість та навіть викликати політичні кризи. Тому розвиток інститутів, здатних протистояти таким загрозам, є важливим елементом забезпечення стабільності країни.

Сучасні виклики інформаційної безпеки не обмежуються національними кордонами. Досвід інших країн у формуванні ефективних політичних інститутів інформаційної безпеки та міжнародна співпраця в цій сфері можуть слугувати важливим джерелом знань та інструментів для підвищення рівня захищеності.

Розвиток політичних інститутів інформаційної безпеки також включає розробку та впровадження правових норм, які б забезпечували захист інформаційного простору без порушення прав і свобод громадян. Вивчення балансу між безпекою та свободою інформації, етичні аспекти використання інформаційних технологій для забезпечення національної безпеки стає все більш актуальним.

Розвиток цифрових технологій та штучного інтелекту вносить нові виклики для інформаційної безпеки, такі як захист персональних даних, боротьба з маніпуляціями в соціальних мережах, протидія кібертероризму. Розробка політик і стратегій в цій сфері вимагає комплексного підходу та постійного оновлення знань та інструментів.

Провідні українські та зарубіжні вчені активно досліджують питання інформаційної безпеки, особливо у контексті глобалізації, стрімкого розвитку інформаційних технологій та зростаючої міжнародної напруженості. Наприклад, Гурковський В. І., Кормич Б. А., Смолянюк В. Ф. у своїх працях аналізують концепції національної інформаційної безпеки та правові аспекти її забезпечення. Вони розглядають інформаційну безпеку як систему захищених законом правил, що регулюють оброблення інформації в межах держави, і

підкреслюють необхідність захисту життєво важливих інтересів особистості, суспільства та держави від загроз у сфері інформаційного простору.

Інші дослідники, такі як Ліпкан В.А., акцентують увагу на соціальних та філософських аспектах інформаційної безпеки, аналізуючи її значення для суспільної стабільності та розвитку. Він підкреслює, що інформаційна безпека є невід'ємною складовою суспільно-політичної стабільності, яка впливає на динаміку та характер соціальних процесів.

Почепцов Г. Г., Бебик В. М., Дмитренко М. А, які у своїх працях досліджують гібридну війну та її інформаційну складову, розглядають методи та стратегії інформаційного впливу як ключові інструменти у сучасних конфліктах, підкреслюючи їхню роль у формуванні громадської думки та впливі на політичну культуру суспільства.

Остапенко М. А., яка внесла вагомий внесок у дослідження питання гібридних війн, зокрема феномену консцієнтальної війни, у своїх наукових працях висвітлює складні аспекти психологічних та інформаційних вимірів гібридних війн, підкреслюючи їх вплив на свідомість та політичну культуру.

Марутян Р. Р. та Зеленін В. В., які у своїх працях досліджують сучасні інформаційно-психологічній операції, аналізують основні постулати та завдання міфодизайну, роблячи акцент на необхідності активного використання інформаційних технологій для збереження територіальної цілісності України та психологічної безпеки її громадян в умовах сучасної інформаційно-психологічної війни.

Новакова О. В., яка досліджує проблематику національної стійкості, політичної комунікації, комунікативних платформ між владою та суспільством, розвитку стратегічних комунікацій як засобу боротьби з дезінформацією в українському суспільстві, акцентує увагу на важливості ролі органів місцевого самоврядування та регіональних медіа у забезпеченні інформаційної безпеки в умовах російської військової агресії.

Чупрій Л. В. аналізує значення історичної пам'яті у контексті інформаційного суверенітету та протидії російській інформаційній агресії,

розглядає історичну пам'ять як інструмент формування національної ідентичності та стабільності.

Проте, незважаючи на значний обсяг наукових розробок, залишаються відкритими питання щодо комплексного аналізу взаємозв'язку між інформаційною безпекою та суспільно-політичною стабільністю в контексті України, особливо в умовах гібридної війни та інформаційно-психологічних атак. Також недостатньо досліджено роль інституційного розвитку у зміцненні інформаційної стійкості держави, а також ефективність механізмів протидії сучасним інформаційним загрозам.

Ця дисертація спрямована на заповнення існуючих прогалин у наукових дослідженнях шляхом комплексного вивчення інституційної структури інформаційної безпеки в Україні та її впливу на забезпечення суспільно-політичної стабільності. Особливу увагу буде приділено аналізу інформаційних викликів та загроз, які постали перед Україною в останні роки, в тому числі через призму гібридної війни та інших форм інформаційного протистояння. Будуть розглянуті стратегії та тактики протидії, зокрема розвиток медіаграмотності, посилення кібербезпеки, реформування законодавчої бази та залучення міжнародного досвіду.

Таким чином, дисертація зосереджується на виявленні та аналізі ефективних механізмів зміцнення інформаційної безпеки як ключового елемента суспільно-політичної стабільності, виходячи з потреби адаптації до сучасних умов інформаційного середовища.

Обрана тема дослідження є вкрай важливою для розуміння сучасних викликів та загроз інформаційній безпеці та розробки ефективних механізмів їх протидії.

Мета і завдання дослідження. Мета дослідження полягає в розкритті впливу інститутів інформаційної безпеки на забезпечення стабільності держави у сучасних умовах війни, посилення міжнародної конфронтації та загроз демократіям, а також у контексті викликів глобалізації та швидкого розвитку інформаційних технологій. Це передбачає вивчення механізмів формування та

функціонування політичних інститутів, здатних ефективно протистояти інформаційним загрозам, та оцінку їхнього впливу на загальну стабільність державного устрою. Досягнення поставленої мети потребує послідовного розв'язання наступних дослідницьких завдань:

- дослідити політологічні та міждисциплінарні аспекти розуміння сутності інформаційної безпеки;
- окреслити теоретичні основи дослідження суспільно-політичної стабільності;
- описати методи вивчення системи інформаційної безпеки як елемента суспільно-політичної стабільності;
- розкрити чинники та критерії суспільно-політичної стабільності, зокрема роль інформаційного компоненту в забезпеченні такої стабільності;
- охарактеризувати виклики та механізми забезпечення політичної стабільності в інформаційному суспільстві;
- виявити особливості забезпечення суспільно-політичної стабільності в умовах інформаційно-психологічної війни;
- провести безпековий аналіз ключових агентів та каналів пропаганди російсько-української війни;
- розробити рекомендації з протидії інформаційному впливу РФ на суспільно-політичну стабільність України;
- окреслити перспективи розвитку інститутів і механізмів забезпечення суспільно-політичної стабільності у публічному інформаційному просторі України.

Об'єктом дослідження є суспільно-політична стабільність як необхідна основа демократизації, ефективного реформування політичної системи, глобальних перетворень, а також стійкості держави і громадськості перед викликами війни, зокрема її інформаційними загрозами.

Предмет дослідження – розвиток сучасних інститутів інформаційної безпеки як чинник суспільно-політичної стабільності України, роль інформаційної стійкості у протидії зовнішній агресії.

Методи дослідження. Методи дослідження у сфері розвитку інститутів інформаційної безпеки сучасної України базуються на комплексному підході, що охоплює ряд методів аналізу, спрямованих на глибоке розуміння теми. Використання різних методів аналізу дозволяє інтегрувати теоретичні розробки, законодавчі акти і практичні заходи для систематичної оцінки існуючих теоретичних підходів і виявлення ключових аспектів, проблем та перспектив розвитку політичних інститутів.

Основними методами дослідження стали аналітичний і порівняльний, які допомогли здійснити систематичну оцінку існуючих теоретичних розробок і законодавчих актів, а також порівняти різні підходи та практики у сфері інформаційної безпеки. Це сприяло виявленню ключових аспектів, проблем і перспектив розвитку політичних інститутів та оцінці ефективності різних інститутів і заходів.

Для детального вивчення конкретних прикладів, що демонструють роль політичних інститутів у забезпеченні інформаційної безпеки, був застосований метод аналізу випадків. Це дозволило зібрати і проаналізувати детальні дані про реальні ситуації, вивчивши ефективність різних стратегій і заходів на практиці. Такий підхід сприяв глибшому розумінню механізмів реагування на інформаційні загрози та впливу політичних інститутів на зміцнення державної стабільності.

Метод експертних оцінок був використаний для збору та аналізу висновків від провідних фахівців у галузі інформаційної безпеки. Залучення досвіду та знань експертів дозволяє оцінити актуальний стан політичних інститутів, їх ефективність та можливості для покращення. Експертні оцінки допомогли поглибити аналіз, забезпечивши більшу точність та валідність висновків дослідження.

Комплексний підхід до дослідження інформаційної безпеки включав інтеграцію міждисциплінарних знань з різних наук, таких як політологія, соціологія, право та інформаційні технології. Це сприяло розгляду інформаційної безпеки як складного феномену, що включає технічні, політичні,

соціальні та культурні аспекти. Системний підхід дозволив проаналізувати взаємодію різних рівнів управління (міжнародного, національного, регіонального) та секторів суспільства (державного, приватного, громадського).

Емпірична база дослідження включає теоретичні розробки, законодавчі акти, практичні заходи та експертні оцінки. Теоретичні розробки забезпечили аналіз наукових праць, що висвітлюють сутність інформаційної безпеки та її роль у суспільно-політичній стабільності. Законодавчі акти надали можливість вивчити законодавчі документи, що регулюють питання інформаційної безпеки в Україні та за кордоном. Практичні заходи допомогли оцінити реальні дії і стратегії, застосовані для забезпечення інформаційної безпеки в різних контекстах. Експертні оцінки доповнили аналіз висновками та рекомендаціями провідних фахівців у галузі інформаційної безпеки.

Наукова новизна отриманих результатів. Наукова новизна дослідження полягає в теоретичному узагальненні та систематизації існуючих підходів до розуміння інститутів інформаційної безпеки, що дозволяє глибше проаналізувати їхню роль і місце в системі державного управління.

Вперше:

- у рамках сучасних політичних наук розвинуто концепт «інформаційної стійкості», тобто здатності політичної системи, держави і суспільства загалом до попередження та протидії негативним впливам, зокрема кібератакам, дезінформації та іншим формам інформаційного втручання; це також спроможність системи інформаційної безпеки ефективно функціонувати, захищаючи свою цілісність, конфіденційність, доступність, автентичність даних навіть в умовах війни. Комплексний аналіз інформаційної стійкості для сучасної політичної системи охоплює розуміння рівня кібербезпеки політичних інституцій (системи е-голосування, веб-сайти партій, системи звітності та інші критичні інформаційні платформи); вивчення заходів з протидії кібершпигунству та іншим інформаційним загрозам; долідження каналів поширення дезінформації; оцінку доступності та прозорості інформації про діяльність політичних інститутів, прийняття рішень тощо; аналіз законодавства

з кібербезпеки, захисту персональних даних, свободи слова тощо; окреслення планів та заходів уряду чи інших політичних інститутів у разі масштабних витоків інформації чи інших кризових ситуацій в інформаційній сфері;

Поглиблено:

- аналіз міжнародного досвіду створення та функціонування політичних інститутів інформаційної безпеки та розробці рекомендацій щодо адаптації успішних практик до умов конкретної держави. Дослідження виявляє новітні механізми та інструменти управління інформаційною безпекою, які можуть бути ефективно імплементовані в інших країнах для підвищення їх державної стабільності.
- наукове розуміння нових інформаційних загроз, що виникають в сучасному динамічному інформаційному просторі, та розробляє стратегії їх протидії, базуючись на аналізі політичних, технологічних та соціальних факторів. Це дозволяє оновити підходи до інформаційної безпеки, зробивши їх більш адаптованими до сучасних викликів.

Отримали подальший розвиток:

- теоретичної основи інформаційної безпеки як багатогранного феномену, що включає не тільки технічні аспекти захисту інформації, але й політичні, соціальні, правові та культурні виміри. Дослідження пропонує інтегративну модель розвитку політичних інститутів інформаційної безпеки, яка враховує взаємозв'язок між різними рівнями управління (міжнародним, національним, регіональним) та різними секторами суспільства (державним, приватним, громадським). Така модель дозволяє оцінити потенційні ефекти синергії від взаємодії цих компонентів, що є новим кроком у розумінні комплексного підходу до забезпечення інформаційної безпеки.

Дослідження вносить вклад у розвиток теоретичних основ інформаційної безпеки, визначаючи її як багатогранний феномен, який охоплює не тільки технічні аспекти захисту інформації, але й політичні, соціальні, правові та культурні виміри.

Дослідження пропонує інтегративну модель розвитку політичних інститутів інформаційної безпеки, що враховує взаємозв'язок між різними рівнями управління (міжнародним, національним, регіональним) та різними секторами суспільства (державним, приватним, громадським). Така модель дозволяє оцінити потенційні ефекти синергії від взаємодії цих компонентів, що є новим кроком у розумінні комплексного підходу до забезпечення інформаційної безпеки.

Наукова новизна також полягає в детальному аналізі міжнародного досвіду створення та функціонування політичних інститутів інформаційної безпеки та розробці рекомендацій щодо адаптації успішних практик до умов конкретної держави. Дослідження виявляє новітні механізми та інструменти управління інформаційною безпекою, які можуть бути ефективно імплементовані в інших країнах для підвищення їх державної стабільності.

Дослідження вносить вклад у наукове розуміння нових інформаційних загроз, що виникають в сучасному динамічному інформаційному просторі, та розробляє стратегії їх протидії, базуючись на аналізі політичних, технологічних та соціальних факторів. Це дозволяє оновити підходи до інформаційної безпеки, зробивши їх більш адаптованими до сучасних викликів.

Нарешті, наукова новизна дослідження полягає у комплексній оцінці впливу політичних інститутів інформаційної безпеки на загальну державну стабільність. Через розроблену модель та аналітичні методики робота демонструє, як заходи з інформаційної безпеки можуть сприяти зміцненню державних інститутів, підтримці соціального порядку та захисту від зовнішніх і внутрішніх загроз.

Теоретичне і практичне значення отриманих результатів. Дослідження забезпечує глибше розуміння концепції політичних інститутів інформаційної безпеки, розширюючи теоретичні рамки в галузі політичних наук та безпекових досліджень. Воно доповнює існуючу літературу новими визначеннями, класифікаціями та концептуальними підходами.

Результати дослідження теоретично обґрунтовують, як розвиток політичних інститутів інформаційної безпеки впливає на забезпечення стабільності держави, демонструючи механізми цього впливу.

Дослідження виявляє новітні тенденції та виклики в галузі інформаційної безпеки, що спонукає до подальших теоретичних розробок у цій сфері.

На основі аналізу інституціональної структури і механізмів функціонування інститутів інформаційної безпеки дослідження пропонує практичні рекомендації для вдосконалення державної політики в цій сфері. Це може сприяти підвищенню ефективності інституційного забезпечення інформаційної безпеки на національному рівні.

Результати дослідження надають нові методологічні інструменти для оцінки стану та ефективності політичних інститутів інформаційної безпеки, що можуть бути використані державними органами, науковцями та експертами у сфері безпеки.

Надаючи оцінку ефективності існуючих підходів та інститутів інформаційної безпеки, дослідження слугує підгрунтям для розробки нових стратегій і програм зміцнення інформаційної стійкості держави перед сучасними загрозами.

Апробація результатів дослідження. Апробація результатів дослідження відбувалася на засіданні кафедри політичних наук ННІ права та політології УДУ імені Михайла Драгоманова. Результати дослідження доповідалися на звітних семінарах аспірантів, наукових конференціях міжнародного та всеукраїнського рівнів: міжнародній науковій інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» (м. Тернопіль, 9 лютого 2021 р.); всеукраїнській науково-практичній конференції «Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні» (Київ, 25 травня 2022 р.); міжнародній науково-практичній конференції «Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи» (Харків, 12-13 грудня 2023 р.); всеукраїнській науково-практичній конференції «Трансформація правової системи України:

виклики сучасності» (Київ, 21 лютого 2024 р.); круглому столі «Крим: 10 років спротиву» (Київ, 28 лютого 2024 р.); XV всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 27 березня 2024 р.); міжнарожній науковій конференції «Політика та право в умовах дії воєнного стану: пошук рішень» (Київ, 23 квітня 2024 р.).

Публікації. За темою дисертації опубліковано 11 наукових праць, серед яких 5 статей – у наукових фахових виданнях України із політичних наук, 1 стаття – у науковому виданні, яке включено до міжнародних наукометричних баз, 5 наукових праць засвідчують апробацію матеріалів дисертації та додатково відображають отримані наукові результати.

Особистий внесок здобувача. Із 11 опублікованих наукових праць 4 − у співавторстві (загальним обсягом 3,95 д.а.). Співавторами наукових праць є науковий керівник та науковці, спільно з якими проведені дослідження (К. Захаренко, Р. Драпушко, О. Волянюк, А. Борсук, Л. Любак, О. Логінов, Г. Ожегова). У цих працях дисертанту належить фактичний матеріал і творчий доробок, концептуалізація поняття суспільно-політичної стабільності, інформаційної стійкості тощо. Особистий внесок здобувача складає 3,35 д. а. Постановка мети та завдань, обговорення результатів проведені разом з науковим керівником.

На початковому етапі була визначена актуальність проблематики, що відображає взаємозв'язок між інформаційною безпекою та стабільністю держави в умовах сучасних викликів. Це включало ідентифікацію прогалин в наявному дослідницькому полі та встановлення конкретної мети для детального вивчення.

Підібрано відповідну методологію для аналізу політичних інститутів інформаційної безпеки, яка включає застосування аналітичного, порівняльного методів та вивчення конкретних випадків. Ці методи дозволили провести глибокий аналіз та забезпечити об'єктивність отриманих результатів.

Зібрані дані були детально проаналізовані, що включало вивчення міжнародного досвіду та оцінку ефективності різноманітних інституційних механізмів. В результаті були сформульовані висновки, які висвітлюють важливість розвитку інститутів у сфері інформаційної безпеки для підвищення стійкості державного управління.

На базі аналізу були розроблені теоретичні положення та практичні рекомендації, спрямовані на покращення діяльності інститутів інформаційної безпеки. Це охоплює кроки для законодавчих змін, зміцнення міжнародних зв'язків та розбудови внутрішніх захисних механізмів.

Важливою частиною роботи стало активне поширення отриманих результатів, включаючи публікації у фахових виданнях та участь у наукових конференціях. Це не тільки сприяло обміну знаннями, але й стимулювало подальші дослідження у цій критично важливій сфері.

Таким чином, виконана робота відображає цілісний підхід до вивчення інформаційної безпеки та її ролі у забезпеченні державної стабільності, пропонуючи конкретні напрями для покращення та розвитку в цій сфері.

Структура дисертації. Робота складається зі вступу, трьох розділів, дев’яти підрозділів, висновків до кожного розділу, загальних висновків, списку використаних джерел у кількості 135 найменувань. Загальний обсяг роботи становить 256 сторінки, з них основного тексту 212 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ АНАЛІЗ РОЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ СУСПІЛЬНО-ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ

1.1 Сутність інформаційної безпеки: міждисциплінарні та політологічні аспекти

Розвиток наукового поля безпеки акцентує увагу на інформаційному аспекті, значною мірою впливаючи на його напрямки через залучення конкретних суспільств і держав до контексту інформаційного впливу та становлення інформаційного суспільства. Інформаційні виклики, які стоять перед суспільством, мають визначальний характер, а інформаційна діяльність, зумовлена необхідністю забезпечення інформаційної безпеки, продовжує бути ключовою складовою інформаційного суспільства.

Однак, з переходом до ери інформаційного суспільства, значення інформаційної безпеки зростає і вимагає застосування сучасних методологій. Багато наукових робіт у сфері інформаційної безпеки починаються з обґрунтування її актуальності, що випливає з посилення проникнення інформаційних технологій у різні сфери суспільного життя та появи інформаційного суспільства як нового етапу його розвитку.

У цьому новому контексті питання інформаційної безпеки набувають нового значення і стають об'єктом правового регулювання [7].

Таким чином, феномен інформаційної безпеки може бути розглянутий через призму активної та цілеспрямованої взаємодії індивіда з державою та суспільством, що ґрунтується на розумінні потреб та інтересів різноманітних суб'єктів безпеки. Безсумнівно, свідоме прагнення до забезпечення безпеки має суттєвий вплив на динаміку та характер соціальних процесів. Саме тому аналіз інформаційної безпеки як наукової категорії та соціального явища є важливим пріоритетом сьогодення.

В умовах, коли інформаційна конфронтація виступає як невід'ємна складова конкурентного глобального середовища сучасного світу, особливу увагу приділяється забезпеченню інформаційної та кібербезпеки як факторам, що забезпечують збалансування інтересів на рівнях індивіда, суспільства, держави та міжнародної спільноти. Концепція інформаційної безпеки як наукової категорії має різноманітні підходи до свого тлумачення. Розбіжності між доктринальними поглядами, енциклопедичними визначеннями та нормативними описами створюють різноманіття в методологічних підходах, обґрунтуванні їх розробки та сферах застосування. Це підтверджується тим, що саме поняття "безпека" має багатозначний характер і визначається залежно від наукової дисципліни, що його досліджує.

Наприклад, психологи інтерпретують безпеку як відчуття, сприйняття та емоційне переживання потреби у захисті життєво значущих аспектів та інтересів особи. Юристи описують її як систему правових гарантій, що забезпечують захист особистості та суспільства, гарантують нормальне функціонування та дотримання прав та свобод. Філософи розглядають безпеку як стан суспільства, тенденції його розвитку та як структуру, що забезпечує гармонію між якісною безпекою, свободою та необхідністю. Політологи аналізують безпеку як характеристику системи та суспільства в цілому.

Враховуючи це, для досягнення комплексного розуміння, необхідно систематично аналізувати знання, що розподілені між різними галузями соціальних наук.

Юридичні науки, соціологія, політологія та економіка пропонують різні підходи до інтерпретації поняття безпеки. Сучасні умови глобалізації та соціальні зміни зумовлюють необхідність рефлексії щодо змісту поняття безпеки в цілому та інформаційної безпеки зокрема.

Оскільки в центрі філософського дослідження лежить відношення "людина - світ" і процес пізнання природи світу та самої людини в цьому світі, необхідно розкрити внутрішній зміст, властивості та природу досліджуваних понять [119].

Зокрема, філософський погляд вимагає розгляду трьох основних аспектів теорії: онтологічного, епістемологічного та логічного.

Онтологічний аспект зосереджується на об'єктивному походженні змісту філософії, що відображає відношення між об'єктивно існуючою "людиною і світом". Отже, філософія як конкретна форма екзистенціальної свідомості людини і суспільної свідомості прагне передати людині знання про світ та про неї саму [119].

З погляду філософії, безпека є формою і способом існування. Деякі дослідники, зокрема А. Шровський та В. Ященко, вбачають в бутті загальний концепт, пов'язаний з безпекою, проте його зміст більш широкий.

Водночас В.А. Ліпкан наголошує, що у філософському сенсі безпека має соціальний зміст і характеризується соціально-історичними особливостями у своєму вияві, як невід'ємна частина практичної діяльності людини.

Безпека існує в контексті суспільства, а її зміст визначається змінами в організації соціального життя [57].

У процесі історичного розвитку формується сутність суб'єкта, що охоплює внутрішній зміст та зовнішні прояви, являючи собою єдність сутності, яка може мати суперечливий характер.

Сутність визначається як сукупність глибинних зв'язків, відносин та внутрішніх законів, що визначають основні риси та тенденції розвитку системи [37].

Вважається, що сутність може бути пізнаною, якщо ми розуміємо її походження, причини її еволюції, способи її створення та можливості її відтворення технічно або моделювання в теорії чи на практиці. З точки зору епістемології, відображення об'єкта в теорії свідчить про те, що світ відтворюється через призму людського розуму.

Людське сприйняття дійсності має практичний спрямований характер, а ставлення людини до світу визначається її потребами та інтересами. Ці потреби та інтереси задовольняються через практичне управління дійсністю [119].

Сучасна соціологічна термінологія використовує категорію "безпека" для опису стану суспільства, який гарантує його нормальне існування та стабільний розвиток [37].

У соціальній моделі безпека розглядається як створення умов, необхідних для оптимального функціонування та прогресивного розвитку суспільства. Безпека у повному розумінні слова є усвідомленим явищем конкретного суб'єкта суспільних відносин. Вона проявляється як активність і відносна незалежність суспільної свідомості від суспільного буття. Ця відносна незалежність суспільної свідомості від суспільного буття призводить до того, що уявлення, почуття, знання і переживання, пов'язані з безпекою, відіграють активну і важливу роль у соціальному житті. Визнання безпеки як усвідомленого явища сприяє глибшому розумінню природи виникаючих проблем і реальних загроз, що підтверджує необхідність створення ефективної системи охорони та безпеки.

Така система є комплексом інструментів, теоретичних підходів і практичних заходів, що забезпечують максимальну життєздатність соціальної системи, враховуючи всі загрози та ризики, що ставлять під загрозу її існування. Безпека як система ґрунтується на життєво важливих інтересах особистості, держави та міжнародної спільноти.

У практичному плані соціальних систем, безпека є не абстрактним явищем, а конкретною умовою життя. Її зміст визначається конкретними соціальними умовами. Безпека є життєво необхідною для існування людей, держав і націй, оскільки її функція пов'язана з задоволенням основних потреб людини. Безпека також пов'язана з можливістю життя, вона є передумовою для його підтримки та основним критерієм потенціалу його розвитку.

У сучасній науковій літературі вважається, що формулювання проблеми безпеки визначається сприйняттям загроз. Іншими словами, суть проблеми безпеки, пов'язаної з безпечним існуванням соціальної системи, полягає в її контрасті до небезпеки і загрози.

З філософського погляду, безпека є усвідомленим явищем, що повинно бути захищеним від можливих негативних впливів. Це підкреслює позитивний зміст суспільної свідомості, яка може передбачати, передчувати та уявляти небезпеку. Принцип самозбереження стає фундаментальною здатністю свідомості. Прагнення до безпеки виражає раціональність соціальної системи, усвідомлений зміст її існування та соціально-моральну значущість. З цього підходу безпека розглядається як невід'ємний атрибут буття.

Присутність безпеки як явища не слід обмежувати лише протилежністю до небезпеки. У контексті діалектики сприйняття проблеми безпеки стає більш повним. Без безпеки неможливий повноцінний розвиток. Іншими словами, безпека також є забезпеченням сталого розвитку будь-якої соціальної системи.

Концепція сталого розвитку орієнтується на досягнення балансу між задоволенням потреб сучасного людства та захистом інтересів майбутніх поколінь, акцентуючи на створенні безпечного та здорового навколишнього середовища. Зокрема, сьогодні відзначається, що такий розвиток базується на системному підході та сучасних інформаційних технологіях, які дозволяють моделювати різні сценарії розвитку, прогнозувати їхні наслідки та вибирати оптимальний варіант з точки зору безпеки.

Безпека - це поняття, що визначає стан стабільності, миру та відсутності загрози. Вона має суб'єктивний характер і включає в себе базові потреби окремих людей, соціальних груп і держав. Безпека включає задоволення таких потреб, як існування, виживання, цілісність, ідентичність, незалежність, спокій (мир), доступність і стабільний розвиток [37].

Функція безпеки, яка пронизує всі сфери соціальної системи та визначає її ефективність, охоплює когнітивні та філософські аспекти. Вона стає методологічною основою для розробки теоретичних підходів та практичних дій особистості, суспільства та держави. Поняття безпеки сприяє розумінню природи існування системи як цілісного організму та є методологічною підставою для аналізу якості життя даної соціальної системи, її ефективності та стійкості до різноманітних загроз, які можуть підірвати її стабільність.

У цьому контексті, безпека може бути розглянута як тенденції розвитку та умови існування суспільства, його структури та інститутів, які визначаються відповідними директивами. Водночас безпека виступає як захист цієї функції від потенційних та реальних загроз, що ставлять під загрозу її стабільність та цілісність.

Логічний аспект теоретичного розгляду об'єктів філософії полягає у фіксації результатів практичного і пізнавального ставлення до дійсності. Сукупність понять, категорій і законів відображає загальні принципи існування людини і світу, сприйняття людиною своєї природи та природи світу, свого місця у світі, мети і сенсу життя. Поняття і категорії слугують індикаторами рівня усвідомлення людиною свого ставлення до світу та до себе. Зміст понятійно-категоріального апарату, його структура і динаміка відображають розвиток як самої дійсності, так і взаємодії індивіда з іншими людьми.

Етимологічно слово "безпека" походить від латинського виразу "sine cura", що означає "без турботи". Це підкреслює зв'язок поняття безпеки з відсутністю турботи та загрози. У сучасному науковому підході до розуміння безпеки використовуються різні аспекти та підходи, оскільки поняття безпеки має глибоке значення для різних сфер життя та досліджень. Розвиток понятійного апарату є невід'ємною частиною розвитку знань і розуміння природи об'єктів та процесів реальності. Використання точної термінології та понять допомагає уникнути непорозумінь та помилок у вивченні реальних явищ.

Інтегративний підхід до вивчення феномена інформаційної безпеки на основі соціально-історичної та соціально-діяльнісної природи людини дійсно є важливим, адже такий підхід допомагає розглядати інформаційну безпеку як складний феномен, що включає не лише технічні аспекти, але й соціокультурні, психологічні та етичні аспекти. Інтеграція цих підходів дозволяє більш повно і глибоко розуміти та аналізувати проблеми інформаційної безпеки в сучасному світі [28].

Поняття безпеки в сучасних соціальних системах включає в себе інформаційну безпеку, яка стає особливо важливою у цифрову епоху.

Інформаційна безпека має різні підходи до свого визначення, і це відображає складність та мінливість вимог із забезпечення безпеки в інформаційному просторі [7].

Підхід, який розглядає інформаційну безпеку як здатність суб'єкта зберігати свої системні та фундаментальні характеристики, підкреслює важливість захисту інформаційних ресурсів та процесів від негативних впливів кіберпростору та технологій. Цей підхід акцентує на забезпеченні стійкості та цілісності інформації, що має вирішальне значення для безпеки як окремої особи, так і суспільства в цілому.

За іншим підходом, інформаційна безпека пов'язана з управлінням ризиками та реагуванням на потенційні та реальні загрози, які виникають у цифровому середовищі. Цей підхід висуває акцент на взаємодію між різними політичними структурами, органами влади та управління, які залучаються до забезпечення безпеки в інформаційному просторі.

Обидва підходи важливі та доповнюють один одного, оскільки інформаційна безпека сьогодні - це багатогранний феномен, що вимагає інтегрованого підходу та співпраці різних суб'єктів та організацій для досягнення оптимальних рівнів захисту в інформаційному середовищі.

Відповідно до визначення Гурковського В.І., національна інформаційна безпека України включає суспільні відносини, спрямовані на захист життєво важливих інтересів особистості, громадян, суспільства і держави від потенційних та актуальних загроз у сфері інформаційного простору [23].

Ці відносини сприяють збереженню та розмноженню духовних і матеріальних цінностей держави, а також є необхідною умовою для прогресивного розвитку України. Цей процес базується на цілеспрямованій інформаційній політиці, спрямованій на гарантування, захист, оборону та забезпечення національних інтересів.

За поглядами Б.А. Кормича, інформаційна безпека визначається як система захищених законом правил, що регулюють оброблення інформації в межах держави. Ця система призначена для забезпечення умов існування і

розвитку особистості, суспільства в цілому та держави, які гарантовані Конституцією [51].

У даному контексті також наголошується на основних аспектах інформаційної безпеки:

1. Сфера інформаційної безпеки поєднує безпекову та інформаційну функції держави.

2. Компетенція держави у сфері інформаційної безпеки визначається взаємодією між правами особи на інформацію та функціями держави та її органів щодо регулювання інформаційних процесів.

3. У демократичному суспільстві регулювання сфери інформації здійснюється через визначення правових норм.

Також важливо зазначити погляд О. Логінова, який стверджує, що визначення поняття "інформаційна безпека" не обов'язково має бути обмеженим лише "державою" [61].

Він наголошує, що концепція "інформаційної безпеки" не повинна обмежуватися поняттям "держава", а скоріше визначається як неперервний процес. Зокрема, він стверджує, що інформаційна безпека є динамічним процесом.

Відповідно до його думки, інформаційну безпеку варто розглядати як складне поєднання таких аспектів, як державність, приналежність та ефективне управління загрозами та ризиками, а також забезпечення оптимальних методів їх запобігання та мінімізації негативних наслідків, особливо в контексті сфери інформаційної діяльності державних органів [61].

Різноманітність підходів до визначення поняття "інформаційна безпека" демонструє її ключове значення та складність у науковій сфері та різних аспектах людської діяльності. Сутність та важливість цього поняття тісно пов'язані з розвитком сучасного інформаційного суспільства.

Основою онтологічного розуміння "інформаційної безпеки" є ціннісний аспект об'єкта безпеки. Коли мова йде про інформаційну безпеку особи, це

передбачає, перш за все, врахування її потреб, які визначені в правовому полі її прав та свобод.

З епістемологічного погляду, зміст "інформаційної безпеки" може бути сприйнятим, з одного боку, як сукупність небезпек і загроз, що впливають на існування суб'єкта, і, з іншого боку, як вияв проактивної здатності суб'єкта створювати безпечні умови для існування об'єкта інформаційної безпеки [37].

Правове розуміння інформаційної безпеки має важливе значення з юридичної перспективи. Коли цей термін отримує юридичний статус, він визначає платформу для побудови системи інформаційної безпеки [28].

Інакше кажучи, він служить основою для захисту об’єкта інформаційної безпеки та регулювання діяльності суб'єктів в цій сфері з точки зору права. Точне визначення логічного контексту інформаційної безпеки великою мірою залежить від розвитку наукових та політичних інститутів.

1.2 Теоретичні основи дослідження суспільно-політичної стабільності

Складне політичне становище в Україні за останнє десятиліття, включаючи прояви гібридної війни та повномасштабне вторгнення росії, обумовлено рядом чинників, серед яких важливу роль відіграє стан системи інформаційної безпеки.

Перед проведенням детального аналізу політичного становища доцільно визначити сутність розглянутих понять. Термін "система" походить від давньогрецького слова "σύστημα", що буквально означає "ціле, яке складається з частин".

У давні часи антична філософія вважала системи організованим порядком та повнотою буття. Тоді загальна організація Всесвіту розглядалася як система, природний порядок, створений богами.

Філософ Георг Вільгельм Фрідріх Гегель розглядав об'єкти як органічні цілі. Він вбачав схожість між об'єктом і цілим, оскільки об'єкт також складався з частин, а ці частини, в свою чергу, з елементів. Відтак, для пізнання об'єкта

(отримання уявлення про нього) було необхідно спочатку виділити всі його частини та елементи, а потім уявно об'єднати їх для розуміння цілого.

Поняття "система" пройшло тривалий історичний шлях і стало ключовим у XXI столітті. Воно отримало значущість як у філософії, так і в методології та науці загалом. Визначення "системи" виступає як одна з найважливіших філософських, методологічних і наукових категорій нашого часу. Відображення об'єктів наукового пізнання у вигляді систем є фундаментальним і універсальним підходом.

Проаналізувавши надані словникові і енциклопедичні визначення, можна виділити основні загальні характеристики поняття "система": повнота, єдність елементів, складність (кількість елементів), організована структура і взаємодія компонентів. Семантика загального визначення терміна "система" включає поняття "ціле", "єдність", "елементи", "зв'язки" і "структура" [114].

Наукова література містить більше ніж 40 різних визначень терміна "система". Залежно від підходу, їх можна розділити на три групи. Перша група визначає системи з використанням понять системного підходу, таких як "елементи", "відносини", "зв'язки". Друга група підходить до системи з погляду теорії регулювання і використовує поняття "вхід", "вихід", "обробка інформації", "закони поведінки" і "управління". Третя група визначає систему як особливий клас математичних моделей [47].

Однак через різноманітність визначень терміна "система", залежно від контексту, мети та галузі знань, в якій він використовується, існують різні підходи до визначення властивостей системи. До таких підходів відносяться:

1. Системи прагнуть зберегти свою структуру, відповідно до закону самозбереження, який базується на об'єктивному законі організації.

2. Системи можуть бути керованими (людиною, твариною, суспільством, великим соціумом). У системі формуються складні відносини, які залежать від індивідуальних властивостей її елементів і підсистем.

3. Кожна система має входи, систему оброблення, кінцевий результат (вихід) і зворотній зв'язок.

4. Система взаємодіє з довкіллям через свої входи і впливає на зовнішнє середовище через свої виходи [16].

Ці різні підходи дозволяють розкрити різноманітні аспекти поняття "система" і враховувати його широкий спектр відтінків у різних дисциплінах і ситуаціях.

У інтернет-енциклопедії Wikipedia властивості систем поділено на чотири групи:

1. Ті, що стосуються цілей і функцій: синергетичний ефект, ієрархія, емерджентність, розмаїття, обґрунтованість, альтернативні режими функціонування та розвитку, робастність.

2. Ті, що стосуються структури: цілісність, неадитивність, структурність, ієрархічність.

3. Ті, що стосуються взаємодії з ресурсами і навколишнім середовищем: переносність, взаємодія та взаємозалежність системи із зовнішнім середовищем, адаптивність, надійність тощо.

4. Ті, що стосуються структури системи: переносність, взаємодія та взаємозалежність системи із зовнішнім середовищем, адаптивність, надійність, надійність.

Важливо зазначити, що безпечний розвиток суспільств, держав та окремих осіб прямо пов'язаний з їхньою інформаційною безпекою, а інформаційне середовище є системоутворювальним чинником цього розвитку [24].

З цього погляду, можна розглядати інформаційну безпеку як системне явище, оскільки інформаційна безпека є невід'ємною частиною будь-якого середовища національної безпеки, забезпечення її є одним з найважливіших завдань державних механізмів.

Відсутність системи інформаційної безпеки унеможливлює забезпечення не тільки інформаційної, а й національної безпеки [42].

Розгляд інформаційної безпеки з урахуванням її місця в системі національної безпеки є критично важливим, особливо в умовах сучасної

геополітичної та технологічної динаміки. Інформаційна безпека має набагато ширший контекст, адже вона об'єднує цифрові, комунікаційні, соціальні, психологічні, економічні, інституційні та політичні аспекти. Україні важливо чітко визначити своє місце та роль в системі національної та міжнародної безпеки, оскільки це допоможе забезпечити ефективний захист і розвиток країни. Це стосується інформаційної складової національної безпеки, оскільки інформаційний простір стає все більш важливим в контексті міжнародних відносин, економічних процесів та культурних взаємодій.

Звернувши увагу на зміни у світовому інформаційному порядку, Україна має адаптувати свої підходи до інформаційної безпеки. Розвиток цифрового простору, зростання кількості цифрових атак та зниження рівня захисту інформації створюють складну ситуацію, яку необхідно контролювати. Також важливо враховувати, що концепція інформаційної безпеки має бути нерозривною складовою загальної системи національної безпеки, забезпечуючи цілісний підхід до захисту країни.

Друга низка обставин полягає в тому, що система забезпечення національної безпеки України стикається зі значущими викликами на всіх рівнях - національному, регіональному та глобальному. Це зумовлено збройною агресією та гібридною війною, що здійснюється проти країни, причому інформаційний аспект виступає як одна з ключових складових цієї війни.

Третім аспектом є те, що процес формування системи національної безпеки України перебуває в умовах становлення держави та нових суспільних відносин. Внутрішнє життя країни характеризується активною соціальною модернізацією, політичними та соціальними змінами, що призводять до внутрішньої конфронтації, політичних та економічних криз. У таких екстремальних умовах триває, хоча й повільно, формування одного з ключових елементів системи інформаційної безпеки - інститутів громадянського суспільства.

В глобальному масштабі поточні кризові явища мають суттєвий вплив на безпеку країн, особливо тих, що перебувають у перехідному стані, і це стосується і України [24].

Поняття інформаційної безпеки - це складне, систематичне та багатогранне явище, на стан та перспективи якого впливають зовнішні та внутрішні фактори [80].

Розглядаючи це з погляду внутрішніх факторів, можна виділити такі аспекти:

1) геополітичне становище та зовнішні виклики,

2) розвиток та впровадження інформаційних технологій,

3) рівень інформатизації та комунікацій,

4) внутрішньополітична ситуація [80].

У контексті системного підходу, аналіз феномена інформаційної безпеки передбачає комплексний розгляд всіх соціальних зв'язків, елементів та компонентів суспільства та держави, а також функцій і проблем, утворюючи єдине ціле. Використання системного підходу визначає загальний напрямок дослідження і встановлює цілісність та організованість об'єкта дослідження (як-то системи, проблеми, соціального явища, процесу тощо) як єдиного цілого.

Згідно з поглядами спеціалістів у галузі методології, можна визначити підходи до розуміння системи інформаційної безпеки:

1. Правові та наукові (доктринальні) основи;
2. Суб'єкт та його структура, включаючи об'єкт інформаційної безпеки та систему організацій (підрозділів), що відповідають за її забезпечення;
3. Політика інформаційної безпеки;
4. Засоби і методи забезпечення інформаційної безпеки.

Такий підхід допомагає створити цілісну картину інформаційної безпеки, охоплюючи різні аспекти її функціонування та забезпечення.

Водночас, головною метою інформаційної безпеки є забезпечення функціонування комплексної системи захисту інформаційних носіїв.

Згідно зі статтею 3 Закону України "Про національну безпеку України", державна політика у сферах національної безпеки і оборони спрямована на захист: людини і громадянина - їхніх життя і гідності, конституційних прав і свобод, безпечних умов життєдіяльності; суспільства - його демократичних цінностей, добробуту та умов для сталого розвитку; держави - її конституційного ладу, суверенітету, територіальної цілісності та недоторканності; території, навколишнього природного середовища - від надзвичайних ситуацій [99].

О.О. Тихомиров пропонує виділяти три основні групи суб'єктів кібербезпеки: держави, які включають міжнародні та урядові організації; неурядові організації; а також громадян та їх об'єднання [117].

Підхід, викладений вище, втілено в Стратегії інформаційної безпеки. Згідно з нею, діяльність органів виконавчої влади в сфері інформаційної безпеки в Україні спрямована на поєднання активності держави та громадянського суспільства [112].

Не менш важливо, що заходи, спрямовані на забезпечення інформаційної безпеки в Україні, охоплюють міжнародний, національний та громадянський рівні інформаційної безпеки.

Система інститутів (суб'єктів) забезпечення безпеки має наступні складові:

Органи загальної законодавчої та виконавчої юрисдикції, зокрема Верховна Рада України та Кабінет Міністрів України, Конституційний Суд України та суди загальної юрисдикції, органи управління, що включають:

1. Правоохоронні органи, такі як Офіс генерального прокурора України, Міністерство внутрішніх справ України, Служба безпеки України.

2. Галузеві органи влади, що регулюють інформаційні відносини, такі як Міністерство культури та інформаційної політики України, Державний комітет зв'язку та інформатизації України, Державний комітет телебачення і радіомовлення України тощо.

Ці суб'єкти взаємодіють і співпрацюють з метою забезпечення інформаційної безпеки.

О.В. Олійник на підставі аналізу чинного законодавства та з урахуванням досвіду інших країн запропонував три рівні організаційно-функціональної системи забезпечення інформаційної безпеки:

Перший рівень - стратегічний національний рівень, включає Верховну Раду України, Кабінет Міністрів України та їх консультативно-дорадчі органи [84].

Цей рівень відповідає за формування політики, створення нормативно-правового середовища, координацію процедур міжнародного співробітництва, використання ресурсів для роботи з інформацією та керування поведінкою суб'єктів у кризових ситуаціях.

Другий рівень - організаційно-адміністративний, галузевий та регіональний рівень, включає центральні органи виконавчої влади, органи місцевого самоврядування, військові структури, органи юстиції та правосуддя. Цей рівень відповідає за організаційно-методичне забезпечення інформаційної безпеки в відомчих, адміністративно-територіальних одиницях, а також за координацію та контроль діяльності органів державної влади [84].

Таким чином, система забезпечення інформаційної безпеки має чітку структуру, яка включає різні рівні організаційно-функціонального підходу.

Третій рівень - національна критична інфраструктура, підприємства, установи, організації та інші суб'єкти, які здійснюють діяльність у галузі телекомунікацій, електронних комунікацій та інформаційних технологій. На цьому рівні вони повинні реалізовувати повноваження щодо забезпечення безпечного функціонування національної та регіональної критичної інфраструктури та запобігання зовнішнім і внутрішнім загрозам і небезпекам, які можуть завдати шкоди населенню, суспільству і державі [84].

Державна інформаційна політика має нести в собі не лише актуальні питання, що розгортаються у міжнародному співтоваристві, але і відображати нагальні питання в галузі інформаційної безпеки. Ця політика також має

гарантувати правовий захист прав та інтересів всіх суб'єктів, що займаються інформаційною діяльністю. Найскладнішим завданням є вирішення гармонізованого забезпечення інформаційної безпеки на рівні держави, індивіда та суспільства [112].

Серед основних завдань інформаційної політики можна виділити:

1. Встановлення та утвердження ключових пунктів захисту національної системи інформаційної безпеки.

2. Практичне втілення планів розвитку ефективної національної системи інформаційної безпеки.

3. Перегляд списку нових інформаційних загроз.

4. Ефективне нейтралізування наявних загроз та оцінка можливих наслідків і ступеня їх серйозності.

Однією з основних цілей державної інформаційної політики є гарантування права на достовірну, повну та своєчасну інформацію, збереження свободи слова та інформаційної діяльності в межах національного інформаційного простору, запобігання втручанню в зміст і внутрішню організацію інформаційного процесу, за винятком випадків, передбачених законом та відповідно до Конституції України [37].

Також важливими аспектами є захист національного інформаційного продукту та технологій, національних культурних та духовних цінностей, а також їх збереження та подальший розвиток, надання інформації громадськості. Вибір політики інформаційної безпеки обумовлений факторами, які впливають на ситуацію та ризики в сфері національної безпеки.

До факторів, що впливають на вибір безпекової політики, можна включити наступні:

1. Демографічні фактори: Чисельність населення держави, демографічні тенденції, структура населення (зростання або зменшення населення), розподіл за віковими групами.

2. Географічні фактори: Місце розташування держави, її розмір території, географічні особливості, клімат та інші географічні чинники, які можуть вплинути на безпеку.

3. Економічні фактори: Сировинна база, економічний потенціал, обсяг виробництва, очікуване економічне зростання, потреби та можливості країни.

4. Історичні, психологічні та соціологічні фактори: Історичний досвід країни, ставлення громадян до життя та безпеки, соціальна згуртованість, національна самосвідомість.

5. Організаційні та адміністративні фактори: Форми управління в країні, ставлення суспільства до влади, ефективність системи управління.

6. Військові фактори: Рівень організації та ефективності військових сил, їх чисельність в порівнянні з населенням призовного віку.

Ці фактори слід враховувати при визначенні та формулюванні політики національної безпеки, оскільки вони впливають на специфічні внутрішні та зовнішні виклики, з якими країна може стикнутися, і визначають її можливості та обмеження у цій сфері.

Діяльність з забезпечення інформаційної безпеки має зосереджуватися на конструктивному поєднанні зусиль держави, громадянського суспільства та окремих громадян в рамках трьох ключових напрямків:

1. Інформаційно-психологічний напрям, що передбачає створення сприятливого психологічного клімату в національному інформаційному просторі. Його основні цілі включають забезпечення конституційних прав і свобод людини і громадянина, популяризацію загальнолюдських та національних моральних цінностей [37].

2. Технологічний розвиток, спрямований на розвиток та інноваційне оновлення інформаційних ресурсів країни. Для цього важливо запровадження новітніх технологій створення, обробки та поширення інформації. Інноваційне оновлення інформаційних ресурсів сприяє зміцненню потенціалу країни у сфері інформаційних технологій.

3. Захист інформації, забезпечення конфіденційності, цілісності та доступності інформації, яка міститься в національних інформаційних ресурсах [37].

Такий підхід до забезпечення інформаційної безпеки передбачає взаємодію різних суб'єктів, від індивідуальних громадян до державних органів, з метою створення стійкого і безпечного інформаційного середовища, що відповідає потребам і інтересам усіх сторін.

1.3 Система інформаційної безпеки як елемент суспільно-політичної стабільності: методи вивчення

Без жодних сумнівів, інформаційна безпека сьогодні є темою загального інтересу, яка активно обговорюється у політичних та бізнес колах. Відірвавшись від теоретичних роздумів, можна виділити два основних підходи до взаємодії людини з інформаційною безпекою.

Перший підхід, що домінує у юриспруденції та безпекознавстві, зосереджується на гарантуванні прав та свобод особи в сфері інформації, включаючи вільну можливість збирати, зберігати, використовувати та поширювати інформацію.

Цей підхід також відомий як технічний аспект, оскільки технічні аспекти інформаційної безпеки охоплюють здібності та навички осіб прогнозувати та запобігати інформаційним загрозам в технічних системах, а також загрозам, що стосуються самих систем. Другий підхід фокусується на захисті психіки та свідомості людей від негативного впливу інформації, такого як маніпуляції та дезінформація. Важливим є також врахування динаміки розвитку інформаційної безпеки. Ця динаміка відображає невід'ємну роль інформаційної безпеки в житті суспільств та держав, де спостерігаються постійні зміни впливу інформації. Це підкреслює наявність взаємозв'язків між суб'єктами та об'єктами цієї безпеки, їхніми інтересами, тенденціями та розвитком, визначаючи сутність інформаційної безпеки як системного явища.

Чинники, які поглиблюють загрози інформаційної безпеки, мають складний і універсальний характер, оскільки вони охоплюють усі сфери людського життя, суспільства та держави [2].

Так, аналіз загроз завжди має суб'єктивний відтінок на практиці, де окремі особи або соціальні групи оцінюють фактори в контексті своїх інтересів і професійного досвіду.

Водночас об'єктивна ідентифікація загрози передбачає чітке розуміння параметрів, при яких явище втрачає можливість для саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також умов, при яких цей фактор може стати реальною чи потенційною загрозою [14].

Не менш важлива є класифікація загроз, яка дозволяє визначити, які з них є найбільш пріоритетними з наукового або нормативного погляду.

Згідно з чинною Стратегією інформаційної безпеки до національних викликів і загроз відносяться: інформаційний вплив Росії як держави-агресора на населення України, Інформаційне домінування Росії як держави-агресора на тимчасово окупованих територіях України, Обмежені можливості реагувати на дезінформаційні кампанії, Несформованість системи стратегічних комунікацій, Недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів, Спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України, Доступ до інформації на місцевому рівні, Недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [7].

Важливо зазначити, що різні категорії суб'єктів можуть мати різні підходи до розуміння сутності інформаційної безпеки. Наприклад, безпека цивільного населення та державних службовців може розглядатися з різних ракурсів. Тому логічно розглядати специфічні загрози, які можуть бути більш вузько спрямованими.

Наприклад, загрози інформаційній безпеці мережевих ресурсів можуть включати:

1. Перехоплення, зчитування або навмисна підміна даних.
2. Неправильна ідентифікація користувачів з метою шахрайства.
3. Міжмережевий несанкціонований доступ.

Це свідчить про необхідність розглядати загрози відповідно до контексту та специфіки суб'єктів, які можуть бути залучені до сфери кібербезпеки.

У контексті цього підходу, загрози можуть бути поділені на дві основні категорії: випадкові та навмисні.

