НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
М. П. ДРАГОМАНОВА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ЗАХАРЕНКО Костянтин Володимирович

УДК 321.022:323.23

ДИСЕРТАЦІЯ

ІНСТИТУЦІЙНИЙ ВИМІР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ТРАНСФОРМАЦІЙНІ ВИКЛИКИ, ГЛОБАЛЬНІ КОНТЕКСТИ, СТРАТЕГІЧНІ ОРІЄНТИРИ

23.00.02 – політичні інститути та процеси

Подається на здобуття ступеня доктора політичних наук

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

Науковий консультант:
ДМИТРЕНКО Микола Андрійович
доктор політичних наук, професор

Київ – 2021

АНОТАЦІЯ

Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.02 – політичні інститути та процеси. – Національний педагогічний університет імені М.П. Драгоманова, Львівський національний університет імені Івана Франка, Львів, 2021.

Репрезонтоване дослідження з позицій сучасного політологічного дискурсу комплексно аналізує основні тенденції процесу формування інформаційної безпеки в трансформаційному суспільстві, зокрема інституційний вимір такого процесу, роль державних і неурядових інститутів у забезпеченні інформаційної безпеки України. Проблема інформаційної безпеки осмислюється на трьох визначальних напрямках: у світлі трасформації українського суспільства загалом та його політичної системи; у контексті глобалізації сучасного світу; у стратегічному баченні – як перспектива розвитку політичних інститутів, відносин і процесів, що забезпечують демократичні зміни та безпеку України загалом.

Історіографічні і теоретико-методологічні особливості дослідження проблеми інформаційної безпеки в умовах політичної трансформації розкриті через узгодження ключових понять, концептуальних підходів, правових означень, ретроспектив. Аналіз численних наукових напрацювань та емпіричних матеріалів дозволив посилити сучасне розуміння феномену інформаційної безпеки, що у будь-якому структурно-функціональному вимірі телеологічно має бути орієнтована, по-перше, на захист прав людини і громадянина, забезпечення повноцінного національно-культурного розвитку та всебічний захист державного суверенітету; по-друге, на формування єдиного функціонально-життєвого соціального простору змістів, що визначають світоглядно-аксіологічні пріоритеті (патріотизм, гідність, державотворення, загальнолюдські цінності тощо). Наголошується, що рівень інформаційної безпеки визначає стан розвитку й інших компонентів національної безпеки України, а

відповідні деструктивні інформаційні впливи проявляються фактично у всіх сферах життя суспільства.

У дисертації проаналізовано законодавчу базу України та міжнародні стандарти щодо функціонування інститутів інформаційної безпеки. Водночас наголошується, що ефективна інформаційна політика державних структур досить часто вимірюється не лише міжнародними стандартами та правилами, але і спроможністю захищати специфічні національні інтереси, приймати актуальні виклики та долати гострі загрози. Геополітичні ж протистояння осмислюються як такі, що переважно ведуться не на полі головних супротивників, а у просторі вразливих суспільств та нестабільних держав. Сучасні політико-правові інструменти рекомендовано посилювати саме у напрямку протидії інформаційній експансії та поступовому поглинання, навіть без очевидного застосування сили.

Обрана проблематика дослідження має глобальний характер, суб'єкт-об'єктні виміри. У системі ризиків, які постають перед Україною в контексті глобального харакетру інформаційної безпеки, серед основних розглядається загроза втрати інформаційного суверенітету, а відтак і пов'язаних з ним національної ідентичності, державного суверенітету, тобто ключових ознак державної самостійності та правосуб'єктності. Із ключових питань зазначається і подільший пошук адекватного балансу між впливами глобального характеру, які ґрунтуються на інтенсифікації переміщення інформації в глобальному інформаційному середовищі, та потребами окремих людей і суспільних груп, в тому числі держав, що не є провідними суб'єктами, здатними впливати на глобальні цивілізаційні тенденції та процеси. Тому в системі інформаційної безпеки значиму роль відведено інформаційній безпеці нації, зокрема таким її структурним компонентам: захист неповторних національно-культурних цінностей, історичних традицій, історичної пам'яті, мови, унікальних субкультур.

Серед авторських пропозицій та рекомендацій важливі ті, що стосуються існуючої інфраструктури державних інститутів інформаційної безпеки України, яка мусить вибудовуватися за принципом стримувань і противаг, коли державні інститути повинні перебувати під громадським контролем, бути відкритими до комунікації, прозорими у своїх рішеннях і звітності, зрозумілими для міжнародних

партнерів. Водночас акцентується, що перед державною владою з розвитком соціальних мереж постає ряд відносно нових завдань (наприклад, структуризація віртуальних спільнот у вітчизняних соціальних мережах; усвідомлення їх впливовості та можливостей; пошук та вироблення адекватних реакцій на реальні та потенційні загрози, приховані у віртуальному громадянському просторі; розвиток доступних механізмів державного регулювання цього соціального феномену; слідування демократичним взірцям та традиціям у відповідній сфері).

Інформаційно-безпекова діяльність партій в Україні визначена суперечливою: фейкові партійні структури або не здійснюють інформаційної діяльності взагалі, або здійснюють пряме й опосередковане інформаційне обслуговування потужних політичних партій, що сприяє викривленню інформаційного та політичного просторів держави й чинить негативний вплив на інформаційну безпеку особистості та суспільства. Натомість серед основних завдань партії у здійсненні інформаційної політики названі політичне партнерство між громадянами та владою, ретрансляція демократичних норм і цінностей заради захисту народних та державних інтересів. У демократіях до цього процесу долучаються як урядові, так і опозиційні сили.

Стверджується, що у сучасній системі інформаційної безпеки значима роль відведена громадянському суспільству та ЗМІ. Послідовно обґрунтовується теза про те, що найвразливіше середовище для інформаційних операцій агресивного характеру формується з пересічних людей, які є апатичні до політики, пасивні у соціальних справах, нігілістичні, замкнені рамками мінімальних знань та вузьких світоглядних орієнтирів. Визначальною ж інформаційною загрозою національній безпеці названо маніпуляцію суспільною свідомістю, тобто дестабілізуючий вплив і на інформаційну структуру країни, і на її інформаційні ресурси та суспільство загалом.

Опрацьовано шість моделей, що демонструють взаємодію ЗМІ та держави: незалежної преси, соціальної відповідальності, демократичного представництва, радянська модель, авторитарна та модель розвитку. За допомогою чотирьох з них на різних історичних етапах запропоновано пояснити ситуацію в Україні, а три моделі дають можливість адекватно характеризувати авторитарні системи правління. Загалом можливість держави і суспільства протистояти зовнішній інформаційній

агресії вбачається у проведенні демократичних реформ; зрілості громадянського суспільства; стабільності правової держави; формуванні демократичної та активістської політичної культури.

В умовах гібридної війни стратегічні орієнтири протидії зовнішнім і внутрішнім інформаційно-дестабілізаційним впливам у дисертації осмислюються через: 1) впровадження кращих безпекових практик, які успішно захищають сучасний інформаційний простір та побудовані на трьох визначальних принципах (ієрархічності, державної координованості та взаємодії); 2) підвищення ролі політичної освіти і просвітництва (тобто змістовної основи вироблення окремими особами, громадянським суспільством, державою імунітету до багатьох загроз, пов'язаних з інформаційно-маніпулятивними впливами); 3) подальший розвиток культури інформаційної безпеки (такий рівень розвитку людини та суспільства, який характеризується значимістю забезпечення безпеки життєдіяльності в системі особистісних і соціальних цінностей, безпечної поведінки в повсякденному житті в умовах небезпечних та надзвичайних ситуацій, рівнем захищеності від загроз та небезпек у всіх сферах життєдіяльності) тощо.

Здійснений теоретичний аналіз основних тенденцій процесу забезпечення інформаційної безпеки в трансформаційному суспільстві має практичне значення, актуалізує потребу залучення і розвитку широкого інструментарію утвердженню демократичної свідомості та ідеології, інтелектуалізації, інформатизації, прагматизації політичного поля, забезпечення всебічної політологічної та правової освіти. Інституційне розуміння формування інформаційно-безпекового порядку денного може зацікавити державних діячів, громадських активістів, партійних лідерів, політичних експертів, консультантів, аналітиків. Матеріали дослідження можуть бути корисними для програм з громадянської та політичної освіти, інформаційної гігієни, при викладанні політичних наук, а акож загалом у визначенні подальших орієнтирів розвитку державної гуманітарної політики.

Ключові слова: інформаційна безпека, політичні інститути, політична трансформація, політична модернізація, інформаційна стратегія, інформаційний суверенітет, глобалізація.

ABSTRACT

Zakharenko K.V. Institutional Dimension of Information Security of Ukraine: Transformational Challenges, Global Contexts and Strategic Landmarks. – Qualifying scientific work on the rights of a manuscript.

Dissertation on acquisition of the scientific degree of the Doctor of Political Science in specialization 23.00.02 – Political institutions and processes. – National Pedagogical Drahomanov University, Ivan Franko National University of Lviv, Lviv, 2021.

From the perspective of modern political discourse, the given research provides a comprehensive analysis of the trends in forming information security in a transformational society, including the institutional dimension of such process and the role of the state and non-governmental institutions in ensuring information security of Ukraine. The problem of information security is considered in three defining directions: in the light of the transformation of the Ukrainian society as a whole and its political system; in the context of globalization of the modern world; in the strategic vision – as a prospect for the development of political institutions, relations and processes that ensure democratic change and security of Ukraine in general.

Historiographical and theoretical-methodological features of the study of the information security issues under political transformation are revealed through the coordination of key concepts, conceptual approaches, legal definitions, retrospectives, etc. The analysis of numerous scientific developments and empirical materials allowed to strengthen the modern understanding of the phenomenon of information security, which in any structural and functional dimension should be teleologically focused on, first, protection of human and civil rights, ensuring full national and cultural development and comprehensive protection of the state sovereignty; second, forming a single functional and vital social space of the senses that determine the worldview and axiological priorities (patriotism, dignity, state formation, universal values, etc.). It is emphasized that the level of information

security determines the state of development of other components of national security of Ukraine, and the corresponding destructive informational influences are manifested in virtually all spheres of society.