До випадкових загроз відносяться такі:

1. Помилки обслуговуючого персоналу або користувачів;
2. Втрата інформації через недбале зберігання;
3. Випадкове знищення або заміну даних;
4. Вихід з ладу обладнання, джерел живлення або мережевих компонентів;
5. Збої в роботі програмного забезпечення, включаючи зараження комп'ютерними шкідливим програмним забезпеченням.

До навмисних загроз відносяться такі:

1. Несанкціонований доступ до інформації та мережевих ресурсів;
2. Розкриття, модифікація та відтворення даних і програм;
3. Розкриття, модифікація та обмін трафіком комп'ютерних мереж;
4. Розробка і розповсюдження шкідливого програмного забезпечення;
5. Викрадення носіїв інформації;
6. Знищення архівної інформації або умисне руйнування її;
7. Фальсифікація повідомлень, відмова від отримання інформації або зміна часу її отримання;
8. Перехоплення інформації, що передається каналами захищеного зв'язку.

Кожна з наведених вище класифікацій визначається певними умовами та критеріями. Вони можуть бути піддані різним методам класифікації залежно від наукової мети та методу дослідження.

Ці класифікації є суб'єктивними, тобто вони залежать від особи, яка їх розглядає, та її здатності розпізнавати характеристики об'єкта класифікації [38].

Перед тим як досліджувати загрози інформаційній безпеці людини як набір умов або факторів, що становлять небезпеку життєво важливим інтересам особи, важливо врахувати, що визначення життєво важливих інтересів людини має нормативний характер.

Згідно з Стратегією інформаційної безпеки, життєво важливі інтереси людини в інформаційній сфері в Україні охоплюють забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, систему захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [112].

Однак, чинне законодавство не містить визначень для термінів "негативний інформаційний вплив" або "деструктивна пропаганда". Такі поняття залишаються невизначеними і не мають чіткого змісту у чинному законодавстві.

Термінологія, така як "загроза", "ризик", "виклик", "небезпека" та "вплив", дійсно мають певну семантичну спорідненість, і їх використання може бути неоднозначним у різних контекстах. Вивчення теорії безпеки дозволяє виявити цей категоріальний апарат і використовувати його для забезпечення точності комунікації та юридичної точності.

Визначення терміну "виклик" вказує на потенційний опір з боку об'єктивних обставин або суб'єктів для реалізації інтересів актора. Виклики

можуть бути вирішені без негайних дій та зазвичай мають меншу ймовірність реалізації.

"Ризик" означає усвідомлену можливість небезпеки, а також потенціал втрат або невдач. Такий термін може застосовуватися до потенційних негативних наслідків або небезпек, які можуть виникнути в результаті певних дій. Словникові визначення "загрози" акцентують на можливості або неминучості небезпеки. Основна концепція полягає в тому, що загрози є факторами або явищами, які створюють умови для або спричиняють обмеження реалізації життєво важливих інтересів суб'єкта.

Підсумовуючи, точне розуміння термінів "виклик", "ризик", "загроза", "небезпека" та "вплив" є важливим для точності комунікації, а використання категоріального апарату теорії безпеки може сприяти уникненню плутанини та непорозумінь.

Г. П. Ситник зробив важливий внесок у класифікацію видів загроз, враховуючи взаємозв'язок між поняттями "виклик", "ризик" та "загроза". Він запропонував використовувати поняття "ризик" для кількісної оцінки загроз, а поняття "виклик" та "загроза" - для якісної класифікації. Ця система визначає різні рівні потенційної небезпеки залежно від ступеня впливу та можливих наслідків, від "потенційного виклику" з низьким ризиком до "потенційної небезпеки" з дуже високим ризиком.

"Вплив" може бути розглянутий з різних точок зору в теорії безпеки як взаємодія між явищами або чинниками та суб'єктами, що призводить до виникнення різних ступенів загроз, викликів, ризиків та небезпек. Філософська категорія "взаємодія" відображає процес впливу об'єктів один на одного, їхню взаємну залежність та зміну стану.

Категорія "впливу" є складною та багатовимірною, охоплюючи різні аспекти взаємодії між об'єктами і може бути використана для пояснення зв'язків між фізичними, хімічними, соціальними, психологічними впливами.

Таким чином, підходи до класифікації загроз та розуміння категорії "вплив" є важливими аспектами теорії безпеки, які допомагають аналізувати та розуміти вплив різних чинників на систему та її компоненти.

Психологи вважають, що наслідки впливу завжди мають психологічний аспект, навіть якщо вони виявляються через фізичні, хімічні або соціальні фактори. Це означає, що будь-який вплив може впливати на психологічний стан та поведінку людини через психічні механізми мозку.

Теорія безпеки також розглядає "інформаційний вплив" як організоване та цілеспрямоване використання спеціальних ІТ-засобів і технологій для зміни свідомості та поведінки особи, соціальної групи чи населення, а також інфраструктури та фізичного стану [37].

Інформаційний вплив може бути використаний для змін у функціонуванні, доступі до інформації, плануванні подій та інших аспектах. Однак, інформаційно-психологічний вплив є частиною інформаційного впливу і спрямований на вплив на психологічний стан, думки та поведінку людей.

Таким чином, в теорії безпеки вживають терміни "інформаційний вплив" та "інформаційно-психологічний вплив" для опису різних аспектів впливу на індивідів, групи та інфраструктуру [37].

"Інформаційний вплив" охоплює ширший спектр змін, включаючи технічні та фізичні аспекти, тоді як "інформаційно-психологічний вплив" зосереджується на впливі на психологічний стан та поведінку. Інформаційно-психологічний вплив можна визначити як цілеспрямовану дію на свідомість чи підсвідомість особи або групи осіб з метою зміни їхньої поведінки, світогляду чи переконань. Цей вплив може здійснюватися різними шляхами, наприклад шляхом переконання, навіювання тощо.

Залежно від ефективності та характеру змін, які він призводить, інформаційні впливи можна розділити на декілька категорій:

1. Ефективні та неефективні: враховуючи результати, які досягаються через вплив.

2. Суттєві та несуттєві: залежно від ступеня важливості впливу на конкретну ситуацію чи об'єкт.

3. Поверхневі, стабілізуючі та дестабілізуючі: відображаючи характер змін, які вони спричиняють.

4. Глобальні, локальні та часткові: з урахуванням масштабів та обсягу впливу на зміни.

Цей масштаб може бути розглянутий за допомогою кількох підходів:

1. Вплив на конкретну дію "тут і зараз".

2. Модифікація стійких установок та настанов щодо певних речей або осіб.

3. Формування або зміна загальних смислових орієнтацій, світогляду та цінностей.

Цей тип впливу також включає маніпуляції взаємодії між особами, рекламу, психотерапію та ідеологічний вплив, які спрямовані на модифікацію думок, переконань та поведінки.

Наслідки інформаційного впливу проявляються через різноманітні ефекти, які можна розділити на наступні категорії. Когнітивні ефекти охоплюють зміни в рівні свідомості, зростання обсягу знань, формування нових когнітивних схем, а також зміну сприйняття реальності та обробки інформації. Вплив на емоції спостерігається через зміну емоційних станів, появу нових або втрату старих емоцій та зміну загального емоційно-психологічного фону, включаючи стимуляцію до активної участі у процесі інформації.

Вплив на ціннісні орієнтації включає формування нових інтересів, уподобань, оцінок та ставлень до різних аспектів життя, а також можливе посилення чи послаблення вже існуючих інтересів. Психофізіологічні впливи проявляються через зміни у психофізіологічному стані, включаючи пульс, артеріальний тиск, дихання, гормональний рівень крові, колір шкіри. Поведінкові впливи відображаються через конкретні дії, вчинки та поведінку, охоплюючи організацію дій та взаємодії, як з оточуючими, так і з самим собою.

Ці класифікації відображають різні аспекти впливу і показують, як він може сильно впливати на різні аспекти особистості та поведінки. Інформаційний вплив є невід'ємною складовою життя сучасної людини в інформаційному просторі, де він відіграє ключову роль у формуванні свідомості, ціннісних орієнтацій, поведінкових моделей та сприйняття навколишнього світу. Інформаційний простір включає різноманітні динамічні чинники, що можуть впливати на індивідуальні та колективні процеси.

Інформаційне середовище служить інструментом трансляції соціальних норм, цінностей, установок та стереотипів до індивідів. Інформація має значний вплив на свідомість, формує когнітивні моделі світу та ситуацій, визначає сприйняття себе та оточення. Однією з ключових характеристик інформації є її здатність існувати незалежно від об'єкта відображення, що дозволяє їй активно впливати на психічні процеси.

У суспільстві кожна особа взаємодіє з інформацією, передає та отримує її, що сприяє її включеності у соціальні відносини та процеси. Саме через взаємодію з інформацією індивіди приєднуються до суспільства, засвоюють його норми, цінності та культурні особливості. Однак цей процес також може викликати проблему інформаційної дискримінації, коли доступ до інформації та її розуміння нерівномірно розподіляються серед різних груп населення [28].

Терміни "цифровий розрив" та "цифрова нерівність" відображають нерівномірний доступ до інформаційних технологій та інтернету, що може зміцнювати інформаційну дискримінацію та поглиблювати різницю між соціальними групами.

Інформаційний вплив є складним та багатогранним явищем, яке визначає багато аспектів сучасного життя та вимагає уваги як з боку індивідів, так і суспільства в цілому. Інформаційна освіта як частина інформаційної культури має запобігати розповсюдженню інформаційної дискримінації. Процес формування інформаційної культури людини аналогічний іншим видам культур, таким як правова, економічна та екологічна, і відбувається під час соціалізації. На рівнях свідомості та підсвідомості вони засвоюють соціальні ролі та моделі

поведінки, які надалі формують їх як повноправних членів суспільства. Тому увага акцентується на специфічних загрозах, які особливо актуальні на ранніх етапах соціалізації.

Сьогодні люди в значній мірі споживають однорідні глобальні інформаційні продукти, такі як новини, реклама, твори мистецтва тощо, що сприяє стандартизації масової свідомості. Це, в свою чергу, підтримує масове поширення способу життя, характерного для технологічно розвинених цивілізованих суспільств. Механізм "глобалізації масової свідомості" особливо сильно впливає на молодь та дітей, що може призводити до втрати національної ідентичності, занепаду мови та знецінення моральних та етичних цінностей, впливаючи на сприйняття правосвідомості.

Суттєвим аспектом інформаційної культури є інформаційна стійкість. З геополітичної перспективи, Україна зіштовхується з конфліктом між різними культурними традиціями. З одного боку, нація прагне до прозахідних цінностей, подібно до багатьох країн Східної Європи. З іншого боку, існує загроза російської пропаганди, яка вже суттєво вплинула на деякі регіони та сприяла веденню гібридної та згодом повномасштабної війни.

Формування нових цінностей та створення ідеологічної системи для їх підтримки є складним завданням, що вимагає ґрунтовного аналізу та дослідження. Відсутність такої системи може впливати на інформаційну безпеку окремих громадян і становити загрозу для загальної безпеки держави. Це підкреслює необхідність зосередження інформаційної культури на підвищенні індивідуального інформаційного імунітету та забезпеченні інформаційної стабільності.

Проблема інформаційного забруднення не може бути ігнорована. Сучасне життя, особливо в мегаполісах, характеризується надлишком інформації, що призводить до її "дублювання" або фрагментації. Це створює інформаційний шум, який може бути оцінений з урахуванням соціальних норм, за якими він регулюється.

Не менш важливим є питання захисту психічного здоров'я громадян України. Необхідно забезпечити належну увагу не тільки людям з психічними розладами, а й здоровим особам, які мають право на збереження свого фізичного та психічного здоров'я. Особливу увагу потрібно приділити наданню спеціалізованої психологічної допомоги військовослужбовцям, їх родинам та внутрішньо переміщеним особам.

Впровадження сучасних інформаційних технологій принесло суспільству не лише позитивні зміни, але й створює додаткові виклики для фізичного та психічного здоров'я. Інформація, отримана через ці технології, може викликати психологічні реакції, які впливають на фізичне самопочуття. Продовжене використання екранів або телевізорів може призводити до сухості очей, погіршення зору та головного болю. Тривале перебування в сидячому положенні сприяє напруженню хребта, викликаючи біль та деформацію постави. Інтенсивна робота з технічними маніпуляторами може призвести до перенапруження м'язів рук. Постійне використання мобільних телефонів, навушників та гучної музики може спричинити погіршення слуху.

Важливо також зазначити, що репрезентація світу через віртуальну реальність може мати значний вплив, іноді навіть більший, ніж реальний світ. Вплив віртуальної реальності на свідомість та підсвідомість людини є непередбачуваним.

Серйозна проблема виникає з адикцією (патологічною залежністю), яка починається, коли бажання втечі від реальності разом зі змінами психічного стану витісняють реальність і стають центральною ідеєю, що в кінцевому підсумку віддаляє від реального життя.

Наслідком вищезазначеного може стати не лише нездатність вирішувати важливі питання, такі як сімейні чи соціальні, але й припинення особистісного розвитку.

У серпні 1997 року патологічне використання Інтернету було додано до списку "нематеріальних" залежностей та офіційно визнано психічним розладом.

На початку повномасштабного вторгнення РФ на територію України значна частина населення перебувала у пригніченому психо-емоційному стані через відсутність доступу до звичних інформаційних потоків, що можна розглядати як дестабілізуючий фактор впливу на суспільну свідомість.

Однак деякі психотерапевти вважають, що інформаційна залежність не є окремим захворюванням. Часто цей діагноз може вказувати на інші серйозні проблеми, такі як депресія або труднощі з соціалізацією. Вони розглядають це як ознаку нездатності впоратися з певним видом реального стресу або невідповідності.

Отже, фактори, що загрожують інформаційно-психологічній безпеці людини, включають вплив суб'єкта, характеристики фізичного та інформаційного середовища та стан самого суб'єкта [37].

Згідно з аналізом наукової літератури, основними факторами ризику в інформаційному середовищі, які можуть бути джерелами інформаційно-психологічної небезпеки, є такі:

1. Обсяг, повнота та кількість інформації, що циркулює в системі, а також точність, доступність та своєчасність її отримання;

2. Відповідність інформації характеристикам сенсорного сприйняття, уваги, пам'яті, мислення, особистості, поведінковим стереотипам, соціально-психологічним установкам суспільства (відповідність сприйняттям повідомлень, дефіцит часу та перевантаження оперативної пам'яті, організація інформаційних потоків тощо).

3. Наявність елементів у інформаційному потоці, що свідомо змінюють психофізіологічний стан великої кількості людей та осіб, які приймають важливі рішення для суспільства;

4. Присутність в інформаційному середовищі модифікованих фізичних носіїв, які впливають на фізіологічні носії (світло, звук, електромагнітні впливи).

Серед основних інформаційно-психологічних факторів ризику, які властиві людині, варто відзначити:

1. Незрілість особистості, яка проявляється у нездатності свідомо та добровільно відбирати інформацію, що відповідає її змінам, переконанням та планам.

2. Особистісні установки, такі як пристосування, наслідування та готовність приймати вплив маніпулятивної інформації.

3. Негативні зміни у функціональному стані мозку та психіки.

4. Масове зараження ідеями та закликами, що може бути спричинене на психофізіологічному рівні соціальним статусом, який сприяє більшій сугестивності, хронічним або гострим психічним та емоційним напруженням, фрустрацією та страхом [37].

Таким чином, необхідно враховувати ще одну загрозу. Низький рівень інформаційної та правової культури породжує еклектицизм як домінанту інформаційної "культури мас". Під еклектикою розуміють механічне поєднання в доктрині розрізнених і органічно несумісних елементів, запозичених з протилежних концепцій.

Низька інформаційна грамотність, поєднана з інформаційним перевантаженням, підриває цілісність особистості, знижує здатність критично сприймати, аналізувати та оцінювати отриману інформацію, а також формувати власну думку.

Свобода, що є первинною умовою існування людини, вимагає гарантій інформаційної безпеки. Загрози інформаційній безпеці людини утворюють складну ієрархію з численними зв'язками на різних рівнях, а їх вплив на особистість також є складним і різноманітним. Тому запропонована класифікація є певною мірою умовною.

У сучасному інформаційному суспільстві можливість реалізації прав та свобод людини значною мірою залежить від адаптивності індивідів, соціальних, політичних інститутів, а також державних та правових систем. Важливою умовою цієї адаптивності та захисту прав та свобод людини є високий рівень інформаційної та правової грамотності.

Це пов'язано з тим, що саме на цьому етапі формується інформаційна грамотність людини, яка дозволяє їй ефективно протистояти загрозам, викликам та ризикам, пов'язаним з інформацією, а також користуватися можливостями, які створює інформаційне суспільство.

У контексті вищезгаданої інформаційної та правової грамотності, особливо актуальним стає питання інформаційно-психологічних операцій, які часто використовуються для маніпуляції громадською думкою, впливу на політичні процеси та навіть підриву стабільності держав.

Інформаційно-психологічні операції (ІПСО) є складовою інформаційних операцій та відіграють важливу роль у веденні інформаційно-психологічної війни. Вони включають застосування різноманітних інтегрованих, узгоджених та координованих методик та заходів психологічного впливу з метою реалізації певних цілей. Такі операції можуть мати різні напрямки, включаючи політичний, військовий, економічний, дипломатичний та розвідувальний аспекти, і спрямовані на певні цільові групи населення. Метою є вплив на ідеологічні погляди, установки, переконання, стереотипи, поведінку, настрої, емоції та волю цих груп.

Інформаційно-пропагандистські заходи є важливою складовою ІПСО. Головна мета таких заходів полягає в дестабілізації суспільства зсередини та створенні умов для подальших політичних, економічних та військових дій. Основна увага приділяється впливу на громадську думку, настрої, ціннісні орієнтації та соціально-психологічний клімат, з метою дестабілізації суспільства шляхом створення атмосфери суспільно-політичної невизначеності, страху та терору.

Психологічні операції мають на меті вплив на психологічний стан, спричиняючи страх, невдоволення, недовіру, а також формування антиурядових настроїв та підтримку опозиційних груп. Вони використовують медіа, друковані матеріали, аудіо- та відеопродукцію, а також особисте спілкування для зміни свідомості та поведінки цільових груп та індивідів.

Ці операції є частиною інформаційної війни та включають застосування різноманітних методів для впливу на лідерів політичних, релігійних, бізнесових та інших груп, а також на різні соціальні верстви населення. Це може включати дезінформацію, психологічний тиск, маніпуляцію інформацією та створення певного образу або ідеології, що відповідає бажаним цілям.

Психологічні операції використовують психологічні механізми та засоби впливу для маніпуляції свідомістю та поведінкою людей, а також для досягнення певних політичних, військових або економічних цілей. Вони можуть включати створення певних образів, формування страху та недовіри, поширення певних інформаційних повідомлень або теорій з метою впливу на переконання та поведінку цільової аудиторії.

Ці аспекти психологічних операцій підкреслюють їхню критичну роль у формуванні інформаційного впливу, особливо в контексті політичних та військових стратегій. Психологічні операції можуть бути застосовані як для деморалізації та дезорганізації противника в рамках військових операцій, так і для підвищення бойового духу, надання розвідувальних даних, зміцнення морального стану населення та власних військових формувань. Це є важливим інструментом військової стратегії та політичної впливової діяльності, оскільки він дозволяє впливати на свідомість і переконання цільових груп, створювати певний образ подій та ситуацій. Координація таких операцій з державною політикою та іншими заходами може підсилити їхню ефективність та досягнення стратегічних цілей. Розуміння сутності ІПСО підкреслює їхню значущість як в аспекті ведення війни, так і у контексті політичного та соціального впливу.

Класифікація психологічних інформаційних операцій може бути узагальнена за наступними критеріями:

1. В залежності від сфери впливу:

• Соціальна сфера: вплив на загальні настрої, переконання та поведінку громадян.

- Державна сфера: вплив на рішення, політику та діяльність органів влади.

2. В залежності від рівня впливу:

- Стратегічні операції: націлені на широку аудиторію або впливових осіб, мають довготермінові цілі.
- Тактичні операції: базуються на актуальних завданнях, спрямовані на короткострокові цілі, включаючи дезорганізацію діяльності конкретних опонентів.

3. В залежності від інтенсивності та тривалості:

- Фундаментальні: вимагають значних зусиль і тривалого впливу.
- Поверхневі: можуть бути менш інтенсивними та короткотривалими.

4. В залежності від характеру впливу:

- Деморалізаційні операції: спрямовані на зниження моральних настроїв, виклик негативних емоцій.
- Мотиваційні операції: прагнуть збільшити моральний дух, мотивацію та підтримку.

5. В залежності від сфери розповсюдження:

- Зовнішньополітичні: вплив на інші держави або міжнародні організації.
- Внутрішньополітичні: спрямовані на внутрішні події, політику та громадську думку власної країни.

В контексті внутрішньої політики, психологічні інформаційні операції зазвичай проявляються у вигляді пропагандистських протистоянь між політичними суб'єктами.

У більш складних сценаріях, особливо під час виборчих кампаній та боротьби за владу, ці операції перетворюються на інструменти, спрямовані на підрив морального стану політичних опонентів, втручання у лідерські позиції та дискредитацію їхніх дій з метою впливу на індивідуальну та колективну громадську думку для досягнення певних цілей.

У сфері конфлікту економічних інтересів, розвідувально-психологічні операції включають низку заходів, які мають на меті дискредитацію конкурентів, їхніх економічних стратегій та союзників на політичній арені. Основна ціль цих операцій полягає у змушенні конкурентів відмовитися від будь-яких дій або стратегій, які можуть надати їм перевагу на ринку.

В рамках зовнішньої політики та економіки, розвідувально-психологічні операції здійснюються з метою забезпечення інтересів державного та військового керівництва, а також підтримки ключових секторів економіки та великих корпорацій, які становлять основу національної економіки, зокрема на міжнародному ринку.

Ці операції можна класифікувати за рівнем взаємодії на такі категорії:

1. Міжнародний рівень: Ці операції відбуваються на міждержавному рівні і можуть включати міжнародні конфлікти та конкурентну боротьбу між транснаціональними корпораціями та організаціями, що діють на глобальному рівні.

2. Національний рівень: Операції на цьому рівні здійснюються з участю національних органів влади та спрямовані на підтримку національної політики та захист національних інтересів, включаючи ідеологічну підтримку та просування національних цінностей.

3. Локальний рівень: Ці операції проводяться на рівні окремих компаній, об'єднань, політичних партій, громадських організацій та релігійних спільнот. Вони можуть бути спрямовані на вирішення конкретних локальних завдань або на вплив на певні цільові групи.

Розвідувально-психологічні операції на кожному з цих рівнів мають свої специфічні цілі, методи та засоби впливу, але всі вони спрямовані на досягнення певних стратегічних цілей в інтересах держави або окремих суб'єктів.

Класифікація інформаційно-психологічних операцій відображає їхню різноманітність та масштабність, що можуть реалізовуватися в різних сферах та під різними умовами. В залежності від інтенсивності та тривалості, інформаційно-психологічні операції можна класифікувати на такі типи:

1. Інтенсивні та відносно короткострокові операції: Це зазвичай інформаційні кампанії, спрямовані на конкретні події, наприклад, виборчі кампанії або гострі конфлікти між конкурентами. Операції цього типу вимагають високої інтенсивності впливу протягом обмеженого часу.

2. Довготривалі та неінтенсивні операції: Ці операції включають організацію інформаційного впливу протягом тривалого часу і можуть бути спрямовані на формування стійких ідеологічних, інтелектуальних або моральних установок.

3. Постійні операції: Цей тип операцій характеризується неперервним характером інформаційного впливу. Вони можуть мати різну інтенсивність, але їхній характер включає постійність впливу на цільову аудиторію.

4. Розподілена інформаційна війна: Це операції, коли розвідувальні дії не є частиною єдиного потоку інформації, а переважно доповнюють таємні дії. Це може бути використано у контексті економічної конкуренції, переговорних процесів, політичного тиску тощо, для здійснення необхідного психологічного тиску на конкурентів у потрібний момент.

Операції інформаційного та психологічного характеру можна класифікувати за основним спрямуванням їх впливу наступним чином:

1. Пропагандистські операції: Цей тип операцій має на меті поширення певної ідеології, концепції або поглядів через використання інформаційних засобів.

2. Дезінформаційні операції: Метою таких операцій є розповсюдження неправдивої, вигаданої або спотвореної інформації з метою вводу в оману або дискредитації конкурента, ворога або противника.

3. Маніпулятивні операції: Метою цих операцій є вплив на свідомість, поведінку та рішення людей шляхом використання психологічних засобів і методів, які мають на меті маніпулювати думками та емоціями цільової аудиторії.

Загалом, інформаційно-психологічні операції є складними та багатоаспектними заходами, які вимагають ретельного аналізу та планування, а

також високої адаптивності та гнучкості у відповідь на динамічні умови середовища та змінювані потреби.

Реалізація інформаційно-психологічних операцій є комплексним процесом, який включає в себе різноманітні сфери діяльності, такі як журналістика, інформаційна політика, соціологія, психологія, право, економіка та інформаційна безпека. Зазвичай цей процес складається з трьох послідовних етапів, кожен з яких базується на попередньому.

На першому етапі, який називається етапом злому опору та створення основи, відбувається підготовка аудиторії до сприйняття нової інформації. Цей процес може включати роз'яснення важливості проблеми, подання аргументів на користь нового підходу та подолання опору щодо змін.

Другий етап, етап впровадження нової інформації, характеризується поступовим введенням інформації щодо нового підходу або моделі світу. Цей етап може охоплювати надання конкретних доказів, детальне пояснення та переконливий вплив на переконання.

На третьому етапі, етапі введення нової теми, відбувається введення нової інформації на нову тему або підхід, який часто є протилежним попереднім переконанням. Цей етап може вимагати подальших змін у сприйнятті та поведінці аудиторії.

Ця схема сприяє забезпеченню переходу від поширення інформації до впровадження нових типів поведінки, заснованих на новій інформації.

Аналіз результативності інформаційно-психологічних операцій передбачає використання специфічних показників, що відображають зміни в соціальних або суспільних параметрах у рамках контрольованого процесу. Ці показники дозволяють оцінювати досягнуті результати та, за необхідності, адаптувати вплив.

Важливо застосувати різні категорії психологічних інформаційних заходів для забезпечення їхньої ефективності та прийняття аудиторією. Ці заходи можуть включати методи переконання, соціального впливу, емоційного резонансу, та когнітивного переосмислення. Ключовим аспектом є не тільки

донесення нової інформації, але й здатність спонукати аудиторію до переоцінки власних переконань та відповідної адаптації їх поведінки. Ці психологічні інформаційні заходи мають бути ретельно сплановані та цілеспрямовані, з особливим фокусом на механізми прийняття та обробки інформації індивідами, що дозволяє зміцнити вплив нової теми або підходу.

В контексті політичної боротьби можна виділити наступні категорії психологічних інформаційних заходів:

1. Інформаційно-пропагандистська діяльність (ІПД): Ця категорія охоплює заходи, які спрямовані на дисемінацію певних інформаційних повідомлень за допомогою засобів масової комунікації та безпосередньої взаємодії з цільовими групами. Застосовуються різноманітні методи та технології для модифікації психологічного стану реципієнтів.

2. Демонстративна діяльність: До цієї категорії відносяться ініціативи, спрямовані на створення психологічного впливу на аудиторію. Вони можуть формувати сприйняття певних образів або концепцій, спонукаючи до емоційної реакції. Головною метою є модифікація психологічного стану осіб, а не досягнення конкретних практичних результатів.

3. Організаційно-практична діяльність: Ця категорія включає заходи, спрямовані на реалізацію конкретних дій, де психологічний вплив на аудиторію виступає як ключовий компонент. Це можуть бути акції зі збору підписів, мітинги, конференції, які одночасно впливають на психологічний стан та стимулюють аудиторію до вжиття певних дій.

Ці категорії використовуються для формування інтегрованої психологічної стратегії в політичній боротьбі, де інформаційні заходи взаємодіють з психологічним впливом на суспільні настрої та поведінку.

Прикладами таких заходів можуть бути висування погроз санкцій або заходів проти певних осіб чи організацій, організація благодійних заходів з певною метою, проведення передвиборчих кампаній, запровадження та реалізація значущих соціальних програм.

Відмінність демонстративних заходів від реальних практичних дій полягає в їх часовій відповідності суспільно важливим подіям (наприклад, виборам) та супроводженні інформаційною кампанією.

Організаційно-практична діяльність реалізується через проведення додаткових заходів та дій, спрямованих на вплив на конкретних осіб або групи, а також на створення умов для підвищення ефективності та результативності загальної психоінформаційної діяльності, а також окремих просвітницьких ініціатив.

Ця діяльність має на меті вплив на психологічний стан окремої особи або групи осіб, а також сприяння покращенню результативності та ефективності загальної психоінформаційної діяльності та окремих просвітницьких ініціатив.

Структура цієї діяльності охоплює три основні групи організаційних заходів:

1. Забезпечення інформаційно-пропагандистських кампаній з використанням засобів масової інформації, а також фінансове та матеріально-технічне забезпечення.

2. Організація акцій протесту, мітингів, демонстрацій, зборів підтримки та інших подій.

3. Реалізація заходів, спрямованих на проведення переговорів, отримання підтримки, організацію фінансової або іншої допомоги, а також досягнення сприятливих рішень на різних рівнях адміністрації та законодавчих органів. Основні форми організації цих дій включають політичні ігри та лобіювання.

В умовах зростаючої загрози від деструктивного потенціалу засобів і методів інформаційної війни проти держави, суспільства та громадян, актуальним стає виявлення та запобігання актам інформаційної агресії та операціям інформаційної війни на ранніх стадіях. Це включає підготовку до застосування засобів інформаційної агресії, в тому числі спеціальних розвідувальних підрозділів та психологічних операцій, з метою нейтралізації впливу іноземних збройних сил та спецпідрозділів.

З огляду на зниження активності цих сил та засобів, важливою стає система заходів щодо попередження та стримування психологічної інформаційної агресії як складова частина системи психологічної інформаційної війни.

У разі оборони від агресії необхідно впроваджувати програми для локалізації шкоди, завданої агресією, та відновлення наступальних і оборонних здібностей національної системи протидії психоінформаційній агресії. Також важливо компенсувати втрати ресурсів та підтримувати збройні сили у стані постійної готовності відповідно до можливих напрямків агресії.

Система заходів протидії психоінформаційній агресії та операціям психоінформаційної війни може бути поділена на три ключові елементи:

1. Превентивні заходи, які включають:

• Сприяння зміні намірів потенційних агресорів шляхом психологічної та інформаційної взаємодії;

• Дискредитація небезпечних напрямів психоінформаційної агресії;

• Аналіз та усунення вразливостей у системах безпеки та оборони;

• Виявлення та ліквідація умов, що можуть бути використані агресорами для реалізації їх намірів.

2. Детекція актів психоінформаційної агресії та війни, яка включає:

• Моніторинг нових джерел інформаційно-психологічної напруженості;

• Аналіз конфліктного потенціалу в інформаційній сфері;

• Слідкування за геополітичними процесами та утворенням нових союзів.

3. Придушення актів психоінформаційної агресії та війни, що передбачає:

• Активну взаємодію з агресорами для зміни їх планів через психологічний та інформаційний вплив;

• Застосування психологічних методів для демаскування агресивних дій;

- Використання інформаційних ресурсів для протидії агресії.

Ці заходи сприяють розробці інтегрованої стратегії, що має на меті попередження, ідентифікацію та придушення психоінформаційної агресії та війни на різних стадіях. Основні дії для виявлення актів інформаційно-психологічної агресії та війни включають:

1. Регулярний моніторинг зовнішніх загроз інформаційно-психологічній безпеці держави та ідентифікацію ознак, свідчень та потенційних проявів актів інформаційно-психологічної агресії та війни;

2. Визначення напрямків зовнішньої державної експансії у розвідувальній (інформаційно-психологічній) сфері та протидія спробам інших держав використовувати інформаційно-психологічну експансію для прихованого управління суспільно-політичними процесами;

3. Виявлення спроб створення умов для прихованого управління системою соціально-економічних та політичних відносин, системою державної влади та місцевого самоврядування;

4. Аналітична реконструкція дій інформаційного вторгнення або операцій інформаційної війни, визначення їх цілей, намірів, планування та потенційних наслідків;

5. Інформування владних структур про виявлені загрози та ризики.

Посилення зусиль для припинення поширення психоінформаційної агресії та ефективна боротьба з операціями психоінформаційної війни на ранніх етапах передбачає:

1. Ліквідацію джерел психоінформаційної агресії, що може включати припинення або знищення каналів поширення дезінформації, неправдивих повідомлень та провокацій з боку ворожих елементів.

2. Реалізацію заходів для нейтралізації джерел психоінформаційної агресії, включаючи застосування контрдезінформаційних та протидійних дій, спрямованих на викриття обману та вплив на цільову аудиторію, яка зазнає негативного впливу.

3. Виявлення та обмеження масштабів та загрози психоінформаційної агресії, що включає ідентифікацію осередків активності та впливу, а також впровадження заходів для обмеження їхнього розповсюдження.

Посилення зусиль для припинення розповсюдження психоінформаційної агресії та ефективної боротьби з операціями психоінформаційної війни на початкових етапах включає ліквідацію джерел агресії.

Це може бути здійснено шляхом відключення від джерела засобів інформаційно-психологічної агресії агресора за допомогою звичайної та кібернетичної зброї, а також знищення центрів управління агресора. Ліквідація може бути як повною, так і частковою, залежно від успішності застосованих заходів та можливостей знищення або припинення впливу цих джерел.

Нейтралізація джерела інформаційно-психологічної агресії може бути також повною або частковою. Це передбачає паралізування коріння агресії, спонукання супротивника утримуватися від агресивних дій, здійснення прихованого контролю над джерелом агресії, інфільтрацію та проведення психологічних операцій серед особового складу збройних сил та засобів масової інформації агресора.

Локалізація масштабів і небезпеки психологічної та інформаційної агресії включає ізоляцію вогнища агресії, створення умов, що обмежують та ускладнюють дії сил і засобів інформаційно-психологічної агресії противника, забезпечення стабільності масштабів агресії та мінімізацію збитків, завданих агресією.

Такі заходи допомагають створити комплексну стратегію, спрямовану на запобігання, виявлення та придушення психоінформаційної агресії та психоінформаційної війни на різних етапах. Система попередження актів психоінформаційної агресії має велике значення у виявленні та придушенні цих актів на ранніх стадіях, з метою мінімізації ризиків для національної безпеки.

Проте, у випадках, коли агресор заздалегідь підготувався до агресії та має перевагу в швидкості атаки, можливість виявлення психоінформаційної агресії може настати лише на етапі її реалізації. Це стає особливо актуальним на стадії

активного проведення інформаційно-психологічної агресії, коли механізми агресії адаптовані та функціонують ефективно, а обстановка характеризується високою напруженістю та концентрацією сил і засобів.

У таких умовах здатність системи протидії актам психоінформаційної агресії на ранніх стадіях може бути обмеженою та недостатньою для запобігання агресії.

Це може потребувати створення нової системи негайного реагування на рівні державної влади, метою якої є припинення агресії, зокрема інформаційної війни, коли дії агресора є несподіваними для існуючої системи контррозвідки держави, а оперативна обстановка не дозволяє негайно активізувати всю систему захисту національних інтересів та інформаційної безпеки для протидії агресії.

Система швидкого реагування на раптово виявлену психологічну інформаційну агресію має декілька ключових елементів.

По-перше, оперативний штаб слугує центром управління, керуючи силами та засобами системи швидкого реагування та координуючи свою діяльність з іншими державними структурами.

По-друге, оперативне командування, що складається з підрозділів та органів державної влади, залучених до інформаційного протиборства, тимчасово приєднується до системи швидкого реагування, а їх керівництво переходить під контроль оперативного командування.

По-третє, сили постійної бойової готовності, які включають спеціальні підрозділи психологічного розвідувального впливу, розвідки, контррозвідки та інші, забезпечують готовність до дій у разі раптової агресії.

Крім того, система включає систему військової цензури та взаємодії з мас-медіа для контролю за інформацією під час оборонних дій, систему оперативного розгортання та застосування сил і засобів для негайного реагування на агресію, системи координації та взаємодії для співпраці з іншими державними органами, а також систему спеціального захищеного зв'язку та

автоматизованого управління для забезпечення зв'язку та керування в умовах конфлікту.

У разі ескалації конфлікту і неможливості стримати зовнішню інформаційно-психологічну агресію на початковому етапі, активується система міждержавного протиборства, що базується на застосуванні сил і засобів інформаційно-психологічної війни, передбачених законами і нормами війни.

До 2014 року термін "гібридна війна" був маловідомим для більшості українців, включаючи ЗМІ, політиків і широку громадськість. В основному лише деякі дослідники в галузі політології та стратегічних комунікацій, а також військові фахівці розуміли цей термін. Спочатку більше поширені були поняття "інформаційна війна", "інформаційне протистояння" та "інформаційна зброя", хоча вони часто вживалися з публіцистичним підтекстом [71].

Однак, сьогодні ситуація кардинально змінилася. Державна політика України в області безпеки, зокрема в інформаційній, значною мірою базується на розумінні сутності та небезпеці гібридної війни як частини повномасштабної збройної агресії. Важливо розуміти, що гібридна війна включає в себе не лише військові дії, але і використання різноманітних невійськових засобів та стратегій, щоб впливати на внутрішні справи і вразливості країни.

Це може включати інформаційну пропаганду, кібератаки, гібридні впливові операції та інші засоби, які спрямовані на підірвання національної безпеки та стабільності [71].

Сам термін "гібридна війна" не має єдиного визначення і може трактуватися різними спеціалістами по-різному. Його розуміння та вживання змінюється залежно від контексту та актуальних подій. Також важливо відзначити, що в західних наукових дослідженнях та дискусіях термін "гібридна війна" почав використовуватися приблизно з середини 2000-х років і може мати відмінні підходи та інтерпретації від тих, що використовуються сьогодні [71].

У 2010 році, представники науковців та службовців Міністерства оборони США визначили гібридну війну як "комбінацію державних і недержавних загроз, включаючи атаки з використанням комп'ютерних мереж, супутників,

переносних ракет класу "земля-повітря", саморобних вибухових пристроїв, маніпуляцій з інформацією та ЗМІ, а також залучення хімічної, біологічної, радіологічної та ядерної зброї" [132].

Сутність гібридної війни можна усвідомити через розуміння сучасного суспільства та його взаємозв'язків, а також у контексті системної кризи глобальної системи безпеки.

Гібридну війну можна розглядати як новий тип глобального протистояння, спрямований на досягнення політичних цілей агресії шляхом генерації внутрішніх конфліктів, а також захоплення стратегічних ресурсів держави-жертви. Цей тип конфлікту реалізується в різних сферах Основна мета гібридної війни полягає в захопленні частини стратегічних ресурсів держави-жертви під керівництвом агресора. При цьому еліта держави-жертви "добровільно" допомагає у передачі цих ресурсів. Такий підхід ускладнює визначення методів та засобів гібридної війни, що у свою чергу гальмує швидке та адекватне реагування на агресію [71].

Відповідно до означення Ф. Магди, гібридна війна представляє собою стратегічний підхід однієї держави з метою підкорення іншої держави, використовуючи політичні, економічні та інформаційні методи. У цьому контексті важливіше інформаційні операції та інші впливові засоби, а не прямі бойові дії. Головна ціль гібридної війни полягає в маніпулюванні свідомістю жителів держави-жертви, не обов'язково вдаючись до масового знищення, а скоріше до залякування та деморалізації. Роль швидкості поширення інформації в сучасному світі відчутно підвищилася, перетворивши її на важливий інструмент і, зараз же, навіть на зброю [62].

Відмінності між "традиційними" війнами та гібридними війнами полягають у незмінності наслідків останніх. Це пов'язано з тим, що процес трансформації вимагає зміни менталітету населення, яке втрачає свою основну мету і духовні цінності, замінюючи їх морально-психологічними ілюзіями та міфами, що створює додаткові труднощі для подолання наслідків гібридних конфліктів [71].

Згідно з висновками Ф. Хоффмана, гібридна війна охоплює наступні напрямки:

1. Географічний - включає у себе контроль над певною територією або усією територією супротивника, використовуючи розвідку та розвідувальні системи. Це також може включати підтримку сепаратистських рухів та провокування військово-політичних конфліктів в країнах противника.

2. Економічний - включає різноманітні методи, такі як намагання здобути кредити за невигідних умов, запровадження економічних санкцій та використання неефективних міжнародних економічних організацій.

3. Ідеологічний - використовує дезінформацію, спотворення інформації, зміну понять, введення ментальних вірусів та міфів у свідомість населення противника.

4. Інформаційний - передбачає організацію атак на комп'ютерні системи, використання шкідливих програм, інфільтрацію в комп'ютерні та телекомунікаційні системи, а також бази даних супротивника [37].

Український досвід ілюструє, що Росія продовжує вести гібридну війну на широкому спектрі напрямків, як зауважує Г. Почепцов. Вона включає не лише інформаційний компонент, але й економічну, репутаційну, смислову, та людську війну. Ця стратегія охоплює акторів різних сфер - від співаків та письменників до режисерів, які впливають на публіку. Військові дії в цьому контексті стають фоном для глибшої війни у свідомості людей.

Згідно з поглядами Захаренка К. В., гібридна війна має наступні аспекти:

1. Вона об'єднує як конвенційні, так і неконвенційні методи війни, та включає учасників, що не обмежуються лише військовими (наприклад, терористами, найманцями, бандформуваннями, спецпідрозділами тощо).

2. Початок гібридної війни асоціюється із застосуванням нетрадиційних методів бойових дій.

3. Головну роль в гібридній війні відіграє боротьба за інформаційний простір, а не лише військові операції. Ця битва за інформацію захоплює інтереси людей на всіх рівнях - індивідуальному, громадському і державному.

Цей негативний розвідувально-психологічний вплив є фундаментом для інших операцій, спрямованих на вплив на інтереси України на всіх рівнях - від індивідуального до державного. Війна у свідомості людей розгортається на декількох фронтах одночасно - серед жителів конфліктної зони, країни-жертви агресії, країни-агресора та міжнародної спільноти [32].

Політична ситуація в Україні мала значні наслідки у різних сферах, зокрема внутрішній, російській та міжнародній. Ще до початку конфлікту, Росія у своїй зовнішній політиці цілеспрямовано намагалася послабити авторитет України на міжнародній арені.

Це було досягнуто через формування спотвореного уявлення про українську владу в європейській спільноті, поширення неправдивої та спотвореної інформації про Україну, створення негативного іміджу Європи та спроби розмежування між "братніми державами". Все це мало на меті ускладнити інтеграцію України в європейські структури.

Гібридна війна, якій Україна зіткнулася, передбачала моніторинг ситуації та використання внутрішніх криз для досягнення своїх цілей. Ці кризи включали ослаблення та "нейтралізацію" центральної влади після зміни уряду, зростання протиріч між центром та регіонами, психологічний та матеріально-технічний незадовільний стан апарату безпеки України, конфлікти між різними службами безпеки та активну інформаційно-пропагандистську діяльність Росії в Криму.

Внутрішньополітичний вплив у гібридній війні реалізовувався через соціокультурну та гуманітарну сфери, включаючи боротьбу зі зміною ментальності стосовно історичної спадщини України, нівелювання українських культурних цінностей та створення проросійських настроїв у суспільстві. Кіберпростір став ключовою ареною для транскордонної інформаційної війни, де різноманітні "хактивісти", "кібервійська", "кіберполіція" та спецпідрозділи різних служб безпеки стали важливими елементами кібератак та психологічних операцій проти соціальних мереж та інтернету загалом.

Аналітики стверджують, що у 2014 році приблизно 90% телекомунікаційної інфраструктури України належали російським суб'єктам [37].

Сучасні технології інформаційно-психологічного впливу на свідомість людей включають широкий спектр засобів і методів.

До них належать:

1. Медіа та спеціальні інформаційно-пропагандистські засоби.
2. Глобальні комп'ютерні мережі для розповсюдження пропагандистських інформаційних матеріалів.
3. Програмне забезпечення для зміни інформаційного середовища та створення віртуальної реальності.
4. Засоби здійснення підсвідомого психологічного впливу, включаючи акустичні та електромагнітні поля.
5. Діяльність "фондів", "культурних об'єднань", "аналітичних центрів" з проросійською орієнтацією.
6. Пропагандистські медіа.
7. Вплив на внутрішню політику через підтримку політичних партій та окремих політиків.
8. Маніпуляції енергетичною залежністю та інвестування в українські компанії, зокрема медіа.
9. Спотворення інформації, заперечення існування етнічних українців як окремого народу.
10. Психологи відзначають, що негативний інформаційно-психологічний вплив може призвести до таких наслідків:
11. Зміни в психічному та емоційному здоров'ї людини, включаючи втрату адекватності у сприйнятті світу.
12. Зміна особистих цінностей, поглядів та позицій на життя, що може вплинути на поведінку.
13. Виникнення антисоціальної поведінки, що загрожує суспільству та державі.

Росія використовує свій досвід радянської школи безпеки для реалізації цих технологій в інформаційній війні проти України [71].

Різні дослідники називають такі засоби та методи впливу на інформаційно-психологічний фронт:

1. Медіа та спеціальні інструменти спрямування інформації та пропаганди.

2. Глобальні комп'ютерні мережі та програмне забезпечення для поширення пропагандистських матеріалів.

3. Методи незаконної модифікації інформаційного середовища, де приймаються рішення.

4. Засоби створення віртуальної реальності, поширення чуток та підсвідомого впливу.

Також, вказують на важливість таких методів як:

1. Пропаганда, напівправда, брехня, дезінформація та маніпуляція.

2. Диверсифікація громадської думки та психологічний та психотропний тиск.

3. Міфодизайн.

Ці методи спрямовані на досягнення різних цілей, включаючи підрив міжнародного іміджу України, дестабілізацію внутрішньої ситуації та формування стереотипів про народи та культури. Такий підхід використовується для досягнення політичних та геополітичних цілей в інформаційній війні [71].

Це призводить до заплутаності між категоріями інформаційного та психологічного впливу, включаючи їх форми, засоби, методи та навіть цілі.

Науковці визначають два типи механізмів інформаційного впливу: лінгвістичні та нелінгвістичні [114].

Лінгвістичні механізми базуються на свідомому сприйнятті інформаційного змісту, що є загальною закономірністю обробки інформації в соціальному середовищі.

Спочатку в індивідів формуються певні уявлення, світогляд, цінності та інтереси. Далі ці уявлення розвиваються в певному напрямку, що веде до

створення моральних та смислових фільтрів. Ці фільтри забезпечують аналіз та засвоєння нової інформації, сприяючи формуванню нових моделей поведінки відповідно до ситуації. Напрямок та стійкість цих фільтрів визначають кінцевий результат.

Ці фільтри зазнають впливу з боку ідеологічної пропаганди, релігії, філософських доктрин, освітніх систем, національних факторів та засобів масової інформації. Вони відіграють важливу роль у формуванні індивідуальної та колективної свідомості, впливаючи на сприйняття та інтерпретацію інформації в суспільстві.

Стійкий "фільтр", якість інформації, контекст та спроможність приймати рішення впливають на адекватність поведінки. Однак існують фактори вербального впливу, що змінюють механізми рішень та поведінки, включаючи цілеспрямовану дезінформацію, викривлення інформації та вибіркову неповну інформацію. Це може призвести до відхилення від адекватної поведінки, коли поведінка не відповідає реальній ситуації [5].

У експертних колах існує думка, що вплив спецслужб на підготовку гібридної війни розпочався ще у 2004 році, коли Україна демонструвала прагнення до активної участі у міжнародних відносинах, відмовляючись від другорядної ролі у російській зовнішній політиці. Відтоді російські спецслужби розпочали свою активність.

Вплив Росії на інформаційному фронті був спрямований на поширення проросійських та антиукраїнських ідей серед власних громадян та українців. Це включало підміну реальних подій симулякрами, розповсюдження напівправди та інші інформаційні методи, що мали на меті спотворення сприйняття ситуації та створення умов для реалізації власних цілей.

Пропаганда мала різні форми в залежності від етапу кампанії та цільової аудиторії. Наприклад, ще до 2014 року російське телебачення, яке транслювалося в Україні, виходили програми, що ставили під сумнів історичні факти, такі як походження Криму чи історія Київської Русі.

Під час військових подій використовувалися маніпулятивні прийоми, такі як анімаційний фільм "Врятуйте людей Донбасу", представлений як робота дітей, що втекли з Донбасу до Росії. Під час анексії Криму російські медіа активно використовували напівправду, поширюючи інформацію про приєднання українських силовиків до російських військ або про передачу військових об'єктів російським військам.

"Фейки", стали поширеним явищем у сучасній журналістиці. Вони представляють собою символи або терміни, які позначають неіснуючі в реальності об'єкти або події, є порожніми словами, позбавленими змісту. Згідно з думкою американського літературознавця Фредеріка Джеймісона, симулякр є "точною копією, для якої не існує оригіналу".

Прикладами симулякрів можуть бути вислови "фашисти в Києві", "жорстокості каральних батальйонів" та інші. Основною метою використання таких симулякрів є підміна об'єктивного сприйняття ситуації "фальшивими інформаційними втручаннями", які вигідні агресору.

Використання симулякрів передбачає комбінацію вербальних та невербальних механізмів впливу. Чим тонша психічна структура людини, тим більш вразливою вона є до впливу інформації, над якою вона не має повного контролю.

Використання спеціальних методів маніпуляції свідомістю людей, таких як звуки, кольори, запахи, зображення та інші інформаційні, енергетичні та психофізичні впливи, може мати деструктивний вплив на психіку.

Інформаційно-психологічний вплив посилюється традиційними адміністративними та силовими методами, що порушують інформаційні права та свободи. Прикладами таких методів є блокування діяльності медіа та обмеження доступу до різних ресурсів, а також блокування ресурсів, які могли активно спростовувати неправдиву інформацію на ранніх стадіях збройного конфлікту.

Традиційні методи пропаганди активно використовують різні медіа, включаючи пресу, радіо, телебачення, кінематограф та інтернет. Захист

інформаційного простору України почався не одразу після початку російської агресії, коли на українському телебаченні та радіо транслювалися антиукраїнські телесеріали, фільми та передачі.

Використання інформаційної зброї для впливу на широку аудиторію, включаючи міжнародну, передбачає існування мережі інституцій, які використовуються Російською Федерацією як засоби інформаційного впливу.

Важливо зазначити, що ситуацію з інформаційною безпекою відносно прав громадян України можна розділити на кілька категорій:

1. Інформаційна безпека громадян України, які проживають в Автономній Республіці Крим та на тимчасово окупованих територіях;

2. Інформаційна безпека військовослужбовців та інших осіб, які безпосередньо беруть участь у бойових діях, їхніх родин та мирного населення на території України, де ведуться бойові дії;

3. Інформаційна безпека громадян України, які проживають на територіях, що не входять до зони ведення бойових дій.

4. Інформаційна безпека громадян України, що вимушено покинули територію України через повномасштабну збройну агресію РФ [37].

Аналіз масштабної інформаційно-пропагандистської діяльності Росії під час анексії Криму виявляє різноманітні методи маніпулювання суспільною свідомістю.

Це включає інформаційну блокаду та створення інформаційного вакууму в українських медіа в Криму, що мало на меті подачу фактів у вигідному світлі для Кремля. Це також охоплює використання посередників, таких як "лідери думок", для впливу на громадську думку, а також застосування ефекту першості для оперативного формування бажаного бачення подій.