The dissertation analyzes the legal framework of Ukraine and international standards for the functioning of information security institutions. At the same time, it is emphasized that the effective information policy of state bodies is often measured not only by international standards and rules, but also by the ability to protect specific national interests, accept current challenges and overcome acute threats. Geopolitical confrontations are viewed as those that are mostly conducted not in the field of the main opponents but in the space of vulnerable societies and unstable states. It is recommended to strengthen modern political and legal instruments in the direction of counteracting information expansion and gradual absorption, even without the open use of force.

The chosen problematics of the research are of a global character and belong to subject-object dimensions. In the system of risks facing Ukraine in the context of the global nature of information security, the main threat is that of losing its information sovereignty, and hence the associated national identity and state sovereignty, i.e., the key features of state independence and legal personality. Among the key issues is the further search for an adequate balance between global impacts, which are based on the intensification of information movement in the global information environment, and the needs of individuals and social groups, including states that are not leading actors in influencing global civilizational tendencies and processes. Therefore, in the information security system in general, a significant role is given to the information security of the nation, in particular the following structural components: protection of unique national and cultural values, historical traditions, historical memory, language, unique subcultures and more.

Among the author’s proposals and recommendations of most importance are those related to the existing infrastructure of Ukrainian governmental institutions of information security, which should be built on the principle of checks and balances, in which state institutions should be under public control, open to communication,

transparent in their decisions and reporting and understandable to international partners. At the same time, it is emphasized that the government faces a number of relatively new tasks with the development of social networks (e.g., structuring virtual communities in domestic social networks; comprehending their impact and opportunities; finding and developing adequate responses to real and potential threats hidden in the virtual civic space; developing available mechanisms of state regulation of this social phenomenon; following democratic patterns and traditions in the relevant field).

The information and security activities of political parties in Ukraine are quite contradictory: fake party structures either do not carry out information activities at all or provide direct and indirect information services to powerful political parties, which distorts the information and political space of the state and has a negative impact on information security. Instead, the main tasks of the party in the implementation of information policy are the political partnership between citizens and the government and retransmission of democratic norms and values for the protection of national and state interests. In democracies, both governmental and opposition forces are involved in this process.

It is argued that civil society and the media play a significant role in the modern information security system. The thesis is that the most vulnerable environment for aggressive information operations is formed of ordinary people who are apathetic to politics, passive in social affairs, nihilistic, closed to the extent of minimal knowledge and narrow worldviews is consistently substantiated. The defining information threat to national security is the manipulation of public consciousness, i.e., creating a destabilizing impact on the information structure of the country and its information resources and society as a whole.

Six models that demonstrate the peculiarities of the interaction between the media and the state have been studied, namely, those of independent press, social responsibility, democratic representation as well as the Soviet, authoritarian and developmental models. With the help of four of them, at different historical stages, it is proposed to explain the situation in Ukraine, and three models make it possible to

adequately characterize the authoritarian systems of government. In general, the ability of the state and society to resist external information aggression is seen in the implementation of democratic reforms; maturity of the civil society; stability of the rule of law; formation of democratic and activist political culture.

Strategic guidelines for counteracting external and internal information and destabilizing influences in a hybrid war are studied herein through: 1) introduction of best security practices that successfully protect the modern information space and are based on three defining principles (hierarchy, state coordination and interaction); 2) increasing the role of political education and enlightenment (i.e., the substantive basis for the development of individuals, civil society, the state of immunity to many threats associated with information and manipulative influences); 3) further development of information security culture (such level of human and social development which is characterized by the importance of life safety in the system of personal and social values, safe behavior in everyday life in dangerous and emergency situations, the level of protection from threats and dangers in all spheres of life), etc.

The provided theoretical analysis of the trends in the process of information security in a transformational society is of practical importance, and it highlights the need to attract and develop various tools to establish democratic consciousness and ideology, intellectualization, informatization and pragmatization of the political field, providing comprehensive political and legal education. Institutional understanding of the formation of the information and security agenda may be of interest to statesmen, public activists, party leaders, political experts, advisers and analysts. The research materials may be useful for programs in civic and political education, information hygiene, in teaching political science and also in determining the guidelines for the development of the state of humanitarian policy.

Keywords: information security, political institutions, political transformation, political modernization, information strategy, information sovereignty, globalization.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Захаренко К. Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток. Київ: Вид-во НПУ імені М.П. Драгоманова, 2017. 389 с.
2. Захаренко К. Відкритість інформаційного простору та контроль за доступністю інформації. 2020. Вип. 14. С. 46–55.
3. Захаренко К. Відповідальність засобів масової інформації в системі інформаційної безпеки суспільства // Політикус. 2019. № 5. С. 4–9.
4. Захаренко К. Глобальна природа інформаційної безпеки // Політологічний вісник. 2015. Вип. 79. С. 181–189.
5. Захаренко К. Держава як суб'єкт інформаційної безпеки суспільства // Політологічний вісник. 2015. Вип. 78. С. 86–96.
6. Захаренко К. Диверсифікація джерел інформації в контексті інфоормаційної безпеки // Политикус. 2019. № 1. С. 5–9.
7. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки // Нова парадигма. 2015. Вип. 127. С. 40–53.
8. Захаренко К. Засоби масової інформації як необхідний елемент розвитку інформаційного суспільства // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 132. С. 250–254.
9. Захаренко К. Информационная безопасность в системе глобального информационного пространства //Strategiю Bakuю 2017. № 3–4 (21–22). С. 223–234.
10. Захаренко К. Інформаційна безпека суспільства як предмет правового регулювання // Гілея: науковий вісник: зб. наук. пр. 2019. Вип. 148. С. 26–31.
11. Захаренко К. Інформаційні впливи як джерела загострення інформаційної небезпеки // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 126. С. 331–336.
12. Захаренко К. Категорія інформаційної безпеки у вітчизняному політологічному дискурсі // Вісник Львівського університету. Серія філос.-політолог. студії. 2019. Вип. 23. С. 158–165.

13. Захаренко К. Міжнародний досвід інформаційної безпеки // Сучасне суспільство: політичні науки, соціологічні, культурологічні науки. 2019. Вип. 1 (17). С. 95–109.
14. Захаренко К. Особливості формування ефективної державної інформаційної політики // Політичне життя. 2019. №3. С. 71–76.
15. Захаренко К. Партії і політичні рухи в інформаційному вимірі сучасної держави // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 116. С. 285–289.
16. Захаренко К. Правовий супровід інформаційної безпеки суспільства // Державо і право. 2019. Вип. 83. С. 128–138.
17. Захаренко К. Протидія маніпулятивним впливам (засоби, технології, можливості) // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 137. С. 181–189.
18. Захаренко К. Роль громадських організацій і рухів у формуванні національної інформаційної безпеки // Гілея: науковий вісник: зб. наук. пр. 2016. Вип. 115. С. 426–430.
19. Захаренко К. Специфіка позиціювання політичної партії в інформаційному просторі держави і суспільства // Державо і право. 2019. Випуск 85. С. 338–348.
20. Захаренко К. Стратегія формування ефективної системи державної інформаційної безпеки // Гілея: науковий вісник. 2018. Вип. 131. С. 268–272.
21. Захаренко К. Теоретичні засади дослідження інформаційної безпеки // Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 2 (4). С. 107–116.
22. Захаренко К. Чинники здійснення державної інформаційної політики України // Регіональні студії. 2019. № 17. С. 15–19.

Наукові праці, що засвідчують апробацію матеріалів та додатково відображають наукові результати дисертації:

23. Захаренко К. До питання про розвиток національної системи інформаційної безпеки: досвід сусідів // Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія. 2018. Вип. 50. С. 176–189.

24. Захаренко К. Засоби масової інформації як інструмент та механізм розвитку інформаційного суспільства // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2018. Вип. 39. С. 79–87.
25. Захаренко К. Засоби масової інформації як чинник розвитку суспільства // Вісник Інституту розвитку дитини. Серія: Філософія, педагогіка, психологія. 2015. Вип. 38. С. 29–36.
26. Захаренко К. Категорія «інформаційної безпеки» у вітчизняному науковому дискурсі // Гуманітарний вісник державного вищого навчального закладу «Переяслав-Хмельницький державний педагогічний університет ім. Г. С. Сковороди». Серія: Філософія. 2015. Вип. 37. С. 106–117.
27. Захаренко К. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі // Гуманітарний вісник ЗДІА. 2018. Випуск 72. С. 44–52.
28. Захаренко К. Місце політичних партій в системі інформаційної безпеки // Політологічні читання імені професора Богдана Яроша: зб. наук. пр. / за заг. ред. В.І. Бортнікова, О.Б. Ярош, Я.Б. Яроша. Луцьк: Вежа-Друк, 2020. Вип. 9. С. 44–49.
29. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки // Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Серія: Філософія. 2017. Вип. 48 (1). С. 212–219.
30. Захаренко К. Проблеми консолідації субєктів інформаційної безпеки // Проблеми соціальної роботи: філософія, психологія, соціологія. 2018. № 1(11). С. 36–43.
31. Захаренко К. Проблеми формування ефективної державної інформаційної політики // Науковий часопис НПУ імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2016. Вип. 36. С. 202–209.
32. Захаренко К. Розвиток системи інформаційної безпеки: досвід зарубіжних країн // Вища освіта України. 2018. № 3. С. 71–77.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Інформаційна революція спонукає бурхливий розвиток інформаційних потоків, електронних засобів комунікації, інформатики, телематики, створення глобальної інформаційної мережі, яка, за висловом Е. Сміта, перетворилась у «становий хребет сучасної цивілізації». Зросла кількість людей, задіяних у процесах накопичення, обробки, розповсюдження, передачі та обміну інформацією. Інформаційний бум у буквальному розумінні охопив суспільство загалом і окрему особистість зокрема, змінив їх спосіб життя, сформував нові виклики і загрози. Актуальним стало поняття «інформаційної безпеки», забезпечення якої цілком справедливо покладається, насамперед, на державу. Останнє потребує більш глибокого вивчення проблеми змісту та функціональних особливостей державної інформаційної політики, її ролі у створенні та реалізації безпечних інформаційних систем та технологій, а відтак і в створенні додаткових можливостей свободи й доступу до інформаційної діяльності, підтримки розвитку інформаційних ресурсів тощо.