Крім цього, було застосовано такі методи, як переписування історії для руйнування історичної пам'яті, інсценування масових акцій на підтримку від'єднання Криму від України, а також використання емоційного резонансу та психологічного шоку для спровокування антиукраїнських та антиісламських

настроїв. Важливо відзначити, що ці методи спрямовані не стільки на ідеологічні установки, скільки на повсякденну свідомість громадян.

Інформаційно-психологічний вплив посилювався традиційними адміністративними та силовими методами, які порушували інформаційні права та свободи.

Наприклад, було використано блокування діяльності медіа та обмеження доступу до різних ресурсів, а також блокування ресурсів, які могли активно спростовувати неправдиву інформацію.

Традиційні методи пропаганди інтенсивно використовували різні медіа, зокрема пресу, радіо, телебачення та інтернет, для поширення своїх повідомлень.

Крім порушення свободи інформації, також порушуються права, що тісно пов'язані з цією свободою, включаючи право на освіту, свободу совісті, віросповідання або переконання, а також право на юридичну допомогу.

Особливо вразливими перед порушеннями є представники кримськотатарського народу, які зіткнулися з незаконними арештами та затриманнями, включенням дітей до збройних формувань, сексуальним насильством та іншими протиправними діями.

У контексті військового конфлікту проблеми порушення права на інформацію можуть виглядати менш актуальними, але без забезпечення свободи інформації неможливо гарантувати реалізацію більшості прав людини в сучасному суспільстві.

На території самопроголошених "ЛНР" і "ДНР" протягом 2014-2015 років було здійснено блокування доступу до українських і міжнародних медіа, а також припинено функціонування місцевих медіа, які підтримували проукраїнську позицію. Органи, відповідальні за контроль та моніторинг медіа, а також за припинення діяльності проукраїнських медіа, були підпорядковані "Міністерству інформації та зв'язку ДНР" і "Комітету інформації ЛНР".

Всі ці дії свідчать про цілеспрямовані спроби обмеження свободи інформації та маніпулювання громадською думкою з метою досягнення політичних цілей, що є порушенням основних прав і свобод людини.

У той же час, завдяки широкій військовій, матеріальній та розвідувальній підтримці з боку Росії, включаючи спеціалістів з інформаційних операцій та психології, була розгорнута система інформаційно-пропагандистської діяльності.

Ця система була спрямована на виправдання екстремістського насильства, легітимізацію дій сепаратистського "уряду", дегуманізацію образу українського народу (а також жителів Європи та США), дискредитацію української влади і деморалізацію української армії [43].

Свідомість населення на тимчасово окупованих територіях характеризується спостерігачами як "розчарована і травмована", що є типовим для зон збройних конфліктів. Інформаційне забезпечення цього населення обмежене через технічні та психологічні фактори.

Більшість медіа була зруйнована або конфіскована, а частина населення не готова сприймати інформацію з точки зору української держави. Люди обирають джерела інформації, які викликають у них психологічний комфорт, враховуючи родинні зв'язки та соціальні фактори, такі як гуманітарна допомога та наявність комунальної інфраструктури.

У контексті інформаційної діяльності спостерігаються такі явища, як приховування важливої інформації про ситуацію на певній території, занурення цінної інформації в потік "інформаційного сміття", трансформація змісту та підміна термінів. Використовуються технології, що передбачають застосування легко розпізнаваних термінів або таких, що не мають чіткого визначення, а також відволікання уваги від подій у даній сфері.

Наповнення інформаційного простору неправдивою інформацією є поширеним явищем. Все це призводить до дезінформації населення та ускладнює об'єктивне сприйняття ситуації, що є важливим аспектом у забезпеченні інформаційної безпеки на тимчасово окупованих територіях.

Інформаційна безпека надзвичайно важлива з урахуванням високої значущості інформаційно-психологічних впливів на учасників бойових дій, членів їх сімей та місцеве населення. Головним завданням є забезпечення захисту військ від впливу інформаційно-психологічних заходів противника, зменшення можливого ризику негативного впливу на органи військового управління, війська та населення, а також забезпечення ефективного управління військами (силами) та покращення їх морально-психологічного стану.

Основні завдання захисту військ (сил) від інформаційно-психологічного впливу противника охоплюють широкий спектр дій, спрямованих на забезпечення інформаційної безпеки та підтримку морально-психологічного стану особового складу.

Це включає розголошення важливих військово-політичних рішень державного керівництва та завдань частин (підрозділів) особовому складу, аналіз та передбачення розвідувальних обставин в зоні бойових дій та оцінка їх можливого впливу на війська (сили) і населення. Також важливим є збір та узагальнення інформації про об'єкти, які можуть бути джерелами негативного інформаційно-психологічного впливу противника.

Заходи щодо зменшення впливу розвідувально-психологічних заходів противника включають уникнення деморалізації чи дезінформації військ (сил) та покращення їх морально-психологічного стану. Організація інформаційних та психологічних заходів (акцій), спрямованих на війська та населення у районах бойових дій, є ключовим елементом у забезпеченні ефективного захисту.

Проведення профілактичних заходів з метою запобігання поширенню неправдивих чуток серед населення, недопущення паніки та незаконних дій, спрямованих на підрив морально-психологічного стану населення (військ), є важливою частиною стратегії захисту від інформаційно-психологічного впливу противника.

Надання якісної та своєчасної психологічної підтримки є ключовою складовою інформаційної безпеки, особливо для осіб, які перебувають у зоні

бойових дій, та після їхнього повернення. Важливо також забезпечити учасників бойових дій та їхні сім'ї необхідною інформаційною та правовою підтримкою. Національна інформаційна політика має враховувати різні особливості та впливи на різні групи населення в контексті інформаційно-психологічних аспектів. Морально-етичні аспекти діяльності медіа та громадських організацій також є важливими.

Варто зазначити, що рівень довіри до владних структур в Україні є нестабільним. Проте, довіра до медіа є вищою: українці найбільше довіряють центральним телеканалам (телемарафону), українським онлайн-медіа, соціальним мережам, місцевому телебаченню, пресі та місцевому радіо. Цікаво, що довіра до медіа залежить від соціальних характеристик аудиторії, таких як вік, місце проживання та регіон.

Наприклад, старші люди довіряють центральним телеканалам більше, ніж молодь до 35 років, а молодь довіряє українським інтернет-медіа та соціальним мережам.

Жителі сільської місцевості менше довіряють центральним телеканалам порівняно з мешканцями малих міст та селищ, а міські жителі більше схильні довіряти національним онлайн-медіа.

Таким чином, проведення профілактичних заходів для запобігання поширенню неправдивих чуток і підтримки морально-психологічного стану населення є критично важливими складовими стратегії інформаційної безпеки. Забезпечення якісної психологічної підтримки особам, які перебувають у зоні бойових дій, та їхнім сім'ям після повернення також має першочергове значення. Національна інформаційна політика повинна враховувати специфіку різних соціальних груп і забезпечувати етичні стандарти діяльності медіа та громадських організацій. Враховуючи нестабільний рівень довіри до владних структур, особливу увагу слід приділити ролі медіа, які користуються більшою довірою серед населення. Залучення різних каналів комунікації з урахуванням соціальних характеристик аудиторії дозволить ефективніше протидіяти

інформаційно-психологічним впливам та забезпечувати інформаційну безпеку в умовах сучасних викликів.

ВИСНОВКИ ДО РОЗДІЛУ 1

Проведений теоретико-методологічний аналіз ролі інформаційної безпеки у забезпеченні суспільно-політичної стабільності, зокрема через неоінституційний підхід, дозволив визначити, що стабільність суспільно-політичної системи залежить від ефективної взаємодії між різними суб'єктами в контексті інформаційного простору. Визначено, що інформаційна безпека є важливим компонентом цієї стабільності, оскільки вона забезпечує захист суспільства від інформаційних загроз, сприяє збереженню цілісності держави та підтримує її здатність до реагування на виклики.

Представлено методи дослідження інформаційних загроз та механізмів їх нейтралізації. Зокрема, було розглянуто аналітичні та порівняльні методи, що дозволяють здійснювати глибокий аналіз діяльності інституцій, залучених до забезпечення інформаційної безпеки. Виявлено необхідність застосування комплексного підходу до оцінки ефективності існуючих інструментів інформаційної безпеки, що включає правові, технічні, соціальні та економічні аспекти.

Проведено аналіз взаємозв'язку між глобалізаційними процесами, стрімким розвитком інформаційних технологій та забезпеченням інформаційної безпеки. Встановлено, що зростання міжнародної напруженості та активізація гібридних війн вимагають нових підходів до захисту інформаційного простору. Це включає розробку та впровадження інноваційних стратегій, спрямованих на протидію інформаційним загрозам, а також підвищення рівня координації між національними та міжнародними організаціями.

Було досліджено політологічні та міждисциплінарні аспекти розуміння сутності інформаційної безпеки. Розкрито сутність інформаційної безпеки як багатогранного феномена, що охоплює технічні, соціальні, політичні, правові та

культурні аспекти. Виявлено, що інформаційна безпека має ключове значення для забезпечення стабільності як на рівні індивіда, так і на рівні суспільства в цілому. Це включає захист від кіберзагроз, боротьбу з дезінформацією та підтримку інформаційної стійкості суспільства.

Підкреслено важливість інтеграції знань з різних наук для досягнення комплексного розуміння феномена інформаційної безпеки. Інформаційна безпека повинна розглядатися в контексті політичних наук, філософії, соціології, права та інформаційних технологій, що дозволяє забезпечити більш цілісний підхід до її аналізу та впровадження ефективних заходів захисту.

РОЗДІЛ 2. СУСПІЛЬНО-ПОЛІТИЧНА СТАБІЛЬНІСТЬ ЯК ОСНОВА НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ БЕЗПЕКИ: ІНФОРМАЦІЙНІ ВИКЛИКИ СУЧАСНОСТІ

2.1 Чинники та критерії суспільно-політичної стабільності: роль інформаційного компоненту

В умовах інтенсивної суспільної трансформації, що охоплює процес реформування, роль політичної стабільності набуває ключового значення для успішної реалізації задекларованих змін у всіх сферах суспільного функціонування.

З одного боку, розробляється теоретико-методологічний підхід для оцінки актуального стану політичної системи, з особливим акцентом на її стабільності. З іншого боку, здійснюється аналіз науково-практичних аспектів, пов'язаних з функціонуванням політичної системи, включаючи її основні компоненти та взаємодію з різними соціальними групами та інститутами.

Набувають значення дослідження, присвячені науково-практичним питанням, що стосуються визначення детермінант та факторів політичної стабільності, а також природи та показників цієї стабільності. Попри розповсюджене використання термінів "стабільність", "суспільна стабільність" та "політична стабільність" у наукових дослідженнях і публікаціях, їх точне тлумачення продовжує залишатися предметом наукового дискурсу.

Враховуючи важливість встановлення єдиного понятійного апарату та наявність різноманітних інтерпретацій, слід звернути увагу на те, що запропоноване визначення політичної стабільності не враховує її властивої динаміки та не вказує на об'єктивні та суб'єктивні умови і чинники, що визначають стабільність, а отже, необхідно більш глибоко розглядання зміст і структуру цього поняття.

У сучасному науковому дискурсі термін «стабільність» (від лат. stabilis - міцний, постійний) в основному розуміється як тривалий період розвитку,

протягом якого елемент може функціонувати без обмежень або порушень. Стабільність виявляється в різних сферах суспільного життя і характеризує ефективність функціонування і життєдіяльності. У соціальних і гуманітарних науках стабільність зазвичай розглядається в контексті конкретних секторів суспільства, таких як економіка, політика і культура, а не як абстрактне поняття [77].

Аналізуючи поняття "стабільності" з теоретичного аспекту, можна виявити його взаємозв'язки з такими суміжними категоріями, як "сталість" і "стійкість", які відображають специфічні процеси, що відбуваються у різних сферах суспільного життя. "Сталість" характеризує стан об'єкта, який залишається незмінним протягом певного періоду часу та простору. З іншого боку, "стабільність" позначає здатність системи зберігати зміни певних параметрів у межах, що вже визначені, і відновлювати порушену рівновагу.

Важливо підкреслити, що саме поняття "стабільності" не імплікує конкретну якість процесу або стану, тоді як "сталість" може вказувати на наявність деструктивних чи генеруючих процесів.

"Сталість" не обов'язково передбачає постійність, але може включати її як частковий випадок, зазвичай вказуючи на постійність та передбачуваність змін, що робить це поняття схожим на "стабільність". Однак слід зазначити, що ці категорії не є тотожними.

"Стабільність" є більш складним поняттям, яке вимагає комплексного аналізу характеру взаємодії та можливих наслідків між різноманітними взаємопов'язаними та взаємозалежними чинниками у процесі розвитку суспільства та держави.

Система, яка надає значні можливості, може виступати не тільки як опора для забезпечення стабільності, але й як стимул для необхідних змін. Співвідношення між стабільністю та змінами є важливим показником ефективності політичної системи. Категорія "стабільність" доречно використовується для характеристики важких систем, які зберігають свою ідентичність та функціонують в умовах відносної нестабільності.

Стабільність завжди пов'язана з внутрішньою логікою еволюції системи, структурою і порядком взаємодії її компонентів, їх взаємодією, параметрами та напрямками контрольованих змін. Ці зміни відбуваються відповідно до властивостей (законів) даної системи, тобто вони є "вродженими" для неї. Вони практично не піддаються впливу зовнішніх збурень або впливів. Іншими словами, поняття "стабільність" можна використовувати для опису процесів та явищ, які відображають лінійні та випадкові зміни властивостей, закономірностей причинно-наслідкових зв'язків. Це також стосується політичної стабільності. Політична система втрачає стабільність, коли в процесі свого функціонування вона порушує межі своєї ідентичності, тобто вступає в конфлікт з власною сутністю.

Політична стабільність є одним з аспектів соціальної стабільності і відображає стан взаємозалежності між соціальними групами та політичними силами, при якому жодна з них не може суттєво змінити політичну систему на свою користь, забезпечуючи тим самим збереження статус-кво.

Цей баланс формується та підтримується через складний механізм вертикальних (внутрішніх) і горизонтальних (зовнішніх) зв'язків всередині політичної системи. Вертикальні зв'язки відносяться до балансу між компонентами політичної системи та взаємодії між її інститутами, тоді як горизонтальні зв'язки стосуються взаємодії політичної системи в цілому з іншими системами суспільства [46].

Нестабільність політичної системи характеризується непередбаченими та небажаними наслідками її функціонування. Оцінка стабільності або нестабільності зумовлюється доступністю відповідної інформації, а також світоглядними та політичними позиціями учасників політичного процесу та суб'єктів політичної діяльності. Це підкреслює важливість розроблення конкретних методів (індикаторів) для об'єктивної оцінки стану політичної системи та її стабільності.

Проте, при цьому необхідно враховувати щонайменше три аспекти.

Перший - системний, який охоплює загальні та складні еволюційні закономірності та тенденції розвитку політичної сфери суспільства та процесів, що відбуваються в ній протягом певного історичного періоду.

Другий - когнітивний, який базується на наявності функціонального суб'єкта (або декількох суб'єктів), які володіють необхідною, своєчасною та достатньою інформацією про події, явища та процеси, що відбуваються на різних рівнях політичного управління.

Третій - функціональний, який передбачає планування та програмування діяльності суб'єктів політичного процесу з урахуванням можливих і реальних наслідків політичної діяльності [119].

Основним елементом політичної системи є політична діяльність, яка має свої специфічні характеристики та суттєві особливості. Так, суб’єкти політичної діяльності (органи влади, політичні партії, рухи, організації тощо) служить для досягнення конкретної суспільної мети [119].

Політичні системи, що здатні інтегрувати різноманітні інтереси, сприяти співпраці та досягненню згоди, координувати групову та суспільно-політичну діяльність, можуть бути віднесені до категорії стабільних політичних систем.

Одним з підходів до розуміння політичної стабільності є розгляд її як якісної характеристики політичної системи. Це означає, що політична стабільність визначається здатністю політичної системи до збереження балансу і уникнення суттєвих змін, конфліктів і кризових ситуацій [77].

Процес встановлення та підтримки політичної стабільності пов'язаний з ефективною основою функціонування політичної системи. Це може включати наявність легітимності політичних інституцій, забезпечення правової держави, функціонування механізмів врегулювання конфліктів та забезпечення соціально-економічної стабільності. Розуміння політичної стабільності може розрізнятись залежно від контексту та дослідницького підходу.

Для більш повного розуміння цього явища важливо проводити дослідження з використанням різних теоретичних рамок, аналізувати його основні аспекти і взаємозв'язки з іншими соціальними процесами [77].

Політична стабільність є динамічним феноменом, який виникає під впливом змін у політичній системі, викликів, що виникають, і реакції системи на них. Вона може бути піддається коливанням та змінам у залежності від ситуації.

Політична стабільність виникає в результаті функціонування політичної системи держави. Це означає, що сама політична система має забезпечувати стабільність у своїй роботі і функціонуванні. Одним із головних завдань політичної стабільності є забезпечення порядку, який виявляється у ефективності влади, легітимності її дій і збереженні норм та цінностей політичної культури [77].

Важливим чинником впливу на політичну стабільність є широка підтримка політичної влади у суспільстві. Ця підтримка залежить від стабільних позитивних думок і суджень, які свідчать про суспільне затвердження дій влади. Суспільна підтримка сприяє запобіганню конфліктам, свідчить про національну єдність і є показником ефективності політичної системи.

Механізми запобігання загрозам суспільно-політичній стабільності в рамках інформаційного суспільства представляють собою систему інститутів держави та громадянського суспільства, які функціонально об'єднані з метою використання сил і засобів системи забезпечення національної безпеки для впливу на причини виникнення загроз суспільно-політичній стабільності та умови, що сприяють їх виникненню і реалізації [77].

Виходячи з робіт С. Ліпсета, можна виділити два основних типи стабільності - демократичну і автократичну (недемократичну). В рамках цих типів можуть існувати підтипи, такі як стабільна/нестабільна демократія та стабільна/нестабільна диктатура [59].

Мінімальна політична стабільність відображає лише відсутність громадянської війни або збройних конфліктів в державі. Ця форма стабільності може бути досягнута за допомогою авторитарних методів управління. З іншого боку, демократична стабільність базується на здатності демократичних структур

швидко реагувати на зміни в народних настроях з метою забезпечення миру та громадянської злагоди.

Це передбачає ефективну роботу демократичних інституцій і процесів для забезпечення стабільності [77].

Крім того, політична стабільність може мати і внутрішні та зовнішні аспекти. Внутрішній елемент стосується параметрів самої системи, таких як стабільність суспільного життя, структура політичної системи і відсутність внутрішньополітичних конфліктів.

Зовнішній елемент охоплює відсутність зовнішніх політичних конфліктів і напруженості, а також різні політичні елементи, пов'язані з міжнародною безпекою, роззброєнням, мирним співіснуванням і стабілізацією міжнародних відносин [77].

Політична діяльність є важливою складовою владних відносин і їх функціонування. Підтримка влади може бути надана або відкликана широкими верствами суспільства та різними групами громадянського суспільства. Вона може бути "ситуаційною", базуючись на оцінці суспільством дій державних інститутів, політичного курсу країни, публічних заяв, конкретних політичних дій та особистих якостей політичних лідерів.

Також існує "екстенсивна" підтримка, яка стосується відносин між суспільством та державою і включає позитивні оцінки, які допомагають суспільству сприймати та підтримувати дії владних структур. Така підтримка має стійкість в часі, пов'язана з процесом соціалізації та набуттям політичного досвіду, а також дозволяє оцінити політичну систему в цілому.

Ключовим елементом для такої підтримки є суспільна довіра до політичних інститутів, яка виникає з задоволення різними групами населення діяльністю владних структур у прийнятті рішень, які відповідають їхнім соціальним інтересам. Підтримка політичної системи походить від двох джерел: еліт та народу. Основним фактором підтримки еліт є рівень соціально-економічного розвитку, який визначає ступінь розподілу ресурсів між різними групами населення.

Підтримка населення включає у себе прийняття більшістю цінностей, на яких базується дана політична система соціальних і політичних норм (наприклад, свобода слова, плюралізм думок, незалежність медіа) і які визначають поведінку політичних лідерів і державних структур.

Основними умовами для народної підтримки влади є довгостроковий і стійкий характер демократичних змін у суспільстві, ступінь участі держави в економічному управлінні, соціальна захищеність громадян, національна рівність, стале покращення рівня життя для різних груп населення та забезпечення реальної безпеки громадян.

Дослідження демонструють, що в авторитарному суспільстві акцент робиться більше на особистості політичного лідера, зокрема глави держави, аніж на політичних програмах чи партіях. Це спричиняє те, що критика останніх сприймається як критика не лише окремих політичних суб'єктів, а й загалом політичної системи, тоді як зміцнення одноосібної влади залишається практично невідчутним у суспільному дискурсі.

Ефективність діяльності політичних інститутів у значній мірі залежить від привабливості та харизми особистостей, які асоціюються з цими інститутами. Для широкого кола громадськості, незалежно від ступеня її участі у політиці, взаємодія з політичними лідерами або їхнім оточенням завжди має ключове значення.

Ця взаємодія сприяє почуттю стабільності, особливо в умовах швидких змін. Подальша соціальна стабільність підтримується через соціальні зв'язки, що формуються між громадянами та політичними лідерами, які часто орієнтовані на підтримку конкретних лідерів. Використання незаконних засобів для захисту корпоративних інтересів становить загрозу не тільки для політичної системи, але й для цілісності суспільства. Особливо небезпечним є потенціал громадянської війни та інших масштабних актів насильства між прихильниками та опонентами політичного режиму.

Сучасна історія містить немало прикладів державних переворотів, багато з яких відбулися у кризових моментах політичних систем або в умовах

тоталітарних режимів, де відсутні чіткі механізми легітимної зміни лідерів або вони діяли неефективно. Після такого «перевороту», призначення нового лідера зазвичай призводить до певної стабілізації політичної системи, проте ця стабільність залишається тимчасовою, якщо основні суперечності, які спричинили політичну боротьбу, залишаються невирішеними.

Нестабільність політичної системи розглядається як наслідок дій влади, яка зосереджує свою увагу лише на власних корпоративних інтересах та ігнорує потреби суспільства.

В такому випадку влада може підтримувати себе лише шляхом застосування насильства та репресій, а це вступає у протиріччя з об'єктивними потребами та природою суспільства [113].

Це веде до скупчення соціального невдоволення та зростання політичної напруженості. Конфлікт у політичній системі може виконувати різні ролі: його поява може свідчити про існуючі проблеми та загострення протиріч, однак у разі наявності в політичній системі механізмів інституційного регулювання, локалізації та розв'язання конфліктів, сам конфлікт не обов'язково призводить до значної дестабілізації цієї системи.

Наприклад, етнічні конфлікти, які базуються на виникненні соціальної дискримінації між етнічними групами, нерівному доступі до влади та ресурсів, правовій та культурній дискримінації, поширенні ксенофобії та негативних етнічних стереотипів, можуть набувати гострих форм і тривати протягом невизначеного часу, загрожуючи стабільності політичної системи суспільства.

Тому необхідність реальних механізмів виявлення, попередження та ефективного врегулювання конфліктів є важливою умовою ефективного функціонування політичної системи і служить індикатором її стійкості.

Відкрита політична система, як інститут, піддається впливам як ззовні, так і зсередини. Ключовим показником стабільності політичної системи є її здатність зменшувати негативні зовнішні чинники, серед яких можна виділити діяльність спеціальних служб і організацій, економічну блокаду, політичний тиск, збройну агресію тощо.

Вчасна та адекватна реакція на ці чинники (впливи) забезпечує захист національних інтересів держави та створює сприятливе оточення для їх втілення [113].

Необхідно зазначити, що негативний вплив на політичну систему в основному є наслідком загальних викликів та невирішених питань, проте цілеспрямована деструктивна діяльність слугує каталізатором дестабілізації політичної системи. Водночас, зовнішні впливи можуть призводити до позитивних результатів для політичної системи у випадку, якщо зовнішня політика держави узгоджується з інтересами глобального суспільства.

Політичні інститути, які діють відповідно до реальних потреб розвитку глобального суспільства, сприяють більш ефективному функціонуванню політичних систем та подальшому зміцненню політичної стабільності, що в свою чергу впливає на глобальну безпеку.

Ефективні суспільні зміни значною мірою залежать від рівня політичної стабільності в державі. Незважаючи на значущість для державної політики, науковцями досі не було приділено достатньо уваги розгляду питання класифікації політичної стабільності.

По-перше, наукова класифікація політичної стабільності є основою для конкретних досліджень її об'єктів, типів та станів в умовах сучасного суспільного розвитку, а також для прогнозування їх тенденцій.

По-друге, така класифікація дозволяє відповідним державним та політичним інститутам на різних рівнях впливати на ключові аспекти суспільного життя та сприяє розробці механізмів усунення соціальних загроз.

По-третє, така класифікація сприяє підвищенню ефективності державної політики на всіх рівнях, від місцевого до глобального. Існує кілька факторів, які визначають політичну стабільність.

Враховуючи складність і специфіку цього питання, можна запропонувати таку класифікацію: політичну стабільність, що базується на сфері впливу, можна розділити на внутрішню та зовнішню. Внутрішня сфера становить передумову для успішної реалізації реформ, спрямованих на якісну

трансформацію суспільства, досягнення внутрішнього спокою та згоди, реалізацію політики соціального упорядкування, суспільного процвітання тощо.

Досягнення політичної стабільності в українському суспільстві означає послаблення рівня поляризації суспільства, політичної напруженості між різними суспільними групами та політичними партіями, які відповідають за представництво їхніх інтересів. Відповідно, зниження напруженості та досягнення суспільної згоди на основі компромісу може створити стійкі умови для поступової трансформації українського суспільства.

Політична стабільність на практиці визначається вибором між демократичними і авторитарними методами управління. Демократична стабільність ґрунтується на гуманістичних цінностях, відсутності соціальних дисонансів та створенні сприятливих умов для розвитку демократії. Вона підтримується принципами багатосторонньої співпраці, поваги до прав особи та відмови від застосування військової сили для вирішення внутрішніх конфліктів.

Авторитарна стабільність, навпаки, встановлюється через домінування політичних і військових сил, порушення народного суверенітету та придушення громадянських прав. У міжнародних відносинах вона передбачає підпорядкування однієї держави іншій через політичний, економічний та військовий вплив. Класифікація політичної стабільності на високу, середню та низьку залежить від рівня довіри суспільства до влади, демократизації політичної сфери та ефективності системи соціального захисту.

Різні рівні політичної стабільності характеризуються певними ознаками та характеристиками.

Високий рівень політичної стабільності проявляється у згуртованості населення і політичного керівництва навколо державних інтересів, підтримці внутрішньої та зовнішньої політики держави, а також у підтримці глибоких демократичних змін.

Середній рівень політичної стабільності характеризується розповсюдженням демократизаційних процесів, наявністю конфліктів та суперечностей, але з загальною підтримкою населення.

Низький рівень політичної стабільності спостерігається у разі загострення соціальних протиріч, які впливають на різні регіони країни, і можуть призвести до дестабілізації політичної ситуації.

Політичну стабільність можна класифікувати за масштабом на регіональний, національний та глобальний рівні, кожен з яких має свої особливості та характеристики.

Регіональна стабільність проявляється через взаємодію обмеженої кількості адміністративних одиниць, які мають спільні адміністративні кордони, та між якими відсутні серйозні внутрішні конфлікти.

У випадку регіональної стабільності "зона безпеки" розширюється на рівень регіону, тобто відбувається взаємодія між декількома територіальними одиницями, що утримують спільний статус стабільності.

Національна політична стабільність охоплює всю територію України і відображає постійний розвиток політичної ситуації у всіх її регіонах. Кожен регіон вносить свій внесок у загальну політичну стабільність.

Глобальна політична стабільність поширюється на міжнаціональний простір і характеризується відсутністю міжнародних конфліктів, що мають системний характер. Глобальна політична стабільність вимагає спільних зусиль усього людства для запобігання конфліктам, які можуть спричинити катастрофу для людської цивілізації. У класифікації політичної стабільності важливі два фактори: внутрішній і зовнішній.

Внутрішній фактор відображає стан внутрішніх відносин у суспільстві, зокрема між громадянами, політичними партіями, державними інститутами тощо. Зовнішній фактор враховує взаємодію держав на міжнародній арені, співпрацю, вирішення міжнародних конфліктів.

Додаткові фактори, які впливають на стабільність держави, включають громадянський консенсус та ідеологічну єдність. Громадянський консенсус відображає згоду між суб'єктами політичного процесу щодо ключових питань суспільного розвитку, що сприяє забезпеченню політичної стабільності.

Ідеологічна єдність характеризується наявністю спільних цінностей і переконань серед політичних акторів, що забезпечує основу для узгоджених дій і зміцнення державності.

Політичні партії відіграють важливу роль у формуванні ідеологічної єдності, оскільки вони артикулюють інтереси різних соціальних груп і забезпечують їх представництво в державних інститутах. Виконання передвиборчих програм та зобов'язань політичними партіями сприяє зміцненню довіри громадян до політичної системи.

Конструктивна політична боротьба в демократичних країнах не призводить до соціальної нестабільності, а навпаки, забезпечує адаптацію влади до нових викликів суспільства та сприяє розвитку політичної культури. Регулятивні умови, такі як дотримання законодавства, забезпечення прав і свобод громадян, відкритий доступ до інформації та прозорість виборчих процесів, відіграють ключову роль у підтримці політичної стабільності та зміцненні демократичних інститутів.

Правові рамки політичної стабільності передбачають узгодженість між населенням та політичними силами щодо легітимності Конституції та конституційного ладу, а також включають нормативно-правові акти, які регламентують поведінку учасників політичного процесу.

Важливим аспектом є встановлення законодавчих меж для методів та засобів політичної боротьби, що запобігає її ескалації та забезпечує прозорість та справедливість виборчих процесів. Державні інститути зобов'язані створювати умови для рівної конкуренції, запобігати маніпуляціям громадською думкою та забезпечувати розподіл влади на основі демократичних принципів. Ефективність цих заходів залежить від механізмів контролю за дотриманням законодавства та відповідальністю політичних суб'єктів.

Законодавче обмеження використання державних силових структур та адміністративних ресурсів у політичних цілях є критичним для збереження демократії та запобігання авторитаризму. Моральні норми, такі як чесність та

відповідальність, відіграють важливу роль у регулюванні політичних відносин та сприяють національній злагоді.

На міжнародному рівні політична стабільність підкріплюється міжнародними договорами та стандартами, які сприяють мирному вирішенню конфліктів та співпраці між державами. Їх втілення в національне законодавство є ключовим для забезпечення зовнішньополітичної стабільності.

Важливим аспектом міжнародного права є заборона застосування навколишнього середовища як засобу ведення війни, що поширюється також на космічний простір. Конвенція, укладена в Женеві в 1977 році, засуджує використання технологій та методів, які можуть призвести до зміни природних характеристик Землі або космосу, спрямовані на порушення екологічної рівноваги.

Пропонована класифікація політичної стабільності охоплює широкий спектр аспектів та вимагає подальшого уточнення окремих елементів. Однак, вона надає можливість виявити ключові проблеми та визначити ефективні стратегії для забезпечення стабільності на різних рівнях політичної системи. Підтримка суспільством політичної системи є фундаментальною умовою для забезпечення державної стабільності. Відношення різних соціальних груп до політичних інститутів і процесів відображається в рівні підтримки чи опозиції до державних структур. Широка суспільна підтримка сприяє зміцненню політичної системи, а її оцінка може бути здійснена за допомогою соціологічних опитувань, що досліджують громадську думку щодо рішень та дій урядових органів.

Політична підтримка, що вважається ключовим фактором стабільності політичної системи, може виражатися як з боку мас населення, так і з боку політичної еліти.

Однак, надмірне протиставлення цих двох видів підтримки не є продуктивним. У демократичних суспільствах необхідно досягти балансу між ними, тоді як в авторитарних суспільствах основна увага зосереджується на зміцненні політичних еліт. Значення політичної підтримки зростає в періоди

реформ, коли суспільство і його політична система знаходяться в стані переходу. Це може призвести до тимчасової незбалансованості та нестабільності.

Такі ситуації викликають розбіжності між новими цінностями, які впроваджуються владою, і традиційними цінностями, які мають глибоке коріння в масовій свідомості.

Посилення цього протиріччя та затримка у прийнятті важливих політичних рішень можуть призвести до зростання напруженості та конфлікту між населенням та владою. Підтримка політичної системи з боку еліти є динамічним процесом, який залежить від змін у соціально-економічному контексті. Різні елітні групи можуть зазнати змін у своєму статусі внаслідок реформ, що може вплинути на їхню підтримку влади. Ослаблення підтримки з боку певних елітних груп може призвести до загального ослаблення політичної еліти та внутрішніх конфліктів.

Аспект народної підтримки політичної системи набуває особливої значущості в умовах суспільної трансформації України. Зростання інтересу до політичного процесу, особливо до виборчої активності, свідчить про зміну ставлення громадян до важливості своєї участі у формуванні влади та задоволенні своїх потреб.

Підтримка політичної системи з боку населення залежить від економічних та політичних чинників, з яких економічні часто мають вирішальне значення. Імідж влади, її цілі та можливість критичного аналізу її дій впливають на ступінь підтримки. Соціологічні та політологічні дослідження підтверджують роль ідеологічних мотивів у масовій підтримці.

Зростаюча критичність громадян свідчить про їхній політичний досвід та готовність активно захищати свої інтереси. У контексті інформаційного суспільства з'являються нові виклики для політичної стабільності, зумовлені величезним обсягом інформації та необхідністю адаптації до глобальної невизначеності.

Сучасні дослідження акцентують на двох основних типах впливу влади в інформаційному суспільстві: "жорсткому" та "м'якому". Перший пов'язаний з примусом, другий – з формуванням цінностей та наративів. Інформаційна епоха, яка характеризується переходом від індустріального до постіндустріального суспільства, вимагає нових підходів до забезпечення політичної стабільності та розуміння змін у характері діяльності, де інтелектуальна праця набуває домінуючого значення. В епоху інформаційного суспільства відбувається трансформація владних відносин, зумовлена динамікою соціальних процесів. Одним із визначальних чинників цих змін є криза держави як суверенного суб'єкта, що може призвести до перегляду традиційних форм політичної демократії.

Інформаційне суспільство характеризується напруженим станом між матеріальними силами обробки абстрактної інформації та державою, орієнтованою на утримання структур влади. Це призводить до того, що держава не може ефективно виконувати свої адміністративні функції, а старі етичні норми стають непродуктивними у нову епоху.

У інформаційному суспільстві влада не зникає, але інтегрується на фундаментальному рівні в культурні норми, що визначають спосіб сприйняття життя та прийняття рішень індивідами та організаціями, включаючи політичні. Влада стає реальною, але нематеріальною, дозволяючи окремим особам та організаціям нав'язувати свої рішення незалежно від думки інших, а також класифікувати життєвий досвід на категорії, які відповідають певній поведінці.

В епоху інформаційного суспільства боротьба за владу перетворюється на культурну боротьбу, яка відбувається переважно через медіа. Медіа використовуються як інструменти для передачі та маніпулювання ідеями та цінностями, впливаючи на ставлення соціальних акторів та інституцій. Комунікаційна революція, спричинена розвитком технологій зв'язку та інформаційних систем, зіграла значну роль у цьому процесі. Глобальна інформаційна мережа, особливо Інтернет, дозволила інформації досягати глобальної аудиторії, посилюючи вплив інформаційної влади.

Розвиток передових методів і технологій впливу на свідомість і поведінку людей став можливим завдяки прогресу в сфері інформаційно-комунікаційних технологій (ІКТ). Сучасні політичні стратегії включають використання різноманітних засобів маніпулювання свідомістю, від впливу на підсвідомість до створення штучної реальності за допомогою комп'ютерних технологій.

Порушення традиційних методів комунікації через технологічний розвиток зробило соціальні відносини більш вразливими до політичного впливу. Ці зміни призвели до підвищення ролі інформаційної влади, формуючи домінуючу парадигму контролю над суспільними процесами. Зростання глобальної інформаційної влади відображає зміну у способі ведення політичної боротьби та впливу на суспільство, що вимагає нових підходів до розуміння владних відносин у сучасному інформаційному світі.

Протягом багатьох століть повсякденне спілкування відігравало ключову роль як основне джерело інформації, формування думок та оцінок, а також для взаємодії в колективі. Проте, процеси індустріалізації та урбанізації суспільства призвели до руйнування традиційних зв'язків та спільних цінностей.

Це спричинило швидке поширення індивідуалізму та розпад громад на окремі одиниці. На сьогодні більшість людей отримує інформацію переважно через електронні медіа, що встановило прямий зв'язок між медіа та політичною поведінкою громадян.

У розвинених країнах Заходу спостерігаються нові соціальні розриви. З одного боку, існує група людей, які досягли високого рівня матеріального благополуччя та віддають перевагу духовному та інтелектуальному розвитку. Цю групу часто називають постматеріалістами. З іншого боку, існує сегмент населення, орієнтований на задоволення матеріальних потреб, який працює в масовому виробництві. Ці дві групи стають все більше відділеними одна від одної, утворюючи два протилежних класи.

Перший клас охоплює тих, хто має доступ до знань та інформації, тоді як другий клас представляє робітничий клас, зайнятий у виробництві споживчих товарів. У сучасному виробництві знання та інформація стали основними

ресурсами, що робить висококваліфікованих фахівців більш значущими для підприємців, ніж робітники для своїх капіталістичних роботодавців. Це може призвести до перерозподілу суспільних благ на користь тих, хто працює у сфері інформації.

Сучасний високотехнологічний світ характеризується високою матеріальною нерівністю, яка не зумовлена політичними та економічними факторами, а має свої корені в інтелектуальних здібностях людей. Це ставить перед суспільством важливі питання щодо створення стабільного світового порядку, який може стримати деструктивні тенденції. Одним з можливих рішень може бути співпраця між країнами з метою створення постекономічного порядку.

У сучасному світі, де можливості виробництва матеріальних благ значні, суспільство має шанс зосередитися на розвитку інших аспектів життя. Проте, існує ризик знецінення праці та виробництва через надмірний акцент на споживання та матеріальне благополуччя. Це може призвести до ситуації, коли значення праці та виробництва визнається лише в кризових моментах.

Важливість інформаційного впливу стає ключовим аспектом у демократичних процесах. Громадяни повинні бути добре інформовані та здатні активно брати участь у політичному житті. Інституції, такі як освітні заклади та медіа, відіграють критичну роль у забезпеченні доступу до якісної інформації та розширенні знань громадян.

У контексті інформаційної ери, доступ до надійної, об'єктивної та різноманітної інформації є фундаментальним для забезпечення здатності громадян приймати обґрунтовані політичні рішення та підтримувати стабільність демократичних систем.

Однією з актуальних проблем для сучасної демократії є монополізація владних ресурсів або медіакратія, що полягає в надмірному впливі певних медійних структур або інформаційних платформ на формування громадської думки, політичні переконання та прийняття рішень. Цей дисбаланс може призвести до політичних маніпуляцій та загрози демократичним процесам.

Політична маніпуляція може розумітися як дії, що суперечать публічно оголошеним цілям або застосовують недемократичні методи для досягнення політичних цілей, такі як виборчі маніпуляції та нерівномірний розподіл ресурсів. Вузьке розуміння полягає в контролі над поглядами та поведінкою людей, що суперечить їхнім власним інтересам.

Медіакратія може використовуватися як інструмент політичної маніпуляції, оскільки контроль над потоком інформації дозволяє впливати на сприйняття подій, політичні погляди та рішення громадян. Це може призвести до порушення балансу в політичних процесах і вплинути на демократичні процедури.

Для запобігання таким ситуаціям необхідно забезпечити різноманітність інформаційних джерел, підтримувати незалежність медіа, сприяти розвитку критичного мислення та медіаграмотності серед громадян. Це допоможе громадянам розрізняти об'єктивну інформацію від маніпулятивної та здійснювати свідомий вибір на підставі аргументів, а не спрямованого інформаційного впливу.

С. О. Терепищий у своїх наукових працях акцентує увагу на значенні медіаграмотності для інформаційної безпеки та формування критичного мислення, особливо в умовах воєнного стану, коли суспільство стикається з інтенсивними інформаційними атаками [116].

У контексті інформаційного суспільства спостерігається значне поширення політичних маніпуляцій, що включають у себе систематичне поширення соціальних міфів, змістовне спотворення фактів, розповсюдження недостовірної інформації, обман та дискредитацію. Коли такі маніпулятивні практики домінують у діяльності політичних та інформаційних інститутів, відбувається приховане перетворення політичної системи з демократичної до тоталітарної форми, що називається інформаційним тоталітаризмом.

Ця нова форма політичної та соціальної влади може базуватися на споживацькому та індивідуалістичному світогляді, який є несумісним з ідеалами демократії. Інформаційно-комунікаційна революція надала

можливості для цифрового контролю над життям, думками, намірами та психологічними станами індивідів та організацій.

Демократичний процес, зведений до формальних процедур, не лише не перешкоджає впровадженню нових форм інформаційного впливу, але й фактично сприяє їм. Формально встановлена демократія надає соціальний та політичний контроль через народні волевиявлення та легітимізацію влади, сприяючи використанню економічної та інформаційної влади вільно, внаслідок чого формується масовий споживач з обмеженими аналітичними здібностями, який стає об'єктом цілеспрямованого впливу.

Питання про те, як здійснити демократизацію інформаційної влади, залишається відкритим. Більшість дослідників вважають, що за допомогою організацій громадянського суспільства можна обмежити маніпулятивну владу в інформаційному просторі. Сучасні держави мають три основних моделі організації інформаційної системи: приватну, державну та громадську.

Інформаційна освіта громадськості, зокрема молодого покоління, відіграє важливу роль у досягненні користі для громадян та запобіганні негативним наслідкам діяльності медіа.

Наука і навчальна дисципліна, відома як інформаційна педагогіка, є теоретичною основою такої освіти. Головною метою цієї педагогіки є формування критичного ставлення та навичок відповідального використання інформації.

У контексті трансформації суспільства до інформаційної моделі спостерігається поступове відокремлення особистостей від традиційних соціальних та ідеологічних груп, що призводить до розриву соціальних зв'язків.

У західних демократіях політичний ринок стає головним засобом зв'язку між лідерами і громадянами, а в країнах з "новою демократією" процес комерціалізації нових сфер життя прискорюється разом з кризою традиційних ринкових моделей економіки. На пострадянському просторі політичні ринки розвиваються швидше, ніж ринки товарів та послуг.

Відносно маркетингових підходів до політики існують різні точки зору серед дослідників. Деякі політологи і практики розглядають ринковий підхід до політики як вже встановлений факт, тоді як інші вчені та теоретики висловлюють обґрунтовані сумніви щодо ринкового підходу, вбачаючи в ньому загрозу для демократії. Таким чином, питання про те, чи є політичний маркетинг технікою чи загальною теорією політичного процесу, залишається й досі невирішеним, а сфера політичного життя у демократичних суспільствах перебуває у стані змін і вимагає подальшого обговорення.

Основною проблемою будь-якого ринку, включаючи політичний, є баланс інтересів покупців і продавців. Цей баланс служить інтересам суспільства в цілому і вимагає регулювання. Для цього необхідно забезпечити вільну конкуренцію в політичному дискурсі.

В деяких дослідженнях відзначається необхідність зміни ролі медіа в політичній системі відповідно до їхньої нової ролі у політичному процесі. Забезпечення рівного доступу політиків до медіа є основною передумовою вільної конкуренції на політичному ринку. Проте доступність інформації та вільна конкуренція на політичному ринку самі по собі не гарантують раціональний політичний вибір, і, навпаки, можуть сприяти ірраціональним тенденціям у поведінці виборців.

Політичний маркетинг перетворюється з простої техніки на фундаментальний елемент політичного процесу, що вимагає теоретичного аналізу. Відбувається зміна розуміння демократії з системи представництва інтересів на ринок політичних товарів, де громадяни стають споживачами. Політичний маркетинг впливає на формування попиту на політичні ідеї, подібно до звичайних ринків товарів і послуг.

Існує як видимий, так і прихований ринок політичних послуг, де фірми змагаються за клієнтів, використовуючи інформацію про суспільні настрої для створення відповідних продуктів.

Поява індустріального суспільства привела до з'явлення нових політичних акторів - мас. Термін "маси" став використовуватися для позначення виборців,

прихильників партій, членів громадських рухів і учасників демонстрацій. Вивчення цієї нової соціальної реальності акцентує увагу на феномені натовпу у політичному контексті.

Знаменита книга Г. Лебона "Психологія мас" вразила класичну демократичну теорію. Термін "натовп" став головною активною силою в політичній історії, а вивчення "психології натовпу" показало, що можливості маніпулювання свідомістю та поведінкою широких мас є майже безмежними [56].

Сучасна інформаційна ситуація має ту особливість, що вона здатна впливати одночасно як на маси в цілому, так і на окремих осіб, наприклад, через телебачення. Роль мас в політичній комунікації стає менш помітною, а сама політична комунікація вже не має вираженої переваги ні в сенсі демонстрації сили, ні в сенсі легітимізації влади.

На початку 1990-х років існувало уявлення, що ми живемо в епоху, коли легітимність демократії не підлягає сумнівам. Однак незабаром настала зворотна реакція проти демократії, і стало очевидним, що сумніви у тривалості процесу демократизації в усьому світі були обґрунтованими.

Поняття демократії стало менш чітким, і термін "демократія" придбав різні означення, такі як "виборча", "ліберальна", "стара" та "нова". Це призвело до відновлення дискусій щодо природи та майбутнього демократії. З одного боку, українська політична наука досліджує потреби та умови впровадження демократії на пострадянському просторі. З іншого боку, виникли питання про тенденції розвитку демократичних інститутів на Заході.

Повернення до проблеми полягає в тому, що західні демократичні цінності не можуть автоматично переношуватися на пострадянський простір. Необхідно порівняти історичні обставини виникнення представницької демократії на Заході та на пострадянському просторі.

Це допоможе виявити наявність або відсутність передумов, які визначають специфіку цього процесу. Також важливо розуміти сучасний стан та

особливості розвитку демократичних інститутів там, де вони існують тривалий час.

Востаннє, західна демократична модель стала основою для розробки теоретичних моделей функціонування демократичних держав, які знайшли своє відображення в сучасній політичній науці. Зміна суспільних та політичних реалій в пострадянському просторі породжує складність розвитку громадянського суспільства та демократії. Відмінності в історичних умовах та культурних особливостях цих країн від західних демократій викликають потребу в адаптації досвіду та моделей демократії до специфічних умов.

Важливо відзначити, що громадянське суспільство може існувати у різних формах, включаючи варіанти, які можуть бути сумісні з авторитаризмом. Актуальність цієї проблеми підкреслюється сучасною кризою довіри до політичних інституцій у західних країнах, що може зумовити зростання авторитарних тенденцій. В умовах інформаційного суспільства загальні тенденції та нюанси розвитку демократії та громадянського суспільства на пострадянському просторі вимагають індивідуального підходу до кожної країни.

Сучасна концепція "народовладдя" через політику більшості стикається з критикою у суспільній думці, а модель представницької демократії переживає значні зміни, особливо у контексті суспільних структур, які переміщуються від політичних партій до обраної влади. Це пов'язано з трансформацією природи представницьких інститутів та сприйняттям громадянами цих змін.

Ідея інституційної демократії, де більшість підкоряється меншості, все частіше змінюється на дотримання прав меншин через запобігання дискримінації за ознаками належності до певних соціальних груп. Відзначається, що гегемонія, ґрунтована на числовій або владній перевазі, є проблемою, і повага до прав меншин може суперечити основному демократичному принципу, який встановлює рівні правила для всіх громадян.

У сучасному інформаційному суспільстві роль політичних партій зменшується, а їх місце займають громадські рухи, які формуються навколо

вирішення певних суспільних проблем. Політичні партії тепер вже не обов'язково представляють певні соціальні групи, а скоріше їхню приналежність визначається орієнтацією на конкретні питання.

Це призвело до зміни стратегій партій, які тепер більше уваги приділяють інтересам різних меншин. Сучасна виборча стратегія не ставить за мету об'єднання прихильників однієї ідеології навколо партійного гасла та переконання якомога більше громадян у перевагах власної політичної платформи.

Соціальні групи тепер не тільки борються за свої політичні та економічні права, але й прагнуть виділити себе в порівнянні з іншими соціальними групами. Вони все частіше намагаються уникнути взаємодії з державою та її традиційними представницькими структурами. Більше того, громадяни все частіше виступають перед державою не як прихильники політичних організацій, а як окремі особистості та члени різних соціальних груп.

Це підтверджує думку тезу, що формування інформаційного суспільства супроводжується кризою політичної демократії, що розвивалася протягом останніх століть. Ця криза підтверджується різними дебатами про майбутнє демократії в інформаційному суспільстві.

2.2 Виклики та механізми забезпечення політичної стабільності в інформаційному суспільстві

На сучасному етапі розвитку, а також у період набуття незалежності, українське суспільство зіткнулося з викликами, пов'язаними зі стабільністю. У десятиліття 1980-1990 років спостерігалася зміна стратегічного напрямку у питаннях стабільності українського суспільства: відбувся перехід від холістичного підходу до ліберального. Ця зміна в якості суспільно-політичних процесів в Україні була обумовлена системними трансформаціями.

В період початку 1990-х років, перехід до демократії був майже беззаперечним для більшості українських науковців і політиків, і суспільство

відчувало ейфорію від швидких та позитивних змін, які відбулися завдяки демократизації [68].

З плином часу, коли темпи демократизації політичної системи влади знижувалися, політологічний дискурс зазнав розширення, охоплюючи концепцію різноманітності траєкторій переходу від тоталітарних або авторитарних режимів до демократичного устрою.

Дискусії тепер також охоплюють "процес переходу", його темпи, затримки та відхилення. Питання якості стабільності політичних інститутів та режимів виступило на задній план [68].

Для українського суспільства, яке продовжує зазнавати трансформацій, важливим стало систематизувати методологічні підходи до вивчення демократії та подолання багатозначності цього поняття.

Проте, для досягнення стабільної якості суспільства, необхідно визначити та стабілізувати конкретні пріоритети розвитку. Аналіз та оцінка реальних моделей суспільно-політичної сфери, а не лише гіпотетичних чи очікуваних, є невід'ємною частиною цього процесу [68].

Книга С. Гантінгтона "Політичний порядок у мінливих суспільствах" аналізує не лише значення політичного порядку, але й різноманітні аспекти трансформацій у суспільствах. Проблематика політичної стабільності займає вагому позицію у політичних науках, відома ще з давніх часів, зокрема з робіт Платона та Аристотеля.

У західній науковій традиції, представленій працями Д. Дьюї, Р. Даля, С. Гантінгтона, Г. Алмонда, С. Ейзенштадта, Ф. Шміттера, А. Пшеворського, дослідження зосереджені на пошуку демократичних моделей управління у колоніально-залежних країнах. Розвал комуністичних режимів у 1990-х роках спонукав зростання інтересу до вивчення політичних трансформацій. У цей час з'явилися наукові праці К.Ф. Ендрейна, Л. Даймонда, Д. Б'юкенена, Е. Острома, Є. Мачкова, Р. Райха, Г. Хейла та інших.