В чому ж полягають фундаментальні витоки та основні детермінанти актуальності проблеми інформаційної безпеки? Формуючи відповідь, насамперед, необхідно підкреслити, що інформаційна революція, що триває вже декілька десятиліть, викликала такі потужні цивілізаційні зрушення у всіх сферах суспільного буття, які важко порівняти з будь-якою іншою епохою. Інформація стала не просто засобом чи зручним способом дії, вона перетворилася для сучасної людини і суспільства на життєвий простір, що містить не тільки нові можливості, але й значні небезпеки. Вплив інформаційної технології і електронних обмінів справляє такий перетворюючий ефект, який не могла викликати навіть промислова революція. Інтернет став таким засобом комунікації, без якого вже не можуть обходитись працівники будь-якої сфери суспільної життєдіяльності. Водночас у новій віртуальній реальності закладено безліч загроз – для індивіда, громади, держави,

міжнародних організацій. Інформаційної агресії зазнають важливі основи сучасного суспільного життя – демократія і подальша демократизація, стабільні політичні системи і системи, що модернізуються, локальні культури та нові глобалізовані формати співробітництва та миру. Усе це потребує мобілізації теоретичних зусиль, які мають передувати практиці, визначати детермінанти, ресурси, технології та напрями реалізації цього непростого завдання.

Доповнюється актуалізація дисертаційної роботи і тим фактом, що інформаційна безпека, яка оперує інформацією, безумовно є важливим чи неодмінним знаряддям конструювання сучасної цивілізації. Відповідно, провідні держави світу, усвідомлюючи це, беззаперечно виходять із постулату, що створення інформації та контроль над інформацією та різними ресурсами й потоками інформації, в тому числі у контексті технологічної модернізації з цього приводу, допомагають їм зберігати своє лідерство і контроль над поточним станом справ. А це ставить на порядок денний проблематику взаємозв'язку інформаційної безпеки та державного суверенітету, який суттєво залежить від різноманітних інформаційних впливів.

Деструктивні та дестабілізуючі інформаційні впливи найперше загрожують вразливим елементам політичної системи. Водночас нерідко цілеспрямовані та регулярні інформаційні атаки самі по собі формують сприятливе для поглинання середовище, коли дієві суб'єкти перетворюються у дезорієнтованих та безпорадних об'єктів політики. Особливо актуальною проблематика інститутів інформаційної безпеки є для нашої країни, суспільство якої та кожен окремий громадянин всі роки незалежності знаходяться під агресивним впливом різних суб'єктів інформаційного простору, як внутрішнього, так і зовнішнього. Для України питання інформаційної безпеки особливо актуалізувалося у зв'язку із гібридною війною, яку розв'язала Росія в останні роки.

Важливі мотиви актуалізації проблематики інформаційної безпеки полягають ще й в тому, що тільки країни з розвинутою інформаційною інфраструктурою здатні ставати конкурентоспроможним суб'єктом сучасного

міжнародного глобального середовища. У зв'язку з цим, важливим аспектом дослідження різних вимірів інформаційної безпеки держави і суспільства є визначення рівня інформатизації всіх сфер суспільної життєдіяльності в кожній окремій країні.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано в межах комплексної наукової теми кафедри політичних наук «Проблеми політичної модернізації і трансформації: світовий досвід і українські реалії», що входить до тематичного плану науково-дослідних робіт Національного педагогічного університету імені М. П. Драгоманова, науковий напрям «Дослідження проблем гуманітарних наук», затверджений Вченою радою НПУ імені М. П. Драгоманова (протокол № 6 від 26 грудня 2013 р.). Тема дисертації затверджена на засіданні Вченої ради НПУ імені М. П. Драгоманова (протокол № 9 від 30 грудня 2015 року).

Мета і завдання дослідження. Метою дослідження є концептуальне визначення суб'єктності політичних інститутів, що мають відношення до забезпечення інформаційної безпеки української держави і суспільства, а також аналіз їх розвитку в сучасних умовах, які складаються внаслідок розгортання глобалізаційних процесів та посилення агресивних дій Росії щодо інформаційного поля України. Досягнення поставленої мети потребує послідовного розв'язання наступних ***дослідницьких завдань***:

- охарактеризувати стан дослідження обраної проблеми, основні джерела та детермінанти питань інформаційної безпеки;
- дослідити теоретико-методологічні особливості засад дослідження феномену «інформаційна безпека» у суспільстві, з'ясувати основні параметри цього поняття;
- вивчити параметри українського правового поля регулювання інформаційної безпеки, структурувати сукупність політико-правових актів, діючих в Україні, окреслити ситуативні лакуни, які потребують доопрацювання в світлі існуючих викликів інформаційної безпеки;
- позиціонувати національну нормативну базу інформаційної безпеки відносно

міжнародних норм та практики забезпечення інформаційної безпеки;

- концептуальна фіксація глобального характеру проблеми інформаційної безпеки та з огляду на це визначення природи останньої;
- провести концептуально-теоретичний аналіз суб'єкт-об'єктних характеристик інформаційної безпеки держави та суспільства;
- з'ясувати інституційну складову проблеми інформаційної безпеки (визначення ролі державних, партійних, громадських органів, установ, організацій у формуванні інформаційно-безпекових пріоритетів соціуму та держави); окреслити організаційно-управлінських акторів, що безпосередньо впливають на стабілізацію чи дестабілізацію інформаційно-безпекової ситуації в країні;
- аналіз діяльності ЗМІ в контексті забезпечення інформаційної стабільності в державі;
- вивчення можливостей ефективної протидії інформаційно-деструктивним впливам, що мають зовнішні та внутрішні джерела у сучасній Україні.

Об'єктом дослідження виступають проблеми інформаційної безпеки України в умовах політичної трансформації, а *предметом дослідження* є державні та недержавні інститути, які функціонально впливають на формування політики інформаційної безпеки України.

Методи дослідження. Проведене дослідження базується на використанні загальнонаукових методів: індукція, дедукція, аналіз, синтез, порівняння, абстрагування, узагальнення та формалізація. Також використано спеціальні методи: порівняльний, структурно-функціональний, системний і інституціональний підходи до дослідження. Для вивчення зв'язків і залежностей в умовах процесів глобалізації застосовано методи екстраполяції, верифікації та типології. З допомогою порівняльного методу (аналіз окремого випадку, кростемпоральний та кроснаціональні порівняння) розглянуто та зіставлено параметри нормативно-політичної бази регулювання інформаційної безпеки в Україні та провідних державах світу; інформаційно-безпекову діяльність державних інститутів та політичних партій; позицію засобів масової інформації у сфері інформаціної

безпеки. Структурно-функціональний метод дозволив проаналізувати суб'єкт-об'єктний вимір інформаційної безпеки. Системний метод дозволив вивчити місце та роль державних та недержавних інститутів у забезпеченні інформаційної безпеки держави. Інституційний метод надав можливість через аналіз основних інститутів зрозуміти функціональне забезпечення інформаційної безпеки. Теоретико-методологічною основою дослідження виступив неоінституціоналізм у форматі історичного, соціологічного та теорії раціонального вибору. При опрацюванні теми була також використана низка концептів демократії, які прийнято застосовувати під час вивчення міжінституціональних відносин.

Наукова новизна отриманих результатів полягає, насамперед, у тім, що в ньому з позицій сучасного науково-політологічного дискурсу комплексно проаналізовані основні тенденції процесу формування інформаційної безпеки в трансформаційному суспільстві та місце і роль державних і не державних інститутів у забезпеченні інформаційної безпеки України. В процесі аналізу отримані висновки і результати, які свідчать про розв'язання визначених наукових завдань та характеризуються елементами наукової новизни, зокрема:

Вперше:

– констатовано, що в системі викликів і ризиків, які постають перед Україною в контексті глобального харакетру інформаційної безпеки, ключовим є втрата власної національної ідентичності, державного суверенітету, особливо інформаційного суверенітету, який визнається сьогодні головною ознакою державної самостійності та правосуб'єктності;

– доведено, що в системі інформаційної безпеки важливе місце займає інформаційна безпека нації, яка включає в себе захист неповторних національно-культурних цінностей, історичних традицій, історичної пам'яті, мови, унікальних субкультур;

– встановлено, що рівень інформаційної безпеки визначає стан розвитку політичної, соціально-економічної, оборонної, закордонної та інших компонентів національної безпеки України, а відповідні деструктивні інформаційні впливи проявляються фактично у всіх сферах життя суспільства;

– обґрунтовано, що існуюча інфраструктура державних інститутів інформаційної безпеки України мусить вибудовуватися за принципом стримувань і противаг, відповідно, що державні інститути повинні постійно перебувати під громадським контролем, бути відкритими до комунікації з ЗМІ, прозорими у своїх рішеннях та звітності, зрозумілими для міжнародних партнерів;

Удосконалено та поглиблено:

– розуміння, що інформаційна безпека у будь-якому структурно-функціональному вимірі телеологічно має бути орієнтована на захист прав людини і громадянина, на забезпечення повноцінного національно-культурного розвитку певного соціуму та на всебічний захист державного суверенітету;

– розуміння інформаційної безпеки з точки зору формування єдиного функціонально-життєвого соціального простору творення суттєвих змістів, що визначають такі світоглядно-аксіологічні пріоритеті, як патріотизм, гідність, державотворення, загальнолюдські цінності;

– параметри взаємодії ЗМІ та держави, опрацьовано шість моделей: незалежної преси, соціальної відповідальності, демократичного представництва, радянська модель, авторитарна та модель розвитку. З допомогою чотирьох з них на різних історичних етапах можна пояснити ситуацію в Україні. Також доведено, що три моделі дають можливість адекватно характеризувати авторитарні системи правління;

– підхід згідно якого найбільш вразливе середовище для інформаційних операцій агресивного характеру формується з людей, які є апатичні до політики, пасивні у соціальних справах, нігілістичні, замкнені рамками мінімальних знань та вузьких світоглядних орієнтирів;

– висновок, що визначальною інформаційною загрозою національній безпеці виступає маніпуляція суспільною свідомістю, оскільки це дестабілізуючий вплив і на інформаційну струтуру країни, і на її інформаційні ресурси та на суспільство загалом, в тому числі на окрему особистість, як громадянина;

– оцінка, що ефективна інформаційна політика державних структур досить часто вимірюється не лише міжнародними стандартами та правилами, але і

спроможністю захищати специфічні національні інтереси, приймати актуальні виклики та долати гострі загрози;

– твердження, що основними формами та умовами колективної протидії маніпулятивним впливам є: просвітницька діяльність; проведення заходів, завдяки яким громадяни могли б навчитися протистояти маніпулюванню; моніторинг діяльності ЗМІ; розвиток у суспільстві конкуруючих мереж розповсюдження інформації; вироблення та популяризація критеріїв оцінки суспільної та політичної відповідальності представників влади;

Дістали подальшого розвитку:

– твердження, що одним з ключових вимірів проблематики інформаційної безпеки сьогодні є пошук адекватного балансу між впливами глобального характеру, які ґрунтуються на інтенсифікації переміщення інформації в глобальному інформаційному середовищі та потребами окремих людей і суспільних груп, в тому числі держав, що не є провідними суб'єктами, здатними впливати на глобальні цивілізаційні тенденції та процеси;

– висновок, що великі геополітичні протистояння найчастіше ведуться не на полі головних супротивників, а у просторі вразливих суспільств та нестабільних держав. Неспроможність цих держав давати адекватні інформаційні відповіді кваліфікується як підстава для інформаційної експансії та поступового поглинання, навіть без очевидного застосування сили;

– положення згідно якого можливість держави і суспільства протистояти зовнішній інформаційній агресії зумовлюється: проведенням деіократичних реформ; зрілим громадянським суспільством; стабільною правовою державою; сформованою демократичною та активістською політичною культурою;

– оцінки, що поняття культури інформаційної безпеки трактується як рівень розвитку людини та суспільства, які характеризуються значимістю забезпечення безпеки життєдіяльності в системі особистісних і соціальних цінностей, безпечної поведінки в повсякденному житті в умовах небезпечних та надзвичайних ситуацій, рівнем захищеності від загроз та небезпек у всіх сферах життєдіяльності. На

індивідуальному рівні культура безпеки проявляється у світогляді та зразках поведінки;

– твердження, що кращі безпекові стратегії та практики, які успішно захищають сучасний інформаційний простір, побудовані на трьох визначальних принципах: ієрархічності, державної координованості та взаємодії;

– оцінки, згідно яких перед державною владою з розвитком соціальних мереж постають такі завдання: структуризація віртуальних спільнот у вітчизняних соціальних мережах; усвідомлення їх впливовості та можливостей; пошук та вироблення адекватних реакцій на реальні та потенційні загрози, приховані у віртуальному громадянському просторі; розвиток доступних механізмів державного регулювання цього соціального феномену; слідування демократичним взірцям та традиціям у цій сфері;

– висновок, що фейкові партійні структури або не здійснюють інформаційної діяльності взагалі, або здійснюють пряме і опосередковане інформаційне обслуговування потужних політичних партій. В будь-якому випадку їх діяльність сприяє викривленню інформаційного та політичного просторів держави й чинить негативний вплив на інформаційну безпеку особистості та суспільства;

– підвищення ролі політичної освіти і просвітництва, як змістовної основи вироблення окремими особами, громадянським суспільством, державою імунітету до багатьох загроз, пов’язаних з інформаційно-маніпулятивними впливами різних зовнішніх и внутрішніх суб’єктів.

Теоретичне і практичне значення отриманих результатів полягає у тім, що в ньому вперше в політологічній літературі останніх років проаналізовані основні тенденції забезпечення інформаційної безпеки в трансформаційному суспільстві за допомогою різного інструментарію – утвердженню демократичної свідомості й ідеології, інтелектуалізації, інформатизації і прагматизації політичного поля, забезпечення всебічної політологічної та правової освіти широким колам громадськості. Автором виявлені основні зміни в трансформаційному соціумі та їхні виклики щодо повноцінного формування інформаційно-безпекового порядку денного, актуального як для держави як політичного утворення та

суспільства як суспільно-політичного феномену, так і для окремих громадян та їхніх груп. У дисертації проаналізовані також зміна інтересів та потреб політичного класу та особистості трансформаційного суспільства з огляду їхньої експектації стосовно різноманітних вимірів проблематики інформаційної безпеки. Матеріали дисертації можуть бути використані в частині політичного виховання особистості як елемента державної гуманітарної політики та в навчальному процесі при викладанні курсів політології, культурології, спеціалізованих курсів інформаційної, та інформаційно-правової безпеки. На основі дисертаційного тексту може бути підготовлений спеціальний курс для студентів політологічних спеціальностей.

Особистий внесок здобувача. Дисертаційна робота є самостійним науковим дослідженням, спрямованим на досягнення мети – концептуального визначення суб'єктності політичних інститутів, які мають відношення до забезпечення інформаційної безпеки української держави і суспільства, а також аналіз їх розвитку в сучасних умовах. Задля цього автором роботи опрацьовано сукупність міжнародних та національних нормативно-правових і політико-правових актів та проаналізовано функціональні аспекти діяльності державних та громадських структур України в царині інформаціної безпеки. Відповідно, особистий внесок здобувача репрезентовано у тексті дисертації, 1 монографії, 21 статті у періодичних фахових виданнях з політичних наук, а також у 10 наукових працях, що засвідчують апробацію матеріалів і додатково відображають наукові результати дисертації. Наукові результати отримані автором самостійно, а усі опубліковані праці за темою дисертації є одноосібними.

Апробація результатів дисертаційної роботи. Основні положення та висновки дослідження оприлюднені на міжнародних, всеукраїнських наукових і науково-практичних конференціях, семінарах, круглих столах, з-поміж яких: Друга міжнародна науково-практична конференція «Управлінські компетенції викладача вищої школи» (28 лютого 2014 р., м. Київ), міжнародна науково-практична конференція «Політика і духовність в умовах глобальних викликів» (2 квітня 2014 р., м. Київ), IV міжнародні Драгоманівські читання: до 180-річчя НПУ імені М. П. Драгоманова (16–17 квітня 2015 р., м. Київ), Одинадцяті

юридичні читання «Форма сучасної національної української держави: реалії та перспективи» (21–22 травня 2015 р., м. Київ), міжнародна науково-практична конференція «Формування державної освітньої політики: філософські, теоретичні та прикладні аспекти» (25–26 лютого 2016 р., м. Київ), міжнародна науково-практична конференція «Сутність та перспективи впровадження електронної демократії в Україні» (15 листопада 2016 р., м. Вінниця), Різдвяні педагогічні читання «Новий вчитель для нової української школи» (23–25 грудня 2016 р., м. Київ), науково-практична конференція «Ціннісний дискурс у суспільстві та освіті» (1–2 березня 2018 р., м. Київ), міжнародна наукова конференція «Тринадцяті юридичні читання «Українська державність: крізь призму часу (до 100-річчя Української національно-демократичної революції 1917–1921 рр.)»» (24–25 травня 2018 р., м. Київ), наукова конференція «Культурологічна практика в системі підготовки майбутнього вчителя» (5–6 жовтня 2018 р., м. Київ), тиждень філософії в НПУ імені М. П. Драгоманова «Майбутнє філософської освіти в Європі: виклики та перспективи» (14–17 травня 2019 р., м. Київ), науково-практична конференція «Значення культурної практики в освітянському процесі університету» (31 травня – 1 червня 2019 р., м. Київ – м. Новгород-Сіверський), Політологічні читання імені професора Богдана Яроша (14 квітня 2020 р., м. Луцьк). Крім того, положення дисертації обговорювались під час засідань й семінарів кафедри політичних наук Національного педагогічного університету імені М. П. Драгоманова.

Публікації. За темою дисертації опубліковано 32 наукові праці, серед яких: 1 – одноосібна монографія, 15 – статті у наукових фахових виданнях України з політичних наук, 6 – статті у наукових фахових виданнях з політичних наук, які включені до міжнародних наукометричних баз, 10 – наукові праці, що засвідчують апробацію матеріалів і додатково відображають наукові результати дисертації.

Структура дисертації. З огляду на об’єкт і предмет, мету та завдання дослідження, робота складається із анотацій, вступу, шести розділів, висновків та списку використаних джерел. Загальний обсяг дисертації – 423 сторінки, а основна частина дисертації становить 362 сторінки. Список використаних джерел складається з 481 позиції.