Виконання дослідження трансформаційних процесів у соціально-політичній арені українського суспільства потребує глибокого

аналітичного підходу. Основною метою цього аналізу є ідентифікація параметрів інституціоналізації, які вже мають місце у сучасному українському суспільстві.

При цьому необхідно зосередитись на виявленні характеристик цієї інституціоналізації та визначенні потенційних впливів, на які повинні звернути увагу ключові актори політичної сфери, з метою прискорення досягнення стабільної демократичної якості, як для політичної системи, так і для суспільства в цілому [68].

Для реалізації вказаних цілей необхідно детально розглянути концепцію "політична система", яка охоплює два ключові аспекти: "політичні інститути" та "інституціоналізацію". Категорія "політичні інститути" описує форми організації, що об'єднують індивідів у певні групи на основі спільних цінностей і раціональних норм. До таких інститутів відносяться організаційні структури та норми, що регулюють взаємодію усередині системи.

Під "інституціоналізацією" розуміють процес стабілізації та закріплення політичних інститутів та практик у суспільстві. Цей процес включає формування правових норм, культурних моделей, ритуалів, які визначають механізми функціонування та взаємодії між учасниками політичної системи. Це свідчить про те, що аналіз політичної системи потребує розгляду не тільки формальних структур, а й норм, цінностей та їх взаємозв'язків. Глибоке вивчення цих аспектів є ключовим для розуміння шляхів впливу на посилення демократичних принципів та забезпечення стабільності політичної системи.

Концепція "трансформація політичних систем" відображає процес переходу від однієї системи до іншої, який може супроводжуватися змінами в розвиткових напрямках і непередбачуваними наслідками. Процес трансформації передбачає створення нової інституційної бази та інфраструктури. Важливим є забезпечення підтримки цих змін більшістю населення, що є запорукою успішної реалізації трансформаційних процесів.

Цей консенсус може бути виражений через референдуми, нову конституцію, відповідні виборчі процеси, що сприяє легітимізації нової моделі державної та політичної влади [68].

Проте, завершення процесу трансформації та досягнення стабільного функціонування політичної системи мають вирішальне значення для забезпечення стійкості сучасного українського суспільства. Це передбачає, що характеристики та атрибути нової системи набувають незворотності.

Це засвідчує, що трансформація політичних систем має глибокий вплив на суспільні процеси та розвиток країни, і тому її ретельне дослідження є дуже актуальним і важливим завданням [68].

Аристотель та Шарль Монтеск'є, обидва видатні політичні філософи, надали вагомі критерії для оцінки різноманітних форм правління та їх впливу на суспільне життя.

Аристотель сфокусував свою увагу на якісних та кількісних аспектах форм правління, розрізняючи різні типи за кількістю правителів та якісними характеристиками їхньої влади. Це дозволяє проводити аналіз організації влади та принципів її функціонування.

Шарль Монтеск'є, з іншого боку, акцентував на важливості духу народу та основних принципів правління для стабільності та ефективності держави. Його підхід до аналізу впливу організаційних принципів влади на якість життя суспільства підкреслює необхідність врахування цих принципів для забезпечення гармонійного розвитку суспільства.

Важливим є також твір С. Гантінгтона "Політичний порядок у мінливих суспільствах". Дослідник підкреслює вагомість концепції "інститутів" в умовах складних та плюралістичних суспільств, де висока потенційна загостреність конфліктів через відмінні ціннісні пріоритети є домінуючою рисою. В цьому контексті, інститути сприяють подоланню розбіжностей та підтриманню єдності всередині суспільства, враховуючи протиріччя між різними інтересами та цінностями [19].

Для забезпечення стійкості соціального устрою необхідна адекватна інституціоналізація інститутів. С. Гантінгтон наголошує, що інститути є стабільними, суттєвими та відтворювальними елементами, що сприяють підтриманню належної поведінки. Їхніми завданнями є не лише запобігання деградації суспільства, але й забезпечення порядку в організаційних структурах. Організації можуть дотримуватися встановлених правил або порушувати їх в залежності від внутрішніх умов.

В кінці минулого століття представники нового інституціонального аналізу в політології, такі як Д. Б'юкенен, Д. Норт і Р. Коуз, зробили важливе розрізнення між концепцією інститутів як правил гри та інститутів як меж, сформованих людьми для організації взаємовідносин між ними.

Інститути також виступають як організаційні структури, які діють в межах цих правил та спрямовані на досягнення спільної мети для суспільства. Такий підхід відображає принципи Аристотеля та підкреслює їхню актуальність у контексті методологічного підходу до аналізу взаємодії в суспільному житті, де ці дві сутності відіграють значущу роль. Очевидно, що ці два ключові аспекти панування відіграють визначальну роль як у житті окремої особистості, так і в діяльності суспільства в цілому. Водночас, з точки зору політичної організації, важливим критерієм оцінки влади є наявність нормативних обмежень, які регулюють принцип управління.

У контексті суспільств, що зазнають трансформацій, процес інституціоналізації набуває особливого значення. Це пояснюється тим, що правила, норми та процедури стають стабільними та універсально прийнятними для всіх учасників політичної взаємодії.

Стійкі інститути в процесі інституціоналізації сприяють динамічній стабільності політичної системи. Вони здатні адаптуватися до змін та модифікувати умови функціонування суспільства та політичної системи.

Отже, проблематика інституціоналізації має ключове значення для стабільності політичної системи та режиму в Україні. Однак існує проблема розриву між офіційним станом, реальним станом та параметрами

інституціоналізації. Більш того, процес трансформації характеризується різноманітністю, невизначеністю та нестабільністю.

На сьогоднішній день в Україні відбувається не тільки формалізація демократичних інститутів, але й формалізація сутності поняття демократії, що може бути небезпечним для перспектив стабілізації курсу на демократичний розвиток українського суспільства [68].

Сучасна дихотомія між формальними аспектами та сутнісними характеристиками інституціоналізації сприяє різноманітності трансформаційного процесу та непередбачуваності його результатів. Ця обставина підсилює одну з основних ознак нестабільних політичних систем. Системна невизначеність створює умови для швидкого розвалу всієї соціально-політичної структури та перегляду або заміни вже встановлених параметрів розвитку.

З практичної та політичної точок зору це може свідчити про те, що внутрішні суперечності, ймовірно, будуть вирішені шляхом встановлення нового радикального авторитарного режиму. Це можливо, особливо якщо тривала та повільна ескалація кризи викличе відчуття втоми як серед громадян, так і серед еліти [68].

Концепція "патронального президентства" може бути інтерпретована як переборення багатовимірності змін і інституційної нестабільності для того, щоб українське суспільство та політична система здобули ознаки динамічної стабільності.

Політична система в значній мірі залежить від взаємодії між еволюцією політичних інститутів та мобілізацією нових соціальних сил у політичне життя, як вказує О. В. Бабкіна. Однак така модернізація не обов'язково веде до встановлення демократії та вільної конкуренції [6].

Вона може викликати "ерозію демократії" та сприяти тенденціям до авторитарних, військових чи однопартійних режимів, як зазначає С. Гантінгтон [19].

Відповідно, ключові елементи політичної модернізації, такі як раціоналізація влади, диференціація структур та політична участь мас, не завжди реалізуються на однаковому рівні. Політична активність та мобілізація громадських елементів можуть бути виражені в той час, як раціоналізація, інтеграція та диференціація можуть залишатися недостатньо розвиненими.

Те, що С. Гантінгтон спостерігав для країн, які переходили від комуністичного режиму, також застосовується до України.

Українське суспільство, зокрема його політична сфера, продовжує залишатися актуальним об'єктом аналізу. Сучасний період надає певну стабільність, але супроводжується також нестабільністю через сам процес модернізації. Ця ситуація створює враження, що самі спроби модернізувати суспільство можуть спричинити політичну нестабільність [68].

Цитата Вінстона Черчілля про "парадокс демократії" як "недосконалої політичної форми" є доречною у контексті розгляду особливостей демократичної системи.

Демократія передбачає вибір компромісів, володіє гнучкістю, але водночас може бути складною у реалізації. Ця система не гарантує простих рішень, але здатна адаптуватися до змін. Демократизація не є самоціллю, але є інструментом для створення стабільних умов життя людини та розвитку потенціалу сучасної політики.

Впровадження демократичних механізмів та інститутів закладає основу для ефективної державної політики, яка сприяє суспільному прогресу, зокрема забезпечує права людини, економічне зростання, рівність доходів та загальний добробут. Водночас високі ідеали демократії, такі як народовладдя, індивідуальна свобода, права людини та мирне вирішення конфліктів, не реалізуються автоматично.

Демократія надає політичні рамки для досягнення цих цілей, але їх втілення залежить від конкретних умов політичного процесу, взаємодії різних сил та відповідних правил. Політичні процедури, готовність громадян, способи

взаємодії, формальні та неформальні політичні інститути відіграють значущу роль у можливостях успішного переходу до демократії.

Зростаюча невизначеність та нестабільність на шляху до стабілізації демократичних інститутів ще більше підкреслюється відсутністю конкретної стратегії для запобігання можливому поверненню до авторитаризму.

2.3 Розвиток суспільно-політичної стабільності в умовах інформаційно-психологічної війни

Сучасний хронологічний та просторовий контекст української незалежної держави представляє собою особливу політичну реальність, в якій політичні інститути, норми та механізми дії виявляються надзвичайно складними, а інформаційний простір характеризується різноманітністю та насиченістю можливостями, викликами та загрозами.

Розглядаючи роль публічного сектору у сфері інформаційної безпеки, доцільно виходити з позиції, що вона відіграє ключову роль у формуванні відповідних правил, норм та орієнтирів розвитку [119].

Інформацію варто розглядати не лише як знання, але і як сучасний ресурс влади. Важливість інформації у соціальному контексті полягає в можливості контролювати соціальні та економічні процеси. Зокрема, інформаційні ресурси стають важливими для зміцнення демократії та стабільності держав, для оновлення продуктивних і організаційних сил суспільства, а також для розвитку потенціалу людей [121].

Саме тому питання домінування конкретних інститутів у структурі інформаційної безпеки залишається об'єктом дискусій, особливо в країнах, як Україна, де протікають суттєві етапи політичної трансформації. Відзначаючи цю взаємозалежність, слід враховувати, що рівень громадянського розвитку сучасних держав в значній мірі залежить від інформаційного простору загалом [119].

Україна, як демократична правова держава, не може відокремлювати свою розвідувальну та безпекову діяльність від інших політичних та соціальних механізмів, враховуючи соціокультурний контекст і глобальний аспект загалом. Це закріплено в статті 17 Конституції України, де заявлено, що "Суверенітет і територіальна цілісність України, економічна та інформаційна безпека є найважливішими завданнями держави, всього Українського народу" [50].

Попри переваги інформатизації, такі як оптимізація політичних структур, швидке реагування держави на виклики, формування соціально-економічних процесів та підвищення взаємодії між державою і суспільством, політичні суб'єкти занепокоєні деструктивним впливом інформації, маніпуляціями, злочинною діяльністю в інформаційному просторі. Інформаційний простір приносить не тільки переваги, але й проблеми. Дослідження зосереджується на визначенні суб'єктів інформаційної безпеки як ключових політичних інститутів, з акцентом на ролі державних суб'єктів. Важливо аналізувати інформаційну динаміку та її взаємодію з політичними структурами України, яка формує специфічний політичний ландшафт.

Роль інформаційної сфери стає особливо актуальною, включаючи можливості, виклики та потенційні загрози. Інформація є не тільки джерелом знання, але й засобом впливу та влади, що дозволяє контролювати соціальні, економічні та політичні процеси. Важливо забезпечити мирне та конкурентне здобуття політичної влади, її демократичне утримання, здійснення реформ та виконання функцій влади. Інформація може бути інструментом політичної боротьби та міжнародних конфліктів.

Застосування інформаційних технологій може бути спрямоване на ініціювання, підтримку та стримування збройних конфліктів, економічну та культурну експансію, терористичні акти та інші форми впливу.

З цього приводу важливо, щоб державні органи діяли узгоджено та взаємодіяли для забезпечення національної інформаційної безпеки [119].

В умовах зростаючої ролі інформації як засобу влади та інструменту впливу, важливо не тільки прагнути до демократичного утвердження влади, але

й розглядати інформаційну політику як ключовий елемент національної безпеки. Взаємодія державних органів, розробка довірчих відносин та впровадження інформаційних технологій у контексті забезпечення безпеки мають визначальне значення. Інформаційна політика сучасної України вимагає взаємодії численних державних органів з диференційованими функціями.

Сутність інформаційної безпеки полягає в захисті ключових сфер громадського життя від небезпечного впливу інформаційних загроз та підтриманні стабільного розвитку суспільства. Для сучасної України інформаційна безпека набуває особливого значення, оскільки формується в умовах відкритого діалогу без примусових методів.

Держава повинна захищати суспільство від негативного інформаційного впливу та забезпечувати належну реакцію на загрози. Це передбачає активну діяльність у створенні та вдосконаленні правових норм і контролю за їх дотриманням.

Модернізація інформаційної політики України передбачає визначення відповідальних суб'єктів. Згідно зі статтею 17 Конституції України, інформаційна безпека є відповідальністю держави, яка здійснюється через ряд державних інститутів. Суб'єктами інформаційної безпеки є не тільки адміністративні органи, але й законодавчі, судові структури та органи місцевого самоврядування. Загалом, будь-яка організація, що захищає конкурентоспроможні інформаційні продукти і протидіє ворожим інформаційним атакам, може бути розглянута як суб'єкт інформаційної безпеки.

Проте, українські науковці справедливо визначають роль політичних інститутів в контексті національної безпеки. Відповідно до підходу В. Богуша, важливість політичних елементів у забезпеченні національної безпеки визначається через такі суб'єкти:

Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України [12];

Міністерства та інші центральні органи виконавчої влади, Національний банк України, суди загальної юрисдикції, Офіс Генерального прокурора

України, центральні органи виконавчої влади та органи місцевого самоврядування, Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України та Національна прикордонна служба України.

Водночас, розділені функції та обов'язки можуть створювати недостатню координацію та взаємодію між органами, що, в свою чергу, могло впливати на ефективність заходів з інформаційної політики та безпеки. Спроби об'єднання та згуртування цих органів можуть сприяти більшій координації та спільній дії в цих напрямках.

Міністерство культури та інформаційної політики України (МКІП) має значний потенціал в контексті інформаційної політики та інформаційної безпеки, особливо в контексті розвитку інформаційного суспільства.

В сучасному світі інформаційна політика та культурна політика стають все більше взаємопов'язаними. Культура не тільки відіграє важливу роль у формуванні національної ідентичності, але й стає важливою частиною інформаційного простору. Розвиток культурних ініціатив, створення та популяризація культурних продуктів, захист культурної спадщини і сприяння творчості можуть відігравати суттєву роль у визначенні напрямів інформаційної політики.

Підвищення культурної грамотності громадян, розвиток культурної співпраці та використання культурних ініціатив у міжнародному дипломатичному спілкуванні можуть сприяти підвищенню впливу та визнання країни на міжнародній арені. Також, забезпечення культурної інформаційної безпеки, захист культурних цінностей від незаконного використання та включення культурних аспектів у національні та міжнародні інформаційні стратегії стають дедалі важливішими завданнями.

Ця взаємодія між інформаційною та культурною сферами може сформувати цілісну стратегію держави у сфері інформаційної політики, яка враховуватиме як технологічний розвиток, так і національні цінності та культурний досвід.

Зв'язок між інформаційною політикою та культурною сферою є важливим аспектом в контексті створення глибокої та впливової інформаційної стратегії держави.

Міністерство культури та інформаційної політики України відіграє важливу роль у забезпеченні цілісності інформації, збереженні культурної спадщини та розповсюдженні культурних цінностей. Воно займається не лише реалізацією культурних програм та заходів, але й важливими аспектами інформаційної безпеки та впливу.

Збереження інформаційної цілісності та документування історико-культурних процесів є ключовими завданнями у забезпеченні національної ідентичності та культурного спадку. Розвиток спеціальних програм для цього може включати не лише технологічні аспекти, але й заходи, спрямовані на освіту громадян щодо важливості культурного розвитку.

Охорона культурної спадщини охоплює заходи з збереження та відновлення архітектурних пам'яток, цінних предметів, художніх творів, а також контроль за їх незаконним переміщенням чи пошкодженням. З цим пов'язана й важлива функція забезпечення сумісності культурної спадщини та її атрибуції, щоб запобігти фальсифікації та недозволеному використанню культурних цінностей.

Крім того, організація обміну та співпраці між культурними, освітніми та медійними установами має велике значення для розповсюдження та популяризації культурних цінностей та вкорінення. Це допомагає підвищити рівень культурної грамотності та збільшити інтерес громадськості до культурного спадку.

Комплексна діяльність Міністерства культури та інформаційної політики України впливає на різні аспекти суспільства, включаючи питання інформаційної безпеки, національної ідентичності, міжкультурного спілкування та м'якої сили країни. Це важлива інституція, яка має потенціал впливати на багато напрямків розвитку держави.

Міністерство має важливу роль у сприянні виробництву якісного українського контенту та обмеженні розповсюдження маніпулятивних, неправдивих, аморальних або небезпечних матеріалів у державному інформаційному просторі. Це пов'язано з важливим завданням забезпечення національної безпеки та інформаційної суверенності. Проте, у контексті демократії та свободи вираження, діяльність міністерства повинна бути узгоджена з принципами публічної свободи та різноманіття думок.

Важливо знайти способи забезпечення належної якості інформації, зокрема шляхом розвитку медіаграмотності в суспільстві, підвищення відповідальності медіа за поширення недостовірної інформації, та водночас запобігання цензурі та обмеженню плюралізму поглядів [78].

З одного боку, це може забезпечити більшу довіру громадськості до інформації, що поширюється у медіа. З іншого боку, це може викликати обурення щодо можливості обмеження свободи слова та намагання контролювати інформаційний простір.

Прозорий і відкритий діалог з журналістами, медіа та громадськістю може сприяти досягненню балансу між інформаційною безпекою та свободою слова. Розвиток незалежної медіаграмотності та підвищення обізнаності громадян щодо способів розпізнавання дезінформації можуть також вплинути на якість інформаційного середовища [78].

Розробка ефективних механізмів регулювання, які б забезпечували баланс між інформаційною безпекою та свободою слова маю бути пріоритетним. Це вимагає участі різних сторін - уряду, медіа, громадськості та експертної спільноти - для знаходження оптимальних рішень, які б забезпечували захист громадськості від дезінформації та зловживань, не обмежуючи водночас свободу вираження думок [78].

Створення Міністерства цифрової трансформації України є важливим кроком у напрямку розвитку інформаційного суспільства та цифрової економіки. Одним з ключових завдань цього міністерства є сприяння

цифровізації різних сфер суспільства та економіки, впровадженню сучасних технологій, електронного урядування та розвитку інновацій.

Поділ на два відносно незалежних органи - Міністерства культури та інформаційної політики та Міністерства цифрової трансформації відображає розмежування між культурною та інформаційною політикою, а також цифровим розвитком та інноваціями. Проте, ефективність такого підходу може вимагати подальшого аналізу та оцінки впливу на кібербезпеку, інформаційну безпеку та інші аспекти державної діяльності.

Ці два міністерства можуть взаємодіяти на різних рівнях. Зокрема, у контексті цифрової трансформації можливий підхід, що поєднує культурний аспект з використанням цифрових технологій для збереження та популяризації культурної спадщини, розвитку культурно-освітніх програм тощо.

Також важливо підтримувати координацію між цими міністерствами у сферах, де їх діяльність перетинається, наприклад, у забезпеченні цифрової грамотності та захисту персональних даних громадян. З огляду на швидкі технологічні зміни та розвиток цифрової сфери, важливо продовжувати моніторинг та адаптацію державних структур для забезпечення ефективності та адекватності відповідей на сучасні виклики.

Історично інформація завжди була важливим ресурсом і предметом боротьби між державами. У цифрову епоху, коли інформація швидко поширюється та має значний вплив на геополітичний, економічний та соціокультурний розвиток, її значення стало ще вищим. Країни здатні маніпулювати інформацією, використовувати її для формування думок і поглядів, а також для досягнення своїх стратегічних цілей.

Україна, як і багато інших держав, розуміє важливість інформаційної безпеки та контролю за інформаційним простором. Різні інституції, такі як Державний комітет телебачення і радіомовлення України, Національна рада з питань телебачення і радіомовлення, Служба безпеки України, виконують різні ролі в забезпеченні інформаційної безпеки та контролю за медійним простором.

Державний комітет телебачення і радіомовлення України грає важливу роль у формуванні та реалізації державної політики у сферах телебачення, радіомовлення та інформації. Його роль полягає у забезпеченні функціонування медійного простору відповідно до стандартів та норм, а також у контролі за додержанням законодавства щодо інформаційної безпеки.

З огляду на те, що інформація має великий вплив на суспільство та розвиток держави, важливо забезпечити її якість, достовірність та захищеність від маніпуляцій. Створення спеціалізованих органів та інструментів, які займаються інформаційною безпекою, є важливою складовою державної політики в цьому напрямку.

Так, Державний комітет телебачення і радіомовлення України має широкий спектр завдань та функцій, пов'язаних з інформаційною безпекою, розвитком медійного простору та контролем у сферах телебачення, радіомовлення, інформації та видавничої справи. Це вказує на важливість ролі, яку цей орган відіграє у забезпеченні правильного функціонування медійної сфери та інформаційної безпеки в Україні.

Серед цих завдань виділяється "Сприяння розвитку державних медіа", що підкреслює важливість підтримки державних медійних ресурсів. Також важливими завданнями є забезпечення дотримання державної мовної політики у медійних сферах, сприяння суспільному телебаченню і радіомовленню, а також ведення моніторингу та контролю за вимірюваннями та метрологією у сферах телебачення та радіомовлення.

Додатково, завдання, пов'язані з обмеженням доступу до видавничої продукції, яка має походження з території держави-агресора, а також ведення державного реєстру видавців, виготівників та розповсюджувачів видавничої продукції, показують спрямованість на забезпечення інформаційної безпеки та контроль за інформаційним впливом.

Загалом, ці завдання свідчать про складність і різноманітність завдань, які відносяться до інформаційної безпеки та розвитку медійної сфери в Україні.

Цей комплексний підхід допомагає забезпечити ефективний контроль за інформаційним простором та забезпечити безпеку та якість інформаційних ресурсів для громадян.

Також, широкий спектр функцій та повноважень у забезпеченні національної інформаційної безпеки має Національної ради України з питань телебачення і радіомовлення (НРТРУ). Ця рада виконує завдання контролю за дотриманням законодавства в сфері телебачення і радіомовлення та здійснює регуляторні повноваження, але при цьому вона також визначила мету захисту інформаційного простору та розвитку мовлення на тимчасово окупованих територіях.

Одним із аспектів, на який вказує Національна рада, є важливість відповідальної журналістики як інструменту захисту від зовнішньої агресії. Це означає, що забезпечення об'єктивної та достовірної інформації в мас-медіа може відігравати ключову роль у протидії зовнішньому впливу та дезінформації.

Крім того, розвиток суспільного мовлення, перехід на цифрові стандарти мовлення, сприяння розвитку конкуренції на інформаційному ринку та суспільному інформаційному ринку також показують стратегічний підхід до забезпечення інформаційної безпеки та розвитку медійного середовища.

Загалом, це підкреслює важливість ролі Національної ради України з питань телебачення і радіомовлення у формуванні національного медійного простору, який відповідає інтересам та потребам громадян та сприяє національній інформаційній безпеці.

Закон України "Про медіа" встановлює нормативні вимоги, спрямовані на регулювання розповсюдження інформаційних продуктів, що можуть негативно впливати на суспільство через свій зміст, включаючи порнографію, пропаганду війни, ворожнечу, розклад суспільного порядку та інші аспекти.

Це є суттєвим аспектом інформаційної безпеки, оскільки деякі типи інформації можуть завдати шкоди соціальним цінностям та гармонії у суспільстві. Виникає питання про відповідальність за порушення законодавства.

Законодавчі заходи можуть відображати спробу досягти балансу між свободою слова і виразу та необхідністю забезпечення гармонії та захисту громадської моралі. Проте, ця сфера часто стає предметом дискусій і порушує питання обмеження свободи вираження та потенційного зловживання владою для придушення критики або неоднозначних поглядів.

Згаданий закон разом з іншими регулятивними заходами в сфері інформаційної безпеки та медіа може впливати на формування медійного ландшафту та інформаційного захисту суспільства в Україні.

Система регулювання інформаційної безпеки в Україні охоплює різні органи державної влади та інституції, відповідальні за різні аспекти цієї сфери. Зокрема, Міністерство внутрішніх справ та Національна поліція можуть бути залучені в цей процес через свої повноваження щодо забезпечення правопорядку та громадської безпеки, включаючи боротьбу зі злочинами, пов'язаними з інформаційною сферою.

Органи культури, кінематографії, податкової та митної політики відіграють значущі ролі у створенні умов для забезпечення інформаційної безпеки, включаючи регулювання розповсюдження інформаційних продуктів та контроль над митними процедурами, які можуть впливати на інформаційний простір.

Державні органи, такі як Державний комітет телебачення і радіомовлення України та Національна рада України з питань телебачення і радіомовлення, відповідають за регулювання медійної та телекомунікаційної сфери, зокрема з точки зору забезпечення стандартів інформаційної безпеки.

Закон України "Про національну безпеку України" та інші нормативно-правові акти встановлюють комплексний підхід до забезпечення інформаційної безпеки, включаючи правові, економічні, соціальні, військові, науково-технічні та інші аспекти. Це необхідно для ефективної відповіді на різноманітні загрози та виклики в інформаційній сфері.

Розподіл компетенцій та ролей різних органів може створювати потребу в співпраці та координації зусиль для досягнення комплексної інформаційної безпеки в Україні.

Згаданий закон надає детальний опис сектору розвідки, який виконує стратегічні завдання з розвідувальної та розвідувально-аналітичної діяльності, спрямованої на забезпечення військової готовності держави, захисту територіальної цілісності, розвідувального простору України та її інтеграції у світовий розвідувальний контекст.

Окрім того, наголошується на створенні розвиненої інфраструктури у розвідувальній галузі, що підкреслює важливість відповідних ресурсів для виконання завдань цього сектору. Особливо зазначається, що Міністерство оборони України активно здійснює розвідувально-аналітичну діяльність, спрямовану на захист національної безпеки та оборони, включаючи аналіз воєнно-політичної обстановки та прогнозування потенційних ризиків.

Повноваження Генерального штабу Збройних Сил України також мають важливе значення, оскільки вони охоплюють визначення необхідних ресурсів для Збройних Сил та інших військових підрозділів, включаючи матеріально-технічні ресурси, а також засоби інформаційного та комунікаційного забезпечення. Використання Збройних Сил України та їхній вплив на національний інформаційний простір, включаючи розвідувально-аналітичну діяльність, також є предметом цільової уваги.

Паралельно, розкривається сутність координаційної ролі військових та центральних органів виконавчої влади, а також інших управлінських органів. Їх спільні дії спрямовані на ефективне використання національного інформаційного простору та координацію в рамках цілей національної безпеки.

Окрім того, виділяється роль та значущість Служби зовнішньої розвідки України, яка відіграє важливу функцію у забезпеченні захисту національної безпеки, в тому числі в контексті кіберзагроз.

Державна служба спеціального зв'язку та захисту інформації України, регульована Законом України "Про Державну службу спеціального зв'язку та

захисту інформації України" в редакції 2006 року з останніми змінами від 31 грудня 2023 року, несе відповідальність за забезпечення безпеки державної інформації.

Згідно зі законом, орган відповідає за формування та реалізацію державної політики у сферах державної системи урядового зв'язку, функціонування та розвитку державної системи спеціального зв'язку, технічного захисту інформації та криптографії, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, а також спеціального поштового зв'язку.

Серед інших функцій Державної служби спеціального зв'язку варто зазначити її взаємодію з системою надзвичайних ситуацій. Діяльність цього органу спрямована на виконання завдань, визначених Урядом, і контролюється Верховною Радою України, включаючи звіти про дотримання законодавства, прав та свобод людини і громадянина, а також передається інформація Президенту щодо питань, пов'язаних з забезпеченням національної безпеки України. Робота цієї організації спрямована на захист держави, що знаходить відображення у її участі у судових процесах та представленні розвідувальних звітів.

Аналіз державних органів, що діють у сфері інформаційної політики, буде неповним без урахування ролі Служби безпеки України. Цей спеціальний державний орган, що виконує безпекові функції, визначає на своєму офіційному веб-сайті п'ять головних пріоритетів, серед яких однією з ключових сфер є забезпечення інформаційної безпеки.

Діяльність Служби безпеки спрямована на забезпечення безпеки українського інформаційного та кіберпростору, включаючи запобігання кібертероризму та кібершпигунству, захист від хакерських атак, розкриття фейкових новин, виявлення фейкових агітаторів та ботоферм, які пропагують патріотичні та сепаратистські позиції.

Особливий акцент робиться на посилення діяльності в галузі інформаційного захисту, що включає міжнародне співробітництво для

забезпечення національної кібербезпеки. Голова Служби безпеки, враховуючи широкі повноваження та обов'язки, підзвітний Верховній Раді та Президенту, і має обов'язок інформувати громадськість про свою діяльність.

Президентська відповідальність за національну інформаційно-технологічну (IT) безпеку держави охоплює координацію різноманітних спеціалізованих структур, консультативно-дорадчих органів і департаментів. У системі організацій, які формують та реалізують інформаційну політику держави, важливу роль відіграють консультативно-дорадчі органи, зокрема Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки, яка відповідає перед Радою національної безпеки і оборони України. Головною метою цієї комісії є підтримка взаєморозуміння між різними організаціями в інформаційній сфері, включаючи аналіз поточної ситуації та загроз національній безпеці в цьому контексті.

Це включає аналіз галузевих програм та заходів із реалізації інформаційної політики та виявлення відповідного міжнародного досвіду.

Крім того, комісія готує рекомендації Президентові та Раді національної безпеки стосовно визначення національних інтересів України в інформаційній сфері, концептуальних підходів до формування та вдосконалення державної інформаційної політики та забезпечення національної інформаційної безпеки, а також впровадження національної стратегії розвитку інформаційного суспільства та інформаційної безпеки [119].

В контексті інституційного розвитку організації, що фокусується на питаннях інформаційної політики, слід відзначити, що вона ще не досягла повної зрілості. Згідно з Указом Президента України від 12 квітня 2014 року "Про Центр воєнної розвідки", була створена структура при Раді національної безпеки і оборони України з активною участю у сфері інформаційної безпеки.

Відомо, що цей центр забезпечував інформацію про ситуацію на сході України та здійснював систематичний моніторинг питань інформаційної безпеки. Однак в даний час ця розвідувально-аналітична структура не

функціонує як державний орган і діє під відомчим керівництвом Ради національної безпеки і оборони.

Важливо зауважити, що діяльність цих органів постійно піддавалася контролю соціальних груп, зокрема журналістської спільноти, яка мала можливість вносити пропозиції та висловлювати критику стосовно їх роботи. Ці органи відіграють важливу роль у забезпеченні свободи слова, інформаційної безпеки та забезпеченні демократичних принципів в Україні.

Загальний огляд джерел, що стосуються національної інформаційної безпеки, вказує на те, що дослідники найбільше акцентують увагу на органах виконавчої влади, зокрема на тих, які відіграють важливу роль у сфері інформаційної політики. Проте, враховуючи парламентсько-президентську форму правління в Україні, важливим аспектом є діяльність законодавчої гілки влади як суб'єкта, відповідального за забезпечення кібербезпеки.

Важливо відзначити, що принципи колегіальності, відкритості та прозорості, на яких базується діяльність Верховної Ради України, є ключовими в аспекті розвідувальної та безпекової діяльності країни.

Забезпечення прозорості роботи Верховної Ради України є важливим завданням, яке також стоїть перед Апаратом Верховної Ради України, відповідальним за управління публічною інформацією, необхідною для парламентської діяльності.

До того ж, Верховна Рада України має спеціалізовані комітети, які займаються питаннями національної інформаційної політики. Комітет з питань свободи слова, Комітет з питань гуманітарної та інформаційної політики та Комітет з питань цифрової трансформації грають важливу роль у формуванні національної інформаційної стратегії та забезпеченні кібербезпеки.

Отже, діяльність законодавчої гілки влади, включаючи Верховну Раду України та її спеціалізовані комітети, має важливе значення у забезпеченні національної інформаційної безпеки та розвитку кібербезпеки в країні.

Комітет з питань свободи слова Верховної Ради України займається важливими питаннями, пов'язаними зі забезпеченням свободи слова, прав

громадян на інформацію, захистом прав журналістів та працівників медіа, а також забезпеченням незалежності та ефективної діяльності медіа.

Цей комітет має вже історію існування в різних формах у структурах Верховної Ради України, а його діяльність та звіти доступні для ознайомлення у відкритому доступі [48]. Важливим завданням цього комітету є забезпечення розвитку і зміцнення демократичних стандартів у сфері інформаційної діяльності та свободи медіа.

Комітет з питань гуманітарної та інформаційної політики займається більш широким спектром питань, що охоплюють різні сфери національного та державного життя. Ця комісія розглядає питання культурно-освітньої та мистецької діяльності, роботи медіа-індустрії, кіноіндустрії, аудіовізуального ринку, туризму, рекреаційної діяльності, охорони історико-культурної спадщини, реклами, діяльності друкованих та електронних медіа, використання національних мов та мов меншин, політики у сфері свободи совісті та релігійних об'єднань, а також інші сфери.

Крім того, цей комітет розглядає питання демографічної політики, а також відіграє роль у формуванні державної політики в сфері інформації та інформаційної безпеки, за винятком питань національної безпеки і оборони [49].

Обидва зазначені комітети мають важливе значення у розвитку національної інформаційної політики та забезпеченні інформаційної безпеки в Україні. Їхні зусилля спрямовані на зміцнення демократії, захист прав громадян, розвиток медіа та культурного простору країни.

Ці комітети відображають важливий аспект інтеграції гуманітарної, культурної та інформаційної політики. Їхня діяльність спрямована на вирішення сучасних викликів, пов'язаних із цифровою трансформацією та розвитком інформаційного суспільства.

Комітет з питань цифрової трансформації також має важливу роль, пов'язану з розвитком цифрового суспільства. Його принципи стосуються правових аспектів цифровізації, електронної демократії, державних

інформаційних систем, використання відкритих даних, інфраструктури та багатьох інших аспектів цифрової трансформації.

Робота Комітету є важливою для розвитку технологій, електронної комерції, кібербезпеки та інших аспектів, що визначають сучасний світ [91].

Загалом, ці комітети сприяють інтеграції різних аспектів суспільного та державного життя в Україні, розвитку національної інформаційної політики, а також вирішенню викликів, пов'язаних із цифровою трансформацією та розвитком інформаційного суспільства.

Визначення проблем та недоліків у роботі державних органів, відповідальних за інформаційну та кібербезпеку в Україні, є важливим для розвитку безпекової політики. Наразі в Україні існує неузгодженість та дублювання повноважень, недостатня координація, відсутність єдиного стандарту звітності, недостатність ресурсів та необхідність удосконалення комунікаційних процедур.

Позитивні зрушення в модернізації та демократизації суб'єктів інформаційної безпеки, а також зусилля органів щодо підвищення інформаційної активності та об'єктивності, є ознаками сучасної інформаційної політики України. Для ефективної державної політики у сфері інформаційної безпеки важливо постійно вдосконалювати співпрацю між органами, комунікаційні канали, розробляти єдині стандарти та сприяти взаєморозумінню.

Глобальна інформаційна безпека, захист від маніпуляцій, інформаційного тиску та інформаційної війни є важливими викликами, особливо в контексті агресії Росії проти України. Потрібно співпрацювати з міжнародними партнерами, встановлювати стандарти для міжнародної інформаційної безпеки та брати участь у глобальних ініціативах.

Захист персональної інформації, конфіденційність комунікацій та доступ до суспільно значущої інформації потребують розробки національних та міжнародних норм і законодавства. Прозорість, співпраця та взаєморозуміння між українськими державними органами та їхніми міжнародними партнерами

можуть сприяти вирішенню цих питань через спільні обговорення, розробку стратегій та підтримку ініціатив.

Активізація міжнародної співпраці у сфері інформаційної безпеки вимагає злагоджених дій та обміну досвідом між державами. Ефективна взаємодія може включати створення спільних робочих груп, проведення міжнародних конференцій та семінарів, розробку та узгодження міжнародних стандартів. Підтримка міжнародних правових ініціатив забезпечує юридичну основу для захисту інформації та персональних даних на глобальному рівні. Співпраця між країнами стає необхідною умовою для ефективного реагування на нові виклики та загрози в інформаційній сфері.

Глобалізація інформаційного простору у сучасному світі призводить до зменшення ефективності механізмів інформаційного суверенітету держав, що має прямий вплив на комплексний стан національної безпеки. У зв'язку з цим виникає актуальна потреба у розробці та оптимізації комплексу заходів, спрямованих на забезпечення міжнародної інформаційної безпеки.

Оскільки масштаби глобальних викликів у інформаційній сфері надзвичайно великі, і вирішення цих проблем зусиллями однієї або навіть декількох держав неможливе, необхідно розвивати міждержавне співробітництво в межах ООН. У 1998 році світ побачив знаковий крок у забезпеченні міжнародної інформаційної безпеки - Резолюція Генеральної Асамблеї ООН A/RES/53/70, яка засвідчила необхідність збереження інформаційної безпеки в умовах росту загроз та викликів [73].

Цей документ зазначив початок посилення міжнародної координації в сфері інформаційної безпеки. Резолюція, ухвалена у 1998 році, ініціювала глибоке обговорення стосовно потреби у формуванні міжнародного правового режиму, який би детально визначав статус інформації, інформаційних технологій та методологій їх застосування, що стало фундаментальним етапом у розробці відповідного правового апарату, призначеного для регуляції питань інформаційної безпеки на міжнародному рівні.

У 1999 році була прийнята Резолюція Генеральної Асамблеї ООН A/RES/54/49, яка наголошувала на загрозах для міжнародного інформаційного простору, як для цивільної, так і військової сфери. Виконуючи цю Резолюцію, в 2000 році були представлені принципи, що внормувала правила поведінки держав в інфопросторі та закладають основу для міжнародної співпраці з вирішення проблем інформаційної безпеки. Принципи надають визначення ключових понять системи міжнародної інформаційної безпеки, таких як "інформаційні простори", "інформаційні війни", "інформаційні ресурси", "інформаційна зброя", "інформаційна безпека" та інші [105].

Майбутні резолюції стосувались боротьби зі злочинним використанням IT-технологій, створення глобальної системи кібербезпеки та захисту інформаційної інфраструктури. Значний внесок у забезпечення міжнародної інформаційної безпеки було зроблено за допомогою Резолюції A/RES/62/17 від 5 грудня 2007 року, яка сприяла розгляду існуючих та потенційних загроз у цій сфері. Крім того, Резолюція A/RES/71/28 від 5 грудня 2016 року відзначила досягнення в галузі інформатизації та телекомунікацій в контексті забезпечення міжнародної безпеки. Обидві резолюції зробили вагомий внесок у розвиток інтернаціонального діалогу з питань інформаційної безпеки [73].

Європейський Союз виступає одним із провідних суб'єктів у сфері забезпечення міжнародної інформаційної безпеки та кіберзахисту. В 2001 році, Комісією ЄС було представлено документ під назвою "Мережева та інформаційна безпека: європейський політичний підхід", який представив концепцію вирішення проблематики інформаційної безпеки. Цей документ запровадив суттєвий прогрес у розробці політик, що націлені на зміцнення інформаційної безпеки. В сучасні часи, Європейський Союз продовжує активно розвивати політику в цій області та здійснює значні зусилля для забезпечення кібербезпеки у інформаційному просторі.

Згідно з визначенням, термін "мережева та інформаційна безпека" відноситься до здатності мережі або інформаційної системи відповідати на випадкові події або зловмисні дії, які можуть становити загрозу доступності,

автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, які надаються через ці мережі та системи [134].

Після прийняття документу "Мережева та інформаційна безпека: європейський політичний підхід" Комісією ЄС в 2001 році, у Європейському Союзі було прийнято значну кількість нормативно-правових актів, які містять різноманітні підходи до забезпечення інформаційної безпеки в країнах-членах [73].

У лютому 2013 року, Європейський Союз випустив стратегію кібербезпеки під назвою "Відкритий, надійний та безпечний кіберпростір", метою якої було закликати держави-члени до розвитку міжнародного співробітництва в контексті протидії кіберзагрозам.

У липні 2016 року, Європейський парламент та Рада ЄС прийняли директиву, орієнтовану на імплементацію заходів, спрямованих на забезпечення високого рівня безпеки мережевих та інформаційних систем всередині Європейського Союзу.

Дана директива визначає універсальні норми та стандарти у сфері кібербезпеки для країн-членів ЄС, з метою підвищення ефективності системи кібербезпеки на різних рівнях, а також накладає обов'язок на операторів ключових та цифрових послуг інформувати про інциденти кібербезпеки.

У вересні 2017 року Комісія ЄС оприлюднила повідомлення про створення сильної кібербезпеки для ЄС, де наголошується на важливості кіберзахисту для безпеки держав-членів ЄС та необхідності колективного підходу у протидії кіберзагрозам [73].

Для зміцнення системи інформаційної безпеки на території Європейського Союзу було засновано спеціалізований орган - Європейське агентство з питань мережевої та інформаційної безпеки (ENISA). Задачею цього агентства є не лише підвищення рівня мережевої та інформаційної безпеки у ЄС, але й створення оптимальних умов для забезпечення такої безпеки для громадян, бізнесу та державних установ Європейського Союзу.

Агентство працює над розвитком культури мережевої та інформаційної безпеки серед всіх зацікавлених сторін, зокрема веде роботу з вирішення проблем безпеки Інтернету речей та інших технологій. Крім того, ENISA забезпечує підтримку безперебійного функціонування ринку ЄС, сприяючи розвитку стандартів та методів для забезпечення мережевої та інформаційної безпеки [131].

ENISA забезпечує координацію між країнами-членами ЄС у сфері кібербезпеки, сприяє обміну інформацією та надає поради щодо розробки та впровадження стратегій кібербезпеки. Крім того, ENISA допомагає забезпечити зв'язок між країнами-членами ЄС та міжнародними організаціями щодо кібербезпеки [73]

Беручи до уваги той факт, що ефективність інформаційного захисту в європейському кіберпросторі залежить від співпраці держав в рамках міжнародних органів, в структурі Європейського поліцейського офісу був створений Європейський центр боротьби з кіберзлочинністю у 2013 році. Цей центр покликаний розслідувати мережеві шахрайства, а також злочини, які становлять загрозу безпеці критично важливих інфраструктур та інформаційних систем ЄС. Напрямки діяльності Центру включають також співпрацю з іншими міжнародними організаціями, які займаються боротьбою з кіберзлочинністю, з метою підвищення рівня захисту інформаційної безпеки в Європі [73].

Враховуючи, що інформаційна безпека є ключовим аспектом національної безпеки, країни по всьому світу активно займаються вирішенням питань безпеки в кіберпросторі, розробляючи комплексні стратегії та заходи для її зміцнення.

Основну увагу приділяється розробці та удосконаленню національного законодавства в сфері кібербезпеки, а також створенню спеціалізованих організаційних структур, призначених для захисту кіберпростору. Крім того, зусилля більшості країн спрямовані на підвищення професійного рівня фахівців у галузі кібербезпеки та на зміцнення захисту критично важливої інфраструктури від потенційних кібератак.

Важливим етапом вдосконалення заходів з кібербезпеки є співпраця між державами у рамках міжнародних організацій [73].

В контексті сучасної глобалізованої епохи, захист критичної інфраструктури стає пріоритетом для багатьох держав світу. Під критичною інфраструктурою розуміють комплекс систем, мереж та активів, що мають взаємозв'язок і є вирішальними для забезпечення стабільного та неперервного функціонування суспільства. Ця інфраструктура може включати як військові, так і цивільні елементи, а також об'єкти, що використовуються в обох сферах, тобто мають подвійне призначення.

До прикладів критичної інфраструктури можна віднести мости, споруди зв'язку, аеропорти, енергетичну інфраструктуру, банківський сектор, виробництво та розподіл електроенергії, медичні установи, державні аварійно-рятувальні служби тощо.

Забезпечення безпеки такої інфраструктури є надзвичайно важливим завданням для кожної країни, оскільки порушення її роботи може призвести до значних наслідків для суспільства та економіки У сучасних умовах захист критичної інфраструктури є все більш важливою та актуальною задачею для багатьох країн світу [73].

Відповідно до Резолюції Ради Безпеки ООН S/RES/2341 (2017), ухваленої 13 лютого 2017 року, кожна держава має право самостійно визначати, які саме об'єкти в її інфраструктурі є критичними та розробляти стратегії їх захисту. Це положення підкреслює суверенітет держав у питанні ідентифікації та захисту об'єктів, важливих для національної безпеки і стабільності.

Внаслідок цього, перелік критичної інфраструктури може істотно відрізнятися залежно від країни. У Сполучених Штатах Америки, наприклад, до цього переліку включаються не лише об'єкти, необхідні для підтримки життєдіяльності суспільства, а й національні пам'ятки, виборчі системи, дипломатичні представництва та інші важливі елементи.

Враховуючи зростаючі загрози кібербезпеці, необхідно забезпечити захист не лише традиційних об'єктів критичної інфраструктури, а й звернути

увагу на нові сегменти інфраструктури, такі як мережі Інтернету речей та інші цифрові технології [106].

В сучасному світі розвитку інформаційного суспільства, критична інфраструктура безпеки не може існувати без інформаційної інфраструктури, що передбачає використання комп'ютерів та мереж, зокрема систем диспетчерського управління та збору даних. Взаємодія цих систем дозволяє обмінюватися інформацією та здійснювати аналіз, що є критично важливим для забезпечення функціонування критичної інфраструктури [73].

З іншого боку, доступ до управління критичною інфраструктурою за допомогою далекого доступу дозволяє підвищити ефективність та зменшити витрати, але також створює загрозу кібербезпеці.

У зв'язку з цим, кібератаки на критичну інфраструктуру можуть бути використані як знаряддя військової агресії в геополітичних конфліктах. Руйнування нафтопроводів, вимкнення електростанцій, припинення постачання води та опалення комунальних підприємств може надати значну військову перевагу [73].

На сьогоднішній день забезпечення інформаційної безпеки є одним із найважливіших завдань для України. Це зумовлено необхідністю боротьби зі злочинними діями, спрямованими на посягання на інформаційний простір країни. Зважаючи на визнаний пріоритет європейської інтеграції в зовнішній політиці України, владі необхідно розвивати ефективний діалог з Європейським Союзом з питань забезпечення інформаційної безпеки [73].

При цьому, для досягнення максимальної ефективності у цій сфері, необхідно вивчати досвід країн, які вже мають відповідну організаційно-правову основу та успішно застосовують її.

Вивчення та використання цього досвіду у національній законотворчості та реалізації заходів забезпечення інформаційної безпеки є надзвичайно важливим для України [73].

Інформаційна безпека розглядається провідними вченими, дипломатами та політичними візіонерами як передумова збереження миру у світі. Розвиток

глобальної системи безпеки прогресує, і суспільства в перехідний період стають особливо вразливими перед кіберзагрозами. Водночас розуміння природи гібридних атак швидко розвивається, і накопичується цінний досвід спільної протидії інформаційним нападам.

Для розвитку інформаційної безпеки в Україні важливо розуміти національні інтереси та загальнолюдські цінності. Сучасні дослідники підкреслюють, що в центрі інформаційної безпеки перебуває індивід, а з іншого боку – держава. Органи, відповідальні за безпеку і оборону, повинні враховувати захист совісті, орієнтації і духу окремих осіб та їхніх спільнот, а також інформаційний суверенітет держави. Інформаційний суверенітет означає виключне право держави на формування та використання всіх інформаційних ресурсів, створених за державний кошт, та належне володіння і розподіл національних інформаційних ресурсів.

Сучасні положення про компетентні органи встановлюють баланс між захистом прав і свобод людини та державним суверенітетом, що є взаємопов'язаними та взаємозалежними в країнах, які прагнуть до демократії. Вчені визначають конкретні напрями державного регулювання в інформаційній сфері як вирішальні для забезпечення інформаційної безпеки.

Ці напрями включають забезпечення права і можливості доступу до інформації та інформаційних ресурсів; гарантування інформаційної безпеки особистості, суспільства і держави; сприяння розвитку конкуренції; боротьба з концентрацією медіа у руках фінансово-промислових груп; боротьба з монополіями, включаючи державний контроль над медіа; дотримання свободи слова; захист інтересів різних соціальних груп (етнічних меншин, молоді, професіоналів); захист національної культурної спадщини та мов; протистояння ідеологічній експансії інших країн; захист інтелектуальної власності; впровадження переваг електронної демократії та електронного урядування; боротьба з кіберзлочинністю; правове регулювання Інтернету тощо [119].

Важливо відзначити, що ці напрями часто відображаються у діяльності різних державних органів в Україні. Рівень інформаційної безпеки держави

тісно пов'язаний із ступенем розвитку політичних, соціально-економічних, оборонних, дипломатичних та інших складових національної безпеки.

В Україні відсутній конкретний гарант інформаційної безпеки, а також необхідний комплекс нормативно-правових актів. Деякі дослідники навіть стверджують, що весь процес інформатизації є стихійним та неконтрольованим, і в результаті використання іноземних інформаційних продуктів переважає [97].

Закон України "Про основи національної безпеки України", який втратив чинність у 2018 році, мав у собі "основні напрями державної політики з питань національної безпеки в інформаційній сфері" [101].

Зокрема, ці напрями включали "забезпечення інформаційного суверенітету України", "розвиток державної інформаційної інфраструктури та ресурсів", а також "удосконалення державного регулювання розвитку інформаційної сфери через створення нормативно-правових та економічних умов для розвитку державної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері та насичення національного та світового інформаційного простору достовірною інформацією про Україну" [123].

Сучасні виклики для інформаційної безпеки включають обмеження свободи слова, проблеми доступу до інформації, насильство в медіа, кіберзлочинність, витік конфіденційних даних, політичну маніпуляцію та загрози державному суверенітету в IT-сфері. Розуміння цих загроз і розробка ефективних стратегій для їх нейтралізації є ключовими для зміцнення інформаційної безпеки.

Важливо забезпечити комплексний підхід, що включає технологічні рішення, освітні програми, правову базу та міжнародну співпрацю. Необхідно створювати механізми для ефективного реагування на інциденти, розробляти політики протидії дезінформації та забезпечувати доступ громадян до надійної інформації. Наукова спільнота наголошує на важливості аналізу внутрішніх та зовнішніх факторів, що впливають на національну кібербезпеку. Внутрішні виклики включають відсутність сталого розвитку історичних традицій,

обмеженість політичного досвіду, недостатнє розуміння основ демократії та правових принципів, що сприяють зростанню кіберзлочинності та зниженню рівня освіти.

На інституційному рівні ці фактори ускладнюють впровадження електронного урядування та забезпечення кібербезпеки. Розробка стратегій зміцнення національної кібербезпеки включає підвищення рівня технологічної готовності, розвиток освітніх програм з кіберграмотності, інвестиції в ІТ-освіту та правову базу, а також ефективну співпрацю між державними структурами, приватним сектором та міжнародними організаціями.

Важливість глибокого аналізу зовнішніх факторів, що впливають на національну кібербезпеку, не можна переоцінити. До таких факторів належать автономні політики національних інституцій в інформаційній сфері, активність міжнародних терористичних організацій, розвиток стратегій інформаційної війни з боку зовнішніх суб'єктів та розширення культурних впливів. Реагування на ці виклики вимагає інтегрованого підходу в рамках національної інформаційної політики з урахуванням як внутрішніх, так і зовнішніх детермінант.

Перший пріоритетний напрям — міжнародне співробітництво. Держава повинна активно брати участь у глобальному діалозі та співпраці у сфері кібербезпеки, обмінюватися знаннями, досвідом та інформацією про загрози. Це сприяє розробці та впровадженню міжнародних стандартів кібербезпеки та зміцненню здатності країни протистояти спільним кіберзагрозам.

Другий напрям — вдосконалення національних механізмів моніторингу та реагування на кіберзагрози. Це включає підвищення ефективності ідентифікації та аналізу потенційних загроз для оборонного сектору, розробку комплексних систем захисту інформаційних ресурсів та інфраструктури, а також своєчасне інформування відповідальних органів про стан кібербезпеки.

Для досягнення цих цілей важлива злагоджена взаємодія між державними органами, приватним сектором та міжнародними партнерами. Ефективна координація зусиль дозволить Україні адекватно реагувати на поточні

кіберзагрози та прогнозувати можливі майбутні ризики, забезпечуючи безпечне інформаційне середовище.

Глибокий аналіз діяльності державних органів в умовах сучасних викликів і загроз у сфері кібербезпеки сприятиме оцінці їхньої ефективності, ідентифікації потенційно неефективних аспектів та розробці планів модернізації. Дослідження національної інформаційної політики, зокрема кібербезпеки, вказують на різноманітність стратегій захисту інформації та необхідність їх детального розгляду.

Сучасні підходи до забезпечення інформаційної безпеки орієнтуються на характеристики інформаційного суспільства, що відрізняється вищим рівнем державної розвиненості та інтелектуальної зрілості суспільства. В сфері державного регулювання виділяються три основні напрями дій для протидії та мінімізації інформаційних загроз:

Правові ініціативи включають розробку та імплементацію нормативно-правових актів і рекомендацій, що регулюють інформаційні відносини та забезпечують юридичну основу для охорони інформаційної безпеки.

Технічні заходи включають впровадження сучасних технологічних рішень для підвищення ефективності обробки інформації та захисту стратегічних інтересів.

Організаційно-економічні методи зосереджені на зміцненні інформаційної стабільності через вдосконалення управління соціально-економічними процесами в країні.

В Україні ці стратегії критично важливі через недостатньо розвинену політичну та правову культуру, обмежене усвідомлення населення про можливості сучасних технологій, цифрову нерівність та її впливи. Для держави важливо не лише запроваджувати демократичні реформи, але й стимулювати суспільство до участі в цьому процесі.

Організаційні дослідження виявляють недоліки в системі забезпечення інформаційної безпеки України, що перешкоджають ефективному виконанню

функцій. Це включає відсутність координації між відомствами, недостатнє фінансування, брак кваліфікованих спеціалістів. Держава повинна вживати комплексних заходів для підвищення рівня інформаційної безпеки, включаючи реформування законодавчої бази, інвестиції в розвиток інфраструктури та підготовку фахівців, а також зміцнення міжвідомчої взаємодії.

Ці недоліки включають неефективне управління діяльністю, несистемність організаційних змін та реформ, відсутність аналітичного забезпечення, а також відсутність позитивної оцінки змісту функцій та напрямів розвитку органів державної влади [119].

Деякі організаційні проблеми в контексті національної інформаційної безпеки України мають тимчасовий характер, але існують і стійкі проблеми, які можуть призвести до кризових явищ у національному інформаційному просторі. Це загрожує національному суверенітету, демократичним основам та безпеці громадян. Соціально-економічні виклики, включаючи обмеження прав і свобод громадян, обмежений доступ до інформації та ускладнення діяльності незалежних медіа, вказують на системні недоліки в управлінських структурах, що обмежують їх здатність адекватно реагувати на інформаційні загрози.

Організаційно-економічні стратегії в області інформаційної безпеки націлені на нейтралізацію політичних, економічних та військових загроз, спричинених інформаційними атаками. Ці методи мають мінімізувати збитки для юридичних та фізичних осіб від деструктивних інформаційних впливів. Реалізація таких стратегій вимагає інтегрованого підходу, що поєднує правові, технічні та організаційні заходи для зміцнення стійкості національної інформаційної системи.

Інформація стала фундаментальною складовою життя суспільства та державної структури, що акцентує на її значущості як об'єкта правового регулювання. Важливо забезпечити стабільність держави та її інститутів через адаптацію національних законів до міжнародних норм і регіональних стандартів, інтеграцію їх у національну правову систему. В Україні детальний

аналіз правового забезпечення інформаційної безпеки є ключовим для національної безпеки.

Розроблення правових рамок, адаптація до технологічних реалій та імплементація організаційно-економічних ініціатив є критичними для посилення інформаційної безпеки. Відсутність ефективної координації між різними рівнями державного управління може ускладнити ці зусилля. Політичні ініціативи також є необхідними для забезпечення інформаційної безпеки на державному рівні, вимагаючи від владних структур як правових, так і політичних втручань.

Плідне співробітництво між ключовими суспільними інституціями, включаючи цивільні, громадські та урядові структури, є вирішальним для ефективної інформаційної політики держави. Така синергія становить основу для побудови соціально-політичного фундаменту безпеки. Академічна спільнота наголошувала на необхідності розвитку системи кібербезпеки ще до кібератак з боку Росії, підкреслюючи, що державні інтереси в сфері інформаційної безпеки тісно пов'язані з розвитком суспільних цінностей та захистом прав і свобод громадян.

Ефективність інформаційної безпеки охоплює широкий соціально-політичний контекст і вимагає комплексного підходу, який інтегрує цінності, права та свободи суспільства. Ключовим до успішної реалізації такої політики є розроблення надійного механізму взаємодії між усіма зацікавленими сторонами, забезпечуючи врахування та узгодження інтересів держави, громадянського суспільства та приватного сектору.

Б. Кормич також висвітлив складну і вагому роль, яку відіграють права і свободи людини і громадянина у сфері інформаційної безпеки. Він підкреслив, що в демократичних суспільствах визнані права і свободи людини у сфері інформації є основними показниками стану інформаційної безпеки, як окремих осіб, так і суспільства загалом [51].

Він також підкреслив, що закріплені в нормативно-правових актах права та свободи людини в контексті інформаційної безпеки слугують інструментом

обмеження можливого державного свавілля. Б. Колміч додатково зазначив, що повноцінна реалізація прав і свобод людини у сфері інформаційної безпеки можлива лише за умови активної підтримки та імплементації політичних рішень на вищому державному рівні.

Політичний вимір інформаційної безпеки є ключовим, оскільки ефективність державних заходів та інструментів залежить від розуміння взаємозв'язку між усіма аспектами інформаційної безпеки. Досягнення інформаційної безпеки включає гарантію конституційних прав на доступ, використання, поширення та збереження інформації, а також захист здоров'я та психічного благополуччя громадян від негативних інформаційних впливів та маніпуляцій, і оборону авторських прав.

Необхідно застосовувати інтегрований підхід до інформаційної безпеки, який враховує не лише технологічні аспекти, але й широкий соціокультурний та політичний контекст. Політичні рішення та стратегії на національному рівні мають узгоджувати інтереси різних соціальних груп, зміцнювати суспільні цінності та підтримувати партнерство між урядовими структурами, громадськістю та приватним сектором.

Держава повинна створити умови для вільного доступу громадян до інформації, захисту від інформаційних ризиків та підвищення обізнаності населення про їхні права та можливості у сфері цифрових технологій.

Для суспільства інформаційна безпека означає забезпечення реалізації вищезазначених конституційних прав, але ще важливіше, щоб сучасне суспільство розвивалося в бік інформаційного суспільства, де культивується та зміцнюється інтелектуальний потенціал, розвивається критичне мислення та плюралізм поглядів, а також зберігалися культурні, моральні та історичні основи національної ідентичності [123].

Для держави забезпечення інформаційної безпеки передбачає підтримку інформаційного суверенітету, розвиток науково-технічного потенціалу, інтеграцію в глобальний інформаційний простір, створення конкурентоспроможних інформаційних продуктів і технологій, а також захист

національних інтересів від монополій, шпигунства, інформаційної злочинності та тероризму. Ефективна імплементація цих заходів є ключовим аспектом суверенітету та стратегічного розвитку держави.

У перехідному періоді до демократії в Україні можуть виникати складнощі через недостатнє усвідомлення взаємозв'язку між різними аспектами інформаційної безпеки та необхідністю комплексного підходу. Суспільство часто покладає відповідальність за інформаційну безпеку виключно на державу, недооцінюючи участь громадянського суспільства та приватного сектора.

Для ефективного розв'язання інформаційних конфліктів влада повинна цінувати громадські ініціативи та інноваційні рішення від науковців та аналітиків. Розширення діалогу та співпраці між державними органами і громадянським суспільством сприятиме демократизації та модернізації в сфері інформаційної безпеки, посилюючи соціальну єдність та зміцнюючи довіру в суспільстві. Політичній еліті України потрібно розробити більш стратегічний і систематичний підхід до інформаційної безпеки, залучаючи до процесу широке коло зацікавлених сторін.

Вибір інструментів інформаційної політики має важливе значення, оскільки впливає на взаємодію між державою та громадянським суспільством і на ефективність відповіді на зовнішні та внутрішні виклики. Місцеві дослідники наголошують на необхідності диференціації між політичними та інформаційними складовими безпеки, підкреслюючи потребу в цілісному підході.

Заходи в рамках інформаційної політики включають комунікаційні ініціативи, обмін інформацією, переговори, освітні заходи та інформаційну підтримку ключових політичних процесів. Важливо створювати умови для неупередженого інформування громадськості про актуальні проблеми, забезпечуючи відкритість інформації та розширення каналів для представлення державної позиції на міжнародному рівні.

Доповнення політичних ініціатив правовими, економічними та технічними заходами є важливим для створення мультидисциплінарної системи

захисту, здатної протистояти інформаційним загрозам. Така система сприяє стабільності, розвитку інформаційного суспільства та зміцнює довіру між державою і громадянами. Інтегрований підхід передбачає активне залучення всіх зацікавлених сторін у формування та виконання інформаційної політики, забезпечуючи комплексну інформаційну безпеку.

Дослідники, включаючи О. Федорука, розглядають роль держави в системі інформаційної безпеки як забезпечення нормативно-правового регулювання управління державними інформаційними ресурсами, розробку та впровадження фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів, забезпечення цілісності створення первинних і похідних інформаційних ресурсів, та інші [118].

У цьому інтегрованому підході до інформаційної безпеки особливе місце займають соціальні та політичні інтереси, ресурси, а також механізми влади, які є центральними категоріями в аналітичному полі сучасної політичної науки. Ці елементи лежать в основі стратегічного формування та реалізації інформаційної політики, спрямованої на реагування на сучасні виклики, захист національних інтересів у контексті глобалізації та інформаційної конкуренції.

Культурні цінності та засоби відіграють ключову роль у формуванні підходу до розуміння інформаційних ресурсів і безпекових стратегій сучасних держав. Культурний контекст впливає на сприйняття інформації суспільством, методи її розповсюдження та захисту, сприяючи формуванню ідентичності та загальноприйнятих цінностей. Це є фундаментом для соціальної згуртованості та здатності суспільства ефективно протистояти інформаційним загрозам.

Залучення державних органів, місцевого самоврядування та державних підприємств до вирішення проблем в інформаційному просторі є ключовим елементом цієї стратегії. Це включає своєчасне реагування на інформаційні виклики та створення позитивного інформаційного середовища, що сприяє демократизації, підтримці громадянського суспільства та формуванню відкритої, відповідальної влади.

Інформаційна безпека перевищує рамки захисту від зовнішніх загроз, охоплюючи зміцнення внутрішніх демократичних основ, зокрема свободи вираження поглядів, доступу до інформації та розвитку культурної та інформаційної диверсифікації. Реалізація такого підходу вимагає відповідальності, відкритості до діалогу та співпраці, а також розробки інноваційних методів захисту та підтримки інформаційного середовища.

Процеси інформатизації, включаючи цифровізацію та інтеграцію інформаційних технологій у всі сфери суспільного життя, пропонують значні виклики та нові можливості для зміцнення безпеки. Відкрите обговорення цих аспектів із залученням українських науковців, моральних лідерів та інтелектуалів є ключовим для розробки ефективної стратегії інформаційної безпеки.

Залучення експертної спільноти до формування стратегічних напрямків і рішень забезпечує високий рівень якості та компетентності підходів, їх актуальність та відповідність сучасним викликам. Інтеграція різноманітних думок і перспектив сприяє глибокому аналізу проблем і можливостей, що стоять перед державою у контексті інформаційної безпеки, створюючи більш збалансовану та ефективну політику.

Активна співпраця між державою та науковою спільнотою відіграє вирішальну роль у розробці ключових політичних, економічних, соціальних та військових стратегій. Ефективна взаємодія з науковою спільнотою підвищує здатність держави протистояти інформаційним загрозам та підтримує розвиток інформаційної інфраструктури, створюючи відкритий, безпечний та доступний для всіх інформаційний простір.

Також існує велика потреба у фахівцях з сучасних систем сертифікації програмного та апаратного забезпечення, впровадження стандартизації, побудови національних баз даних, розвитку телекомунікаційних систем та забезпечення безпеки праці в глобальному інформаційному просторі [97].

Стратегічне усвідомлення ролі освітніх, культурних та наукових установ, що перебувають під егідою держави, є ключовим для забезпечення

інформаційної безпеки та розвитку національного контексту. Ефективна система інформаційної безпеки повинна опиратися на міцний ціннісний фундамент і чітко визначені концептуальні рамки, які значною мірою залежать від інституційної ефективності цих закладів.

У дебатах про ціннісні орієнтири та політичні стратегії часто пріоритет надається політичним ідеологіям, а не культурним або науковим установам. Значимість політичної волі держави, орієнтованої на розвиток і підтримку інформаційного та гуманітарного просторів, стає вирішальною. Це підкреслює необхідність переосмислення та розширення політичних стратегій, що включають підтримку освітніх, культурних та наукових інституцій як фундаментальних елементів для створення стійкої та ефективної системи інформаційної безпеки.

Публічний простір, що включає медійні структури, політичні партії, громадські об'єднання, а також державні, культурні та релігійні інституції, відіграє важливу роль у формуванні громадської думки, базових прав та свобод, плюралізму та незалежності висловлювань. Еволюція українських цінностей і культурного контексту є ключовою для морально-ідеологічної стабільності та національної безпеки.

Основні виклики розвитку цінностей та культури включають відсутність інтегрованої системи інформаційно-аналітичного забезпечення у державному управлінні, зниження інтелектуального потенціалу, недоліки в освітній системі, обмежену ефективність економічного розвитку та відставання в соціальній стратифікації. Критично важливим є низький рівень розвитку інформаційної інфраструктури, що обмежує здатність країни конкурувати на міжнародному ринку інформаційних послуг.

Інформаційна експансія з боку зарубіжних держав, особливо великих країн, потребує ретельної уваги. Розвиток інформаційної інфраструктури може сприяти внутрішньому зростанню, але існує ризик впливу іноземних корпорацій на національний ринок інформаційних послуг. Сучасні методи проникнення міжнародними та внутрішніми злочинними організаціями

вимагають систематизованого контролю та відповіді. Держава і суспільство повинні бути готові ефективно протидіяти такому втручанню.

На державному та суспільному рівнях орієнтація інформаційної безпеки на захист у сфері інформаційного простору може призвести до дезорієнтації та дезінформації населення та представників влади. В умовах збройної агресії та інформаційної війни проблематика інформаційної безпеки стає все більш актуальною, вимагаючи адаптивних і прогнозованих стратегій для забезпечення національної стабільності та суверенітету.

Розробка та оптимізація національної стратегії в галузі інформаційної безпеки є важливою для захисту національних інтересів, особливо в умовах існуючої нестабільності в державній ідеології та суспільних розбіжностях. Визначення системи національних інтересів, яка охоплює матеріальні та духовні цінності, і її інтеграція у суспільну свідомість без провокування внутрішньополітичних, ідеологічних конфліктів чи економічної нестабільності є ключовою для забезпечення цілісності та стабільності України.

Держава несе відповідальність за безпеку громадян у всіх сферах життя, регулює суспільно-політичні відносини у контексті національної безпеки та визначає стратегічні напрямки діяльності своїх органів. Важливо також створення та оновлення структур, що забезпечують національну безпеку, розробка стратегій взаємодії між відповідальними суб'єктами та забезпечення цивільного демократичного контролю над управлінням національною безпекою.

У контексті інформаційного простору розрізняють дві основні форми державного регулювання і контролю над медіа: прямий і непрямий. Прямий контроль поділяється на ex-ante (до публікації) та ex-post (після публікації). Ex-ante контроль переважно застосовується в умовах диктатур, тоді як ex-post контроль широко використовується в демократичних державах через судові та інші процедури. Непрямий контроль включає використання економічних важелів для впливу на медіа без прямої цензури.

Регулятивна функція залишається ключовою в діяльності державних інституцій, що прагнуть захистити суспільство від небажаного ідеологічного

впливу. Однак, ефективність такого контролю є обмеженою у формуванні внутрішньої системи цінностей держави. Інтеграція правових та політичних механізмів з культурними цінностями та методами є перспективним підходом.

Оновлення існуючих доктринальних підходів є критично важливим, враховуючи, що попередні версії не завжди відображали потреби сучасного суспільства. Реформування доктрин має стати відповіддю на сучасні виклики, забезпечуючи адекватний розвиток у відповідності до динамічних змін у глобальному та національному контекстах.

Згідно з прийнятим рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року, яке було ухвалено Указом Президента України № 685/2021 від 28 грудня 2021 року, нова "Стратегія інформаційної безпеки України" набула чинності [112].

Одним із основоположних принципів нової стратегії є диференціація та взаємовизначення життєво необхідних інтересів індивіда, суспільства та держави, що складають національні інтереси України в інформаційному просторі. Це сприяє створенню балансу між особистими правами, суспільним благом та державною безпекою, що є ключовим для ефективного управління інформаційним простором. Врахування та гармонізація цих інтересів створюють стійку основу для розвитку інформаційного суспільства.

Громадські організації, державні структури та громадські ініціативи відіграють важливу роль у формуванні та реалізації національної стратегії інформаційної безпеки. Їх активна участь забезпечує обговорення, визначення пріоритетів та врахування різних точок зору, що збагачує стратегію реальним досвідом. Це дозволяє адаптувати законодавчу базу, політику та заходи до змінних умов цифрового світу. Залучення широкого кола учасників до формування інформаційної безпеки зміцнює національну стратегію та її відповідність сучасним викликам.

Сфера інформаційної безпеки вимагає глибокого аналізу в контексті збільшення комунікаційних потоків, технологічного прогресу та зміни життєвих цінностей. Глобалізація та технологічний розвиток збільшили економічну,

політичну та культурну інтеграцію, але цифровізація суспільства впливає на громадянські ініціативи через онлайн-агресію та спроби дестабілізації. Розвиток громадянської ініціативи в умовах цифрового суспільства є складним процесом, що вимагає виваженого підходу до технологічних інновацій і ризиків.

Законодавство надає громадянам можливість взаємодії з державою через вибори, референдуми та структури місцевого самоврядування, сприяючи вираженню національних інтересів. Ці механізми підвищують рівень громадянської свідомості та зміцнюють демократичні основи суспільства. Різноманітні форми громадянської активності, зокрема участь через громадські організації, відіграють вирішальну роль у формуванні сфери національної безпеки, сприяючи більш відкритому та адаптивному підходу до вирішення викликів.

Громадянська участь у визначенні та імплементації політик в сфері інформаційної безпеки забезпечує всебічний підхід до управління інформаційним простором. Інформаційний простір, за концепцією Л. Абрамова і Т. Азарової, охоплює різноманітні рівні взаємодії, створюючи мережу для постійного обміну інформацією. Важливою є участь громадських організацій у формуванні, сприйнятті та поширенні інформації, що підвищує інформаційну культуру та готовність до взаємодії.

Інформаційний простір не обмежується лише людською взаємодією, але включає територіальні, просторові, технологічні та економічні аспекти. Інформаційний простір стає всеосяжним, переплітаючись з різними сферами життєдіяльності. Акцент на індивіда як центральну фігуру в інформаційному просторі підкреслює його важливість у сучасному світі, де інформація є ключовим ресурсом у процесах управління, освіти, комунікації та соціального розвитку.

Дослідники виділяють три основні функції інформаційного простору: інтегративну, комунікативну та геополітичну. Інформаційний простір консолідує індивідів, спільноти, державні та корпоративні суб'єкти, сприяє транснаціональній взаємодії та переосмислює традиційні поняття

міждержавних відносин. Обмеження розуміння інформаційного простору лише територіальними межами є недостатнім, важливо враховувати комплексний спектр політичних суб'єктів, акторів та ресурсів для забезпечення національних інтересів.

Є позиція дослідників, які класифікують суб'єкти інформаційного простору на державні та недержавні категорії. В цьому контексті значну увагу приділяється ролі недержавних суб'єктів інформаційної діяльності, які відіграють ключову роль у конфігурації інформаційного поля. Недержавні інформаційні агентства та організації формують інформаційні сервіси, діяльність яких здійснюється в рамках існуючих нормативних вимог.

Також важливу роль відіграють "недержавні установи, служби і центри зі збору, зберігання, аналізу та розповсюдження важливої соціальної інформації", а також "спеціалізовані галузеві та міжгалузеві установи та центри (публікації, банківська інформація, довідкова інформація тощо)" [60].

Науковий, літературний та художній доробок, інноваційна діяльність та мистецькі практики визнаються ключовими елементами, що формують структуру інформаційного простору.

Не менш суттєвою є роль культурно-освітніх інституцій, таких як бібліотеки, музеї та клуби, які служать важливими центрами інформаційної активності.

Прогнозується, що державні структури відіграватимуть вирішальну роль у сфері інформаційного простору, зокрема, зосереджуючи зусилля на захисті від інформаційних втручань. Паралельно, громадяни розглядаються як ключові учасники у процесах розроблення політик, прийняття рішень та формування законодавства, що підкреслює необхідність їхньої активної інволюції у ці процеси.

Науковці також розглядають громадські організації як універсальних посередників між суспільством та державою, які представляють різноманітні суспільні інтереси та допомагають вирішувати соціальні проблеми [17].

Громадські організації та рухи конституюють суттєвий елемент соціальної структури, виконуючи не лише роль інформаційної підтримки для громадян і виявлення суспільних проблем, але й активно втілюють заходи, спрямовані на їх вирішення та мобілізацію громад у напрямку спільної мети.

На сучасному етапі громадські організації та асоціації виступають важливими інструментами нагляду за діяльністю державних установ. Це питання знаходить широке відображення в правових документах різного рівня, включно з міжнародним, а також у наукових дослідженнях та громадських обговореннях, де воно розглядається через такі концепції, як "третій сектор", "організації громадянського суспільства", "неурядові організації" та "НУО".

У своїй дослідницькій роботі Матвічук звертає увагу на необхідність розмежування між поняттями "неурядові організації" та "недержавні організації", підкреслюючи, що поняття державного апарату не покриває всю сферу публічної влади.

Термін "неурядові організації" визначається як "формалізовані незалежні об'єднання громадян, які не переслідують мети отримання прибутку", основною метою яких є "реалізація колективних інтересів та захист колективних прав".

З такою перспективою, "неурядові організації" відрізняються від політичних партій, громадських об'єднань, органів місцевого самоврядування та некомерційних установ та організацій [17].

Неурядові організації (НУО) представляють об'єднання осіб, що функціонують на різних рівнях з неприбутковими цілями, охоплюючи діяльність від захисту прав людини до підтримки біженців, наукових досліджень та освітніх ініціатив. В Україні відбувається трансформація ролі політичних партій, які стають "партіями влади", інтегрованими з бізнес-інтересами, що зменшує їхню роль як репрезентативних громадських об'єднань. У цьому контексті активізація громадянського суспільства через НУО стає важливою для зміцнення демократичних процесів.

Активна участь громадян і НУО в політичному житті сприяє демократизації, легітимності державного управління, боротьбі з корупцією та

запобіганню кризам. О. Корнієвський підкреслює важливість внеску НУО у вирішення соціальних проблем та підвищення ефективності державної політики. Недостатня активність громадського сектору може спричинити згортання демократичних процесів та стагнацію розвитку.

Громадянська участь у процесах ухвалення рішень забезпечує підвищення ефективності державних рішень. НУО сприяють медійному плюралізму, незалежності та соціальному розвитку, допомагаючи розбудові демократичного суспільства. Вони відіграють ключову роль у забезпеченні представництва місцевих інтересів, особливо в умовах децентралізації. Їхня діяльність варіюється від критики державних ініціатив до активної співпраці з урядом.

Громадянська активність сприяє формуванню нового соціального контексту, де інформаційний простір є фундаментальною складовою. Учасники комунікаційних процесів використовують інформацію як ресурс для впливу, що може призводити до маніпуляцій. Тому важливо забезпечити прозорість та об'єктивність в інформаційному просторі.

Інформаційний простір розглядається як комплексна система, де учасники конкурують за вплив, що ускладнюється динамічністю сучасного світу. Важливість інформації визначається її сприйняттям та інтерпретацією учасниками комунікації. Вони використовують інформацію для формування суспільних настроїв та політичних переконань.

НУО відіграють важливу роль у політичних процесах, забезпечуючи демократизацію та нагляд за державними органами. Їхній вплив може бути як безпосереднім, через участь у виборчих кампаніях та адвокації інтересів, так і непрямим, через участь у міжнародних асоціаціях. Непрямий вплив включає моніторинг державної діяльності, надання консультативних послуг та вплив на формування національної політики.

Активність НУО є важливою для забезпечення рівноваги інтересів, підтримки національної безпеки та сприяння демократичному прогресу. Вони забезпечують створення незалежних інформаційних ресурсів, підвищують громадську обізнаність та сприяють критичному аналізу інформації. Таким

чином, НУО відіграють фундаментальну роль у зміцненні інформаційної грамотності та розвитку суспільної обізнаності в контексті національної безпеки.

Зростає значущість компетентності неурядових організацій (НУО) у взаємодії з державними структурами для забезпечення інформаційної безпеки. Це включає розробку методологій аналізу даних, ідентифікацію кіберзагроз та співпрацю з міжнародними партнерами у сфері безпеки. Ефективне партнерство з міжнародними НУО для створення безпекових мережевих просторів стає пріоритетним завданням. Аналітичні центри набувають стратегічного значення у поширенні верифікованої інформації та боротьбі з дезінформацією, особливо під час воєнних дій.

У виборчих кампаніях НУО відіграють вирішальну роль у формуванні інформаційної політики, сприяючи балансу між інтересами політичних еліт та соціальних страт. Вони забезпечують активізацію громадського сектору, що сприяє стабілізації та гармонізації суспільних відносин. Участь НУО у виборах дає змогу ефективно впливати на суспільні динаміки та сприяти прогресу у сфері демократії. Хоча попит на інформаційні продукти НУО ще не сформований повністю, їх значення у зміцненні виборчого процесу постійно зростає.

Ефективна взаємодія між державними органами та НУО є ключовою для формування позитивного сприйняття влади та залучення громадян до управління державними і суспільними ініціативами. Використання інформаційних ресурсів НУО може значно покращити ефективність виборчого процесу, забезпечити його прозорість та відповідність демократичним стандартам.

НУО також відіграють важливу роль у моніторингу виборчих процесів, проведенні освітніх кампаній для виборців, аналізі діяльності виборчих комісій та забезпеченні методичної підтримки членів виборчих комісій. Вони сприяють оскарженню порушень виборчого законодавства, зміцнюючи демократичні процеси та підвищуючи рівень громадянської відповідальності.

Інформування міжнародної спільноти, реалізація екзит-полів та моніторинг виборчих процесів є ключовими для забезпечення стабільності в соціально-політичних процесах. НУО організовують інформаційні кампанії для стимулювання реєстрації виборців та спостереження за порушеннями виборчих прав, забезпечуючи чесні та відкриті вибори.

Діяльність НУО в Україні зосереджена на контролі за виборчими процесами, забезпеченні чесності та прозорості виборів, сприянні політичній конкуренції та формуванні суспільного порядку денного. Вони впливають на зміст передвиборчих програм політичних партій та перевіряють виконання виборчих обіцянок після виборів, сприяючи зміцненню демократичних інституцій та відповідальності політичних акторів перед виборцями.

З іншого погляду, громадські організації, які захищають суспільно значущі інтереси, все частіше використовують політичний тиск на владу та мають вагомий вплив на формування політичних рішень. Вони стали важливими учасниками політичного процесу разом з державними структурами та іншими політичними акторами [119].

В останні роки мережеві структури стали популярними у виборчих штабах на місцевому та регіональному рівнях, використовуючись для розповсюдження як позитивної інформації про кандидатів, так і негативної про їхніх суперників. Це демонструє стратегічний підхід до інформаційної війни, де динаміка поширення інформації є вирішальною.

Громадські організації можуть використовуватися як інструменти політичних стратегій, підтримуючи певні політичні інтереси через цілеспрямовані кампанії та пропаганду. Деякі з них починають як незалежні ініціативи, але з часом стають політичними силами. Водночас, незалежні дослідницькі ініціативи, що аналізують виборчий процес та виробляють аналітичні звіти для державних структур, відіграють важливу роль у формуванні інформаційної політики та підвищенні обізнаності суспільства.

Громадські організації, що забезпечують чесні і прозорі вибори, є ключовими агентами демократизації та зміцнення політичної стабільності.

Вони сприяють довірі громадян до виборчого процесу, легітимності владних інститутів та підвищенню якості демократії. Вони також забезпечують вільне обговорення та критику виборчого процесу, надаючи громадянам інструменти для активної участі в політичному житті.

Завдяки українському виборчому законодавству, громадські організації можуть брати участь у виборчому процесі як офіційні спостерігачі. Їхня присутність на виборчих дільницях та засіданнях виборчих комісій сприяє законності, прозорості та чесності виборів, захищаючи права виборців та забезпечуючи загальну чесність виборів.

Активізація громадських організацій у виборчому процесі, особливо з використанням "чорної" реклами, дезінформації та маніпулятивних технологій, викликає серйозну стурбованість. Такі методи підривають довіру до виборчого процесу, знижують якість демократичного діалогу та ведуть до поляризації суспільства. Це перетворює політичну конкуренцію на деструктивну діяльність, що вимагає уваги з боку регуляторних органів, суспільства та міжнародної спільноти.

Важливо, щоб громадські організації, які прагнуть сприяти демократичному розвитку, відстоювали принципи чесності, прозорості та відповідальності у своїй діяльності, а також сприяли зміцненню інститутів громадянського суспільства та довіри до них. Забезпечення відповідальної комунікації та використання перевіреної інформації, а також протидія поширенню дезінформації і маніпуляцій повинні стати пріоритетами для усіх учасників політичного процесу.

Особливу увагу приділяється тому, що така діяльність може завдати шкоди національним інтересам та національній безпеці України [85].

Серед ключових викликів сучасності є проблема розмежування конспірологічних ініціатив, ініційованих деякими громадськими об'єднаннями, від легітимних адвокаційних заходів. Це складно, адже часто ці феномени розділяє тонка грань. Особливу увагу привертають "квазі-громадські

організації", що спотворюють основоположні принципи демократичної конкуренції та колективної активності.

Дослідження Інституту стратегічних досліджень показують, що в перехідних суспільствах часто створюються штучні структури масової підтримки політичних лідерів, які маскуються під громадські організації. Мануель Кастельс зазначає, що в сучасному суспільстві реальність і віртуальний світ переплітаються, де віртуальні образи можуть заміняти реальний досвід.

Інформаційні технології дозволяють громадським організаціям маніпулювати виборчим процесом, використовуючи інтернет для анонімних дебатів та оцінки громадської підтримки. В умовах мережевого суспільства індивіди стають вузлами складної конфігурації, де кожен вузол впливає на загальну структуру. Сучасні соціальні феномени, такі як "мережеві протести" та "твіттер-революції", підтверджують важливість інтернет-технологій у мобілізації громадських протестів.

У контексті української політичної реальності виокремлюються кілька ключових форм активності організацій громадянського суспільства (ОГС) у виборчому процесі:

1. Трансформація ОГС у політичні партії та блоки.
2. Колаборація ОГС з політичними партіями або лідерами.
3. Участь ОГС у виборах як офіційних спостерігачів.
4. Громадський моніторинг прозорості виборчого процесу.
5. Захист прав людини у виборчому процесі.
6. Освітня діяльність щодо виборів.
7. Аналітична робота, оцінка програм політичних партій.

Ці напрямки діяльності відображають різні шляхи впливу на виборчий процес та сприяння розвитку демократичних ініціатив. ОГС забезпечують прозорість, легітимність та посилення демократичних процесів, розширюючи вплив громадян на виборчі механізми та рішення. Вони активно взаємодіють з владою, пропонуючи стратегії для подолання викликів.

У країнах з розвинутою демократією ОГС мають значний вплив на політичні, економічні, культурні та освітні аспекти, контролюючи та представляючи інтереси громадян. Вони сприяють вирішенню соціальних, економічних, екологічних та освітніх проблем, підтримуючи духовну гармонію особистості. Дослідник Д. Коулман називає можливість взаємної довіри та підтримки "соціальним капіталом".

Сучасні дослідження підтверджують, що інформаційно-комунікаційні технології підвищують ефективність управління, захищаючи права громадян, залучаючи їх до прийняття рішень та забезпечуючи доступ до інформації про діяльність влади.

Водночас, інформаційні технології мають потенціал перетворити громадські організації на значущу політичну силу, залучаючи до спільної діяльності людей з однаковими переконаннями, стимулюючи індивідуальну активність та самоорганізацію в межах цих організацій.

Це підтверджує, що громадянське суспільство - це динамічна організація, що бореться за вплив на рішення влади та сприяє їх реалізації [11].

Враховуючи новітні можливості, які відкриває розвиток громадянського суспільства, необхідно рефлексувати на державну політику в цій сфері. Зокрема, ідея створення єдиного координаційного органу, що діятиме в рамках недержавної системи національної безпеки, представляє собою прогресивний крок.

Такий центр, в контексті української моделі, пропонується утворити під патронатом Ради національної безпеки і оборони України. Включення до складу Центру представників експертної спільноти з громадських організацій, аналітичних центрів та правозахисних груп дозволить сформувати міжсекторальну платформу для обміну досвідом, розробки та реалізації стратегій у сфері національної безпеки. Водночас, критичний аналіз потенційних ризиків такого рішення виявляє занепокоєння щодо створення додаткової інституції, яка може зіткнутися з викликами самостійності та ефективності в умовах комплексної інформаційної безпеки держави.

Така перспектива вимагає глибокого аналізу можливих механізмів взаємодії цього центру з існуючими органами влади та його ролі в загальній структурі національної безпеки, з метою оптимізації його функціональності та уникнення дублювання вже існуючих процесів.

Подальша співпраця недержавних організацій з органами влади може набувати різних форм, таких як громадські слухання, робота громадських та консультативно-дорадчих органів, реагування на звернення громадян, проведення семінарів, круглих столів, конференцій, громадських експертиз та впровадження механізмів громадського моніторингу [17].

В Україні спостерігається позитивний прогрес у сфері розвитку громадянського суспільства та демократичних ініціатив, проте існує вагома потреба в подальшому вдосконаленні правового регулювання, підвищенні кваліфікації кадрів та культивуванні культури демократії.

Актуальність даного дослідження акцентується на необхідності інформаційної підтримки різноманітних громадських ініціатив в контексті сучасного цифрового середовища. При цьому, важливо забезпечити належний доступ до інформації та інформаційних технологій для ефективної реалізації та просування цих ініціатив.

Особливе значення у високотехнологічному суспільстві набуває переорієнтація з матеріальних та фінансових ресурсів на інформаційні потоки та технології. Сектор інформаційних послуг виступає як один з лідерів зайнятості, підкреслюючи важливість комп'ютерних технологій та доступу до інформації як невід'ємних компонентів загального інформаційного прогресу. Це підтверджує необхідність забезпечення інформаційної підтримки як фундаментального елемента для розвитку суспільства та зміцнення демократичних процесів.

Також, політична комунікація набуває важливого інформаційного аспекту, а соціальна девіація може виникнути як результат маніпулювання інформацією. Тому, згідно з дослідженнями, багато форм громадської діяльності мають

амбівалентний характер, оскільки їх розвиток і вплив формуються і виявляються в інформаційному просторі суспільства [87].

З поширенням комп'ютерних мереж виникає новий вид загрози для національної інформаційної безпеки, пов'язаний з діяльністю мережевих спільнот. Ці спільноти здатні впливати значно сильніше, ніж традиційні громадські організації, завдяки інтеграції в активне громадське життя. Мережеві спільноти слугують платформами для соціальної взаємодії та формування суспільної ідентичності. Однак, важливо розглядати вплив віртуальних просторів на індивідів, громади та суспільство загалом.

Віртуальні спільноти мають потенціал як позитивно впливати на демократичні процеси та соціальну мобілізацію, так і нести ризики маніпуляції свідомістю, розпалювання конфліктів і порушення інформаційної безпеки. Тому забезпечення збалансованого підходу до регулювання цих спільнот, захисту прав індивідів та гарантування національної безпеки стає важливим завданням для держави та громадськості.

Ця ситуація має як позитивні, так і негативні аспекти. Розвиток інформаційного суспільства відкриває нові можливості для людського розвитку та інтеграції, але також існує ризик заміни реальності віртуальною, що впливає на формування ідентичності особистості.

Нові інформаційно-комунікаційні технології внесли суттєвий вклад у формування та розвиток віртуальних спільнот завдяки їх особливостям: інтерактивність, низька вартість, мультимедійність, асинхронність, глобальність та анонімність [119].

Сучасна політична практика та міжнародні комунікації ще не повністю використовують потенціал новітніх механізмів для ідентифікації спільних інтересів, вирішення конфліктів та розвитку взаєморозуміння між різними акторами. В Україні спостерігається активність соціально-мобілізаційного характеру з елементами деструктивної поведінки, організованої через соціальні мережі, громадські рухи, масові демонстрації та блокування інфраструктурних об'єктів.

Дослідники припускають, що віртуальні спільноти можуть виступати каталізаторами протестних рухів, створюючи ілюзію активності, яка відволікає від фізичних акцій протесту. Це може деформувати інтенції політичного протесту та обмежувати його ефективність. Тому важливо вдосконалювати медіаосвіту та інформаційну грамотність для розпізнавання загроз та критичного аналізу інформації.

Віртуальні спільноти мають двоякий потенціал: вони можуть консолідувати та об'єднувати, а також дезорганізувати та дестабілізувати. Вони можуть використовуватися для мобілізації підтримки політичних амбіцій, а також для поширення негативних ідеологій, що загрожують принципам державності.

Інформаційно-комунікаційні технології відкривають нові можливості та виклики. Розвиток медіаосвіти, критичного мислення та відкритого діалогу стають фундаментальними завданнями. Державні інституції повинні структурувати віртуальні спільноти, формувати ефективні реакції на загрози та розвивати регуляторні механізми.

Враховуючи потенціал громадянського суспільства, спонтанні ініціативи та неформальні групи можуть стати джерелом інноваційних рішень. Якість інформування громадськості має важливе значення для підвищення рівня політичної культури та громадянської свідомості.

Громадянські ініціативи, що надають достовірну інформацію, можуть подолати нігілізм, корумпованість та відчуття безсилля. Медіа відіграють вирішальну роль у формуванні громадської думки та політичної культури, сприяючи прозорості урядування та залученню громадян до активної участі у державному житті.

Здатність медіа надавати глибокий аналіз та об'єктивну оцінку подій стає основою для зміцнення державної стабільності. Медіа підтримують демократію, права людини та розвиток цивільного суспільства, сприяючи формуванню стійкого інформаційного простору.

Теоретики інформаційного суспільства, такі як Маршал Маклюен та Мануель Кастельс, акцентують на принципі загальнодоступності інформації. Важливо враховувати ці принципи для розвитку інформаційного суспільства та забезпечення інформаційної безпеки

Вони стверджують, що інформація, яка є життєво необхідною для функціонування суспільства, має бути вільно доступною, а медіа відіграють ключову роль у забезпеченні цього доступу.

Особливу увагу привертає концепція Маршала Маклюена, який визначає три історичні епохи розвитку комунікації: усну, письмову та аудіовізуальну. Маклюен особливо наголошує на значущості сучасних медіа, зокрема електронних, як характерної ознаки аудіовізуальної епохи. Він вважає, що електронні медіа кардинально змінили спосіб, яким люди сприймають світ навколо, віддаючи перевагу візуальному та аудіальному сприйняттю [31].

Маршал Маклюен акцентує на зростаючій значущості каналів комунікації у процесі передавання повідомлень. Він аргументує, що сутність комунікаційного процесу криється не стільки в змісті повідомлення, скільки у формі його передачі, яка, в свою чергу, організовує та керує патернами людської взаємодії та поведінки.

За Маклюеном, саме метод комунікації слід розглядати як "зміст", оскільки він визначає характер інформації, яка передається через інші комунікативні канали як "зміст". Таке твердження розкриває, як медіа формують свідомість і поведінкові реакції людей, стаючи розширенням людських сенсорних та емоційних функцій. [31].

Маршал Маклюен розрізняє "гарячі" та "холодні" медіа на основі їх впливу на сенсорну систему. "Гарячі" медіа характеризуються високою визначеністю і надають значний обсяг інформації одному сенсору, зменшуючи активність сприймача. "Холодні" медіа, навпаки, мають нижчу визначеність і вимагають активного сприйняття та використання додаткових сенсорів. Маклюен аргументує, що епоха електронних медіа характеризується станами несвідомості та автоматизованих реакцій у споживачів інформації.

Алвін Тоффлер у своїх роботах "Вплив на майбутнє", "Третя хвиля" та "Трансформація влади" розглядає еволюцію медіа через призму трьох хвиль розвитку суспільства. У першій хвилі (аграрно-орієнтоване суспільство) переважала комунікація в межах невеликих груп. Друга хвиля (масове виробництво) розширила комунікаційні можливості на значні відстані, сприяючи розвитку традиційних масових медіа. У третій хвилі (постмасове виробництво) комунікація стає більш різноманітною, медіа стають посередниками у передачі ширшого спектру образів та ідей, а аудиторія диференціюється на численні сегменти.

Тоффлер підкреслює, що нові мережеві структури збільшують доступність вибору для споживачів медіаконтенту, що має вагомі політичні імплікації, змінюючи політичну динаміку та владні відносини. Він також відзначає конвергенцію медіа, яка перетворює медійний ландшафт у єдину систему, що впливає на глобальні соціальні структури.

Мануель Кастельс у своїй праці "Інформаційна епоха: економіка, культура і суспільство" пропонує поняття "медіакультури" та "культури справжньої віртуальності". Він розглядає медіа як засіб трансформації реальності і підкреслює важливість активної ролі реципієнта у комунікаційному процесі. Кастельс наголошує, що комп'ютерні мережі сприяли децентралізації процесу передачі інформації, відкриваючи шлях для двосторонньої взаємодії.

Сучасні дослідження підтверджують, що Інтернет забезпечує інтеграцію тексту, аудіо, зображень та відео, виходить за рамки одностороннього звернення і дозволяє персоналізувати контент. Інтернет створює умови для обходу традиційних маніпуляцій та протидії пропаганді, забезпечуючи доступ до різноманітних точок зору.

Розвиток нових медійних технологій стимулює активну участь громадян у суспільно-політичному житті. Концепція кібердемократії, зокрема, ґрунтується на уявленні кіберпростору як платформи для взаємодії між громадянами, громадськими організаціями та державними інститутами, що впливає на

модернізацію політичних процесів та створення нових форм демократичної взаємодії.

"Е-демократія" передбачає активну політичну участь громадян у процесах ухвалення державних рішень. Важливо зазначити, що в сучасних політичних практиках сутність е-демократії зосереджена на використанні інформаційних технологій для активізації громадян у демократичних процесах, включаючи ухвалення рішень та вплив на державну політику. Такий підхід сприяє розширенню доступу до демократії та сприяє більш прозорій взаємодії між громадянами, громадськими структурами та державними установами. Це виявляється в застосуванні інформаційно-комунікаційних технологій (ІКТ) у виборчому процесі, проведенні електронних референдумів та наданні доступу до інформації та публічних консультацій. Практично мова йде про перехід від системи представницької демократії до її віртуальної форми в кіберпросторі [31].

У контексті культури віртуальності спостерігається значний вплив на політичний процес. В академічній літературі існує консенсус щодо того, що політика набуває характеристик "медіатизації", тобто її формування та викладання все більше залежать від медійних технологій та логіки.

Водночас, політичний дискурс і взаємодія між політичними акторами і громадськістю відбуваються в умовах "віртуалізації" політичного простору, де цифрові технології та платформи стають основним майданчиком для політичних дебатів, кампаній та голосувань.

Дослідники наголошують, що медіатизація політики має негативні наслідки, такі як зміна системи представництва громадянських інтересів під впливом медіа, перетворення політики в медійний процес, створення "гіперреальності" політики та медіа, що у свою чергу призводить до явища медіакратії [130].

Також підкреслюється, що віртуалізація політичного простору, яка виражається в переплетінні реальності та фікції, підриває основи раціональної

політичної орієнтації та спричиняє появу елементів скептицизму та цинізму серед людей [31].

Згідно з поглядами А. Дюрнера, політична культура інформаційного суспільства включає в себе "культуру політичних розваг", яка за допомогою створюваного нею утопічного світу дозволяє користувачам медіа та ІКТ спрощено сприймати, інтерпретувати та сприймати політичну реальність [30].

Ця спрощена реалізація політичних подій значно полегшує контроль над політичною поведінкою осіб. Реакції на політичні події стають штучно конструйованими, і люди, які не розуміють своїх справжніх інтересів, приймають участь у політичних акціях, що були вигадані іншими [31].

Загалом, наше попереднє дослідження показало, що прогнози і погляди вищезгаданих провідних теоретиків інформаційного суспільства, а також дослідження багатьох їхніх наступників у всьому світі, дозволяють виділити спільні риси сучасної масової комунікації:

1. Збільшення кількості та сфери застосування нових медіа.
2. Зростання можливостей двостороннього та багатостороннього обміну інформацією, а також перехід від моноцентричної моделі традиційних медіа до мультицентричної.
3. Швидке розширення можливостей та сфери застосування нових медіа.
4. Зростаюча персоналізація інформації, більш швидке, цілеспрямоване та широке її розповсюдження.
5. Зростаюча віртуалізація соціальної реальності через вплив медіа.
6. Зростаюча здатність медіа до маніпуляцій та мобілізації [31]

У контексті інформаційного суспільства, медіа займають центральне місце, пронизуючи всі аспекти людського життя. Однак, критично важливо усвідомлювати, що існує ризик надмірної атрибуції медіа ролей, які традиційно приписуються іншим інституціям суспільства.

Таке перевищення меж може призвести до ситуації, де медіа виступають як нібито голос громадської думки або намагаються виконувати функції, що

належать державним органам, освітнім чи культурним установам, що може спотворювати їхню первинну місію і впливати на об'єктивність і баланс інформації.

Це може перетворити медіа на органи влади або їхні антагоністи (медіадемократію) [31].

Робота медіа повинна бути сприянням інформаційних послуг, а їхні права, пов'язані зі свободою інформації, залежать від громадян - отримувачів цих послуг [30].

Ці умови підкреслюють вагомість нагляду соціуму та держави за медійною сферою, а також необхідність формування та реалізації державної інформаційної політики в багатьох країнах світу. Українське законодавство відносно медіа покликане забезпечувати свободу їхньої діяльності та протидіяти будь-яким формам зловживань цією свободою.

Закон визначає правові, економічні, соціальні та організаційні рамки для функціонування медіа, встановлює процедури реєстрації та ліцензування аудіовізуальних медіа. Він закріплює права журналістів, редакторів, видавців, дистриб'юторів (для друкованих медіа та інформаційних агентств), а також права і обов'язки медійних організацій та їх аудиторії (для електронних медіа), окреслює відповідальність за порушення медійних свобод. Ці норми та положення відображені у Законі "Про інформацію", який виступає проти цензури.

Основні принципи державної політики у сфері медіа включають:

1. Держава гарантує умови для розвитку та захисту медійної сфери.
2. Політика держави спрямована на гарантування доступу громадян до широкого спектру інформації та культурних продуктів.
3. Держава підтримує незалежність інформаційних агентств, захищаючи їх від зовнішнього впливу.
4. Підтримка мовлення національних меншин і використання регіональних мов у медійному контенті.

5. Гарантування можливості безперешкодного прийому телерадіопрограм з інших країн.

6. Запобігання монополізації медійного простору та захист від фінансового чи політичного тиску.

7. Забезпечення права на доступ до інформації та підтримка відкритого обговорення суспільно значущих питань.

Ці принципи сприяють створенню здорового інформаційного середовища та розвитку демократичного суспільства.

Закон України "Про медіа" забезпечує прозорість і відкритість діяльності державних органів у взаємодії з громадськістю та медійним середовищем, а також гарантує свободу журналістських розслідувань. Це відображає основні принципи демократичного суспільства, де право громадян на інформацію є ключовим для забезпечення прозорості та ефективності державного управління.

Правове регулювання діяльності медіа в Інтернеті є актуальним через стрімкий технологічний розвиток, що породжує нові виклики для законодавства та захисту прав громадян. З огляду на значний вплив інтернет-медіа на поширення інформації, виникає потреба у їх адаптації до сучасних умов. Це завдання вимагає збалансованого підходу, що поєднує свободу слова та право на інформацію з необхідністю захисту від неправдивого контенту. Аналіз досвіду інших держав і врахування потреб сучасного інформаційного суспільства мають бути ключовими при розробці ефективних регулятивних механізмів.

Стаття 277 Цивільного кодексу України встановлює процедуру спростування інформації, що вважається недостовірною та завдає шкоди особистим або немайновим правам особи, а також правам членів її сім'ї. Відповідно до цього положення, особа, чиї права були порушені через поширення таких даних, наділена правом вимагати їх офіційного спростування [123].

Процес спростування інформації вимагає втручання особи, яка відповідає за поширення початкових даних. Проте, в контексті Інтернету, де значна частина

контенту може поширюватися анонімно, ідентифікація відповідального за публікацію стає складним завданням.

У ситуаціях, коли автор недостовірної інформації не може бути встановлений, четверта частина статті 277 Цивільного кодексу України дозволяє постраждалим особам ініціювати судовий процес з метою визнання інформації недостовірною та її подальшого спростування [123].

Це зумовлено тим, що в процесі спростування недостовірної інформації багато потерпілих осіб не лише прагнуть відновлення достовірності даних, але й прагнуть отримання компенсації за зазнану моральну та матеріальну шкоду. У сучасному інформаційному просторі поширення неправдивої інформації в інтернет-медіа представляє собою серйозний виклик для інформаційної безпеки суспільства. В цьому контексті, зростає необхідність у виявленні авторів неправдивих публікацій та збільшенні обсягу перевіреної та достовірної інформації.