РОЗДІЛ 1

ІСТОРІОГРАФІЧНІ ТА ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСОБЛИВОСТІ ТА ПАРАМЕТРИ ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ПОЛІТИЧНОЇ ТРАНСФОРМАЦІЇ

1.1. Стан дослідження й історіографія проблематики інформаційної безпеки в умовах політичної трансформації у зарубіжній та вітчизняній науці

Проблематика інституційного виміру інформаційної безпеки України, зокрема з погляду трансформаційних викликів, глобальних контекстів і стратегічних орієнтирів розвитку нашої держави на тлі загальносвітових процесів, є доволі багатогранною, а тому й потребує історіографічної структуризації. Головна причина цього полягає в тому факті, що означена тематика компонує питання як теоретико-методологічного, так і практично-емпіричного порядків, а також стосується як нашої держави, так і інших країн світу й, неодмінно, означеного блоку проблем також у загальному розумінні. Відповідно, аксіоматичним є той факт, що різноспрямовані і різні за важливістю й наповненням складові проблематики інформаційної безпеки, в тому числі в Україні, компонуються градуйовано, зокрема у географічному (в зарубіжних і вітчизняних дослідженнях), часовому (в класичних і новітніх розвідках) та джерельному відтинку.

З цього приводу передусім потрібно підкреслити, що впродовж останніх 50-70 років, тобто із другої половини ХХ століття, у західній філософській, соціологічній, політологічній і загалом соціогуманітарній науковій думці було розроблено значний категоріально-понятійний та концептуально-теоретичний, методичний та методологічний апарат, присвячений всебічному аналізу не просто інформаційної безпеки, але й таких глобальних феноменів, як інформація й інформаційна цивілізація, а також

окремим вимірам нового цивілізаційного простору, що ставить перед сучасним суспільством і людиною нові виклики та проблеми, причому як національного, так і глобального масштабу, а також як індивідуального, так і групового чи суспільного відтінку.

На цьому тлі зафіксовано, що тематика специфіки інформаційної цивілізації та її проблемно-безпекових аспектів, зокрема інформаційної безпеки як такої, піднімалась у цілому масиві фундаментальних і навіть класичних доробків (виданих головно до початку 90-х рр. XX ст.) за авторством таких відомих західних філософів і науковців, як Е. Аронсон [316], М. Балфур [293], З. Бауман [441; 442], Х. Бей [295], Д. Белл [443; 444], З. Бжезинський [445; 446], Ж. Бодрійяр [447; 448], Г. Вайнштейн [37; 38], У. Дайзард [449], Р. Дарендорф [450], Ж. Доменак [451], А. Ендмюллер [351], А. Кампен [296], Г. Кан [452; 453], М. Кастельс [131], Е. Кац і П. Лазарфельд [454; 455], Г. Лассуел [355], М. Маклюен [176], Е. Масуда, Г. Міллер, В. Парето [456], А. Тойнбі [457-459], Е. Тоффлер [261], С. Хантінгтон [460-462], Ю. Габермас [356; 463-465], Д. Шарп [466; 467] та чимало інших. Праці цих філософів й науковців постали базою і фундаментом у дослідженні різних аспектів, виявів, опцій та наслідків функціонування інформаційного суспільства, а відтак в обрамленні його безпеки – так званої інформаційної безпеки. Відповідно, на основі праць перелічених та інших мислителів і вчених було сформульовано й навіть визначено ключові поняття, які змальовують і конфігурують специфіку сучасної цивілізації, в тому числі її інформаційно-безпекового виміру, важливого як для окремої людини й окремих соціальних спільнот, так і для людства в цілому.

Саме тому отримані у вже класичних філософських і наукових працях результати й доробки із означеної проблематики постали підґрунтям її подальшого розвитку як у зарубіжній, так і у вітчизняній науці, в тому числі політичній тощо. Це, приміром, можемо спостерігати у суттєвому зростанні кількості досліджень, які присвячені тематиці інформаційної безпеки, інформаційного простору й інформаційного суспільства загалом, а також у

їхньому значному урізноманітненні – профільному, тематичному, структурному, географічному, методичному тощо. Якщо говорити про західну політичну науку, то це відображено навіть у формуванні й розвитку спеціалізованих періодичних наукових топ-видань (приміром «Information Security Journal: A Global Perspective», «The Information Society», «International Journal of Information and Communication Technology», «International Journal of Communication» та ціла низка інших) і своєрідних баз та каталогів відповідних цифрових даних (наприклад, «Global Terrorism Database», «World Development Indicators: The information society» тощо), які дотичні до проблематики інформаційної або інформаційно-політичної безпеки і тероризму як в окремих країнах, так і в їхніх групах, регіонах чи навіть у всьому світі. Що стосується доволі відомих і навіть знакових постатей у світі новітньої західної науки (з 90-х рр. XX ст., але головно з початку XXI ст.), в тому числі політичної, то серед них потрібно виокремлювати такі прізвища дослідників означеної проблематики (в тому числі й у контексті України), як М. Браут-Хеггхаммер [427], К. Вайт і Б. Мазанец [481], Є. Ву і Ф. Менг [428], Дж. Л. Грама [468], М. Гупта та Р. Шарман [474], Р. Дейберт і Р. Рогозінскі [297], К. Джаклін [426], Й. Еріксон та Г. Гіакомелло [473], М. Д. Кавелті [471], Ч. Кахл [477], Ж.-Ф. Кремер та Б. Мюллер [472], М. Лейсі та П. Вілкін [480], М. Манджікіан [476], Т. Маурер і С. Ланц [304], Т. Мур, Д. Пім і К. Іоннідіс [469], Х. Нематі [470], Е. Пейн [305], Я. Райчев [429], В. Рід [307], Дж. Розенау і Дж. Сінгх [478], М. Сміт [479], Н. Снов [310], Р. вон Солмс і Й. ван Ніекерк [423], Х. Тумбер та Ф. Вебстер [313], Х. Хауккала [299], Дж. Хенріксен [425], Н. Чоукрі [475] та чимало інших. Різні з них фокусуються на окремішні, але взаємопов’язані профілі розуміння інформаційної безпеки у сучасному світі, причому часто не лише у технологічному, але й у соціологічному та політичному/суспільно-політичному і навіть глобальному розрізі.

За аналогією, доволі значного розвитку означена проблематика набула в східноєвропейській політичній науці, однак у цьому регіональному розрізі вона є різноспрямованою політично та геополітично, зокрема на тлі особливих

взаємин між державами. Тим не менше, вже історично склалось так, що проблематика інформаційної безпеки, пропаганди та тероризму доволі активно вивчається (і практикується) у Росії та інших пострадянських країнах, в тому числі такими дослідниками, як Р. Абрамов [4], М. Алієва [9], А. Баранов [18], Ю. Воробйов [44], М. Грачов [56], Ю. Єрмаков [325], А. Заббаров [88], С. Кара-Мурза [326], А. Курочкін [160], А. Лазаревіч [161; 162], В. Лопатін [173], А. Манойло [182], І. Панарін [340], А. Соловйов [252], Л. Федотова [271] та дуже багато інших. При цьому, за останні десятиліття з-поміж їхніх доробків доцільно окремо виокремлювати як цілком раціоналізовані та більш-менш об'єктивовані такі монографії, як «Государственная информационная политика в особых условиях» (автор – А. Манойло) і «Информационная война и геополитика» (автор – І. Панарін). Також доволі цікаво й те, що раніше на російську школу інформаційної безпеки у рамках політичної науки доволі активно орієнтувались вчені з більшості інших пострадянських країн Європи й Азії, однак сьогодні, головно в силу відомих політичних подій останнього десятиліття, спектр таких суттєво скоротився і продовжує це робити й надалі.

Врешті-решт, що стосується означення проблематики інформаційної безпеки у контексті титульної країни представленого дослідження, то в сучасному українському теоретичному, аналітичному та дослідницькому дискурсі, зверненому до проблематики інформаційної безпеки, можна спостерігати доволі високу активність науковців, адже ця проблематика сьогодні і раніше була та залишається як теоретичною, так і практичною, оскільки безпосередньо пов'язана зі становленням молодої української держави, вибудовуванням всієї структури правової держави і активного громадянського суспільства, захисту прав та свобод громадян. Окрім того, дуже гострою раніше поставала, однак найбільше гостро поточно постає проблема зовнішніх інформаційних впливів на Україну і в Україні зі сторони інших держав й міжнародних організацій, особливо сусідніх.

На цьому тлі потрібно зазначити, що в Україні, вивчаючи актуальні напрями, проблеми й аспекти інформаційної безпеки, дуже важливо не оминути

ґрунтовних напрацювань політологів, філософів, економістів, соціологів, юристів й інших дослідників, котрі різного часу аналізували її доволі відмінні прояви у сенсі особливостей поступу інформаційного суспільства та інформаційного середовища тощо. З-поміж них треба згадати передусім таких вчених (у переліку подано лише тих, до яких апелюємо в дисертаційній роботі, хоча їхня кількість набагато більша), як Л. Абрамов і Т. Азарова [2], А. Баранов [18], Т. Бєльська [21], О. Бойко [317], Ю. Бондар [31], В. Горбулін [52; 321], В. Брижко [33], Н. Глебова [50], Ю. Горбань [51], В. Григор'єв [58], В. Гурковський [62; 63], С. Даниленко [65], О. Дзьобань і В. Пилипчук [73], В. Ільганаєва [119], Б. Кормич [148; 149], С. Кудрявцева і В. Колос [159], О. Логінов [171; 272], Є. Макаренко [174], Б. Остроухой, Б. Петрик і М. Присяжнюк [121], В. Петрик [121; 214; 215], Т. Пода [218], В. Попов [220], Г. Почепцов [223; 343], О. Степко [254], С. Терепищий [256-258], А. Чічановський і О. Старіш [281], С. Ягодзінський [288] та дуже багато інших.