Спільна дія громадських організацій, органів влади і медіа може сприяти розв'язанню цієї проблеми, забезпечуючи інформаційну безпеку та відповідальну роль медіа у формуванні громадської свідомості та цінностей [29].

Аналіз виявляє, що питання про роль медіа у поширенні інформації про правду, неправду та суперечності є частиною більш широкого роздуму про їхню функцію в суспільстві та державі.

Сучасна соціальна теорія пропонує два протилежних підходи, які відображають демократичну та авторитарну традиції [29].

У контексті сучасних медіа існує два фундаментальні підходи до розуміння їх ролі у суспільстві.

Перший, ліберальний підхід акцентує на ідеї, що медіа мають служити агентами публічної інформації, відображаючи всі значущі події та гарантуючи доступ до широкого спектру думок. Медіа в конкурентному середовищі несуть відповідальність за розповсюдження інформації різного ступеня достовірності, підкоряючись при цьому законам ринку.

Другий підхід орієнтований на соціально відповідальну журналістику, яка позиціонує медіа як інструмент підвищення моральних цінностей та свідомості громадян. Медіа виступають не лише як носії інформації, але й як каталізатори соціальних змін, активно впливаючи на формування громадської думки. Цей підхід часто зустрічається в суспільствах, де існує певний рівень державного контролю над медійним простором, і передбачає ключову роль держави у регулюванні інформаційного потоку.

Обидва підходи відображають різні візії взаємодії медіа, держави та суспільства, кожен з яких має свої переваги та недоліки щодо забезпечення прав громадян на інформацію, свободу слова та відповідальність перед суспільством.

З урахуванням цих двох підходів можна виділити моделі взаємодії медіа та держави:

1. Незалежна преса - ліберальний підхід, що підкреслює важливість надання громадянам вільного доступу до інформації без обмежень.
2. Соціально відповідальна модель - акцентує на обов'язках медіа перед суспільством, включаючи надання різноманітних точок зору та відкритість до критики.
3. Демократичне представництво - висуває заслуги медіа перед аудиторією та право окремих осіб та груп використовувати медіа для власної вигоди.
4. Радянська модель - медіа як агенти держави.
5. Авторитарна модель - медіа як інструмент державного контролю.
6. Модель розвитку - медіа, спрямовані на підтримку розвитку суспільства.

Перші три моделі належать до демократичної традиції, де медіа виступають агентами суспільства, тоді як інші три відображають авторитарний підхід, де медіа є агентами держави. Проте, навіть у країнах з ліберальними традиціями, таких як США, де право на інформацію гарантоване Конституцією, існують законодавчі ініціативи, що регламентують окремі аспекти поширення інформації. Водночас, соціально відповідальна модель вимагає від медіа

високого рівня професійної компетентності, точності, об'єктивності та збалансованості контенту.

Економічний контроль над медіа набуває не меншої значущості. В Україні з кінця 1990-х років спостерігається зростаючий контроль над медіа з боку великих бізнес-груп, що прагнуть політичного впливу та вигідних відносин із державною владою. Це створює потенційні можливості маніпуляції інформаційним простором з метою досягнення певних політичних цілей, що може суттєво вплинути на політичний ландшафт країни.

Такі недемократичні моделі, як радянська, передбачають сильний регуляторний та структурний контроль з боку держави. Вони абсолютизують концепцію соціально відповідальної журналістики та встановлюють жорстку систему цензури та санкцій проти неугодних поглядів. У таких моделях держава визначає правдиву інформацію, контролює зміст та використовує медіа для панування ідеології та політичного впливу. Україна мала досвід реалізації радянської моделі під час радянського періоду, коли держава здійснювала жорсткий контроль над медіа [29].

Авторитарна модель медіа базується на принципі, що медійні ресурси не повинні загрожувати стабільності існуючого режиму, а мають виступати як інструменти забезпечення інформаційної безпеки держави. Інформаційний контент у цій моделі суттєво контролюється фінансово-промисловими групами, що тісно взаємодіють з державним апаратом. Такий підхід був характерним для України наприкінці 1990-х — на початку 2000-х років, коли розвивалися різні форми цензури та контролю над інформаційним потоком.

Модель розвитку медіа, асоційована з країнами, що розвиваються, базується на принципі, що медійний простір має сприяти національному державотворенню. Свобода медіа тут може бути обмежена економічними пріоритетами та соціальними потребами суспільства, включаючи заходи, спрямовані на підтримку інформаційної безпеки, такі як цензура або обмеження на деякі види медійної діяльності.

У контексті сучасної України, яка стикається з інформаційною війною та негативним зовнішнім впливом, концепція обмеження свободи медіа може вважатися обґрунтованою для захисту національної ідентичності та інформаційної безпеки. Такі обмеження спрямовані на недопущення поширення неправдивої, дестабілізуючої інформації, що сприяє процесам депривації, денаціоналізації чи деморалізації у суспільстві.

Проблема обмеження свободи медіа викликає гострі дебати, адже право на інформацію та свобода слова є фундаментальними елементами демократичного суспільства. Знайти баланс між захистом інформаційної безпеки та забезпеченням прав громадян на доступ до інформації є складним завданням, що потребує обережного виважування та постійного аналізу.

Україна потребує динамічного балансу між двома підходами до регуляції медіа та держави. Модель соціальної відповідальності підкреслює важливість суспільної безпеки та підтримує демократичний характер взаємодії, дозволяючи медіа виконувати роль наглядача за діями влади та забезпечувати громадський контроль. Модель розвитку, що виправдовується національно-державними цілями, може мати менш демократичний відтінок через потенційне втручання держави в медійний простір та обмеження свободи слова в ім'я національних інтересів.

Таким чином, українське суспільство та державні органи зіштовхуються з необхідністю знаходження оптимальних рішень, які забезпечували б інформаційну безпеку країни без необґрунтованого обмеження основоположних прав та свобод громадян.

Цей напружений стан обумовлений необхідністю забезпечити не лише національну безпеку, але й цілісний національний інформаційно-культурний простір, без якого стає складною як національна політична єдність, так і формування національної ідентичності [29].

Перед Україною постає складне завдання розробки сучасної, збалансованої національної інформаційної політики, яка б враховувала потребу захисту національних інформаційних ресурсів та простору, забезпечуючи їх

правовий та адміністративний захист. Політика має також на меті оптимізацію управління національними інформаційними ресурсами, запобігаючи спробам інформаційної маніпуляції, які становлять серйозну загрозу національній безпеці.

Основне завдання національної інформаційної політики полягає в розробці та впровадженні нормативно-правового фундаменту, що регулюватиме інформаційні відносини, а також у створенні ефективної системи суспільного мовлення. Ці заходи спрямовані на усунення практик прийняття непрозорих рішень державними органами та на запобігання спотворенню інформації, що може бути нав'язано суспільству. Втілення цих принципів стане ключовим кроком до гарантування інформаційної безпеки країни та стимулювання вільного обміну ідеями, сприяючи розвитку демократії в Україні.

Ухвалений 17 квітня 2014 року Закон України "Про Суспільне телебачення і радіомовлення України" спрямований на встановлення незалежного суспільного мовлення, яке стоїть на захисті інтересів усього суспільства, а не лише обмеженої групи впливових політичних сил [103].

Відповідно до Закону України «Про Суспільне телебачення і радіомовлення України» (нині – Закону України «Про суспільні медіа України») [103], для поступового та послідовного розвитку суспільного телебачення і радіомовлення в Україні, Кабінет Міністрів України створює юридичну особу публічного права на базі декількох телерадіоорганізацій. Ця юридична особа називається "Національна суспільна телерадіокомпанія України" [29]. Основними завданнями цієї компанії є:

Забезпечення об'єктивного, повного, своєчасного та безпристрасного інформування про суспільно важливі події в Україні та за її межами.

Підтримка інтеграції українського суспільства.

Розвиток та зміцнення статусу української мови та культури, а також сприяння розвитку мов та культур національних меншин.

Забезпечення максимального задоволення інформаційних, культурних та освітніх потреб українського народу, включаючи виробництво та поширення різноманітних програм для різних соціальних груп.

Забезпечення своєчасного інформування населення у надзвичайних ситуаціях та загрозі життю та здоров'ю людини.

Забезпечення населення України інформаційною продукцією, якої немає на ринку.

Сприяння зміцненню міжнародного авторитету України [103].

Прийняття закону, який легалізує створення Національної суспільної телерадіокомпанії України, маркує значний прогрес у розвитку медійного ландшафту країни, відкриваючи шлях до забезпечення громадськості доступу до об'єктивної та різноманітної інформації.

Перехід від державного до суспільного мовлення ставить перед законодавчою владою складне завдання, адже суспільне мовлення повинне керуватися принципами, що відрізняються від тих, що є основою для державних та комерційних медіа.

В процесі розробки законодавства важливим виходить принцип, згідно з яким суспільне мовлення повинно бути орієнтованим на суспільні інтереси у своєму змісті, але мати державну підтримку у формальному аспекті. Це має на меті створення медіаплатформи, яка служить інтересам усього суспільства, надаючи якісний та збалансований контент без впливу комерційних чи політичних інтересів, при цьому забезпечуючи стабільність і незалежність мовлення завдяки державній підтримці.

Фінансування суспільного мовлення в Україні також є питанням обговорення. Закон передбачає фінансування Національної суспільної телерадіокомпанії України (НСТУ) з державного бюджету протягом перших чотирьох років [29].

Розширення джерел фінансування для суспільного мовлення, включаючи продаж телерадіопродукції, отримання роялті від авторських прав, добровільні

внески, благодійні внески та інші неурядові джерела, є ключовим аспектом забезпечення його стійкості та незалежності.

У багатьох країнах світу суспільне мовлення частково або повністю фінансується за рахунок громадських коштів, що дозволяє мінімізувати комерційний та політичний вплив на зміст мовлення.

У контексті України розглядається можливість переходу до такої моделі фінансування, що сприятиме створенню більш збалансованого та різноманітного інформаційного простору. Запровадження ширшого спектру фінансування може забезпечити додаткову підтримку суспільного мовлення, зробити його більш відкритим та доступним для широких верств населення, а також підвищити якість та різноманітність телерадіопродукції.

Наприклад, в Німеччині суспільне мовлення фінансується переважно за рахунок спеціального збору з глядачів, а також за рахунок реклами, спонсорства, продажу програм тощо [29].

Аналіз показує, що суспільне мовлення, яке фінансується безпосередньо громадянами або через публічні фонди, має тенденцію асоціюватися з високими стандартами правдивості, чесності, нейтральності та об'єктивності. Фундаментальна довіра між громадянами та суспільними мовниками відіграє ключову роль у підтримці інформаційної якості та об'єктивності, створюючи міцний фундамент для якісного інформаційного середовища.

В Україні дебати про фінансування суспільного мовлення віддзеркалюють складний вибір між забезпеченням незалежності від зовнішніх, зокрема державних та комерційних, впливів та необхідністю знайти стабільне джерело фінансування для підтримки високоякісного мовлення, що служить громадським інтересам.

Активна участь суспільства у процесі контролю за мовленням та інформаційним потоком є критично важливою для забезпечення об'єктивності та якості інформації. Громадяни, усвідомлюючи свою роль у цьому процесі, можуть ефективно відфільтровувати неправдиву та маніпулятивну інформацію, сприяючи тим самим інформаційній безпеці суспільства. Такий підхід сприяє

формуванню відкритого, збалансованого інформаційного середовища, в якому підтримується висока якість мовлення та дотримуються демократичні принципи.

Державна політика та правове регулювання грають важливу роль у забезпеченні інформаційної безпеки суспільства. Але не лише держава, а й самі медіа мають брати на себе відповідальність у цій сфері [29].

Системи добровільного саморегулювання у медійній сфері відіграють ключову роль у підтримці високих стандартів професійної поведінки журналістів, забезпеченні якості, точності та об'єктивності поширюваної інформації. Вони дозволяють медіа-спільноті самостійно вирішувати етичні питання та конфлікти, пов'язані з журналістською діяльністю, без втручання держави, сприяючи зміцненню професійних стандартів та підвищенню довіри громадськості до медійних продуктів.

Міжнародні документи та кодекси журналістської етики встановлюють загальноприйняті етичні стандарти для журналістської діяльності, акцентуючи на відповідальності медіа перед суспільством. Вони включають рекомендації щодо збалансованого висвітлення подій, перевірки фактів перед публікацією, уникнення конфлікту інтересів, поваги до приватності та гідності осіб, а також зобов'язання уникати дискримінації та мови ненависті.

Зважаючи на важливість інформаційної безпеки, де інформація може впливати на громадську думку, політичні процеси та соціальну стабільність, дотримання етичних стандартів журналістики стає основою для забезпечення довіри та захисту інтересів суспільства. Тому підтримка та поширення практик добровільного саморегулювання, а також дотримання міжнародно визнаних етичних принципів, є важливими аспектами у підтримці якості та об'єктивності журналістської роботи.

Прийняті на міжнародних конгресах Міжнародної федерації журналістів, кодекси етики та декларації принципів відзначають важливість працювати з правдивою та об'єктивною інформацією, а також звертають увагу на небезпеку підбурювання до дискримінації через медіа [29].

Відповідальне ставлення до журналістської професії та її впливу на інформаційну безпеку суспільства є надзвичайно важливим. Резолюції та рекомендації, прийняті Парламентською асамблеєю Ради Європи (ПАРЄ), підкреслюють необхідність дотримання відповідальної журналістики та етичних норм у медійній сфері. Вони наголошують на ролі медіа як інституцій, що несуть моральну відповідальність перед громадянами та суспільством, акцентуючи на зобов'язанні медійних організацій слідувати етичним принципам.

ПАРЄ висвітлює важливість збалансованого висвітлення подій, уникнення маніпулювання інформацією та обмеження свободи висловлювань, що сприяє захисту прав дітей, підлітків та інших вразливих груп населення. Дотримання високих моральних і етичних стандартів у журналістиці є основою для забезпечення інформаційної безпеки та збереження довіри громадян до медійних організацій. Це вимагає спільної відповідальності як медійних організацій, так і суспільства загалом.

Резолюції ПАРЄ акцентують на необхідності врахування впливу сучасних комунікаційних технологій на демократичні процеси та суспільні структури. Вони пропонують заходи для зменшення потенційних ризиків, включаючи маніпуляцію інформацією та фрагментацію комунікацій. Такі ініціативи сприяють більш демократичному та ефективному використанню інноваційних технологій.

В Україні національне законодавство та професійні стандарти журналістики також відображають ці підходи. Кодекс професійної етики журналіста, ратифікований Національною спілкою журналістів України, встановлює норми поведінки журналістів у відповідь на виклики нових технологій та змін в інформаційному просторі. Він закликає журналістів дотримуватися принципів чесності, точності, об'єктивності та відповідальності.

Зусилля, спрямовані на адаптацію журналістики до нових технологічних реалій, мають забезпечувати не лише розширення доступу до інформації, але й підтримувати високі стандарти якості, етичності та професійної

відповідальності. На десятому з'їзді Національної спілки журналістів України у 2002 році було ухвалено Кодекс етики українського журналіста, що містить 11 основних принципів. Вони зобов'язують журналістів уникати розповсюдження недостовірної інформації та створення образливих зображень чи коментарів. Кодекс підкреслює моральну відповідальність журналіста перед суспільством за достовірність та справедливість інформації.

Етичний кодекс українських журналістів, прийнятий у 2013 році, містить 19 принципів і закликає журналістів служити інтересам суспільства, а не влади чи фінансових засновників. Він акцентує на підтримці стандартів правдивої та неперекрученої інформації, засуджує фальсифікації та спотворення. Кодекс також передбачає механізми розгляду конфліктів через етичні комітети преси. Міжнародні та національні документи, що регулюють професійну етику журналістів, хоч і не завжди прямо, але захищають індивідів та різні соціальні групи від інформаційних впливів, що можуть негативно вплинути на їхній психоемоційний стан. Вони обмежують небажані впливи, забезпечуючи захист свободи вибору як окремих осіб, так і суспільства в цілому.

Таким чином, ці принципи виконують роль практичного керівництва для журналістів, спрямованого на забезпечення етичності та відповідальності у медійному просторі, що є ключовим для підтримки інформаційної безпеки.

ВИСНОВКИ ДО РОЗДІЛУ 2

Проведено детальний аналіз суспільно-політичної стабільності як основи національної та міжнародної безпеки в умовах сучасних інформаційних викликів, що дозволило визначити основні чинники та критерії, які впливають на суспільно-політичну стабільність, зокрема підкреслюючи важливість інформаційного компонента у їх формуванні.

Розглянуто роль інформаційної безпеки у забезпеченні стабільності держави в контексті гібридних загроз. Висвітлено значення інформаційної стійкості як ключового елементу захисту національних інтересів. Виявлено, що

ефективна інформаційна політика повинна враховувати специфіку інформаційного впливу на різні соціальні групи населення, особливо у періоди кризових ситуацій та конфліктів. Представлено аналіз сучасних викликів та механізмів забезпечення політичної стабільності в інформаційному суспільстві. Виявлено, що глобалізаційні процеси та стрімкий розвиток інформаційних технологій створюють нові загрози, які вимагають адаптації існуючих методів захисту, що включає впровадження інноваційних технологій та методів протидії дезінформації та пропаганді.

Особливо підкреслено важливість медіаграмотності та розвитку критичного мислення серед населення, важливість освітніх програм та ініціатив, спрямованих на підвищення рівня обізнаності громадян про інформаційні загрози, що допомагає зміцнювати інформаційну стійкість та знижувати вплив дезінформації. Акцентовано на необхідності вдосконалення законодавчої бази та розширення міжнародної співпраці у сфері інформаційної безпеки. Визначено, що інтегрований підхід до забезпечення інформаційної безпеки включає правові, технічні та соціальні аспекти. Важливою складовою є координація між державними структурами та громадянським суспільством для створення стійкого інформаційного простору.

Розглянуто вплив інформаційно-психологічної війни на суспільно-політичну стабільність, проаналізовано методи інформаційного впливу, що використовуються під час гібридних конфліктів, та розроблено рекомендації для їх нейтралізації. Підкреслено необхідність постійного моніторингу інформаційного простору та адаптації до змінюваних умов. Описано питання етичної відповідальності медіа та громадських організацій у контексті інформаційної безпеки. Визначено, що морально-етичні норми діяльності медіа відіграють важливу роль у формуванні довіри населення та забезпеченні стабільності суспільства.

РОЗДІЛ 3. ІНСТИТУЦІЙНИЙ РОЗВИТОК ІНФОРМАЦІЙНОЇ СТІЙКОСТІ СУЧАСНОЇ УКРАЇНИ: ГІБРИДНІ ЗАГРОЗИ ТА МЕХАНІЗМИ ПРОТИДІЇ

3.1 Безпековий аналіз ключових агентів і каналів пропаганди російсько-української війни

24 лютого 2022 року Росія розпочала великомасштабне військове вторгнення в Україну, перетворивши восьмирічну агресію на надзвичайне звірство. Російські війська вчинили геноцид українського народу, вбиваючи дітей та руйнуючи міста [67].

У своєму відеозверненні від 25 травня 2022 року, Президент України Володимир Зеленський зробив заяву, в якій висловив думку про те, що росіяни перебувають у стані відчуженості від реальності. Він також наголосив на непохитній рішучості українського народу захищати свої свободи до кінця, незважаючи на використання пропагандистських наративів, що мають на меті виправдання військових дій.

Основною метою так званої "спеціальної військової операції" Росії було втілення путінського наративу про "демілітаризацію" та "денацифікацію" України, щоб припинити нібито геноцид населення ДНР та ЛНР. Протягом восьми років Росія вела "операцію впливу", спрямовану на просування своєї точки зору на війну, ігноруючи альтернативні погляди [67].

22 травня 2022 року Верховна Рада України прийняла законодавчий акт, спрямований на заборону пропаганди тоталітарного неонацистського режиму Росії та символіки збройних сил РФ, що здійснюють військові дії проти України. Це рішення є значущим елементом у контексті протидії російській агресії та її пропагандистській кампанії.

На окупованих територіях України критичною проблемою є блокування доступу до українських мобільних операторів та телебачення з боку Росії, що перешкоджає розповсюдженню достовірної інформації серед місцевого

населення. Ці дії спрямовані на створення помилкового враження про те, що проблеми з комунікаціями та доступом до медіа є наслідком дій української сторони.

Крім того, Росія активно замінює українські телеканали на окупованих територіях своїми, щоб поширювати власну пропаганду та дезінформацію. Це призводить до того, що громадяни Росії не мають доступу до об'єктивної інформації про події в Україні [67].

Основою сучасної інформаційної війни, яку веде Росія, є активне використання офіційних телевізійних каналів як інструментів розповсюдження недостовірної інформації.

Ці канали здійснюють пропаганду, спрямовану на масову аудиторію, особливо на територіях, що перебувають під тимчасовим контролем російських окупаційних сил. Їхня діяльність має на меті не лише виправдати агресивну політику Росії, але й викривити факти, створюючи ілюзорний образ подій, який розходиться із реальністю.

Окрім традиційних медіа, значну роль у розповсюдженні пропаганди відіграють соціальні мережі, зокрема Telegram та Facebook. Ці платформи використовуються для широкомасштабного поширення фейкових новин, спрямованих на дискредитацію України та поширення дезінформації. Соціальні мережі дозволяють пропагандистам швидко та ефективно досягати великої аудиторії, маніпулюючи громадською думкою та формуючи вороже ставлення до України і її західних союзників.

Серед інших фігур, що відіграють важливу роль у пропагандистській машині, варто зазначити Президента Білорусі Олександра Лукашенка. Він активно підтримує кремлівську ідеологію, сприяючи поширенню спотвореної картини світу. Така підтримка є частиною більшої стратегії Росії, яка спрямована на утвердження свого впливу у пострадянському просторі та подальшу ізоляцію України від її європейського курсу.

Символіка "V" та "Z", що активно використовується російськими лідерами та окупаційними силами, стала візуальним вираженням пропаганди та

ідеології війни. Ці символи проникають у різні аспекти життя російського суспільства, зокрема, в освітній процес, де дітей та молодь стимулюють до підтримки військових дій проти України. Таким чином, через використання цих символів, пропаганда спрямовується на формування агресивних наративів серед молодшого покоління.

У сукупності, ці засоби та методи пропаганди створюють потужну інформаційну кампанію, спрямовану на підрив суверенітету України та зміцнення авторитарного режиму Росії. Подолання цих викликів вимагає злагоджених зусиль з боку міжнародної спільноти та активізації внутрішніх ресурсів України для захисту інформаційного простору та протидії дезінформації.

Російська пропаганда активно використовує історичний наратив "великої перемоги" у Другій світовій війні як інструмент для розпалювання антиукраїнських настроїв, при цьому вдаючись до спотворення історичної правди та маніпуляції фактами. Цей наратив сприяє формуванню ідеологічної основи, що виправдовує агресивні дії Росії проти України, і створює викривлене уявлення про історичні події, презентуючи Росію як виключно "визволительну" силу, що призводить до викривлення історичної ідентичності та переоцінки історичних фактів.

Серед методів інформаційної війни, яку веде Росія, особливе місце займає приховування реальних втрат власних військ та надмірне величання своїх успіхів. Така тактика має на меті підтримання високого рівня морального духу внутрішньої аудиторії та створення ілюзії непереможності російської армії. Водночас, використання провокаційних та агресивних прийомів у медіа спрямоване на виклик емоційної реакції, створення полеміки та відвернення уваги від реальних подій та проблем.

Міфологізація масової свідомості стає важливим елементом у формуванні спотвореної картини світу в рамках російської антиукраїнської пропаганди. Використання різноманітних міфів та створення "інформаційної бульбашки" дозволяє ізолювати аудиторію від об'єктивної реальності, стимулюючи віру в

альтернативну реальність, яка виправдовує дії Росії та дискредитує Україну та її західних союзників.

Російські медійні засоби та політичні лідери грають ключову роль у розповсюдженні пропагандистських наративів, особливо після анексії Криму. Пропагандистська кампанія, спрямована на легітимізацію нелегітимного референдуму в Криму та швидку інтеграцію півострова до складу Росії, маніпулювання демографічною інформацією та розповсюдження дезінформації про становище в окупованому Криму, стали основними інструментами в цій стратегії.

Завданням міжнародної спільноти та українського суспільства є виявлення та протидія цим маніпулятивним та пропагандистським діям. Критичне мислення, медіаграмотність, підтримка незалежних медійних організацій, а також активне використання міжнародних правових механізмів для викриття та засудження інформаційних маніпуляцій та пропаганди є ключовими аспектами у захисті правди та демократичних цінностей.

Процес міфологізації масової свідомості та організована пропагандистська кампанія, що ведеться Росією, мають за мету сформувати у громадян Росії та на тимчасово окупованих територіях України переконання про легітимність дій російської влади.

Ця стратегія включає в себе апеляцію до історичних міфів про "спільну історію" та "культурну єдність", спрямовані на виправдання анексії Криму та підтримку сепаратистських дій на сході України. Через це створюється віртуальна реальність, яка дистанціює громадян від об'єктивних фактів та спонукає їх до підтримки агресивних дій їхнього уряду.

Активне розповсюдження російської пропаганди на міжнародному рівні через медіа та соціальні мережі є спробою не лише виправдати свою зовнішню агресивну політику, але й підривати міжнародну підтримку України.

Через взаємодію з проросійськими політичними силами у різних країнах світу, Росія намагається посіяти розбрат між Україною та її міжнародними союзниками, що є ключовим елементом її геополітичної стратегії.

Протистояння цій інформаційній агресії вимагає від України та її партнерів комплексного підходу, який включає як внутрішні заходи з підвищення інформаційної стійкості, так і активізацію міжнародної співпраці. Одним з ключових елементів у цій боротьбі є підвищення рівня медіаграмотності населення, щоб громадяни могли критично аналізувати отриману інформацію та виявляти маніпулятивні техніки.

Підтримка незалежних медіа, які надають об'єктивну інформацію про події в Україні та світі, також відіграє важливу роль у протидії пропаганді. Крім того, розвиток міжнародних механізмів реагування на інформаційні виклики, включаючи створення спільних інструментів моніторингу та аналізу пропагандистських кампаній, може зміцнити здатність міжнародної спільноти протистояти дезінформації.

У підсумку, вирішення проблеми російської інформаційної агресії вимагає скоординованих зусиль на національному та міжнародному рівнях. Це не лише боротьба за правду в інформаційному просторі, але й захист основ демократії, прав людини та міжнародного правопорядку.

3.2 Методи інформаційного впливу РФ на на суспільно-політичну стабільність України: рекомендації з протидії

Пропаганда має на меті спонукати індивідів до певної поведінки чи прийняття конкретної точки зору. У зв'язку з початком воєнних дій на території України, російські медіаінституції ініціювали кампанію, спрямовану на формування толерантного ставлення населення країни до збройного конфлікту [67].

Створення ефективної пропаганди часто засновується на використанні методів, які мають глибоке коріння в соціальній психології та психологічних теоріях. Пропагандистські техніки вибудовуються таким чином, щоб впливати на переконання та емоції аудиторії, використовуючи аргументацію, яка, хоча й

може здаватися переконливою на перший погляд, часто не витримує критики з точки зору логіки та надійності.

Така аргументація використовує логічні помилки, маніпулюючи логікою та фактами для досягнення своїх цілей.

Одним із часто використовуваних прийомів у пропаганді є апеляція до епізодичних доказів. Цей метод полягає у виборі та презентації конкретних прикладів чи історій, які підтримують бажаний наратив, в той час як альтернативні точки зору або контраргументи ігноруються або мінімізуються. Таким чином, пропагандисти створюють сприйняття загальної тенденції або правди, базуючись на обмеженій або упередженій вибірці фактів.

У контексті воєнних дій російських військ в Україні, використання терміна "нацист" як ярлика є яскравим прикладом такої пропаганди. Цей термін вибірково застосовується для дискредитації українського уряду та збройних сил, намагаючись викликати негативні асоціації та емоційну реакцію, ігноруючи реальний контекст та фактичні дії обох сторін конфлікту.

Така маніпуляція інформацією не лише вводить в оману громадськість, але й сприяє поляризації суспільства, посилюючи поділи та ворожнечу. Важливим аспектом протидії такій пропаганді є підвищення критичного мислення та медіаграмотності серед населення, щоб люди могли розпізнавати та аналізувати маніпулятивні техніки та не ставати жертвами дезінформації.

Розуміння механізмів та методів пропаганди, заснованих на соціально-психологічних дослідженнях, є ключовим для розробки ефективних стратегій інформаційної безпеки. Це передбачає не лише відкидання недостовірної інформації, а й активне просування об'єктивних, перевірених даних та підтримку вільних, незалежних медіа, які здатні забезпечувати балансоване та всебічне висвітлення подій.

Коли Путін оголосив про свою "спеціальну воєнну операцію" в лютому, він закликав українських солдатів до державного перевороту і назвав нинішній режим в Україні "купкою наркоманів і неонацистів". Відтоді слово "нацисти" стало невід'ємною частиною політичної риторики [67].

Наступний метод, який використовується в пропаганді, - це "свідчення авторитетних особистостей". Цей метод полягає в використанні імен знаменитостей для просування певної ідеї, оскільки люди схильні довіряти, захоплюватися та розглядати знаменитостей як приклад для наслідування. Таким чином, знаменитість стає інструментом пропаганди [67].

Ще один метод - "гнилий оселедець", який полягає в використанні неправдивих звинувачень з метою дискредитації особи та відволікання уваги громадськості від важливих питань, таких як вибори, соціальні проблеми тощо. Пропагандисти та піарники вибирають скандальні теми для створення неправдивих звинувачень, які можуть бути пов'язані з криміналом, жорстоким поводженням з дітьми, зв'язками з мафією, спецслужбами чи іноземними урядами [67].

Використання риторичних прийомів для відволікання уваги від проблематичних питань є важливою частиною стратегії російської пропаганди. "Переведення стрілок" на Захід дозволяє російському уряду уникати відповідальності та критики за свої дії, перекладаючи вину на зовнішніх "ворогів". Ця тактика не лише зміщує фокус дискусії, але й створює образ Заходу як постійної загрози, що, у свою чергу, має на меті згуртувати російське суспільство навколо керівництва країни.

Прикладом такої тактики є заяви путіна про існування законів про іноземних агентів, які, за його словами, були вперше введені на Заході у 1930-х роках, і що російське законодавство в цій сфері є більш ліберальним порівняно з американським.

Такі заяви спрямовані на виправдання суворої внутрішньої політики під прикриттям історичних фактів та порівняльного аналізу, намагаючись знизити ступінь критики від міжнародної спільноти.

З початком збройного конфлікту на Донбасі у 2022 році російська пропаганда активізувала використання стереотипного запитання "Де ви були останні вісім років?", що спрямоване на тих, хто критикує дії Росії в Україні. Це запитання має на меті не лише перекласти вину за конфлікт на Україну та її

західних союзників, але й виправдати агресію Росії як "відповідь" на дії інших сторін.

Такі методи мають велике значення у контексті інформаційної війни, оскільки вони не лише допомагають уряду Росії уникати безпосередньої критики, але й сприяють формуванню у громадськості переконання про "несправедливе" ставлення до Росії з боку міжнародної спільноти. Таким чином, пропаганда не лише маніпулює фактами, але й спотворює сприйняття реальності, створюючи альтернативну картину світу, де Росія виступає як жертва зовнішньої агресії.

Протидія таким пропагандистським стратегіям вимагає комплексного підходу, який включає зміцнення медіаграмотності населення, підтримку незалежних медіа, які забезпечують об'єктивне висвітлення подій, та активну міжнародну співпрацю для викриття та засудження пропагандистських кампаній, спрямованих на підірвання демократичних цінностей та міжнародного правопорядку.

Особливості підходу Росії у гібридній війні з Україною, яка розпочалася у 2014 році, поєднують військові, воєнізовані, дипломатичні, інформаційні та економічні засоби і не зупиняються перед шантажем ядерною зброєю [67].

Технології, які Росія продовжує використовувати проти України, включають:

1. Кіноіндустрія - формує образи героїв, популяризує акторів, створює цінності та впливає на сприйняття конкретних історичних подій.
2. Телесеріали - "мильні опери", покликані утримувати глядачів прикутими до екрану. Короткі повідомлення та реклама в перервах між розважальним контентом мають більше шансів залишитися в пам'яті слухачів.
3. Телевізійні та інформаційні програми - формування хроніки подій.
4. Повідомлення на каналах Facebook і Telegram, відео на YouTube та Instagram - найбільш цікава та легка для сприйняття аудіовізуальна інформація.
5. Вірусні повідомлення у Viber/WhatsApp/Telegram/Messenger - один з найефективніших способів поширення паніки.

Ці інструменти використовуються для маніпулювання свідомістю громадян і використання різних засобів дезінформації для досягнення своїх цілей. На тимчасово окупованих територіях Росія впроваджує агресивну пропагандистську політику, обмежуючи доступ до інтернету та забезпечуючи своїх громадян лише федеральними телевізійними програмами [67].

Пропагандистські методи, які використовуються в сучасному інформаційному просторі, базуються на стратегіях зловживання владою та контролю над суспільною думкою. У контексті російської пропаганди, сучасні медіа трансформуються з інформаційних платформ у ідеологічні інструменти. Центральним елементом їх повідомлень є ідеологія, яка систематично впроваджується у свідомість громадян, використовуючи різноманітні засоби і методи пропаганди, спрямовані на формування певного світогляду та переконань.

Фундамент російської дезінформації покладається на маніпуляції як з фактами, так і з емоціями аудиторії. Сучасне інформаційне середовище, з його широким доступом до інтернету, соціальних мереж та телебачення, створює сприятливі умови для поширення дезінформації. Анонімність в інтернеті та на платформах соціальних мереж сприяє безкарному розповсюдженню неправдивих даних та маніпулятивного контенту.

В країнах Східної Європи інструментарій російської пропаганди включає не тільки інтернет-ресурси та системи обміну повідомленнями, але й соціальні мережі та російські телеканали. З початком російської агресії проти України у 2014 році, пропаганда набула особливої ваги у концепції гібридної війни, ставши однією з ключових її складових. Це підкреслює стратегічне значення інформаційних операцій в сучасних конфліктах, де боротьба за вплив на громадську думку є одним з вирішальних фронтів.

Протидія такій масштабній пропаганді та дезінформації вимагає злагоджених зусиль не тільки на національному рівні, але й міжнародної співпраці. Важливою складовою є розвиток критичного мислення серед

населення, зміцнення інституцій незалежних медіа, а також впровадження ефективних механізмів верифікації інформації та протидії маніпуляціям.

Окрім того, важливим аспектом є підтримка відкритого та прозорого інформаційного простору, де кожен має доступ до різноманітних джерел інформації та можливість формувати власну об'єктивну думку. Антиукраїнська пропаганда в Росії досягла безпрецедентного масштабу, формуючи образ "ворожої України" та забезпечуючи підтримку вторгнення в сусідні країни.

Серед найбільш кричущих прикладів російської пропаганди можна виділити події в містах Бучі, Ірпені та Гостомелі, які повернулися під контроль України 2 квітня 2022 року. Медіа з усього світу транслювали фотографії та відео з тілами людей, що лежали на вулицях, вбитими російськими військами. Російська пропаганда почала поширювати інформацію про "фейкові" вбивства, зображуючи акторів, які грали трупи.

Іноземні медіа відіграли важливу роль у руйнуванні цього образу, публікуючи знімки з дронів і супутників, які підтверджували справжність подій. Російська антиукраїнська пропаганда базується на міфологізації масової свідомості та трансформації її в діаметрально протилежну картину світу [67].

У літературному контексті наратив відіграє ключову роль у створенні змістовної структури твору, представляючи послідовність подій, що розкриває дії та розвиток персонажів у певному часовому проміжку. Наратив служить не лише для викладу подій, але й для передачі глибших значень, ідей та переконань, що лежать в основі історії. Відмінність між наративом та історією полягає у тому, що наратив включає в себе спосіб подання історії, її інтерпретацію та побудову зв'язку між подіями, тоді як історія фокусується на самій послідовності подій та їх сюжетній структурі.

Пропагандистські повідомлення використовують наратив як могутній інструмент для формування громадської думки та переконань. Через різноманітні медіа - від друкованих видань до цифрових платформ - наративи розповсюджуються з метою впливу на сприйняття та ставлення аудиторії до певних подій, ідей або персонажів.

Використання конкретних наративних прийомів, таких як вибіркове представлення фактів, емоційне забарвлення подій, а також створення спрощених чорно-білих картин, дозволяє пропагандистам маніпулювати реальністю та керувати громадською свідомістю.

Розуміння механізмів, через які наративи впливають на сприйняття людей, є важливим для критичного аналізу пропагандистських повідомлень. Відокремлення факту від фікції, аналіз контексту подій та врахування різних точок зору допомагає виявити маніпулятивні наративи та зменшити їх вплив на формування власних переконань.

У сучасному світі, де інформація поширюється з надзвичайною швидкістю через глобальні мережі, критичне мислення та медіаграмотність стають ключовими інструментами для захисту від дезінформації та пропаганди. Освіта та постійне навчання у цих напрямках сприяють розвитку здатності ідентифікувати маніпулятивні наративи та обирати об'єктивну інформацію, що є невід'ємною частиною інформаційної безпеки та суспільного здоров'я.

Російська пропаганда використовує ряд наративів для досягнення своїх цілей.

Перший наратив полягає в тому, що Україна є "недержавою" і її нація не існує окремо від російської. Цей наратив спрямований на заперечення існування української нації та культури.

Другий наратив стверджує, що українська влада є "нелегітимною" і "неонацистською", що має на меті дискредитувати українську владу та розділити суспільство.

Третій наратив вказує на те, що Захід, на чолі зі США, експлуатує Україну для своїх геополітичних інтересів (зовнішнє управління), що призводить до руйнування світового порядку.

Четвертий наратив стверджує, що російські меншини в Україні утискаються, і має на меті показати, що російська культура та історія переслідуються в Україні.

П'ятий наратив стверджує, що існує зовнішня загроза для Росії, і має на меті переконати населення у неминучості та необхідності «захисту вітчизняних інтересів» [67].

Пропагандистська кампанія Кремля, активно запущена задовго до відкритого воєнного втручання в Україну 24 лютого 2022 року, мала на меті масштабне дезінформування не лише внутрішньої, а й світової громадської думки. Використання дезінформації як інструменту ведення гібридної війни дозволяло Росії маніпулювати фактами, спотворювати реальність та формувати сприйняття, яке відповідало її геополітичним інтересам. Це було спрямовано на підірвання довіри до українського уряду, дискредитацію України на міжнародній арені та виправдання власних агресивних дій під виглядом "захисту російськомовного населення".

В контексті Автономної Республіки Крим у 2014 році, російська пропагандистська машина використовувала відсутність ефективних заходів з боку української влади для протидії інформаційному впливу. Пропаганда була націлена на створення ілюзії легітимності анексії та підкреслення ідеї про "волевиявлення" кримського населення. Масова інформаційно-пропагандистська кампанія вдало використовувала існуючі соціальні та культурні тріщини, спотворюючи самосприйняття кримчан та намагаючись розколоти їхні традиційні цінності.

Ця кампанія в Криму демонструє важливість створення та ефективного застосування нормативно-правових механізмів захисту інформаційної безпеки на державному рівні.

Наявність законодавства є ключовим аспектом, але без реальних інструментів застосування, координації між різними органами влади та активної роботи з громадськістю, такі механізми не здатні ефективно протистояти пропагандистському впливу.

Уроки, винесені з подій в Криму, підкреслюють важливість посилення інформаційної резистентності суспільства через освіту, медіаграмотність та активне використання незалежних медіа як контрваги пропаганді. Це включає

залучення експертів, активістів та журналістів для створення реальної картини подій, спростування фейків та забезпечення населення достовірною інформацією.

Протидія інформаційній агресії вимагає комплексного підходу, що охоплює не лише законодавчі ініціативи, але й активну роботу з громадськістю, розвиток міжнародної співпраці та посилення механізмів моніторингу інформаційного простору. Забезпечення інформаційної безпеки є одним з ключових елементів зміцнення державного суверенітету та захисту демократичних цінностей.

Однією з ключових переваг Кремля в контексті анексії Криму була здатність ефективно транслювати російську пропаганду на півострові, спрямовану на вплив на традиційні цінності місцевого населення. Ця пропаганда використовувала вже існуючу мережу українських телеканалів та радіостанцій, які до 2014 року переважно транслювали проросійський контент, створюючи сприятливий інформаційний фон для російських дій у регіоні.

Нерішуча та неефективна реакція українських медіа на російську пропаганду лише посилила цю тенденцію, відкриваючи шлях для поширення ворожих наративів і створюючи умови для інформаційної та психологічної війни, до якої Україна була недостатньо підготовлена.

Суспільство в Криму, яке не сприймало Росію як потенційного агресора, опинилося під потужним впливом системи відтворення ворожої пропаганди. Російські пропагандисти, використовуючи свої професійні навички та психологічні прийоми, розробили низку теорій, спрямованих на об'єднання російськомовного населення навколо ідеї "єдиного російського народу" та концепції "русского мира".

Ця ідеологія була спрямована на створення уявлення про культурну та цивілізаційну єдність, яка виправдовувала анексію Криму як "повернення до рідної гавані".

Подібні дії Кремля свідчать про важливість інформаційної безпеки як невід'ємного елемента національної безпеки країни. Завдання протидії

пропаганді та дезінформації вимагає комплексного підходу, який включає підтримку незалежних медіа, зміцнення медіаграмотності населення та активізацію роботи з міжнародними партнерами для протистояння спробам впливу на внутрішньополітичні процеси.

Події в Криму також підкреслюють необхідність розвитку ефективних механізмів моніторингу інформаційного простору та своєчасної реакції на пропагандистські кампанії. Впровадження цих заходів дозволить не тільки захистити інформаційний простір від ворожого впливу, але й зміцнити довіру громадян до державних інституцій, підтримуючи стабільність та єдність суспільства в умовах зовнішнього тиску.

Також, використання інформаційних ресурсів Російської православної церкви (РПЦ) стало основою пропагандистського та психологічного впливу. Це пов'язано з тим, що для реалізації своїх імперських амбіцій наближені до влади кола використовують РПЦ як об'єднуючий чинник, заснований на релігійній ідентичності народу [67].

Російські релігійні діячі сформулювали і постійно вдосконалюють концепцію "русского мира". Термін "русский мир" фактично є терміном Російської православної церкви і асоціюється з її статусом і діяльністю, а не з російськими високопосадовцями. Одночасне використання РПЦ термінів "російськомовні" та "православні" значно розширює сферу інформаційного впливу концепції "русского мира" [67].

Роль Російської Православної Церкви (РПЦ) в контексті гібридної війни Росії проти України стала предметом глибокого аналізу та дискусій, оскільки РПЦ активно використовується як інструмент інформаційного впливу. Виправдання воєнних дій Росії в Україні лідерами РПЦ під гаслами "збереження цілісності Святої Русі" та "мирної місії" є спробою маніпулювати релігійними почуттями та історичними уявленнями віруючих. Такі дії не тільки спотворюють реальну картину конфлікту, але й активно впливають на цінності та установки національної ідентичності українців, підкреслюючи ідею возз'єднання з "братньою" Росією.

Використання РПЦ як засобу пропаганди спрямоване на досягнення кількох цілей: виправдання російської агресії, підтримка ідеї "русского мира" як інструменту розширення впливу Росії, поширення проросійської ідеології, нівелювання української національної ідентичності та підтримка сепаратистських рухів. РПЦ та УПЦ (Московського патріархату) зображуються у проросійських медіа як миротворчі організації, тоді як реальну роль Росії в ескалації конфлікту замовчують.

Однією з найбільш небезпечних діяльностей РПЦ є сприяння загостренню міжрелігійного конфлікту в Україні. Це веде до поділу в суспільстві, підриває єдність країни та створює додаткові точки напруженості, які можуть бути використані проти України на зовнішньополітичному та внутрішньополітичному рівнях.

Протидія такому впливу вимагає посилення інформаційної політики, спрямованої на зміцнення національної ідентичності, підтримку незалежності релігійних інституцій в Україні та виховання толерантності й взаємоповаги між представниками різних конфесій. Також важливим є розвиток міжнародного співробітництва для висвітлення реального стану релігійної свободи та прав людини в Україні, а також протидії спробам використання релігії як інструменту гібридної війни.

Таким чином, можна зробити висновок, що російська військова доктрина базується на розробках Радянського Союзу і використовує більш агресивну наративну пропаганду в інформаційному та віртуальному просторі. Росія продовжує здійснювати геноцид в Україні та посилює гібридну агресію проти Заходу, використовуючи біженців, продовольство, газ та інформацію як зброю [67].

З початком так званої «спеціальної військової операції» Росією в Україні, ефективність російської пропаганди зазнала значних збоїв. Слабкі сторони такої пропаганди стали більш вираженими і полягають у непослідовності передачі інформації, її несвоєчасності та відсутності ефективної підтримки. Це

спричинило зменшення довіри до російських інформаційних джерел, як в самій Росії, так і за її межами.

Основною проблемою російської пропаганди стало її розширення за межі Росії, особливо в контексті європейського інформаційного простору. Тут пропаганда була націлена на створення позитивного образу російського уряду та виправдання військових дій на території України. Проте, зростання критичного сприйняття та доступ до різноманітних джерел інформації у європейських країнах зменшило вплив російських наративів.

Європейський інформаційний простір, оснащений механізмами перевірки фактів та протидії дезінформації, став важливим фронтом боротьби з російською пропагандою. Це змусило Кремль шукати нові методи інформаційного впливу, однак спроби адаптації часто зустрічають ефективний опір.

Активізація громадськості, медійних організацій та урядових структур європейських країн щодо протидії пропаганді та дезінформації стала вагомою відповіддю на спроби Росії маніпулювати громадською думкою. Зусилля щодо підвищення обізнаності населення, розвиток критичного мислення та медіаграмотності є ключовими елементами ефективної стратегії протидії інформаційному впливу.

Таким чином, хоча російська пропаганда намагається адаптуватися до змінних умов сучасного інформаційного простору, її здатність впливати на громадську думку за межами Росії стикається зі зростаючими викликами. Це відкриває перспективи для подальшої консолідації зусиль у боротьбі з дезінформацією та зміцненні інформаційної стійкості суспільств.

Заборона російської пропаганди в Європі не стала остаточним рішенням проблеми її впливу на громадську думку. Росія активно використовує стратегії створення "клонів" своїх медіа ресурсів, таких як Russia Today і Sputnik, у системі медіа та соціальних мереж на міжнародному рівні, включно з випусками на всіх основних європейських мовах. Ці клони імітують

національні новинні джерела, створюючи ілюзію локального контенту, але насправді продовжують висвітлювати події з точки зору Кремля.

Розвиток "м'якої сили" Росією за кордоном через інформаційні ресурси триває вже понад півтора десятиліття. Створення версій Russia Today і Sputnik у таких країнах, як Грузія, Азербайджан, Вірменія, а також у великих європейських країнах, США, Канаді, Японії та Великобританії, свідчить про масштабність і глибину стратегії інформаційного впливу.

Інцидент з блокуванням Sputnik в Естонії у 2021 році і швидке створення Sputnik Media як нібито незалежного медіа, керованого тими ж особами, з тим самим проектом та порядком денним, підкреслює адаптивність російської пропагандистської машини до спроб її обмеження. Це свідчить про необхідність більш ефективних міжнародних заходів для ідентифікації та протидії російським інформаційним операціям.

В цьому контексті критично важливим стає розвиток механізмів моніторингу та верифікації інформації, підвищення медіаграмотності населення та підтримка незалежних медіа, які можуть протистояти спробам маніпулювання громадською думкою. Координація зусиль на міжнародному рівні, включаючи обмін інформацією та досвідом між країнами, є ключовим фактором у боротьбі з глобальним викликом російської пропаганди та дезінформації.

Створення клонів німецькомовних видань Russia Today і Sputnik під назвою "SNA" або "Sputnik News Agency" у квітні 2022 року свідчить про адаптивність та рішучість російської пропагандистської машини продовжувати свою діяльність в Європі навіть після введення обмежень. Ідентичність цих клонів за змістом і оформленням до оригінальних Russia Today і Sputnik підкреслює спробу зберегти впізнаваність бренду та продовжувати вплив на громадську думку, обходячи законодавчі обмеження.

Реакція ЄС на російське вторгнення в Україну, що включала блокування дезінформаційних сайтів та компаній, пов'язаних з Russia Today і Sputnik, стала свідченням визнання загрози, яку така пропаганда становить для інформаційної

безпеки та стабільності в регіоні. Обмеження доступу до спільнот цих медіа в Telegram ініційовано рішенням Ради ЄС, стало одним із заходів протидії.

Однак поява нових каналів, які продовжують працювати без обмежень, підкреслює складність проблеми та необхідність пошуку додаткових механізмів контролю та протидії. Це свідчить про необхідність вдосконалення законодавчих та технологічних засобів виявлення та блокування пропагандистського контенту, а також про важливість міжнародної співпраці у цій сфері.

Боротьба з російською пропагандою в Європі вимагає комплексного підходу, який включає не тільки обмеження та санкції, але й освітні кампанії для підвищення медіаграмотності населення, підтримку незалежних медіа та розвиток технологій штучного інтелекту для ідентифікації фейкового контенту. Також критично важливим є зміцнення законодавчої бази для захисту інформаційного простору від зовнішнього втручання.

Ситуація з клонами Russia Today і Sputnik в Європі підкреслює не лише виклики, з якими стикаються європейські країни у боротьбі з дезінформацією, але й необхідність непоступливої та послідовної реакції на спроби маніпулювати громадською думкою та підривати демократичні цінності.

Поширення правдивої інформації про війну в Україні, особливо в контексті російської аудиторії, є важливим і водночас складним завданням, що вимагає цілеспрямованої стратегії та координації зусиль. Головна мета полягає в тому, щоб надати громадянам Росії об'єктивну інформацію про агресію Кремля проти України, спростувати міфи та пропагандистські наративи, поширені російським урядом.

Ефективне досягнення цієї мети вимагає визначення ключових адресатів, до яких буде спрямована інформаційна кампанія, а також розробки відповідного формату та змісту інформаційних повідомлень. Важливим є вибір каналів комунікації, які здатні ефективно долати інформаційну блокаду та донести факти до громадян Росії. Це можуть бути не тільки традиційні медіа та

соціальні мережі, але й альтернативні платформи, такі як месенджери та блоги, де можливий вільний обмін думками.

Координація дій між державними органами, неурядовим сектором, незалежними медіа та міжнародними партнерами стає вирішальною у цьому процесі. Підтримка з боку цих учасників може забезпечити не тільки фінансові та технічні ресурси, але й розширити охоплення аудиторії та підвищити довіру до поширюваної інформації.

Важливою стратегією є створення умов для критичного осмислення інформації серед громадян Росії, спонукання до поставлення питань та засівання сумнівів у правдивість офіційних наративів. Це вимагає не лише прямого спростування фейків, але й подання вичерпної, перевіреної інформації про події в Україні, що може сприяти змінам у ставленні до дій російської влади та формуванні більш критичного сприйняття медійного контенту.

Завданням є не просто "переконати" громадян в іншій точці зору, але змінити парадигму мислення, створити платформу для вільного обміну ідеями та допомогти людям самостійно прийти до висновків про реальну ситуацію. Це довготривалий процес, який вимагає системного підходу, витримки та постійної роботи з аудиторією.