У працях вітчизняних дослідників також детально аналізуються різноманітні загальнотеоретичні аспекти проблематики інформаційної і національної безпеки, причому такі дослідження зовсім не втрачають своєї актуальності. У той же час, з нашої точки зору, сьогодні особливу увагу треба звернути на системність цієї проблематики, а відтак й виробити найзагальніші концептуально-теоретичні принципи, що дозволили б на науковому рівні не тільки вирішувати окремі безпекові проблеми, але й ефективно вписали би Україну у загальний і глобально-цивілізаційний контекст світоглядно-ціннісного й інформаційно-технологічного вирішення безлічі викликів, з якими стикається сучасне інформаційне суспільство, в тому числу у категоріях політичного процесу. На цьому тлі доречно, приміром, апелювати щодо дослідників, які займаються проблематикою національної безпеки як такої, серед яких, зокрема, такі як В. Ананьїн [7], І. Боднар [26], В. Дзюндзюк [75] тощо.

Водночас особливо важливими для нашого дослідження є теоретичні джерела, в яких аналізується зв'язок поміж загальним функціонуванням

глобального інформаційного середовища і специфікою протидії держави ключовим викликам, котрі можуть загрожувати інформаційній безпеці держави, суспільства та особистості. З-поміж них потрібно виділяти за авторством таких науковців, як Є. Архипова [14], А. Баранов [18], В. Богуш і О. Юдін [25], І. Боднар [26], О. Бойченко [28; 29], Р. Гумінський [61], О. Дзьобань і В. Пилипчук [73], Л. Дорош [80], В. Желіховський [168], І. Забара [86; 87], О. Золотар та І. Трубін [117], В. Карпенко [126; 127], О. Кісілевич-Чорнойван [137], М. Корольов і О. Скопа [152], О. Крюков [158], О. Левченко [164], О. Литвиненко [165; 166], В. Ліпкан [168], Є. Макаренко [175], Ю. Максименко [168; 177], Г. Несвіт [198], Ю. Нестеряк [200-202], О. Олійник [205; 206], В. Петрик [214], Ю. Романчук [240], О. Тихомиров [260], В. Триняк [262], Ч. Фань [269] й інші. У їхніх працях створено важливу категоріально-понятійну базу для подальшого аналізу проблематики, пов’язаної із всебічним забезпеченням та регулюванням державою, в тому числі й Україною, інформаційної безпеки для поступу громадянського суспільства загалом і для кожного громадянина зокрема.

А вже на цьому тлі важливо виокремити певні тематичні групи, у рамках яких дослідники звертаються до аналізу і систематизації окремих важливих аспектів проблеми інформаційного суспільства й інформаційної безпеки як в Україні, так і в інших країнах світу. У цьому зрізі окремо вирізняємо дослідження структурних основ безпеки в інформаційному суспільстві й середовищі, в тому числі сутність інформаційного простору та інформаційної політики в нашій та інших країнах світу. Це можемо простежувати у доробках таких вчених, як Л. Біловус [24], Ю. Бондар [31], В. Брижко [33], Ю. Бурило [34], О. Гіда [47; 48], Л. Губерський та Є. Камінський [60], С. Даниленко [65], О. Данильян [224], О. Дзьобань і В. Пилипчук [73], А. Добровольська [77], О. Дубас [83], Л. Задорожня, М. Коваль та В. Брижко [89], Р. Калюжний [124], А. Литвиненко [165], А. Марущак [185], Л. Наливайко [194], О. Петкова [213], А. Петрицький [215], О. Проскуріна [230], І. Сопілко [253], А. Ярошенко [290] та інші.

Своєю чергою, проблематику сутності розуміння політики і влади,

міжінституційних і політичних відносин в інформаційну епоху розкривають такі вітчизняні дослідники, як Т. Авксентьева [6], Н. Астряб [15], В. Бабіна [16], Ю. Бондар [31], О. Бухтатий та В. Вакулич [39], Я. Варивода [40], Н. Вахрамєєва [41], С. Даниленко [65], С. Денисюк [68], М. Дмитренко [76], О. Зернецька [116], В. Карлова [125], О. Прасюк [225], Л. Смола [250], В. Яковлев [289] тощо. Паралельно із ними, аналізується в українській науці і проблематика національної безпеки як такої, що помічаємо в ідеях та працях таких науковців, як В. Ананьїн [7], Л. Борисова та В. Тулупов [32], О. Гіда [47; 48], О. Дзьобань [72], В. Дзюндзюк [75], С. Каштелян [133], Н. Колісніченко [142], О. Корнівєвський [150; 151], В. Крутов та Г. Новицький [157], Я. Лантінов [163], В. Ліпкан [167; 169], К. Павлюк [211], В. Українчук [267], В. Шахов і В. Мадіссон [292] і чимало інших.

У рамках своєрідного синтезу попередніх груп досліджень вчені з України дуже часто розкривають специфічні особливості й інструменти забезпечення інформаційної безпеки нашої й інших держав, суспільства і людини. Це можемо бачити на підставі апелювання до наукових розвідок таких дослідників, як Р. Алямкін [11; 12], А. Баранов [18], І. Березовська [20], В. Богуш і О. Юдін [25], О. Бойченко [30], Л. Борисова і В. Тулупов [32], В. Горбулін, О. Додонов і Д. Ланде [52], В. Григор'єв [58], І. Громико і Т. Саханчук [59], В. Гурковський [62; 63], В. Гусаров [64], М. Гуцалюк [323], О. Дзьобань і В. Пилипчук [72-74], Л. Євдоченко [84], Т. Жовтенко [85], М. Зайцев [90], О. Зозуля [430], М. Карчевський [130], Є. Кирильчук [134; 135], З. Коваль [138], В. Конах [143], М. Копійка [439], Б. Кормич [148; 149], О. Косогов [153], Н. Крилова [156], О. Крюков [158], В. Ліпкан [168], Ю. Лісовська [170], О. Логінов [171], Ю. Максименко [177], І. Малик [178; 179; 434], В. Марков [184], О. Морозов [190], Л. Наливайко [194], А. Нашинець-Наумова [197], Г. Несвіт [198], О. Олійник [207], В. Отрешко [210], В. Петров [216], С. Попов й О. Бойченко [220], М. Присяжнюк та Я. Бєлошевич [227], О. Руснак [244], О. Сагайдак [245], Т. Субіна [255], О. Федорук [270], В. Хімей [273], О. Юдін і С. Бучик [284; 285], А. Юричко [286] та інші.

Серед цих та інших авторів, враховуючи проблематику їхніх ідей і пошуків, можна виокремлювати певні профілі розуміння та розкриття тематики інформаційної безпеки у нашій та інших країнах. Наприклад, таку важливу проблему як інформаційно-психологічне протиборство в сучасних умовах аналізують Л. Дорош [80], О. Зозуля [430], З. Коваль [138], Е. Макаренко [174-175], Н. Ничта [337], Є. Скулиш [123], Л. Смола [250], П. Шевчук [350] тощо. Своєю чергою, особливу увагу в нашому дослідженні також приділено таким вимірам збудження інформаційної небезпеки, як агресивні впливи, протистояння та війни. З огляду на це, було встановлено, що проблемі інформаційних воєн присвячують свої дослідження В. Абакумов [1], В. Горбулін, О. Додонов та Д. Ланде [52], В. Петров [216], В. Полевий [219], Г. Почепцов [223; 343], Ю. Рубан [241], М. Сенченко [345; 346], П. Шевчук [350] й інші. Особливою актуальністю сьогодні також відзначаються і концептуально-теоретичні розвідки тих українських авторів, котрі досліджують різноманітні джерела, причини, фактори, специфіку і наслідки виникнення інформаційних загроз різного масштабу, їхню етимологію і характер. Різні питання, пов’язані з темою сутності та виявлення загроз інформаційній безпеці, зустрічаємо, для прикладу, у працях Р. Калюжного [124], Б. Кормича [148; 149], В. Ліпкана [167-169], А. Марущака [185], Ю. Максименка [168; 177], В. Пилипчука [73; 74], В. Цимбалюка [278] й інших дослідників.

Таким чином можна констатувати, що сьогодні існує достатньо широка концептуально-парадигмальна й емпірична база і доволі активний теоретичний і практичний дискурс, спрямовані на вивчення інформаційних загроз, інформаційної безпеки, інформаційного суспільства тощо, як у теорії, так і в нашій державі. Водночас, з нашої точки зору, існує необхідність більш чіткої систематизації даної проблематики, яка б дозволила цілісно підійти до вивчення конкретних можливостей організованої протидії тим викликам, які постають перед людиною, суспільством і державою з боку глобального інформаційного суспільства, а також з боку внутрішніх та зовнішніх суб’єктів збурювання інформаційної небезпеки. У цьому зрізі за доцільне вважаємо виокремлення тих

праць за авторством українських дослідників, котрі характеризуються елементами монографічності або є дисертаційними роботами із означеної чи близької проблематики.

Так, близькими за спрямованістю та змістовним наповненням до тематики інформаційної безпеки є монографії за авторовим таких вчених, як (у хронологічному порядку опублікування) О. Дзьобань («Національна безпека України: концептуальні засади та світоглядний сенс» [72], 2007 р.), В. Ананьїн («Актуальні проблеми національної безпеки суспільства» [7], 2008 р.), С. Денисюк («Технологічні виміри політичної комунікації» [68], 2010 р.), В. Цимбалюк («Інформаційне право (основи теорії і практики)» [278], 2010 р.), М. Дмитренко («Політична система України: розвиток в умовах глобалізації та інформаційної революції» [76], 2011 р.), а також Т. Авксентьєва («Політика і влада в інформаційну епоху: український контекст» [6], 2013 р.). Своєю чергою, безпосередньо означеної в нашій роботі проблематики стосуються монографії таких українських вчених, як О. Литвиненко («Спеціальні інформаційні операції» [166], 1999 р.), В. Горбулін, О. Додонов та Д. Ланде («Інформаційні операції та безпека суспільства: загрози, протидія, моделювання» [52], 2009 р.), а також О. Дзьобань та В. Пилипчук («Інформаційне насильство та безпека: світоглядно-правові аспекти» [73], 2011 р.).

Паралельно з цим, в Україні було захищено кілька дисертаційних робіт різного рівня (на різний кваліфікаційний рівень), котрі прямо або опосередковано стосуються проблематики інформаційної безпеки у нашій та інших державах. Зокрема, різного часу було захищено кандидатські дисертації, які оперували проблематикою інформаційної безпеки та доволі суміжними питаннями на прикладі власне України, а також більшою мірою загальнотеоретично. Це було зроблено такими дослідниками (у хронологічному порядку захисту кваліфікаційних робіт), як Г. Несвіт («Інформаційна політика держави як фактор реформування суспільства» [198], 2001 р.), В. Гурковський («Організаційно-правові питання взаємодії органів

державної влади у сфері національної інформаційної безпеки» [63], 2004 р.), О. Дубас («Інформаційний розвиток сучасної України у світовому контексті: політологічний аналіз» [83], 2004 р.), О. Логінов («Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади» [171], 2005 р.), Ю. Максименко («Теоретико-правові засади забезпечення інформаційної безпеки України» [177], 2007 р.), А. Юричко («Інформаційні маніпуляції у повідомленнях світової періодичної преси в контексті інформаційної безпеки України: стан та шляхи протидії» [286], 2007 р.), Ю. Романчук («Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти» [240], 2009 р.), В. Триняк («Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз)» [262], 2009 р.), О. Петкова («Політичні імперативи позиціонування України в міжнародному інформаційному просторі» [213], 2010 р.), В. Петров («Воєнно-інформаційна безпека України за умов посилення загроз інформаційних війн» [216], 2010 р.), Т. Субіна («Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України» [255], 2010 р.), В. Абакумов («Правове регулювання протидії інформаційним війнам в Україні» [1], 2011 р.), Л. Євдоченко («Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації» [84], 2011 р.), З. Коваль («Політико-правові механізми державного управління інформаційно-психологічною безпекою України» [138], 2011 р.), О. Зозуля («Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства» [430], 2017 р.) тощо.

Натомість захищені в Україні кандидатські дисертаційні роботи, які стосуються питань і проблем інформаційної безпеки тощо в інших країнах світу, передусім у США, Росії та Китаї, є значно менш репрезентованими у вітчизняній науці. Тим не менше, вони все-ж мають місце, зокрема за авторством таких вчених (також у хронологічному порядку захисту цих кваліфікаційних робіт), як Я. Варивода («Інформаційні стратегії у зовнішній політиці США та Росії за кризових умов» [40], 2004 р.), О. Степко («Інформаційна діяльність ООН»

[254], 2004 р.), В. Конах («Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США)» [143], 2005 р.), Хуан Цинь («Інформаційна політика Китайської Народної Республіки в сучасних міжнародних відносинах» [275], 2007 р.), Т. Жовтенко («Інформаційне забезпечення політики держави у боротьбі з міжнародним тероризмом: на прикладі США» [85], 2010 р.) тощо.

Ще менше в Україні захищено дисертаційних робіт на отримання кваліфікації доктора наук із проблематики інформаційної безпеки та інформаційної політики, в тому числі у нашій державі. Зокрема, у 2002 р. Є. Макаренко підготував і захистив дисертацію «Міжнародна інформаційна політика: структура, тенденції, перспективи» [174] (спеціальність – політичні проблеми міжнародних систем та глобального розвитку), у 2004 р. Б. Кормич – роботу «Організаційно-правові основи політики інформаційної безпеки України» [149] (спеціальність – теорія управління, адміністративне право і процес, фінансове право, інформаційне право), у 2011 р. Л. Смола – дисертацію «Інформаційно-психологічні детермінанти сучасного політичного процесу (світовий та вітчизняний контексти)» [250] (спеціальність – теорія та історія політичної науки), у 2011 р. С. Даниленко – дисертаційну роботу «Громадянський вимір інформаційно-комунікаційної революції: концептуально-теоретичні та політико-прикладні аспекти» [65] (спеціальність – політична культура та ідеологія). Сумарно це означає, що станом на момент аналізу та завершення нашого дослідження, особливо із огляду на дуже велику теоретичну та практичну актуальність й значимість, в Україні не було підготовлено і захищено жодної докторської дисертації зі спеціальності 23.00.02 – політичні інститути та процеси, котра би стосувалась саме проблематики трансформаційних викликів, глобальних контекстів та стратегічних орієнтирів інституційного виміру інформаційної безпеки в Україні.

Хоча, як продемонстровано вище, для цього є належна історіографічна та теоретико-методологічна база, яка може бути помічною в означеному завданні. Паралельно з цим, в Україні є відповідна нормативно-правова база, яка значною

мірою регулює проблематику інформаційної політики й інформаційної безпеки тощо у нашій державі. У цьому контексті серед базових нормативно-правових актів і документів, які регулюють чи хоча б принаймні частково структурують інформаційний простір і створення й функціонування системи забезпечення інформаційної безпеки в нашій державі, треба, крім Конституції України 1996 р. [145], виокремлювати закони України (у хронологічному порядку їхнього первинного прийняття, звісно з змінами й доповненнями) «Про оборону України» [104] від 1991 р., «Про інформацію» [101] від 1992 р., «Про друковані засоби масової інформації (пресу) в Україні» [101; 111] від 1992 р., «Про телебачення і радіомовлення» [92; 108] від 1993 р., «Про державну таємницю» [94] від 1994 р., «Про інформаційні агентства» [112] від 1995 р., «Про Концепцію Національної програми інформатизації» [102] від 1998 р., «Про захист суспільної моралі» [99] від 2004 р., «Про Службу зовнішньої розвідки України» [107] від 2006 р., «Про Державну службу спеціального зв'язку та захисту інформації України» [93] від 2006 р., «Про основні засади розвитку інформаційного суспільства в Україні 2007–2015 років» [106] від 2007 р., «Про захист персональних даних» [98] від 2010 р., «Про Національну раду України з питань телебачення і радіомовлення» [103] від 2014 р. (у попередній версії від 1997 р.), «Про Суспільне телебачення і радіомовлення України» [115] від 2014 р., «Про національну безпеку України» [385] від 2018 р. (на відміну від закону «Про основи національної безпеки України» [114] від 2003 р.) та чимало інших.

Також доцільно апелювати і до деяких указів Президента України та рішень Ради національної безпеки і оборони України, зокрема «Про Раду з питань інформаційної політики при Президентові України» [406] від 2001 р., «Про Національну комісію з утвердження свободи слова та розвитку інформаційної галузі» [407] від 2006 р., «Про Доктрину інформаційної безпеки України» [263; 265] від 2009 та 2017 рр., «Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації» [398] від 2011 р., «Про заходи щодо вдосконалення формування та реалізації державної

політики у сфері інформаційної безпеки України» [264] від 2014 р. тощо. Ці укази та рішення головно й різного часу були направлені на розвиток Національної програми інформатизації і Доктрини інформаційної безпеки України. Так, Національна програма інформатизації як важливий орієнтир розвитку системи інформаційної безпеки в нашій державі була визначена ще в 1998 р. Своєю чергою, Доктрина інформаційної безпеки України ініціально була затверджена указом Президента України 2009 р., а згодом вже в оновленій формі – указом Президента України від 2017 р. [387].

Урешті-решт, примітно, що в нормативно-регулятивному контексті українське законодавство в сфері інформаційної безпеки деякою мірою опирається на рекомендації і декларації також міжнародного характеру, зокрема на такі з них, як рекомендація Ради Європи «Про показ насильства електронними ЗМІ» [232] від 1997 р., Рекомендація Ради Європи державам-членам Ради, які зацікавлені в організації медіації у кримінальних справах [239] від 1999 р., Окінавська хартія глобального інформаційного суспільства [204] від 2000 р., Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» [388] від 2003 р., Декларація ОБСЄ «На шляху до спільноти безпеки» [419] від 2010 р. та чимало інших.

Тим не менше, треба відзначити, що декларованe в українському і міжнародному законодавстві та фактично реалізовуване у політичному житті суспільства часто не збігається. Тож навіть при прийнятті або ж перейнятті низки важливих нормативно-правових актів та документів у галузі інформаційної безпеки поки що в Україні надто зарано говорити про цілісну, зрозумілу й ефективну систему захисту інформації. Відповідно, суперечність інституційно й регламентаційно закріпленого та фактично впровадженого у цій проблематиці є доволі складною та багатогранною проблемою сучасної політичної науки, яка позначається на реальному розумінні тематики інформаційної безпеки в Україні та світі.

Загалом на підставі історіографічних пошуків можна констатувати, що категорія інформаційної безпеки у сучасному науковому і філософсько-

політологічному дискурсі, в тім числі українському, постала предметом окремішнього фокусу й зацікавленості. Але аргументувавши існування і функціонування в Україні досить розвинутого теоретичного дискурсу з проблеми інформаційної безпеки, треба зауважити, що мова все ж йде про досить комплексну та багатоскладову категорію, бачення якої іноді відрізняються від практики. А тому зважаючи на таку багатовимірність, системну складність й структурно-функціональну поліморфність, варто вирізняти різні підходи до розуміння сутності категорії інформаційна безпека й аналізувати їх більш поглиблено, про що йтиметься далі.

1.2. Ключові поняття, концептуальні та наукові підходи і правові означення як теоретико-методологічна основна дослідження інформаційної безпеки за політичної трансформації

Концептуально-теоретичну основу нашого дослідження з огляду на фундаментальні й історіографічні витоки та ключові детермінанти проблеми інформаційної безпеки складає триєдність факторів та цілей, що визначають сутність та структурно-функціональні характеристики такої безпеки. Ми виходимо з того, що інформаційна безпека в будь-якому структурно-функціональному вимірі телеологічно орієнтована на захист прав людини і громадянина, на забезпечення повноцінного національно-культурного розвитку певного соціуму та на всебічний захист державного суверенітету.