Існує три основні фактори, що впливають на настрої і ставлення російських громадян.

Перший фактор, що впливає на настрої і ставлення російських громадян, - це динаміка ситуації воєнного часу. Провал "бліц-наступу" в Україні та ефективний опір українських військових російській інтервенції розвіяли образ непереможної "другої армії" світу. Декларації Міністерства оборони Росії про перемогу все більше розходяться з реальністю на фронті.

Другий фактор - безпрецедентні масштаби "безповоротних" втрат російських військ. Загибель росіян матиме кумулятивний ефект, особливо в азійських регіонах Росії. Зростає кількість осіб, які відмовляються вступати до лав Збройних сил Росії, а також кількість "дезертирів".

Третій фактор - міжнародні санкції, які впливають на соціальний клімат, повсякденне життя і психічний стан громадян Росії. Ефекти звикання і адаптації до санкцій більш виражені у старших поколінь, які пережили радянську епоху. Молодші покоління, інтегровані в міжнародне співтовариство, більш чутливі до санкцій і ізоляції Росії на міжнародній арені.

Протидія російській пропаганді вимагає комплексного підходу, який включає розробку та реалізацію стратегій, спрямованих на мінімізацію її впливу та досягнення протилежних результатів. НАТО та США, використовуючи свої численні розвідувальні та інформаційні ресурси, мають змогу впливати на цільові групи та переконувати їх у підтримці власних цілей. Активізація зусиль зі збільшення обсягу переконливої інформації, яка підтримує інтереси США та НАТО, є однією з ключових стратегій у цій боротьбі.

Один з ефективних підходів до протидії російській пропаганді полягає в усуненні або зменшенні її потоку через застосування технічних засобів. Це може включати співпрацю з інтернет-провайдерами та соціальними мережами для забезпечення дотримання угод, а також використання сучасних технологій для блокування або придушення небажаної комунікації в кіберпросторі.

Інформаційні кампанії, спрямовані на підвищення обізнаності громадян про небезпеку пропаганди та методи протидії дезінформації, є важливою частиною стратегії. Це передбачає розвиток медіаграмотності, навчання громадськості критично сприймати інформацію та розпізнавати ознаки маніпуляцій.

Ефективна боротьба з російською пропагандою також вимагає співпраці на міжнародному рівні, обміну досвідом і інформацією між країнами та організаціями. Це допомагає створювати єдиний фронт протистояння, здатний ефективно реагувати на виклики та адаптуватися до змінюваних тактик противника.

Залучення громадськості до процесу протидії пропаганді, забезпечення доступу до надійної інформації, а також формування стійкості до маніпулятивних впливів є ключовими аспектами успішної стратегії. Тільки

через спільні зусилля можливо забезпечити захист інформаційного простору та збереження демократичних цінностей.

Навчання громадян критичному мисленню та інформаційній гігієні є ключовими елементами боротьби з дезінформацією. Ці навички допомагають індивідам розрізняти достовірну інформацію від маніпулятивної та фальсифікованої. Стратегічні комунікаційні кампанії, розроблені у співпраці між державою та суспільством, можуть слугувати міцною основою для інформування громадян про загрози дезінформації та методи її протидії.

Важливість об'єднання зусиль держави та суспільства у боротьбі з пропагандою та дезінформацією, що поширюються Кремлем, не може бути недооцінена. Урядові програми та ініціативи, які забезпечують надання об'єктивної інформації, є критично важливими у цьому процесі. Активна співпраця з іноземними партнерами та створення високоякісної інформаційної продукції, яка була б зрозуміла та прийнятна для російської аудиторії, є ефективним способом контрпропаганди.

Доступність такої інформації для всіх груп населення, зокрема для молоді та мешканців окупованих територій, є важливим для забезпечення широкого охоплення та впливу. Це передбачає використання різноманітних медійних платформ і технологій для забезпечення того, щоб інформація була доступна там, де вона найбільш потрібна, і могла ефективно протистояти спробам маніпуляції.

Залучення громадськості до активної участі у процесі протидії дезінформації, через освітні програми, публічні дискусії та сприяння розвитку медіаграмотності, може значно підвищити резистентність суспільства до маніпулятивних впливів. Врешті-решт, підвищення рівня обізнаності та критичного мислення є одним із найефективніших способів зміцнення демократичних суспільств та захисту їх від зовнішніх загроз.

Ефективна боротьба з дезінформацією та пропагандою передбачає активізацію медійної присутності представників центральних та місцевих органів влади. Їхня регулярна участь у медійному просторі та соціальних

мережах відіграє ключову роль у забезпеченні об'єктивного інформування громадськості та активній протидії поширенню неправдивих новин. Забезпечення постійної взаємодії з аудиторією, використання фактчекінгу та аргументованих відповідей на поширення фейків є основою для побудови довіри та зміцнення інформаційної безпеки.

Комунікаційна кампанія, спрямована проти російської пропаганди, вимагає координованих дій не лише з боку України, але й з боку міжнародних партнерів. Єдність зусиль є важливою не тільки для ефективного протистояння агресивним інформаційним кампаніям Росії, але й для захисту та просування універсальних цінностей демократії.

Розвиток стратегічних комунікацій, які базуються на принципах правди, прозорості та відповідальності, сприятиме підвищенню обізнаності громадськості та зміцненню демократичних інституцій.

З метою забезпечення ефективності інформаційних кампаній важливо також залучати експертів, журналістів, громадських діячів та інших впливових осіб у процес формування та розповсюдження повідомлень. Це допоможе розширити охоплення та забезпечити більшу переконливість комунікацій.

На заключному етапі, важливим є вимірювання впливу проведених кампаній та адаптація стратегій зв'язку відповідно до отриманих результатів. Моніторинг реакцій аудиторії, аналіз ефективності використаних інструментів та змісту повідомлень дозволить оптимізувати подальші дії для досягнення найкращих результатів у боротьбі з дезінформацією та зміцнення інформаційної стійкості суспільства.

3.3 Перспективи розвитку інститутів і механізмів забезпечення суспільно-політичної стабільності у публічному інформаційному просторі України

Використання інформаційних ресурсів як засобу маніпуляції свідомістю в сучасному суспільстві набуває особливої актуальності у контексті зростаючої

інформаційної відкритості та доступності. В цьому процесі важливу роль відіграє не лише кількість доступної інформації, але й її якість та надійність.

Прозорість інформаційних джерел та забезпечення відкритого доступу до них є критичними аспектами, які сприяють підвищенню обізнаності громадян та їх здатності критично оцінювати надходження інформації.

Спроможність громадянського суспільства протистояти маніпулятивним впливам значною мірою залежить від розвиненості соціально-психологічних механізмів захисту на індивідуальному та загальносуспільному рівнях. Існуючі системи захисту часто виявляються неефективними у боротьбі з новітніми маніпуляціями через їхню здатність швидко адаптуватися до змінюваного інформаційного середовища.

Це вимагає від суспільства шукати нові підходи та розробляти стратегії захисту, що відповідали б сучасним викликам інформаційного простору.

Наразі особлива увага має бути приділена розвитку медіаграмотності та критичного мислення серед громадян. Навчання громадян розпізнавати маніпулятивні техніки, оцінювати джерела інформації та розуміти приховані інтереси за певними повідомленнями є ключовим у формуванні стійкого суспільства, здатного протистояти спробам маніпуляції.

Розвиток та підтримка ініціатив, які спрямовані на покращення інформаційної гігієни серед населення, включаючи розробку і впровадження освітніх програм, публічних лекцій та тренінгів, є важливими для зміцнення суспільної стійкості до інформаційних загроз.

Останнім, але не менш важливим аспектом, є співпраця між державними установами, недержавним сектором та міжнародною спільнотою у сфері боротьби з дезінформацією та пропагандою. Об'єднання зусиль, обмін досвідом та координація дій можуть значно підвищити ефективність запобігання та протидії маніпулятивним впливам в інформаційному просторі.

Сучасні маніпулятивні технології, такі як нейролінгвістичне програмування (НЛП), мають значний вплив на різні сфери суспільства, включаючи політику [78].

У сучасному інформаційному суспільстві, яке характеризується швидкісним обміном даними та зростанням доступності інформації, важливість інформаційної компетентності окремих членів суспільства стає дедалі більшою.

Інформаційна компетентність не лише сприяє ефективній адаптації до швидкозмінних умов, але й служить надійним засобом захисту від маніпулятивних впливів, які можуть впливати на формування громадської думки, політичні переконання, та особистісні цінності індивіда. В контексті інформаційного суспільства, недолік інформаційної компетентності може призвести до значного збільшення вразливості до інформаційних атак та маніпуляцій, що здійснюються через медіа та соціальні мережі.

Розвинені країни мають тривалу історію в розробці ефективних механізмів протидії маніпулятивним впливам, включаючи законодавчу регуляцію медійного простору, освітні програми з підвищення медіаграмотності населення, та розробку інструментів критичного аналізу інформації.

Україна, зазнаючи динамічних змін після здобуття незалежності, стикається з необхідністю адаптації до нових інформаційних викликів. Відсутність достатньої підготовки до ефективного сприйняття та аналізу інформації створює умови для поширення маніпуляційних впливів, що можуть мати негативний вплив на суспільство в цілому.

Захист від маніпуляцій вимагає комплексного підходу, який включає як індивідуальні зусилля з розвитку критичного мислення та медіаграмотності, так і колективні заходи, спрямовані на формування стійких до маніпуляцій спільнот. Захист може включати аналіз потенційних джерел маніпуляції, визначення їх мотивів та методів, а також розробку стратегій нейтралізації впливів, що підривають довіру до інформації та сприяють соціальній дезорієнтації.

Основні підходи до оборони від маніпуляцій об'єднують утвердження особистісної незалежності та розвиток здатності критично оцінювати інформацію.

Утвердження незалежності полягає в зміцненні власних переконань та цінностей, що знижує вразливість до маніпуляцій. Критичний аналіз інформації

передбачає глибоке розуміння механізмів маніпуляції, включаючи логічні помилки та недостовірність джерел, що дозволяє ефективно спростовувати недостовірну інформацію.

Важливо, що ефективність захисту від маніпуляцій в інформаційному просторі залежить не лише від рівня інформаційної компетентності окремих осіб, але й від здатності суспільства в цілому розвивати і підтримувати механізми критичного аналізу та відкритого діалогу.

Це передбачає необхідність створення умов для регулярного оновлення освітніх програм, зміцнення правових основ захисту інформаційної безпеки, та активізації громадської участі в процесах формування медійної політики та стандартів.

Науковці пропонують три стратегії для зменшення вразливості до маніпуляцій. Перша стратегія полягає в введенні законодавчого регулювання та обмеження методів маніпуляції, щоб надати їм характеристики "чистоти", "ясності" та "чесності" [28].

В контексті сучасного політичного дискурсу, аналогії з судовими процесами, де окремі свідчення можуть бути визнані недопустимими через їх ненадійність або маніпулятивність, набувають особливої актуальності.

Ідея обмеження недобросовісних та маніпулятивних практик у політичному дискурсі є спробою втілення подібних принципів справедливості та прозорості у публічній комунікації.

Проте, на відміну від чітко регульованої судової системи, політичний дискурс існує у значно більш вільному та менш визначеному просторі, де введення будь-яких обмежень на свободу вираження поглядів викликає побоювання щодо потенційного порушення фундаментальних демократичних прав.

У контексті українського законодавства, спроби формування цілісної системи захисту від маніпулятивних впливів у політичному дискурсі стикаються з рядом викликів.

Ці виклики включають внутрішні протиріччя в законодавстві, що обмежують ефективність захисту громадян від маніпуляцій, а також складність визначення межі між захистом від маніпуляцій та обмеженням свободи слова.

Це створює потребу в додаткових дослідженнях та розробці збалансованих правових механізмів, які змогли б захистити суспільство від недобросовісних впливів, не обмежуючи при цьому основоположні демократичні права.

Друга стратегія захисту від маніпуляцій передбачає не лише усвідомлення маніпулятивних інтенцій, але й здатність застосувати можливі дії та реакції на них. Такий підхід вимагає від особистості розвитку критичного мислення та аналітичних навичок, які дозволяють не тільки ідентифікувати маніпулятивні повідомлення, але й ефективно захищатись від них, формуючи обгрунтовану власну думку.

Третя стратегія акцентує на розробці специфічних методів протидії маніпуляціям, заснованих на глибокому розумінні конкретних тем чи проблематик. Важливою частиною цієї стратегії є усвідомлення власної вразливості до маніпулятивних впливів та розвиток здатності своєчасно розпізнавати та нейтралізувати потенційні маніпуляції. Такий підхід не лише зміцнює індивідуальну стійкість до маніпуляцій, але й сприяє розвитку навичок організації інформації та психологічного захисту, підвищуючи загальну інформаційну резилієнтність особистості.

У сучасному медійному ландшафті, де пропагандистські впливи стають дедалі вишуканішими і всеохоплюючими, розробка стратегій опору вимагає комплексного підходу, заснованого на розумінні основних механізмів маніпуляції. Серед них, активна протидія та пасивний захист виступають як дві основні стратегії, кожна з яких має свої особливості та область застосування в залежності від контексту і мети маніпулятивного впливу.

Активна протидія заснована на розумінні та визнанні маніпуляції, що вимагає від осіб критичного аналізу отриманої інформації та здатності ідентифікувати потенційні маніпулятивні техніки. Такий підхід передбачає

освітні програми, розвиток медіаграмотності, а також навчання розпізнаванню емоційних апелів та логічних помилок у аргументації. Водночас, активна протидія може включати і розвиток навичок опору маніпуляції, таких як формулювання контраргументів та участь у публічному діалозі.

Пасивний захист, в свою чергу, випливає з еволюційного розвитку суспільства та включає функціонування психічних захисних механізмів, як-от придушення, раціоналізація та ідентифікація. Ці механізми, діючи на підсвідомому рівні, допомагають індивідам захистити себе від психологічного дискомфорту, що виникає в результаті маніпуляцій. Однак, ці захисні механізми можуть спотворювати реальне сприйняття, віддаляючи особу від раціонального аналізу ситуації і рішень.

Складність проблеми маніпуляції посилюється, коли мас-медіа виступають не просто як інструменти інформаційного впливу, а як засоби масової маніпуляції, що охоплюють широку аудиторію і впливають на формування суспільної думки. В таких умовах, забезпечення ізоляції від маніпулятивного впливу є вкрай складним, а іноді і неможливим, задачею.

Для розробки ефективних методів протидії необхідне глибоке розуміння цілей маніпуляції, які можуть охоплювати вплив на думки, емоції та поведінку особистості. У цьому контексті, важливо розробляти стратегії, які враховують комплексність людської психіки, здатні адаптуватися до різноманітних форм та каналів маніпуляції, і спроможні протистояти як емоційним, так і раціональним впливам. Це може включати розвиток програм, спрямованих на підвищення критичного мислення, емоційного інтелекту, а також формування стійкості до психологічного тиску і маніпуляцій, які спрямовані на маніпулювання емоціями та переконаннями.

Важливо зауважити, що емоції та афекти є основними інструментальними цілями маніпуляторів. Проте емоційна, поведінкова та когнітивна сфери не є лише мішенями, а й інструментами проти маніпуляції [28].

Афективна сфера індивіда грає важливу роль у виявленні та усвідомленні маніпулятивних втручань. Вона діє як інтуїтивний сенсор, що попереджає особу

про потенційно небезпечні або маніпулятивні повідомлення. Однак, існує значна переоцінка власних когнітивних здібностей, що може зробити когнітивну сферу особливо вразливою до маніпуляцій. Люди схильні приймати інформацію за вірну, якщо вона представлена з використанням розумних аргументів, особливо коли ці аргументи активізують емоційну реакцію.

Ця тенденція стає особливо помітною у контексті політичних кампаній, де маніпулятивні техніки, спрямовані на емоції, можуть значно впливати на увагу електорату до певних питань. Маніпуляції, які спотворюють реальність або приділяють надмірну увагу певним фактам, можуть змінити сприйняття важливості теми або події, відволікаючи від більш критичних питань.

Проте, когнітивна сфера надає інструменти для критичної оцінки інформації, які є ключовими для протидії маніпуляціям. Критичне мислення дозволяє особі піддавати сумніву достовірність, джерела інформації та потенційні упередження, що можуть спотворити повідомлення. У контексті суспільного дискурсу та виборчих кампаній, особливо в умовах інформаційної війни та активних збройних конфліктів, такий обережний аналіз стає ще більш критично важливим.

Поведінка індивіда є результатом взаємодії його волі, інтелекту та емоцій. У сучасних умовах, коли застосування репресивних методів має обмеження, важливість критичного мислення перед виявленням підтримки політичним силам набуває нового значення. Задаючи собі питання "Що я роблю?" та "Чому я повинен це робити?", індивід може здійснювати більш обдумані та відповідальні політичні рішення, засновані не на емоційних імпульсах або маніпулятивних техніках, а на раціональному аналізі та переконаннях.

Здатність індивіда до опору маніпуляціям, за оцінкою Л. Кучми, є результатом складної взаємодії між зовнішніми та внутрішніми факторами. Оптимальна здатність до протидії включає не лише наявність знань про методи та характеристики маніпуляцій, але й підтримку соціального оточення. Такий підхід підкреслює важливість колективних зусиль у боротьбі з маніпулятивними впливами.

Колективний захист передбачає злагоджену взаємодію на різних рівнях суспільства, від окремих осіб до інституцій громадянського суспільства, включаючи урядові структури, освітні установи, та медійний сектор. Це може охоплювати впровадження освітніх програм, спрямованих на розвиток критичного мислення та медіаграмотності, моніторинг медійного простору для виявлення маніпулятивних повідомлень, та створення альтернативних інформаційних мереж, які б пропонували перевірену та надійну інформацію.

Інформаційно-психологічна безпека є ключовою для захисту осіб та соціальних груп від деструктивних інформаційних впливів. В умовах глобальних викликів та процесів демократизації, що актуальні для України, важливо, щоб усі сегменти суспільства — від держави до окремих громадян — розуміли потенційний вплив інформаційно-психологічних операцій на прийняття рішень, поведінку, та соціальне планування. Це підкреслює необхідність активних дій з боку індивідів для протидії цим загрозам, зокрема через освітні та саморозвиткові програми.

У цьому контексті, роль держави та суспільства в інформаційно-психологічній безпеці не може бути переоцінена. Від урядових ініціатив до громадських рухів та індивідуальної відповідальності кожного громадянина — усі рівні взаємодії є важливими для створення стійкого та захищеного інформаційного простору.

Підривна діяльність російських медіа становить серйозну загрозу для національної безпеки України, викликаючи необхідність ефективної протидії не лише на військовому, а й на інформаційному фронті. Як підкреслює В. Василенко, русифікація України та спроби втягнути її в так званий "русский мир" є частиною більш широкої стратегії, яка має на меті підірвати українську національну ідентичність. Ці дії включають мілітаризовану агресію та інформаційно-пропагандистські кампанії, спрямовані на ерозію мови, культури, історії та, в остаточному підсумку, самої ідеї незалежної української державності.

У відповідь на ці виклики, ключовим елементом стратегії України має стати збереження національної ідентичності. Це означає не лише відродження та підтримку української мови, культури та історичної пам'яті, а й підтримку критичного мислення серед громадян. Здатність критично аналізувати інформацію, розрізняти факти від маніпуляцій, є життєво важливою в умовах інформаційного протистояння.

Розвиток медіаграмотності серед населення є одним із найефективніших інструментів у боротьбі з пропагандою та інформаційними впливами. Освітні програми та ініціативи, спрямовані на розвиток навичок критичного сприйняття медіа, можуть допомогти громадянам уникати впливу маніпулятивних повідомлень. Підтримка незалежних медій, які пропонують перевірену та збалансовану інформацію, також відіграє важливу роль у формуванні об'єктивного світогляду.

Соціальна та громадянська активність є невід'ємною частиною захисту національних інтересів. Демонстрація лояльності до держави, активна участь у громадському житті та захист своїх прав та свобод — всі ці аспекти сприяють зміцненню демократичних засад і національної безпеки. Важливо, що кожен громадянин відчував свою відповідальність за долю країни та був готовий захищати її на різних рівнях.

На міжнародному рівні, Україна може залучати підтримку та співпрацю з іншими державами для ефективної протидії інформаційній агресії. Обмін досвідом, спільні освітні проєкти та медійні ініціативи можуть значно підвищити стійкість до пропаганди не лише в Україні, але й у світовому масштабі. Зміцнення міжнародної співпраці в інформаційній сфері дозволить створити більш безпечне інформаційне середовище та захистити демократичні цінності.

Адекватна гуманітарна та інформаційна політика є фундаментом зміцнення національної безпеки кожної держави, особливо в умовах сучасних викликів. У контексті України, роль медіа та соціально-комунікаційної складової в державній політиці набуває особливої ваги. Неадекватне управління

інформаційним простором може призвести не лише до внутрішніх соціальних напружень, але й до міжнародних криз, як це було у 2013 та 2022 роках в Україні. Ці події виявили критичну потребу в розумінні впливу інформаційних кампаній на суспільну думку та національну безпеку.

Інформаційні кампанії, що супроводжували анексію Криму Росією, конфлікт на Донбасі та повномасштабне вторгнення, демонструють, як інформаційні війни ведуться за допомогою маніпуляцій та дезінформації. Росія використовувала широкий спектр інформаційних засобів для досягнення своїх цілей, включаючи пропаганду через державні медіа, соціальні мережі та інші платформи. Розуміння цих методів та стратегій є важливим для розробки ефективних контрзаходів.

Вплив Росії на інформаційний простір України має глибокі корені, що сягають 1990-х років, коли за допомогою своїх медійних ресурсів Росія змогла здобути значний вплив на українське телебачення, радіомовлення, розважальну індустрію та видавничу справу. Це стало можливим завдяки державному фінансуванню російської продукції та активному лобіюванню з боку деяких українських політиків, що сприяло русифікації інформаційного простору.

У 2000-х роках, на тлі збільшення цін на нафту і газ, Росія значно підсилила свій економічний та інформаційний вплив на Україну. Розширення економічних можливостей дозволило Росії збільшити обсяги фінансування своїх інформаційних операцій, використовуючи медіа як інструмент геополітичної та культурної експансії.

В умовах інформаційної війни, адекватна реакція на інформаційні загрози та розробка стратегій протидії є невідкладним завданням для забезпечення національної безпеки України. Це вимагає зміцнення інформаційної незалежності, підтримки національних медійних інституцій та розвитку медіаграмотності серед населення, щоб українське суспільство могло ефективно протистояти зовнішнім інформаційним впливам.

Розгортання масштабної кампанії зі створення та розповсюдження російських художніх, анімаційних фільмів, серіалів, та телепрограм,

підтриманої державними замовленнями та фінансуванням, мала значний вплив на інформаційний простір України та інших пострадянських країн. Ці медійні продукти, нерідко несучи яскраво виражений ідеологічний зміст, ефективно виконували роль інструментів інформаційної війни, сприяючи підкріпленню російського наративу. Зображення "руського миру" як альтернативи західним цінностям, а також апеляції до ностальгії за радянським минулим, спрямовані на формування позитивного образу Росії та негативних стереотипів про інші культури.

Активне використання новітніх медійних платформ, таких як інтернет-видання, соціальні мережі та форуми, стало ефективним засобом розповсюдження російської пропаганди. Через популярні соціальні мережі, зокрема "ВКонтакте" та Facebook, які користуються великою популярністю серед населення Росії та України, поширюються ключові ідеї російської пропаганди. Це сприяє розпалюванню антиукраїнських настроїв та підтримці сепаратистських тенденцій, поглиблюючи розколи в суспільстві.

В умовах глобального інформаційного простору, де доступ до інформації є майже необмеженим, здатність розрізняти достовірну інформацію від пропаганди стає критично важливою. Розвиток медіаграмотності та критичного мислення серед населення є одним із ключових аспектів протидії інформаційному впливу, що має на меті маніпулювати громадською думкою та посилювати соціальні розбіжності.

У цьому контексті, значення національної інформаційної політики, яка зосереджена на підтримці незалежних медіа, захисті культурної ідентичності, та просуванні об'єктивної інформації, стає надзвичайно високим. Важливою складовою цієї політики є також співпраця з міжнародними партнерами для забезпечення більшої координації у боротьбі з інформаційними загрозами та розробки спільних стратегій протидії пропаганді.

Таким чином, усвідомлення ролі медіа та соціально-комунікаційних платформ у сучасному світі є вирішальним для формування ефективної стратегії національної безпеки. Зміцнення інформаційної резилієнтності країни,

розвиток медіаграмотності населення та підтримка незалежних медійних ініціатив є ключовими аспектами у захисті суверенітету та культурної ідентичності України в умовах інформаційної війни.

Кремль має спеціальну "армію" оплачуваних інтернет-ботів, чия робота полягає в розміщенні пропагандистських коментарів на соціальних мережах та форумах з метою впливу на громадську думку не лише в росії та Україні, а й у Європі та США [28].

Українська медійна сфера зіткнулася з викликом недостатньої готовності протистояти російським інформаційно-технологічним стратегіям. Це призвело до того, що вітчизняні медіа, невміло керуючи інформаційними потоками, стали неусвідомленими розповсюджувачами російської пропаганди.

Одним з прикладів такої діяльності є заміна ключових термінів, що описують агресивні дії Росії, на більш нейтральні вирази, зокрема "окупанти" і "російські війська" на "зелені чоловічки". Такі мовні маніпуляції не лише спотворюють реальність, але й надають легітимності самопроголошеним лідерам сепаратистських угруповань, вводячи поняття "народний мер" та "народний губернатор".

Росія, в свою чергу, проводила цілеспрямовану підготовку до інформаційно-ідеологічної конфронтації протягом багатьох років, використовуючи глобальний досвід у сфері соціальних і масових комунікаційних технологій. Численні наукові роботи російських авторів, присвячені інформаційній війні та її використанню для досягнення геополітичних цілей, свідчать про адаптацію західних комунікаційних теорій до потреб офіційної кремлівської пропаганди.

Комбінуючи методи радянської авторитарної пропаганди з сучасними західними інноваціями у сфері комунікацій, Росія розробила ефективну модель інформаційного впливу.

Ця модель була закріплена на державному рівні через такі документи, як оновлена Концепція зовнішньої політики та Федеральний закон "Про державну

політику Росії у зв'язках зі співвітчизниками за кордоном", що демонструє стратегічний підхід до використання інформаційних технологій.

Для ефективної протидії російській пропаганді та інформаційному впливу, Україні необхідно розробити комплексну стратегію, яка охоплюватиме підвищення рівня медіаграмотності населення, підтримку незалежних медійних ініціатив та розвиток власної інформаційної інфраструктури. Також важливим є залучення міжнародного досвіду та кооперація з міжнародними партнерами для обміну знаннями та ресурсами у боротьбі з інформаційним впливом.

Створення міцної, різноманітної та незалежної медійної сфери є ключовим елементом у забезпеченні інформаційної безпеки держави. Це вимагає як внутрішніх зусиль з боку уряду та громадськості, так і зовнішньої підтримки та солідарності міжнародної спільноти. Тільки через спільні дії можна протистояти викликам, які ставить перед Україною сучасна інформаційно-технологічна війна.

Вплив Росії на сусідні держави, зокрема на Україну, визначається стратегією руйнування національних ідентичностей та сприяння інтеграції громадян цих країн у "руський мир".

Ця стратегія реалізується через мас-медіа, що пропагують російсько-євразійську ідентичність, метою якої є стирання кордонів між культурами та перетворення сусідніх народів на частину єдиного російського культурного простору.

Застосування медій та технологій соціальної комунікації мало на меті вплинути на свідомість громадян України, ускладнивши процес формування української національної ідентичності, особливо серед старшого покоління у східній та південній частинах країни.

Ці заходи сприяли збереженню радянсько-російської ментальності та україно фобії серед частини населення, включаючи молодь, що зумовило глибокий культурний розкол.

Особливу увагу Росія приділяла населенню Кримського півострова та Донбасу, що постійно перебувало під впливом російських медіа з моменту

проголошення незалежності України. Посилене російське мовлення на цих територіях перед окупацією сприяло зростанню сепаратистських настроїв, використовуючи як інструмент кримінальні моделі поведінки та дискредитацію української державності.

За словами В. Голубріна, російська розвідка активно веде інформаційну війну проти України, використовуючи фейкові новини для створення негативного образу українського уряду та збройних сил, звинувачуючи їх у фашизмі, репресіях та застосуванні біологічної зброї. В цій війні активно застосовуються відеоматеріали, вирвані з контексту, та фейкові фотографії для дискредитації України на міжнародній арені.

Така систематична інформаційно-пропагандистська кампанія вимагає від України розвитку ефективних механізмів протидії, зокрема через зміцнення інформаційної безпеки, підтримку незалежних медіа та формування критичного мислення серед населення. Важливою складовою захисту національної ідентичності є також активізація громадянського суспільства та залучення міжнародної підтримки для протистояння зовнішньому інформаційному впливу.

Російська інформаційна кампанія, націлена на підрив внутрішнього та міжнародного іміджу України, підкреслює критичну необхідність розвитку та активізації української інформаційної політики. Це особливо важливо для протидії не лише поточним, але й майбутнім інформаційним загрозам. Російські спецслужби використовують різноманітні методи для дискредитації України, включаючи фальсифікації процесу мобілізації, що створює додаткові виклики для збереження соціальної стабільності та об'єднання громадянського суспільства.

Зусилля, спрямовані на дискредитацію мобілізації в Україні, включають тактики, як-от затримання молодих людей на вулицях та розповсюдження чуток через соціальні мережі про нібито примусове відправлення до зони бойових дій. Такі дії спрямовані на посіяння страху та недовіри серед населення, що є частиною ширшої стратегії психологічного тиску.

Цей комплексний підхід до пропаганди, що був активно використаний російськими агентами ще до подій Революції Гідності та значно посилений після 2014 року, демонструє стратегічне планування та впровадження інформаційної війни проти України. Це свідчить про необхідність постійного моніторингу інформаційного простору та розвитку засобів протидії дезінформації та маніпуляціям.

У відповідь на ці виклики, Україні необхідно зміцнювати власні інформаційні ресурси, розвивати стратегії комунікації, які сприятимуть формуванню позитивного національного образу та протистоянню спробам зовнішнього втручання у внутрішні справи. Залучення громадянського суспільства, зміцнення медійної грамотності населення та підтримка незалежних медіа стануть ключовими складовими успішної інформаційної політики.

Важливою стратегією протидії інформаційній агресії є також міжнародна співпраця та обмін досвідом із країнами, які зіткнулися з подібними викликами. Спільні зусилля допоможуть сформувати більш ефективні механізми захисту інформаційного простору, а також забезпечити підтримку України на міжнародному рівні у боротьбі з інформаційною війною.

Так, згідно з опитуванням, проведеним у лютому 2014 року, 78% жителів сходу та півдня України вважали російські телеканали головним джерелом політичних новин [28].

Після офіційного припинення ретрансляції деяких російських телеканалів, значна частина місцевих телекомунікаційних операторів у східних регіонах України продовжувала надавати доступ до їх мовлення. Цей факт мав суттєвий вплив на формування громадської думки, що підтверджено результатами соціологічного опитування, проведеного у квітні 2014 року.

Згідно з даними опитування, 17% населення Луганської та Донецької областей висловили підтримку ідеї відокремлення цих регіонів від України та створення незалежної держави. Такий рівень підтримки свідчить про значний вплив російської пропаганди на настрої частини мешканців цих територій.

В контексті міста Донецьк, опитування виявило, що страх перед "бандитами" з Західної України був висловлений 60% опитаних, тоді як 47% респондентів вбачали загрозу у діях центральної влади в Києві. Це демонструє, як ефективно російські медіа змогли створити образ "ворожого" українського уряду та націоналістичних рухів. Західні та американські політики також були представлені як загроза 38% респондентів, що свідчить про успіх спроб Росії представити зовнішнє втручання як ключовий чинник української кризи.

В Луганській області, проросійські настрої були виявлені серед 95% населення деяких населених пунктів, що є вражаючим показником.

Однак, в історично українізованих районах така підтримка складала лише 30%. Це підкреслює, що вплив пропаганди може значно варіюватися залежно від культурних, історичних та регіональних особливостей населення.

Дії Росії в інформаційній сфері були спрямовані на дискредитацію української влади, Збройних Сил та українського суспільства в цілому, використовуючи неправдиву інформацію про "фашистський режим" в Києві, міфи про звірства "бандерівців", та маніпуляції з відеофрагментами. Фейкові новини та зображення, поширені через соціальні мережі, слугували засобом посіяння страху, недовіри та розколу серед українського населення.

Отже, інформаційна агресія Росії виявилася комплексною та багатовекторною, включаючи не тільки традиційні медіа, але й цифрові платформи для досягнення своїх цілей. У відповідь на цю загрозу, Україні необхідно розвивати власні інформаційні ресурси та стратегії для захисту національної ідентичності, зміцнення державного суверенітету та протидії інформаційним атакам.

Методи маніпуляції, які Росія застосовувала у своїй інформаційній кампанії проти України, справді суперечать міжнародним нормам, зокрема Європейській конвенції про транскордонне телебачення. Згідно зі статтею 7 цієї конвенції, програми повинні підтримувати гідність людини та основоположні права, уникаючи неправдивої інформації та сприяння расовій чи будь-якій іншій формі неприязні.

В умовах повномасштабної інформаційної агресії, яку здійснює проти України зовнішній агресор, необхідною є всебічна відповідь на державному рівні. Це включає розробку чітких механізмів для ідентифікації пропаганди та маніпуляцій, оцінку їх впливу на внутрішній і міжнародний імідж країни, а також розробку стратегій протидії. Важливим є створення аналітичних центрів та розвиток досліджень, що зосереджуються на вивченні гібридної війни та інформаційних атак.

Залучення вітчизняних науковців та експертів до розробки комплексу заходів є критично важливим для формування ефективної відповіді на інформаційні загрози. Створення мережі науково-дослідних інституцій та аналітичних центрів дозволить систематизувати зусилля у сфері боротьби з пропагандою та маніпуляціями, забезпечивши Україну необхідними знаннями та інструментами для протистояння інформаційній війні.

Підтримка з боку держави, приватного сектору, та міжнародних організацій є важливою для розвитку аналітичних центрів, наукових досліджень, та забезпечення свободи наукової діяльності. Українські аналітичні центри, маючи унікальне розуміння механізмів гібридної агресії, можуть стати конкурентоспроможними на світовій арені та внести значний вклад у глобальну боротьбу з дезінформацією.

Таким чином, комплексний підхід до боротьби з інформаційною агресією, заснований на розробці ефективних механізмів ідентифікації пропаганди, наукових дослідженнях, та активному залученні спільноти експертів, є ключовим для зміцнення інформаційної безпеки України та протидії зовнішнім загрозам.

Проблема політичних упереджень та їх вплив на об'єктивність досліджень є глобальним викликом, що стосується не тільки України, а й розвинутих демократій, включаючи США. Наукове співтовариство зіштовхується з необхідністю боротьби з національними упередженнями, які можуть спотворювати аналіз питань безпеки та інших глобальних викликів. Це

підкреслює важливість об'єктивності та наукового підходу в дослідженнях, щоб забезпечити точність результатів та ефективне рішення проблем.

У воєнний час повне усунення упереджень стає ще більш складним завданням через посилення національних емоцій та підвищену чутливість до безпекових питань. Проте, розвиток наукового потенціалу в таких умовах може слугувати важливим ресурсом для підвищення об'єктивності досліджень. Зосередження уваги на наукових методах та об'єктивному аналізі даних може сприяти виявленню об'єктивних фактів і формуванню ефективних стратегій вирішення складних соціальних та політичних проблем, включаючи питання післявоєнного відновлення.

Систематичний аналіз, дискусії та міждисциплінарний обмін досвідом вважаються ключовими елементами в процесі подолання упереджень та забезпечення точності наукових досліджень. Взаємодія між науковцями з різних дисциплін та культурних контекстів може збагатити дослідження новими перспективами та сприяти виробленню більш об'єктивного погляду на проблеми, що вивчаються.

У цьому контексті, підтримка наукових досліджень та розвитку наукової спільноти, зокрема через державне фінансування, приватні інвестиції та міжнародну співпрацю, стає критично важливою. Це дозволить не лише зміцнити наукову об'єктивність, але й забезпечити свободу наукових досліджень, яка є фундаментальною для прогресу та інновацій у будь-якому суспільстві.

Отже, важливість зосередження на об'єктивності та наукових методах у дослідженнях, особливо у контексті глобальних безпекових викликів та воєнного стану, не може бути переоцінена. Розвиток наукового потенціалу та взаємодія наукової спільноти мають ключове значення для подолання упереджень і забезпечення точності та ефективності наукових досліджень.

Створення координаційного органу інформаційно-психологічного призначення є важливим кроком для протидії інформаційній експансії та психологічній нестабільності, яку намагається спровокувати зовнішній агресор.

Цей орган повинен займатися психологічною безпекою особистості, суспільства, та держави в цілому, розробляючи та імплементуючи комплекс стратегічних і оперативних заходів проти негативних інформаційних впливів. Така діяльність допоможе зміцнити інформаційну стійкість населення та підвищити рівень національної безпеки.

Не менш важливим є розвиток соціальної безпеки та створення національної системи інформаційного спостереження, яка дозволить проводити глибокий аналіз даних на різних рівнях і використовувати отримані результати у прийнятті рішень щодо забезпечення національної безпеки. Важливість об'єктивності та застосування наукового підходу в цьому процесі не може бути переоцінена, оскільки лише точні та достовірні дані забезпечують ефективність прийнятих заходів.

Вивчення історичного досвіду та культурної пам'яті також відіграє ключову роль у протидії інформаційній агресії та відновленні національної свідомості. Розуміння історичних подій, спільних цінностей та культурних зв'язків допоможе формувати єдину національну ідентичність, що стане міцним фундаментом для опору дезінформації та зовнішнім інформаційним впливам.

Розуміння механізмів функціонування інформаційних мереж противника є ще одним важливим аспектом ефективної протидії інформаційній війні. Це передбачає не лише ідентифікацію каналів розповсюдження дезінформації, але й розробку контрзаходів, здатних нейтралізувати негативний вплив і захистити суспільство від маніпуляцій.

Таким чином, комплексний підхід до зміцнення інформаційної та психологічної безпеки, який включає створення спеціалізованих органів, розвиток систем спостереження, а також вивчення історичного та культурного контексту, є ключовим для захисту національних інтересів та забезпечення стабільності в умовах інформаційної війни.

Також необхідно взяти до уваги процес інтеграції систем розвідки та управління Росії з аналогічними системами України, оскільки це підкреслює

потребу у розробці та впровадженні ефективних заходів для зниження впливу зазначеної інтеграції на національну безпеку та суверенітет України.

Вказані аспекти можуть слугувати ключовими елементами у формуванні комплексної стратегії протидії інформаційній агресії та зміцненню національної резилієнтності у контексті інформаційних викликів. З наукової точки зору, стратегія побудови позитивного громадського дискурсу в умовах збройного конфлікту на території України розглядається як довготерміновий комплекс заходів, спрямованих на досягнення конкретних цілей у міжнародному інформаційному просторі.

Ця стратегія включає взаємодію зі спеціалізованими інформаційно-психологічними структурами на різних рівнях державного, регіонального та місцевого управління в Україні, акцентуючи на важливості їхнього партнерства з медійними організаціями.

Медіа відіграють ключову роль у формуванні громадської думки через розповсюдження інформаційних повідомлень та коментарів. Стратегічна взаємодія з медіа охоплює наступні напрямки:

1) негайне поширення достовірної та об'єктивної інформації про діяльність українських військових у зоні конфлікту;

2) розробка та розповсюдження інформаційних, довідкових та роз'яснювальних матеріалів для спрощення процесу комунікації з органами влади та силовими структурами;

3) аналіз громадської реакції на дії державних органів під час конфлікту з метою адаптації інформаційної стратегії;

4) розвиток стратегічної та оперативної взаємодії з медійними представниками;

5) організація заходів, брифінгів та інтерв'ю з керівництвом держави, правоохоронних органів та представниками сектору безпеки;

6) розповсюдження друкованої, аудіо- та відеоінформації про активності Збройних Сил України та управлінську систему в умовах конфлікту, включаючи розвіддані;

7) проведення системного аналізу публікацій, пов'язаних із діяльністю органів влади та силових структур;

8) надання ексклюзивної інформації медіа про оперативну ситуацію; 9) захист прав та інтересів державних органів у випадку неправдивого зображення інформації.

Сучасна інформаційна війна представляє собою складний процес соціальної взаємодії, де учасники, регулюючи свою поведінку в рамках власних світоглядних орієнтирів, використовують різноманітні форми інформаційного впливу.

Лідери світових держав використовують інформаційний потенціал для досягнення різноманітних цілей, включно з військовими, політичними, культурними, та економічними. Прикладом є Національна стратегія кібербезпеки США, країни з великим досвідом у сфері кібербезпеки, що продовжує боротьбу з кіберзагрозами. Збільшення частоти та складності кібератак вимагає від усіх учасників — як державних, так і приватних — адаптації захисних механізмів та розробки нових методів протидії.

В контексті глобальної інформаційної безпеки, важливою є робота над створенням ефективних стратегій протидії інформаційним загрозам, що включають як захист від кібератак, так і протидію дезінформації. Інтеграція спеціалізованих розвідувальних структур у склад спецпідрозділів, як зазначає М. Сенченко, дозволяє забезпечити ефективне протистояння розвідувальним загрозам, як у оборонному, так і в наступальному планах.

Також, зростання інформаційного впливу на міжнародну політику та безпеку підкреслює необхідність міждержавної та міжсекторальної співпраці. Створення міжнародних альянсів та партнерств для обміну інформацією та досвідом у сфері кібербезпеки та інформаційної війни може значно зміцнити глобальну стійкість до цих загроз.

Усвідомлення глобального характеру інформаційної війни, розуміння її складності та різноманітності методів впливу вимагають комплексного підходу до розвитку стратегій безпеки, зосередження на наукових дослідженнях та

технологічних інноваціях. Такий підхід дозволить ефективно протистояти інформаційним загрозам та забезпечити стабільність та безпеку на національному та міжнародному рівнях.

Охорона інформації та кіберінфраструктури в сучасному світі вимагає від держави не тільки технічних заходів, а й політичної волі та стратегічного планування. Враховуючи виклики, перед якими стоїть Україна, впровадження спеціалізованих кібернетичних підрозділів у структурі ЗСУ стає критично важливим аспектом забезпечення національної безпеки. Такі підрозділи, до складу яких входитимуть фахівці з різних сфер, відіграють ключову роль у захисті вітчизняних інформаційних ресурсів від кіберзагроз.

Координація з різними державними установами, взаємодія з медіа та науковою спільнотою є важливою для створення ефективної системи кібербезпеки. Такий підхід дозволить не тільки виявляти та нейтралізувати потенційні загрози, але й адекватно інформувати суспільство про реальні виклики та загрози, з якими воно стикається.

Розробка комплексних стратегічних рішень, включаючи створення "Центру інформаційного управління", антикризового центру у форматі державного медіа-холдингу, та спеціалізованих центрів для виявлення та нейтралізації критичних об'єктів противника, є актуальним в умовах інформаційних викликів.

Такий підхід не лише сприятиме захисту держави від зовнішньої агресії, але й забезпечить належний рівень інформаційної безпеки.

Створення національної комплексної системи інформаційної боротьби, що дозволяє контролювати національний інформаційний простір і ефективно протидіяти смисловим атакам та деструктивним інформаційним впливам, стане вирішальним кроком у зміцненні національної безпеки. В цьому контексті, підготовка висококваліфікованих фахівців у сферах кібербезпеки та інформаційної безпеки є необхідною для виконання поставлених завдань та ефективного протистояння сучасним інформаційним загрозам.

Підготовка кадрів, здатних забезпечувати ідеологічну та морально-психологічну стабільність суспільства, є суттєвою у вирішенні сучасних інформаційних викликів. Розробка освітньої програми для мультидисциплінарної підготовки фахівців у сфері стратегічного аналізу, інформаційного впливу, та ведення інформаційно-психологічної війни стає невідкладним завданням.

Така програма має включати в себе вивчення методів критичного мислення, аналізу даних, основ кібербезпеки, та особливостей інформаційної війни.

Журналісти, як ключові посередники інформації в суспільстві, потребують особливої уваги у контексті підготовки до протистояння інформаційним загрозам. Розвиток навичок критичного аналізу, верифікації джерел інформації, дотримання етичних стандартів у журналістиці є важливим для підвищення рівня інформаційної безпеки. Враховуючи сучасні виклики, такі як хакерські атаки на медійні компанії та журналістів, освітні програми мають також зосередитися на підготовці фахівців до ефективної роботи в умовах кіберзагроз.

Міжнародний досвід показує, що медійні організації та журналісти часто стають мішенями для хакерських атак, що ставить під загрозу їхню здатність виконувати свої функції. В контексті зростаючої вразливості, особливо в соціальних мережах, зміцнення інформаційної та кібербезпеки стає пріоритетом. Це вимагає не лише підвищення обізнаності та готовності до протидії кібератакам, але й розробки комплексних стратегій захисту інформаційних ресурсів.

За таких умов, формування міцного інформаційного простору вимагає співпраці урядових структур, медіа, наукових інституцій, та громадянського суспільства. Інвестування в освіту та розвиток навичок, необхідних для забезпечення інформаційної безпеки, є важливим кроком у створенні стійкого суспільства, здатного ефективно протистояти інформаційним загрозам та сприяти збереженню демократичних цінностей.

Важливість уваги до безпекових питань в інформаційній сфері є критичною для суспільної стабільності, особливо в умовах, коли не всі інформаційні суб'єкти та об'єкти приділяють цьому належну увагу. В цьому контексті, державні інституції повинні займатися розробленням та імплементацією ефективних захисних стратегій, що є ключовими для забезпечення захисту інформаційної інфраструктури та запобігання дестабілізації суспільства через інформаційні атаки.

Сучасна глобальна ситуація показує, що інформаційна війна вже інтегрована в геополітичні процеси, проте визнання цього факту довго не знаходило розуміння з боку українських політичних еліт.

Розбіжності в підходах та розумінні інформаційних загроз між Україною та західними партнерами можуть послаблювати спільні зусилля у протидії цим загрозам, надаючи перевагу агресору. Різниця в інтерпретації концепції "кібервійни" між Росією та Сполученими Штатами створює додаткові складнощі в співпраці між країнами та розробці єдиної стратегії протидії кіберзагрозам. Росія використовує кіберпростір як елемент ширшої політичної та розвідувальної стратегії, тоді як США та інші країни Заходу розглядають кібервійну як нову форму конфлікту, яка вимагає особливих методів протидії.

Для ефективної боротьби з інформаційними загрозами та кібератаками необхідно:

1. Зміцнити міжнародну співпрацю та координацію зусиль для розробки спільних стандартів кібербезпеки та протидії інформаційним загрозам.

2. Розробити комплексні національні стратегії, що включають як технічні, так і політичні заходи для захисту інформаційної інфраструктури.

3. Провести широкомасштабну освітню кампанію для підвищення обізнаності громадян і організацій про кіберзагрози та методи їхньої протидії.

4. Забезпечити постійний розвиток кібернетичних підрозділів і спеціалізованих центрів з аналізу та нейтралізації кіберзагроз.

Розв'язання цих завдань дозволить не тільки захистити критичну інфраструктуру від кібератак, але й забезпечити стабільність суспільства в умовах постійно зростаючих інформаційних викликів.

У контексті сучасних глобальних інформаційних викликів набуває особливої актуальності розроблення уніфікованої стратегії взаємодії з міжнародними партнерами. Основоположними компонентами такої стратегії мають стати створення незалежних медійних платформ, активізація розвитку інформаційного простору та підвищення рівня якості національних інформаційних продуктів.

Такий підхід забезпечує зміцнення інформаційної сфери та створення більш ефективної системи протидії інформаційним загрозам, підвищуючи стійкість суспільства до інформаційних атак.

Консолідація суспільства в умовах збройної агресії, утвердження державності та незалежності України виступає ключовим елементом зміцнення національної ідентичності та обороноздатності. В цьому аспекті важливу роль відіграє інституційна підтримка, наявність комплексної інформаційної освіти та готовність до ефективних контрзаходів проти інформаційних загроз. Забезпечення належної уваги до цих аспектів сприятиме підвищенню ефективності національної системи інформаційної безпеки.

Розробка та імплементація комплексної стратегії вимагають від державних інститутів не лише технічного забезпечення, але й врахування політичних, соціальних та культурних аспектів. Це передбачає інтеграцію зусиль на всіх рівнях управління, включаючи активну співпрацю з громадськістю, медіа та науковими кругами для створення умов, за яких інформаційна безпека стане невід'ємною складовою національної безпеки.

З огляду на міжнародний досвід, зокрема розбіжності у підходах до інформаційних загроз між різними країнами, Україні необхідно акцентувати увагу на розробці гнучких механізмів співпраці, що дозволяють адаптуватися до змінних умов глобального інформаційного середовища. Взаємодія з

міжнародними партнерами має сприяти обміну досвідом, технологіями та розробкам у сфері кібербезпеки, зміцнюючи глобальну стабільність.

Нарешті, стратегічний аналіз глобальних інформаційних процесів та адаптація до їх динаміки є важливими для формування ефективної відповіді на інформаційні загрози. Це передбачає створення міцної інфраструктури незалежних медіа, розвиток інформаційного простору на основі якісного контенту та виховання суспільної свідомості, здатної критично сприймати інформацію та відстоювати принципи демократії та незалежності.

ВИСНОВОК ДО РОЗДІЛУ 3

Трансформація інформаційної політики Росії щодо України в інформаційну та гібридну війну поставила перед Україною серйозні виклики у сфері забезпечення інформаційної безпеки та захисту власного інформаційного простору. Активне відстеження ситуації на інформаційному фронті та використання широкого арсеналу інструментів для протидії пропаганді є ключовими елементами стратегії України у цій війні.

Розробка та впровадження стратегічного комунікаційного плану, який спрямований на створення позитивного іміджу України на міжнародній арені та вплив на громадську думку, стає вирішальним. Важливою складовою є активна робота з міжнародними партнерами та організаціями, а також ефективне використання різних каналів комунікації для поширення перевіреної та достовірної інформації про події в Україні.

Підвищення рівня інформаційної грамотності населення через освітні кампанії є ще однією важливою стратегією. Навчання громадян розумінню механізмів поширення дезінформації, вмінню критично оцінювати інформацію та відрізняти фейкові новини від достовірних, допомагає зміцнити інформаційну стійкість суспільства.

Значну роль у протидії гібридним загрозам відіграє співпраця з міжнародними партнерами у сфері кібербезпеки. Обмін досвідом, координація зусиль та спільна розробка механізмів захисту від кібератак і інформаційних операцій дозволяють ефективніше протистояти ворожим діям.

У цьому контексті, посилення міжнародного співробітництва, розвиток інформаційної грамотності населення та створення комплексних комунікаційних стратегій стають ключовими елементами у боротьбі з інформаційною агресією.

Ці заходи дозволять не лише захистити інформаційний простір України, але й активно впливати на формування об'єктивної думки про події в країні на

міжнародному рівні, сприяючи зміцненню міжнародного іміджу та політичної підтримки України.

Дослідження зосереджене на аналізі механізмів та заходів, застосованих Україною для забезпечення кібербезпеки в контексті війни з росією виявило, що країна здійснила значні кроки у цьому напрямку. Впровадження комплексу заходів, які охоплюють розвиток кібербезпеки, криптографії, контролю над інформаційним простором, медіаосвіти та боротьби з дезінформацією, свідчить про відданість України створенню ефективної системи протидії інформаційним загрозам.

Проте, незважаючи на досягнуті успіхи, існують певні прогалини та виклики, які потребують уваги та вдосконалення. Зокрема, важливим аспектом є розвиток міжнародної співпраці з організаціями, такими як НАТО, ОБСЄ та ЄС, що відкриває нові перспективи для зміцнення інформаційної безпеки та інтеграції України у глобальні безпекові альянси.

Інформаційна безпека охоплює не тільки технічні аспекти, але й широкий спектр соціально-політичних, культурних та економічних факторів, що вимагає комплексного та мультидисциплінарного підходу до забезпечення захисту інформаційного простору. Цей підхід передбачає інтеграцію технічних, організаційних, правових та освітніх зусиль для створення всебічної та ефективної системи кібербезпеки.

Активне залучення міжнародних партнерів та використання їхнього досвіду та ресурсів дозволить Україні ефективніше протистояти сучасним викликам у сфері кібербезпеки, а також сприятиме створенню умов для її інтеграції в міжнародні безпекові структури. Розвиток міжнародної співпраці, зокрема у сфері обміну інформацією про кіберзагрози та координації зусиль з їх нейтралізації, стане ключовим фактором у підвищенні рівня національної безпеки.

Таким чином, забезпечення інформаційної безпеки в умовах війни з росією вимагає від України не лише застосування внутрішніх заходів та ресурсів, але й активної міжнародної співпраці. Це дозволить не тільки

вирішити існуючі проблеми та прогалини у системі кібербезпеки, але й зміцнити стійкість України до зовнішніх загроз, сприяючи її стратегічній безпеці на міжнародному рівні.

Законодавство України у сфері інформаційної безпеки створює умови для формування єдиної концепції та державної політики в цій галузі, сприяючи визначенню ключових цілей, суб'єктів безпеки та відповідних правових рамок діяльності органів, задіяних у забезпеченні інформаційної безпеки країни. Законодавча база встановлює чіткі механізми координації між різними учасниками процесу – від державних структур до медіа – для ефективного реагування на інформаційні загрози національній безпеці.

Згідно з законодавчими нормами, визначені процедури регулюють взаємодію між органами національної безпеки та іншими державними, приватними та громадськими суб'єктами, що беруть участь у забезпеченні інформаційної безпеки. Це дозволяє створити системний та організований підхід до протидії інформаційним загрозам.

Формування українського наративу та забезпечення інформаційної безпеки вимагають злагодженої взаємодії між усіма рівнями влади, як в межах країни, так і на міжнародній арені. Важливу роль відіграє прозора комунікація з громадськістю, що передбачає відкрите інформування про поточну ситуацію та роз'яснення прийнятих заходів безпеки.

Особлива увага приділяється розвитку механізмів забезпечення національної безпеки в інформаційному просторі, який включає захист критичної інфраструктури, протидію кіберзагрозам, боротьбу з дезінформацією, а також зміцнення медійної грамотності населення. Це дозволяє створити ефективний бар'єр проти зовнішнього впливу та внутрішньої дестабілізації.

Таким чином, українське законодавство в сфері інформаційної безпеки покликане забезпечити комплексний підхід до захисту інформаційного простору країни, координуючи дії різних суб'єктів і залучаючи до співпраці міжнародні організації. Реалізація цієї політики потребує не лише правового

регулювання, а й активної участі всіх зацікавлених сторін, що сприятиме зміцненню національної безпеки та суверенітету України.

Забезпечення інформаційної безпеки в Україні представляє собою комплексне завдання, яке об'єднує технічні, правові, освітні та організаційні аспекти, вимагаючи від держави цілісного та багатогранного підходу. Важливим елементом ефективного захисту національного інформаційного простору є розвиток внутрішніх ресурсів та співпраця на міжнародному рівні, що дозволяє об'єднати зусилля для досягнення стратегічних цілей національної безпеки.

В умовах збройного конфлікту, особлива увага зосереджується на інформаційній безпеці як ключовому елементі захисту національних інтересів і суверенітету. Державні органи мають активно імплементувати стратегічні плани, націлені на протидію ворожій пропаганді та дезінформації, співпрацюючи з громадянським суспільством для формування об'єктивного іміджу України та забезпечення доступу до правдивої інформації.

Міжнародна співпраця відіграє ключову роль у підсиленні інформаційної безпеки, дозволяючи Україні інтегруватися у глобальні безпекові ініціативи, обмінюватися досвідом та впроваджувати кращі практики в сфері кібербезпеки та протидії дезінформації. Важливим аспектом є також підтримка з боку міжнародних організацій та союзників, які можуть надавати технічну та консультативну допомогу.

Освітні ініціативи та програми з підвищення медійної грамотності населення є невід'ємною частиною стратегії забезпечення інформаційної безпеки, оскільки вони сприяють формуванню критичного мислення, здатного розрізняти дезінформацію та фейки. Такий підхід не тільки зміцнює інформаційний суверенітет країни, але й сприяє формуванню відповідального ставлення до споживання інформації серед громадян.

З огляду на ці аспекти, забезпечення інформаційної безпеки в Україні вимагає інтегрованого підходу, який включає посилення внутрішніх інституційних механізмів, активізацію міжнародної співпраці, розвиток освітніх

програм та залучення широких верств населення до процесу формування інформаційної стійкості суспільства.

Такі заходи дозволять Україні ефективно протистояти інформаційним загрозам, зміцнити національну безпеку та захистити інформаційний простір країни.

ВИСНОВКИ

1. У процесі дослідження політологічних та міждисциплінарних аспектів розуміння сутності інформаційної безпеки було встановлено, що цей феномен є багатовимірним і охоплює технічні, соціальні, правові, політичні та культурні аспекти. Інформаційна безпека в сучасному інформаційному суспільстві визначається як складне поєднання державності, ефективного управління загрозами та ризиками, а також забезпечення оптимальних методів запобігання та мінімізації негативних наслідків.

Аналіз правових, соціальних та економічних аспектів інформаційної безпеки показав, що її забезпечення вимагає інтегрованого підходу, який включає взаємодію різних суб'єктів – від індивідуальних громадян до державних органів. Встановлено, що зростання міжнародної напруженості та активізація гібридних воєн вимагають нових підходів до захисту інформаційного простору. Особлива увага приділяється правовому регулюванню, яке встановлює рамки для регулювання інформаційних відносин та забезпечує юридичну основу для охорони інформаційної безпеки

2. В ході дослідження було виявлено, що теоретичні основи дослідження суспільно-політичної стабільності включають інституційний підхід, який дозволяє глибше зрозуміти механізми взаємодії між різними суб'єктами в контексті інформаційного простору. Цей підхід забезпечує аналіз правових, соціальних та економічних аспектів, які формують умови для забезпечення стабільності на національному та міжнародному рівнях.

Акцентовано увагу на важливості підтримки політичної влади у суспільстві, що сприяє запобіганню конфліктам і збереженню національної єдності. Підтримка громадянської злагоди та ідеологічної єдності є ключовими факторами, що впливають на стабільність політичної системи. Важливу роль у цьому процесі відіграють політичні партії, які забезпечують представництво інтересів різних соціальних груп і сприяють легітимізації політичної влади через виконання передвиборчих програм.

3. Дослідження системи інформаційної безпеки як елемента суспільно-політичної стабільності вимагає використання комплексного підходу, що поєднує аналітичні, порівняльні та емпіричні методи. Основою цього підходу є аналіз правових, соціальних та економічних аспектів, які визначають умови для ефективного функціонування інформаційної безпеки на національному та міжнародному рівнях. Аналітичний метод дозволяє глибоко оцінити діяльність інституцій, залучених до забезпечення інформаційної безпеки, та визначити їхній вплив на суспільно-політичну стабільність.

Порівняльний метод застосовується для оцінки ефективності різних інституційних механізмів і підходів, які використовуються у різних країнах. Це дозволяє виявити найкращі практики і адаптувати їх до національних умов. Метод аналізу випадків надає можливість вивчити конкретні приклади інформаційних загроз та ефективності застосованих контрзаходів. Зокрема, аналізуються методи інформаційного впливу та маніпуляцій, використовувані під час гібридних воєн, і їхній вплив на суспільно-політичну стабільність держави

4. Суспільно-політична стабільність є результатом взаємодії низки чинників, серед яких важливе місце займає інформаційний компонент. Основні чинники, що впливають на суспільно-політичну стабільність, включають політичну легітимність, економічну стабільність, соціальну згуртованість та ефективність державних інститутів. У цьому контексті інформаційна безпека виступає як критичний елемент, що забезпечує стабільність через захист інформаційного простору від внутрішніх та зовнішніх загроз.

Роль інформаційного компоненту у забезпеченні суспільно-політичної стабільності проявляється у здатності держави ефективно протистояти дезінформації, інформаційним атакам та маніпуляціям. Висвітлення важливості медіаграмотності населення та інформаційної культури підтверджує, що освітні програми і ініціативи, спрямовані на підвищення критичного сприйняття інформації, є ключовими для формування стійкого інформаційного середовища.

Це дозволяє зменшити вплив ворожих інформаційних кампаній і сприяє збереженню внутрішньої єдності та політичної стабільності.

Визначено, що міжнародні інформаційні конфлікти значною мірою впливають на суспільно-політичну стабільність країн. Глобальні інформаційні потоки та медійні кампанії можуть використовуватися для дестабілізації ситуації в окремих державах. У зв'язку з цим важливою є розробка національних стратегій інформаційної безпеки, що включають вдосконалення законодавчої бази, розвиток технологічної інфраструктури та підвищення рівня медіаграмотності населення. Комплексний підхід до забезпечення інформаційної безпеки сприяє зміцненню суспільно-політичної стабільності і підвищенню стійкості держави до зовнішніх інформаційних загроз

5. Політична стабільність в умовах інформаційного суспільства стикається з численними викликами, серед яких ключовими є гібридні загрози, інформаційно-психологічні впливи та швидкі зміни в інформаційному середовищі. Зростання масштабів інформаційних атак та дезінформаційних кампаній потребує від держав розробки ефективних механізмів протидії, які включають вдосконалення законодавчої бази, розвиток технологічної інфраструктури та підвищення рівня медіаграмотності населення.

Одним із основних механізмів забезпечення політичної стабільності є створення і підтримка системи інформаційної безпеки, яка охоплює моніторинг і аналіз інформаційних потоків, ідентифікацію загроз та їх нейтралізацію. Державні інститути, зокрема, повинні активно залучати експертів, журналістів та громадські організації до формування стратегій протидії інформаційним загрозам. Важливу роль відіграє міжвідомча координація та міжнародна співпраця, що дозволяє адаптувати найкращі практики та технологічні рішення для захисту національних інтересів.

Інформаційна культура та медіаграмотність населення є критичними факторами для зміцнення політичної стабільності. Освітні програми та ініціативи, спрямовані на підвищення критичного мислення, здатність до аналізу та оцінки інформації, сприяють зменшенню впливу дезінформації та

маніпуляцій. Таким чином, комплексний підхід до забезпечення політичної стабільності в інформаційному суспільстві включає розвиток технологій, посилення правового регулювання, підвищення обізнаності громадян та створення ефективних механізмів міжнародної співпраці.

Аналіз сучасних дискурсів щодо інформаційної безпеки виявив її мультидисциплінарний характер, який охоплює філософські, політологічні, і національно-безпекові аспекти, з огляду на зростаючу роль інформаційно-комунікаційних технологій у глобальному контексті. Визнання інформаційної безпеки критично важливою компонентою національної та міжнародної безпеки підкреслюється необхідністю захисту суспільства від недостовірної, маніпулятивної та шкідливої інформації, що може підривати стабільність, соціальну згуртованість та демократичні цінності.

Центральне місце в дослідженні інформаційної безпеки займає вивчення впливу інформаційних втручань на рівні регіональної та глобальної геополітики, що вимагає аналізу зовнішніх і внутрішніх загроз. Такі загрози охоплюють широкий спектр дій, від кібератак та поширення дезінформації до цілеспрямованих інформаційних кампаній, що впливають на громадську думку та політичні процеси.

Враховуючи ці виклики, ключовими принципами дослідження інформаційної безпеки є комплексність та системність підходів, що дозволяють всебічно оцінити ризики та розробити ефективні стратегії захисту. Важливу роль у цьому процесі відіграє налагодження співпраці з міжнародними організаціями та партнерами, що сприяє обміну досвідом, знаннями та найкращими практиками у галузі інформаційної безпеки.

Також, акцент робиться на необхідності розвитку кадрового потенціалу, оскільки підготовка висококваліфікованих фахівців з інформаційної безпеки є критичною для створення стійкої та ефективної системи захисту інформаційного простору. Розробка та впровадження інноваційних технологічних рішень, забезпечення правової підтримки, а також підвищення

рівня обізнаності громадян у сфері інформаційної гігієни стають вирішальними у протидії сучасним загрозам.

6. Рабезпечення суспільно-політичної стабільності в умовах інформаційно-психологічної війни вимагає комплексного підходу, що включає моніторинг, аналіз та протидію інформаційним загрозам. Одним з ключових аспектів є постійний моніторинг інформаційного простору для виявлення та нейтралізації загроз на ранніх етапах. Це включає ідентифікацію джерел дезінформації та пропаганди, а також аналіз їхнього впливу на суспільно-політичну ситуацію.

Також, важливим аспектом є розробка та впровадження стратегії інформаційної протидії, що включає використання медіа, соціальних мереж та інших платформ для поширення достовірної інформації та викриття фальсифікацій. Важливу роль відіграють освітні програми, спрямовані на підвищення рівня медіаграмотності та критичного мислення серед населення. Підвищення обізнаності громадян про методи та прийоми інформаційно-психологічної війни дозволяє зменшити їхню вразливість до маніпуляцій.

Ключовим аспектом реформування сектору інформаційної безпеки є підвищення свідомості і компетенції як держави, так і громадянського суспільства у сфері інформаційної безпеки. Це передбачає розробку та реалізацію освітніх програм, спрямованих на зміцнення інформаційної грамотності населення, а також створення правової та інституціональної бази для ефективного регулювання інформаційного простору.

Серед важливих завдань також стоїть розробка норм та стандартів, спрямованих на забезпечення прозорості та відповідальності в сфері медіа, зокрема у контексті власності на медіа та регулювання інтернет-діяльності. Це дозволить обмежити вплив олігархічних структур на інформаційний простір та захистити суспільство від дезінформації та маніпуляцій.

Розробка та впровадження комплексної стратегії інформаційної безпеки, що базується на кращих міжнародних практиках та враховує унікальні

національні особливості, стане фундаментом для забезпечення стійкості та розвитку українського інформаційного простору в умовах глобальних викликів.

Значущість інтеграції суб'єктів та об'єктів інформаційної безпеки в державі та суспільстві не може бути переоцінена, оскільки вона лежить в основі стабільного та безпечного інформаційного простору. Державні органи, відповідальні за інформаційну безпеку, відіграють ключову роль у визначенні стратегій та політик, що забезпечують захист інформації та простору країни. Їх робота, спрямована на розробку та імплементацію законодавчих рамок, є фундаментом для створення ефективної системи інформаційної безпеки.

Політичні актори, включаючи партії та політиків, впливають на інформаційний дискурс та формують публічну думку через активну участь у політичному житті та медійному просторі. Їх здатність адекватно реагувати на інформаційні виклики та використовувати інформацію відповідально є вирішальною для забезпечення інформаційної стабільності.

Громадські організації, медіа та інші інформаційні агенти мають величезний потенціал у питаннях виявлення та протидії дезінформації. Вони сприяють підвищенню рівня інформаційної грамотності населення, захисту прав на доступ до інформації та забезпеченню свободи слова. Їх роль в інформаційній безпеці держави є незамінною, оскільки вони формують альтернативний інформаційний потік, який може контрбалансувати спроби маніпуляцій та впливів.

Взаємодія між усіма цими суб'єктами та ефективна координація їх діяльності є критично важливою для досягнення мети інформаційної безпеки. Важливо, щоб держава забезпечила рівні умови для всіх учасників інформаційного простору, встановлюючи чіткі правила гри, що ґрунтуються на принципах демократії та захисту основних прав та свобод громадян.

7. Нагальною потребою є створення ефективної системи інформаційної безпеки, яка б відповідала сучасним соціальним і геополітичним реаліям. Така система повинна включати в себе не тільки захист інформаційних технологій і

мереж, але й механізми контролю та регулювання інформаційного простору, щоб протистояти як зовнішнім, так і внутрішнім загрозам.

Забезпечення інформаційної безпеки національного рівня вимагає злагоджених зусиль і координації між різними державними органами та інституціями. Ключову роль у цьому процесі відіграє держава, яка через встановлення законодавчих та регуляторних рамок визначає основні напрями і стратегії захисту інформаційного простору. Це включає в себе не тільки розробку та впровадження законів і норм, що регулюють інформаційну безпеку, але й забезпечення їх дотримання та контролю за їх виконанням.

Функції держави в інформаційній сфері охоплюють широкий спектр діяльності, починаючи від захисту державного суверенітету в інформаційному просторі до гарантування прав і свобод громадян в інформаційній діяльності. Важливим є також забезпечення прозорості та відкритості державних органів, що сприяє побудові довіри між державою, громадянським суспільством та міжнародними партнерами.

Комплексний підхід до вирішення проблеми інформаційної безпеки передбачає інтеграцію зусиль усіх зацікавлених сторін, включаючи державні органи, політичні інститути, громадські організації, медіа та індивідуальних користувачів інформації. Така інтеграція дозволяє створити міцну та ефективну систему інформаційної безпеки, яка зможе протистояти сучасним загрозам та викликам.

Основні агенти пропаганди включають російські державні медіа, такі як RT (Russia Today) та Sputnik, які активно поширюють дезінформацію і маніпулятивні матеріали, спрямовані на дискредитацію України та підтримку агресивної політики Росії. Російська Православна Церква також відіграє важливу роль у поширенні пропаганди, використовуючи релігійні наративи для легітимізації військових дій Росії.

Канали пропаганди включають традиційні медіа (телебачення, радіо, друковані видання) та нові медіа (соціальні мережі, інтернет-платформи). Соціальні мережі, такі як Telegram та Facebook, широко використовуються для

швидкого поширення фейкових новин та маніпулятивних матеріалів. Аналіз показав, що Росія активно використовує ці платформи для впливу на громадську думку як в Україні, так і на міжнародному рівні, створюючи ілюзію підтримки своїх дій та формуючи негативне ставлення до України та її західних союзників.

Для ефективної протидії російській пропаганді необхідна комплексна стратегія, яка включає підвищення рівня медіаграмотності населення, підтримку незалежних медіа та розвиток власної інформаційної інфраструктури. Важливим є також міжнародне співробітництво та обмін досвідом у боротьбі з інформаційними загрозами. Тільки через спільні дії та координацію можна протистояти викликам сучасної інформаційно-технологічної війни, забезпечуючи захист національних інтересів та суспільно-політичну стабільність України.

8. Розробка рекомендацій з протидії інформаційному впливу Російської Федерації на суспільно-політичну стабільність України є ключовим завданням для забезпечення національної безпеки в умовах сучасних інформаційних загроз. У ході дослідження було встановлено необхідність комплексного підходу, який включає як технічні, так і соціальні аспекти.

Впровадження освітніх програм, спрямованих на розвиток критичного мислення та навичок аналізу інформації серед громадян різного віку, допоможе підвищити стійкість до дезінформації. Організація тренінгів та семінарів для журналістів, освітян та державних службовців з метою підвищення їхньої компетентності у сфері медіаграмотності та протидії дезінформації також є критичною необхідністю.

Розвиток незалежних медіа та підтримка інформаційної інфраструктури сприятимуть забезпеченню об'єктивної та якісної інформації. Створення умов для розвитку незалежних медіа та забезпечення фінансової і правової підтримки допоможе зміцнити їхню стійкість до зовнішнього впливу та маніпуляцій.

Активне громадянське суспільство відіграє вирішальну роль у забезпеченні принципу повної юридичної рівності учасників інформаційної взаємодії, вимагаючи від держави дотримання стандартів прозорості та

відкритості незалежно від соціального, економічного чи політичного статусу громадян. Залученість громадян та їх готовність до захисту своїх прав спонукають до формування правової системи, яка враховує потреби суспільства в цілому, забезпечуючи рівний доступ до інформації та можливість її вільного обігу.

Обмеження доступу до інформації, хоч і вважається винятком з основного принципу вільного доступу, може бути обґрунтовано необхідністю захисту суспільства від інформації, що носить недостовірний, спотворений або навмисно шкідливий характер. У цьому аспекті, правові механізми стають ключовим інструментом держави для ефективної боротьби з інформаційними загрозами, які можуть підірвати фундаменти національної безпеки, публічного порядку та цінностей демократії.

Роль правового регулювання полягає не тільки в накладенні обмежень, але й у забезпеченні збалансованого підходу, що дозволяє гармонійно поєднувати інтереси національної безпеки з дотриманням основоположних прав і свобод особистості, включно зі свободою вираження поглядів та доступом до інформації. Важливо, щоб законодавство та його застосування були прозорими і передбачали можливість судового оскарження рішень, які обмежують доступ до інформації, забезпечуючи цим захист прав громадян у незалежних судових інстанціях.

Таким чином, формування ефективної правової бази та механізмів її реалізації, які відповідають як національним, так і міжнародним стандартам, стає основою для створення безпечного інформаційного простору, де забезпечено захист суспільства від дезінформації та одночасно дотримуються права і свободи кожного громадянина.

Гармонізація національного законодавства України в інформаційній сфері з європейськими стандартами є стратегічно важливим кроком у зміцненні інформаційної безпеки та підвищенні рівня національної безпеки в цифровому просторі. Такий процес передбачає не тільки адаптацію існуючих законодавчих

норм до міжнародних вимог, а й створення ефективних механізмів їх дотримання та контролю.

Адаптація до європейських стандартів охоплює широкий спектр заходів, включно з розробкою політик, що сприяють захисту прав людини в мережі, гарантують свободу вираження поглядів, забезпечують прозорість та відповідальність медійних ресурсів, а також ефективно борються з дезінформацією та пропагандою. Це передбачає залучення всіх секторів суспільства до активної участі в процесі формування безпечного інформаційного середовища.

Стратегічні комунікації відіграють важливу роль у створенні позитивного іміджу України на міжнародній арені та інформуванні громадян про загрози дезінформації. Розробка стратегічного комунікаційного плану для поширення перевіреної та достовірної інформації про події в Україні, зокрема для міжнародної аудиторії, допоможе зміцнити суспільно-політичну стабільність.

Запровадження цих рекомендацій дозволить підвищити рівень інформаційної безпеки України, зменшити вплив російської пропаганди на суспільно-політичну стабільність та зміцнити національну безпеку в умовах сучасних інформаційних викликів.

9. Забезпечення суспільно-політичної стабільності в умовах інформаційного суспільства вимагає постійного розвитку та адаптації інститутів і механізмів, які здатні ефективно реагувати на нові виклики. Важливу роль у цьому процесі відіграє створення прозорих і надійних інформаційних джерел, що забезпечують доступ громадян до об'єктивної та якісної інформації. Це сприятиме підвищенню обізнаності громадян і їх здатності критично оцінювати надходження інформації, що є важливим для протидії маніпуляціям і дезінформації.

Враховуючи зростання інформаційних загроз, Україні необхідно вжити вичерпних заходів для забезпечення ефективної протидії та створення надійної системи захисту інформаційного простору. Гармонізація законодавства, розвиток технічної та організаційної інфраструктури, міжнародна співпраця, а

також залучення до цього процесу широкої громадськості стануть запорукою створення безпечного та стабільного інформаційного простору в країні.

Оптимізація кадрової політики є фундаментальною для зміцнення національної безпеки України у контексті інформаційних загроз та кіберзлочинності. Підвищення кваліфікації фахівців у цій сфері та розвиток міжнародного співробітництва відіграють вирішальну роль у побудові ефективної системи протидії інформаційним атакам. Такий підхід не тільки збагачує внутрішні ресурси держави шляхом обміну знаннями та досвідом, але й забезпечує важливу міжнародну підтримку в боротьбі проти глобальних загроз.

Визнання медіа як інструменту впливу вимагає від них не тільки професіоналізму, але й високого рівня соціальної відповідальності.

Розвиток технологій та інтернету привів до появи нових характеристик медіа: мультимедійності, інтерактивності, персоналізації контенту, а також відсутності посередників у процесі комунікації. Ці нововведення мають потенціал позитивно впливати на демократичні процеси, сприяючи активній участі громадян у соціальному житті та формуванні їхньої індивідуальної позиції. Однак, з іншого боку, вони також створюють сприятливе середовище для маніпуляцій громадською думкою та поширення дезінформації, що може мати деструктивний вплив на суспільство.

Збільшення впливу медіа в сучасному світі ставить під загрозу концепцію демократичного контролю і представництва, викликаючи занепокоєння щодо ризиків встановлення медіакратії – ситуації, коли медіаінституції здобувають непропорційно великий вплив на політичне та соціальне життя країни.

Це підкреслює необхідність розробки та імплементації державної політики, що забезпечує баланс між свободою слова та необхідністю захисту суспільства від шкідливих інформаційних впливів.

Невдале впровадження або відсутність політики інформаційної безпеки може призвести до серйозних наслідків, зокрема до підриву основ української державності, розколу суспільства та ерозії соціальних зв'язків. Сучасна

інформаційна війна, що ведеться з використанням медіа як зброї, здатна спричинити дезінтеграцію національної ідентичності та послабити демократичні інституції.

Таким чином, відповідальність медіа у контексті інформаційної безпеки набуває особливого значення, вимагаючи від медійних організацій, журналістів, а також від державної влади активних дій щодо запобігання розповсюдженню неправдивої інформації та зміцнення демократичних цінностей. Забезпечення інформаційної безпеки є критичним аспектом у зміцненні суспільної стабільності та підтримці демократичного розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамов Л. Інформаційний компонент діяльності НДО. Кіровоград: ІСКМ, 2009. 80 с.

2. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). [Електронне видання]. – Київ : Нац. акад. СБУ, 2019. – 384 с.

3. Алещенко В. І., Сербін В. Г. Проблеми захисту від негативного інформаційно-психологічного впливу противника. Мат. машини і системи. 2010. № 1. С. 77-86.

4. Антіпова О. Філософсько-аксіологічні проблеми свободи слова в українському інформаційному просторі // Гілея: науковий вісник. 2013. № 74. С. 207–209.

5. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір : дис. … кандидата філософ. наук : 09.00.03 / НТУ України «Київський політехнічний інститут». К., 2012. 199 с.

6. Бабкіна О. В. Передумови переходу до демократії : ризики транзитивного суспільства. Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 22 : Політичні науки та методика викладання соціально-політичних дисциплін : зб. наук. праць. Київ : Вид-во НПУ імені М.П. Драгоманова, 2015. Вип. 17. С. 3–11.

7. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні. – Кваліфікаційна наукова праця на правах рукопису.

8. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи. Київ: СофтПрес, 2005. 316 с.

9. Беззубов Д. О. Суспільна безпека: (організаційно-правові засади забезпечення): Моногр. К.: МП Леся, 2013. 451 с.

10. Бєляков К. І., Ярмиш О. Н. Національна безпека України в інформаційній сфері: проблеми організаційного та правового забезпечення.

Безпекотворення: питання теорії і практики та правові аспекти : зб. наук.-практ. конф. (Київ, 16 лют. 2007 р.): у 2 ч. Ч. 2 . К. : Вид-во Європ. ун-ту, 2007. С. 8–15.

11. Бєльська Т. Комунікаційна взаємодія влади та громадськості в інформаційному суспільстві // Публічне управління: теорія та практика. 2012. № 3. С. 163–169.

12. Богуш В. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.

13. Богуш В., Юдін О. Інформаційна безпека держави. К.: «МК-Прес», 2005. 432 с.

14. Бодрук О. С. Структура воєнної безпеки: національний та міжнародний аспекти: Моногор. К.: НІПМБ, 2001. 300 с.

15. Васильєва Н. В. Пропаганда як складова інформаційно-комунікативної політики і загроза національній безпеці. Таврійський науковий вісник. Серія: Публічне управління та адміністрування. 2022. С. 34–41. URL: https://journals.ksauniv.ks.ua/index.php/public/article/view/201/188.

16. Василенко В. О. Антикризове управління підприємством: Навч. посібник. К.: Центр навч. л-ри, 2005. 504 с.

17. Вінцукевич К. Громадські організації у політичному процесі сучасної України: автореф. дис…канд. політ. н. (спеціальність: 23.00.02 – політичні інститути і процеси). Київ: Київськ. нац. ун-т ім. Т. Шевченка. 2010. 19 с.

18. Волошина Н. М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. Сучасні інформаційні технології у сфері безпеки та оборони. 2010. № 2. С. 53-56.

19. Гантінгтон С. Політичний порядок у мінливих суспільствах / пер. з англ. Т. Цимбал. Київ : Наш формат, 2019. 448 с.

20. Головій В. Механізми взаємодії влади та ЗМІ в контексті становлення громадянського суспільства в Україні: автореф. дис. канд. н. з

держ. упр. (спеціальність: 25.00.02 – механізми державного управління). Київ: КПУ. 2009. 22 с.

21. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу URL:https://dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrumentrosiyskoyi-geostrategiyi-revanshu-_.html (дата звернення: 03.09.2023)

22. Гурковський В. І. Деякі організаційно-правові питання взаємовідносин органів державної влади в сфері інформаційної безпеки. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2002. Вип. 5. С. 87.

23. Гурковський В. І. 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, 2004. 22 с.

24. Державно-правові проблеми інформаційної безпеки людини і суспільства в умовах інтеграції України у світовий інформаційний прості: Звіт про науково-дослідну роботу НДІІП НАПрН України. Київ, 2016. 364 с.

25. Дмитренко М. Інформаційна війна як складова політичних ризиків / Вісник воєнної розвідки – 2021. № 65. С. 85-91.

26. Дмитренко М. А. Проблемні питання інформаційної безпеки України: монографія Національна безпека в умовах інформаційних та гібридних війн: / за заг. ред. : В. Куйбіди і В. Бебика. – Київ : В-во НАДУ. – 2019. С. 145-160.

27. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія. Київ: НАПрН України, НДІІП, НАН України, Національна бібліотека України імені В.І. Вернадського, 2015. 388 с.

28. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. – Кваліфікаційна наукова праця на правах рукопису.

29. Захаренко К. Відповідальність засобів масової інформації в системі інформаційної безпеки суспільства // Політикус. 2019. № 5. С. 4–9.

30. Захаренко К. Глобальна природа інформаційної безпеки // Політологічний вісник. 2015. Вип. 79. С. 181–189

31. Захаренко К. Медіа як чинник розвитку суспільства // Вісник Інституту розвитку дитини. Серія: Філософія, педагогіка, психологія. 2015. Вип. 38. С. 29–36.

32. Захаренко К. Відкритість інформаційного простору та контроль за доступністю інформації. 2020. Вип. 14. С. 46–55.

33. Зеленін В. В. Метамодель як анти-сугестивна психотехнологія сучасної інформаційно-пропагандистської війни. Проблеми сучасної психології. 2015. № 1 (7). С. 69–76.

34. Зеленін В. В. Основи міфодизайну : психотехнології керування медіареальністю. Навчально-методичний посібник. – К. : Вид-во «Гнозіс», 2017. – 168 с. URL: https://books.zelenin.com.ua/wp-content/uploads/2022/12/MIFODESIGN_NEW__fakultet_PRINT12.pdf

35. Зеленін В. В. Психотехнології інформаційної війни. Імперативи розвитку цивілізації. 2015. № 2. С. 136–139.

36. Зеленін В. В. Історичний міфодизайн як психотехнологія сучасної інформаційно-психологічної війни: базові постулати, завдання та структура міфотворення / В. В. Зеленін // Український психологічний журнал. - 2018. - № 1. - С. 58-73. - URL: http://nbuv.gov.ua/UJRN/ukpsj_2018_1_7

37. Золотар О. О. Інформаційна безпека людини:теорія і практика : монографія. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

38. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. Інформація і право. 2013. № 3(9). С. 105-114

39. Золотар О. О. Віртуальна реальність. Моделі колективної безпеки: інформаційний вимір: Зб. мат. / Упоряди. Ланде Д. В. К.: НДЦПІ НАПрН України, 2011. С. 63-66.

40. Золотар О. О. Про поняття “інформаційний шум” у правовідносинах» Інформація і право. 2012. № 1(4). С. 70-74.

41. Інформаційна безпека (соціально-правові аспекти): Підр. / Остроухов В.В., Петрик В.М. та ін.; за ред. Є. Д. Скулиша. – Київ : КНТ, 2010. 776 с.

42. Інформаційна безпека України в умовах євроінтеграції: Навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К.: КНТ, 2006. 280 с.

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

44. Калюжний К. Р. Сутність інформаційних прав людини в науці інформаційного права. Юридичний вісник. 2012. № 4(25). С. 55–58.

45. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. К., ІПНБ, НА СБУ, 2004. 472 с.

46. Кіянка І. Б. Політична стабільність: суть і основні засоби її досягнення в Україні : автореф. дис. ... канд. політ. наук: 23.00.02 / І. Б. Кіянка. – Львів : Львів нац. ун-т ім. І. Франка, 2003. – 18 с.

47. Коваленко І. І., Бідюк П. І., Гожий О. П. Вступ до системного аналізу: Навч. посіб. Миколаїв: МДГУ ім. Петра Могили, 2004. 148 с.

48. Комітет ВРУ з питань цифрової трансформації // Офіційний сайт. URL: http://komit.rada.gov.ua/

49. Комітет ВРУ з питань свободи слова // Сайт. URL: http://komsvobslova.rada.gov.ua/

50. Конституція України // Відомості Верховної Ради України. 1996. № 30. С. 141.

51. Кормич Б. Інформаційна безпека: організаційно-правові основи: навч. посібн. Київ: Кондор, 2008. 382 с.

52. Корнієвський О. Громадські об’єднання як суб’єкт політики національної безпеки: постановка проблеми // Стратегічні пріоритети. 2009. №1 (10). С. 44–51.

53. Корнієвський О. Громадські об’єднання у системі національної безпеки України: автореф. дис…д-ра політ наук (23.00.02 – політичні інститути і процеси). Київ: Педагогічний університет ім. М. П. Драгоманова. 2011. 38 с.

54. Кравець Є. А. Інформаційна безпека держави. Юридична енциклопедія: в 6 т. К.: Укр. енцикл., 1992. С. 744.

55. Лепська Н. Диверсифікація геополітичного простору в умовах сучасної трансформації світоустрою // Вісник Львівського університету. Серія філософсько-політологічні студії. 2018. Вип. 17. С. 201–208.

56. Лебон Г. Психологія мас. Київ : Мультимед. вид-во Стрельб., 2020.

57. Ліпкан В. А. Національна безпека України: навч. посіб. К.: КНТ, 2009. 576 с.

58. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: Навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К.: КНТ, 2006. 280 с.

59. Ліпсет С. М. Політична людина. Соціальні основи політики / С. М. Ліпсет // Політична наука. – 2011.– № 3. – С. 195–245.

60. Логовський І. Проблеми розвитку інформаційного простору України як чинника формування духовно-моральнісних якостей сучасного студентства // Духовноморальнісні основи та відповідальність особистості у долі людської цивілізації: зб. наук. праць: за матер. міжнарод. наук.-практ. конф. 5–6 листопада 2014 р. Ч. 1 / Під ред. О.Г. Романовського, Ю.І. Панфілова. Харків: НТУ «ХПІ». 2015. С. 139–142.

61. Логінов О. В. Гносеологічний аспект управління інформаційною безпекою України . Наук. вісн. Юридичної академії МВС України. 2004. № 2. С. 153-161.

62. Магда Є. В. Гібридна війна: вижити і перемогти. Х.: Віват, 2015. 304с.

63. Мамука С. Особливості формування державної регуляторної політики у сфері телебачення і радіомовлення в Україні // Державне управління: теорія та практика. 2010. № 1. С. 118–128.

64. Марутян Р. Р. Інтелектуально-ресурсне забезпечення державного управління у сфері національної безпеки України: монографія /Р.Р. Марутян. – К.: ЦП «Компринт», 2020. – 410 с.

65. Марутян Р. Р. Інтелектуальні ресурси державного управління: особливості використання та відтворення. World Science. 2019. Т. 2, № 10(50). С. 28–32. URL: https://doi.org/10.31435/rsglobal_ws/31102019/6727 (дата звернення: 21.06.2024).

66. Мельник С. В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016. Т. 55. №5. С. 187–197.

67. Міненко Є. Вплив російської пропаганди на суспільно-державну стабільність України: аналіз методів та наслідків. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2023. Т. 3, № 69. URL: http://journals.maup.com.ua/index.php/political/article/view/2827/3286.

68. Міненко Є. Інституційна основа державної стабільності в епоху інформаційного суспільства. Актуальні проблеми управління інформаційною безпекою держави : XV Всеукр. науково-практична конф., м. Київ, 27 берез. 2024 р.

69. Міненко Є. С. Аналіз забезпечення інформаційної безпеки: суспільно-політичний аспект. Конференція «Політика та право в умовах дії воєнного стану: пошук рішень».

70. Міненко Є. С. Вплив сучасних інформаційних технологій на психологічний стан особистості. The 4th International scientific and practical conference ―Modern research in world science‖ (July 10-12, 2022) SPC «Sci-conf.com.ua», Lviv, Ukraine. 2022. 1161 p. URL: https://sci-conf.com.ua/wp-content/uploads/2022/07/MODERN-RESEARCH-IN-WORLD-SCIENCE-10-12.07.22.pdf

71. Міненко Є. С. Виклики інформаційній безпеці людини в умовах гібридної війни проти України. Протидія дезінформації в умовах російської

агресії проти України: виклики і перспективи тези доп. учасників міжн. наук.-практ. конф. (Анн-Арбор - Харків, 12-13 груд. 2023 р.) , 252-254. URL: https://doi.org/10.32782/PPSS.2023.1.66

72. Міненко Є. С. Ключові аспекти забезпечення суспільно-політичної стабільності деокупованих територій України. Матеріали круглого столу «Крим: 10 років спротиву».

73. Міненко Є. С. Організаційно-правовий аналіз забезпечення інформаційної безпеки як фактор суспільно-політичної стабільності. Науковий часопис НПУ імені М.П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін, 22(33), 76–84. URL: https://sj.udu.edu.ua/index.php/pnspd/article/view/1446/1183

74. Міненко Є. С. Організаційно-правовий аналіз інформаційної безпеки в умовах гібридних загроз. Конференція «Трансформація вітчизняної правової системи в сучасних умовах».

75. Міненко Є.С. Основні засади формування та реалізації державної політики інформаційної безпеки в умовах вітчизняної війни. Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні : матеріали Всеукр. наук.-практ. конф. у трьох томах, м. Київ, ДЗВО «Університет менеджменту освіти» НАПН України, 15-28 квітня 2022 р.; ред. колегія : І.О. Дегтярьова, В.С. Куйбіда, П.М. Петровський та ін., уклад. Т.О. Мельник. Т. 1. К. : ДЗВО «УМО» НАПН України, 2022. 213 с. URL: https://www.researchgate.net/profile/Vitalij-Kruglov/publication/361262262_PUBLICNE_UPRAVLINNA_TA_ADMINISTRUVANNA_V_UMOVAH_VIJNI_I_V_POSTVOENNIJ_PERIOD_V_UKRAINI_MATERIALI_VSEUKRAINSKOI_NAUKOVO-PRAKTICNOI_KONFERENCII/links/62a74e49416ec50bdb22cb5e/PUBLICNE-UPRAVLINNA-TA-ADMINISTRUVANNA-V-UMOVAH-VIJNI-I-V-POSTVOENNIJ-PERIOD-V-UKRAINI-MATERIALI-VSEUKRAINSKOI-NAUKOVO-PRAKTICNOI-KONFERENCII.pdf#page=38

76. Міненко Є.С. Основні засади формування та реалізації державної політики інформаційної безпеки. Міжнародна наукова інтернет-конференція

"Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 55)" / Збірник тез доповідей: випуск 55 (м. Тернопіль, 9 лютого 2021 р.). – Тернопіль. – 2021. – 90 с. URL: https://drive.google.com/file/d/1TeaiQWRCWwxcrhSX_k6sCXCCv4KFMRYk/view?usp=sharing

77. Міненко Є. С. Сутність політичної стабільності в умовах інформаційного суспільства. Науковий журнал «Politicus». 2023. № 5. С. 155–160. URL: http://politicus.od.ua/5_2023/24.pdf.

78. Міненко, Є., Захаренко К. Інститут медіа як суб'єкт інформаційної безпеки. Науковий часопис НПУ імені М.П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін, 22(34). URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/44664/Zakharenko-29-36.pdf?sequence=1&isAllowed=y

79. Мошковська С. Передумови входження України у глобальний інформаційний простір в контексті вимог міжнародної інформаційної безпеки // Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців: всеукраїнська наукова конференція (Львів, 27 травня 2011 р.). Львів: «Львівська політехніка». 2011. С. 118–122.

80. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. Віче. 2007. №12. С. 23-25.

81. Національна безпека України: забезпечення в інформаційній сфері: монографія // за редакцією М.А. Дмитренко 2021.- 325 с.

82. Новакова О. Розвиток місцевого самоврядування як чинник стійкості українського суспільства в умовах російської військової агресії. Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін. 2023. Т. 22, № 34. URL: https://sj.udu.edu.ua/index.php/pnspd/article/view/1448/1186.

83. Новакова О. Розвиток стратегічних комунікацій як засіб боротьби з дезінформацією в українському суспільстві [Текст] / О. Новакова, О. Черненко // Вісник Львівського університету. Серія: Філософсько-політологічні студії. –

2023. – Вип. 49. – С. 308-314. URL: https://files.znu.edu.ua/files/2020/scachano/VLUFPS/VLUFPS2023v49/308.pdf

84. Олійник О. В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України. Моногр. К., Вид. підпр-во «Український пріоритет», 2012. 400 с.

85. Опалько Ю. Організації громадянського суспільства як чинник впливу на виборчій процес // Наукові записки ін-ту політичних досліджень ім. І.Ф. Кураса НАН України. 2019. № 6 (50). С. 224–232.

86. Остапенко М. А. Соціальна напруженість: зміни в умовах війни. Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін. 2022. Т. 22, № 33. С. 13–24. URL: https://doi.org/10.31392/udu-nc.series22.2023.33.02 (дата звернення: 21.06.2024).

87. Петкова О. Політичні імперативи позиціонування України в міжнародному інформаційному просторі: автореф. дис. …канд. політ. н. (спеціальність: 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку). Київ: Інститут світової економіки і міжнародних відносин НАНУ. 2010. 23 с.

88. Петрик В. М. Забезпечення інформаційної безпеки держави: підручник; за заг. ред. О. А. Семченка та В. М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.

89. Положення «Про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України» (затверджено постановою Кабінету Міністрів України від 3 вересня 2014 р. № 411) // Верховна Рада України. Вебсайт. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text

90. Положення «Про Державний комітет телебачення і радіомовлення України» (затверджено постановою Кабінету Міністрів України від 13 серпня 2014 р. № 341) // Верховна Рада України. Офіційний вебсайт. URL: https://zakon.rada.gov.ua/laws/show/341-2014-%D0%BF#Text

91. Положення «Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України» (затверджено Указом Президента України від 22 січня 2002 року № 63/2002) // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/63/2002#Text

92. Положення про Міністерство інформаційної політики України (затверджено Постановою Кабінету Міністрів України від 14 січня 2015 р. № 2). Верховна Рада України. Сайт. URL: https://zakon.rada.gov.ua/laws/show/en/2-2015- %D0%BF?lang=uk#Text

93. Положення «Про Міністерство цифрової трансформації України» (затверджено постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856) // Верховна Рада України. Сайт. URL: https://zakon.rada.gov.ua/laws/show/856- 2019-%D0%BF#Text

94. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14 січня 2015 р. № 2 // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF#Text

95. Почепцов Г. Гібридна війна: інформаційна складова. URL: https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/ (дата звернення: 03.09.2023)

96. Почепцов Г., Чукут С. Інформаційна політика: навч. посіб.: 2-ге вид. К., 2008. 663 с.

97. Попов С. Проблеми інформаційної безпеки України // Форум права. 2011. № 1. С. 798–801.

98. Правова політологія: проблеми концептуалізації та інтитуціоналізації: монографія / За ред. І. Кресіної. Київ: Інститут держави і права імені В. М. Корецького НАН України, 2019. 288 с.

99. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 22.06.2024).

100. Про Національну раду України з питань телебачення і радіомовлення : Закон України від 23.09.1997 р. № 538/97-ВР : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/538/97-вр#Text (дата звернення: 22.06.2024).

101. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV : станом на 8 лип. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 22.06.2024).

102. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII : станом на 2 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 22.06.2024).

103. Про Суспільне телебачення і радіомовлення України : Закон України від 17.04.2014 р. № 1227-VII : станом на 2 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1227-18#Text (дата звернення: 22.06.2024).

104. Про медіа : Закон України від 13.12.2022 р. № 2849-IX : станом на 11 лют. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 22.06.2024).

105. Резолюція A/RES/54/49 ГА ООН "Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки" [Електронний ресурс]. - Режим доступу: https://undocs.org/ru/A/RES/54/49 (дата звернення: 25.04.2023).

106. Резолюція Ради Безпеки ООН S/RES/2341 (2017) «Про захист критичної інфраструктури» [Електронний ресурс]. – Режим доступу : https://undocs.org/ru/S/RES/2341(2017). (дата звернення: 25.04.2023).

107. Рущенко І. П. Ідеологія рашизму : монографія / І. П. Рущенко. – Харків : Харківський національний університет імені В.Н. Каразіна, 2023. – 276 с.

108. Ситник Г. Безпека як інтегральна характеристика розвитку соціальних систем. Державне управління в Україні: реалії та перспективи: зб. наук. праць. К., 2005. – С. 278-282.

109. Ситник Г. Державне управління національною безпекою України. К.: Вид-во НАДУ, 2004. С. 69.

110. Смолянюк В. Національна безпека незалежної України: осягнення сутності. Політичні дослідження. 2021. No 1. С. 163–186. URL: https://ipiend.gov.ua/wp-content/uploads/2021/06/smolianiuk_natsionalna.pdf

111. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : дис. на здоб. наук. ступеня доктора політ. наук : спец. 23.00.02. / Одес. нац. юрид. акад. О., 2005. 264 с.

112. Стратегія інформаційної безпеки (ЗАТВЕРДЖЕНО Указом Президента України від 28 грудня 2021 року № 685/2021).

113. Таран В. О., Зотов В. М., Рєзанова Н. О. Соціальна філософія: Навч. посіб. К.: Центр учбової літератури, 2009. 272 с

114. Тарнавська Т. В. Генеза поняття «система»: історичний огляд. Духовність особистості: методологія, теорія і практика. 2011. № 6 (47). С.130-139.

115. Терепищий С. О. Проблема медіаграмотності дорослого населення після повномасштабної російської агресії 2022–2023 років. *Наукове пізнання: методологія та технологія*. 2023. Т. 2, № 52. С. 45–51. URL: https://doi.org/10.24195/sk1561-1264/2023-2-6 (дата звернення: 24.06.2024).

116. Терепищий С. О. Філософські принципи медіаграмотності в епоху інформаційних війн. *Актуальні проблеми філософії та соціології*. 2023. № 43. С. 119–123. URL: https://doi.org/10.32782/apfs.v043.2023.20 (дата звернення: 24.06.2024).

117. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : дис. ... кандидата юрид. наук: 12.00.01 / Нац. акад. внутр. справ. К., 2011. 234 с.

118. Федорук О. Концептуальні засади формування системи забезпечення національної інформаційної безпеки // Вісник соціально-економічних досліджень. 2013. Вип. 2 (1). С. 182–188.

119. Філософія. Навч. посіб. / За заг. ред. Ю.В. Осічнюка. К.: Атіка, 2003. 464 с.

120. Хворост Х. Ю. Інформаційно-психологічний вплив у розрізі безпеки здоров'я. Наука і освіта. 2016. №2-3. с.184-191.

121. Хімей В. Основні сучасні проблеми інформаційної безпеки України // Телетарадіожурналістика. 2014. Вип. 13. С. 127–132.

122. Цимбалюк В. Сутність інформаційної безпеки в умовах входження України до глобальної кіберцивілізації. Науковий вісник Нац. академії Держ. податк. служби України. 2004. № 4(26). С. 135–141.

123. Цивільний кодекс України // Відомості Верховної Ради України. 2003. № 40−44. С. 356.

124. Чупрій Л. Історична пам'ять як важливий чинник державотворення в умовах протидії російській інформаційній агресії. Міжнародні відносини, суспільні комунікації та регіональні студії. 2023. № 3 (17). С. 278–290. URL: https://doi.org/10.29038/2524-2679-2023-03-278-290 (дата звернення: 21.06.2024).

125. Шайгородський Ю. Ж. Довіра як політико-психологічний феномен. Політичне життя. 2021. № 4. С. 63–39. URL: https://doi.org/10.31558/2519-2949.2021.4.10 (дата звернення: 21.06.2024).

126. Шайгородський Ю. Ж. Українські ЗМІ в утвердженні суспільної моралі. Відповідальна політика в сучасній Україні: ілюзії та реалії / за ред. О. М. Майбороди. Київ : Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України, 2021. С. 131–165. URL: https://lib.iitta.gov.ua/730008/1/Українські_ЗМІ.pdf

127. Шайгородський Ю. Ж. Вплив медіа на суспільно-політичні та етико-моральні процеси в Україні. Політикус. 2021. Вип. 6. С. 89–95. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/14729/1/Shaihorodskyi.pdf

128. Шайгородський Ю. Ж. Масмедіа як суспільно-політичний інститут: структура і функції. Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін.

2022. Т. 22, № 31. С. 26–34. URL: https://sj.udu.edu.ua/index.php/pnspd/article/view/1235/1011

129. Шайгородський Ю. Ж. Українські ЗМІ в утвердженні суспільної моралі. Відповідальна політика в сучасній Україні: ілюзії та реалії / за ред. О. М. Майбороди. Київ : Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України, 2021. С. 131–165. URL: https://lib.iitta.gov.ua/730008/1/Українські_ЗМІ.pdf

130. Ягодзінський С. Інформаційний простір глобальних мереж: соціально-філософський аспект // Вісник Національного авіаційного університету. Серія: Філософія. Культурологія: Збірник наукових праць. 2013. Вип. 1 (17). С. 77−80.

131. European Union Agency for Network and Information Security [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/about-enisa. (дата звернення: 25.04.2023).

132. Hybrid Warfare URL: http://www.gao.gov/assets/100/97053.pdf (Last accessed: 03.09.2023).

133. Lasswell H. Propaganda, Communication and Public Order. Princeton, 1946. 120 p.

134. Network and information security: proposal for a european policy approach [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN. (дата звернення: 25.04.2023).

135. Raychev Y. Cyberwar in Russian and US Military-Political Thought: A Comparative View // Information & Security Journal. 2019. Vol. 43. No. P. 349–361.