Людина, суспільство та держава традиційно складають три основні безпекові орієнтири. У сучасних наукових джерелах йдеться про відповідну «тріаду соціальних інститутів», що й визначають соціально-політичну сутність безпеки. Безпека людини, безпека суспільства, безпека держави, на думку дослідників, і є змістом безпеки національної, усвідомленим захистом інтересів, соціальних потреб названих суб’єктів, безпечним їх задоволенням [138, с. 11]. Ця наскрізна теза дає принципове розуміння проблем безпеки загалом, та інформаційної зокрема, її інституційного виміру.

Принагідно відмітимо, що сучасний політологічний словник не завжди передбачав та передбачає безпекову тематику. Однак дослідники політичного життя суспільства у різній мірі (прямо чи опосередковано) звертаються до проблеми актуальних суспільно-політичних загроз, викликів та необхідних політичних заходів у відповідь (чи на їх випередження). Наприклад, у оксфордській «Енциклопедії політичної думки» [див. 359] відсутні окремі статті з проблем безпеки, але в оглядах політичних вчень різного часу, в ключових категоріях політики часто відображається комплекс саме безпекових проблем: миру та війни, насильства, патерналізму, політичного популізму, (не)стабільності політичного розвитку, захищеної політичної системи, політичних обов'язків, забезпечення безпеки громадян через добробут, демократію тощо. Навіть поверхове вивчення статей вказує на те, що політичні мислителі минулого (Аристотель, Ф. Аквінський, Е. Берк, Н. Макіавеллі, Дж. Мілль, Ш. Монтеск'є, В. Оккам, Дж. Солсбері, А. Токвіль, Д. Юм та багато ін.), як і сучасні політичні концепції часто пов'язують проблеми політики з безпековими викликами.

Вже київське видання «Політична енциклопедія» (2011 р.) передбачило окрему статтю з безпеки міжнародної політики. Поняття тлумачать як «якісний показник стану … системи міжнародних відносин та світового порядку», а власне безпеку – як «політичну та військову стабільність», «ситуацію відсутності загроз існуванню індивідуальної чи колективної одиниці» (в разі коли подібні загрози все ж існують, безпека передбачає дію ефективного захисту від них). Інституційний аспект також знаходить політологічне трактування: міжнародну безпеку розглядають і як безпеку окремо взятого суб'єкта міжнародних відносин, і як безпеку груп таких суб'єктів зі спільними інтересами, і як безпеку всієї системи міжнародних відносин, загалом усієї спільноти [див. 360, с. 52-53]. Зауважимо, що у цьому академічному виданні, крім міжнародної, інші прояви та виміри безпеки спеціально не висвітлюються.

З розвитком політичної науки в Україні, а також зі зростанням числа загроз і викликів політичному розвитку українського суспільства проблематика безпеки

також увиразнювалась. Тож і нове покоління підручників, словників, збірників наукових праць з політології якісно і кількісно поповнилось безпековою тематикою. Зокрема вже львівське видання «Сучасна політична лексика» (2015 р.) пропонує до осмислення окремі статті з національної та міжнародної безпеки, безпеки людини, безпеки кордону, а також безпекової політики загалом. Прикметно, що проблематика осмислюється у статиці та динаміці, через інтереси нації, джерела її духовного та матеріального благополуччя, життєво важливі інтереси людини, суспільства, невразливості держави [див. 361, с. 23-25]. Відтак ще чіткіше розмежовується згадана нами на початку розділу тріада, у якій варто розглядати обране предметне поле дослідження.

У наш час постає необхідність цілісного осмислення проблем безпеки у політологічному ключі, зокрема різних її напрямків у зв'язку з проблемами демократії, політичного режиму, політичних структур та організацій, ідеологій та цінностей. Словниковий апарат політолога тут вочевидь буде збагачуватися. У XXI ст. особливо актуальним видається інформаційний вимір безпеки, потенціал політичної науки в осмисленні якого є незаперечним.

Поняття інформаційної безпеки ще недостатньо розвинуте у сучасній політологічній науці. Тут вочевидь варто слідувати за логікою тріадної структури. Частково її відображають дослідники *державного* управління. Так, як констатує З. Коваль, інформаційна безпека держави розуміється як «захищеність інформації та забезпечення цілісності й надійності критичної інформаційної інфраструктури держави від випадкових та навмисних впливів природного чи штучного характеру» [138, с. 11], а інформаційна ж безпека особи та суспільства – як «захищеність психіки і свідомості від небезпечних інформаційно-психологічних впливів: маніпулювання, дезінформації, спонукання до запланованих противником дій» [138, с. 11]. Подібні визначення однак потребують політологічного наповнення.

З огляду на це, однією з ключових цілей дисертаційного дослідження є концептуально-теоретичне вивчення можливостей протидії інформаційним загрозам, що так поширені в сучасному глобалізованому світі, на

індивідуальному, громадянському, соціальному та державному рівнях. Всі ці рівні взаємопов'язані, а отже значної актуальності набуває загальна проблема інформаційної безпеки, що інтегрує в собі різні аспекти суспільної життєдіяльності та державно-безпекового функціонування.

Більшість сучасних вчених, в тому числі О. Кісілевич-Чорнойван, зауважують, що «інформаційна безпека – це складова частина національної безпеки, яка, по-перше, відображає стан захищеності життєво-важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через неповність, несвоєчасність та недостовірність інформації або негативного інформаційного впливу через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації» [137, с. 13], і, по-друге, «стан захищеності інформаційного середовища/простору загалом, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави» [137, с. 13]. Поняття «інформаційна безпека» широко використовується в наукових публікаціях, навчальній і публіцистичній літературі, в нормативних документах різного рівня.

Однак в інтерпретаціях феномену немає однозначної єдності, що пов'язано ще й з прочитанням самого поняття різними мовами. Трапляються навіть деякі парадокси з розумінням терміну «інформаційна безпека». Справедливі ті вчені, що саме відсутністю центральної дефініції у сфері інформаційної безпеки, а також недоліками його законодавчого визначення пояснюють методологічну невизначеність ряду інших положень та термінів, що приводить до полісемії, знижує ефективність та прикладне значення наукових розробок в галузі інформаційної безпеки [див. напр. 205]. Нерідко окремі дослідники запозичують основний зміст визначення терміну з міжнародних стандартів, однак не враховують при цьому його багатозначність. Поняття «information security» може перекладатись з англійської і як «інформаційна безпека», і як «безпека інформації», що не є синонімічними. Тож *герменевтичний підхід* також не зайвий при виборі методології такого дослідження.

Проблематика інформаційної безпеки не тільки не втрачає, але й постійно

набирає нової актуальності через те, що вона є надзвичайно багатовимірною і складною. Це, насамперед, зумовлено тим, що з кожним днем в сучасному світі зростає масив і динаміка інформаційних потоків, постійно нарощується потужність інформаційних технологій, які можуть використовуватися, в тому числі, й для шкідливих впливів і справжньої агресії. Окрім науки державного управління, ми також звертаємося до напрацювань *соціальної філософії*, адже, як зауважує В. Триняк, «складну динамічну структуру інформаційної безпеки, а також системи інформаційних зв'язків визначає велика кількість інформаційних потоків» [262, с. 11]. *Міждисциплінарний підхід* до проблем безпеки розширює горизонти нашого розуміння та збагачує категоріальний апарат.

У значному масиві проблем, пов'язаних із різними аспектами феномену інформаційної безпеки, наше дослідження концентрується на зовнішніх і внутрішніх виявах державної, суспільної та індивідуальної інформаційної безпеки і захищеності. Ще до подій 2014 р. українські вчені наголошували, що інформаційна безпека складає зміст внутрішніх і зовнішніх аспектів безпеки національної, адже «покликана надійно захищати культурне надбання країни, інтелектуальну власність господарюючих суб'єктів і громадян, а також спеціальні відомості, що становлять державну і професійну таємницю» [227, с. 43]. Цілком логічним, послідовним та до певної міри завбачливим є висновок авторів про те, що суверенна, стабільна, демократична, правова держава відбувається лише через забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин. Досліджуючи та аналізуючи основні внутрішні та зовнішні фактори збудження інформаційної небезпеки в нашій країні, у дослідженні робиться концептуально-теоретична спроба визначення основних шляхів подолання шкідливих наслідків руйнівних інформаційних впливів, а також виокремлюється питання про необхідність побудови дієвої системи протидії та упередження таким шкідливим та небезпечним внутрішнім і зовнішнім інформаційним впливам і агресивним діям.

Особлива увага в нашому дослідженні приділяється проблематиці інформаційно-безпекової ситуації в сучасній системі міжнародних відносин. У

цьому аспекті особливо актуальним є те, що інформація сьогодні перетворилася на ключовий економічний, політичний, соціальний і навіть військовий інструмент міждержавної взаємодії. Знаково, що саме сучасні політологи, зокрема Я. Варивода підкреслює зв'язок інформації та влади: «Хоча інформація і комунікації завжди були важливими складовими державної зовнішньополітичної стратегії, у сучасному світі йдеться про виникнення якісно нової ситуації, коли «контроль за інформацією», «могутність» і «впливовість» нерозривно пов'язані між собою» [40, с. 3]. Дійсно, про який різновид зовнішньої політики не йшлося б – від культурної чи екологічної до економічної чи військової – чільне місце у ній відводиться управлінню інформаційними ресурсами та інформаційними потоками. У наш час це вже органічний елемент влади, невід'ємна складова стратегії, основа планування та реалізації політико-владних функцій. Особливу важливість і актуальність посилення ефективності інформаційної безпекової політики в міжнародних відносинах нашої держави підтверджують події останніх років, коли Україна піддалася значним агресивним впливам ззовні. Сьогодні Україні вкрай важливо виробити ефективну стратегію та нормативно-правове і ресурсне забезпечення розвитку системи інформаційної безпеки держави, яка б могла реально протистояти зовнішнім викликам, що з'являються на геополітичному фронті та в глобально-цивілізаційному і національно-культурному вимірах.

Водночас важливою детермінантною проблематики інформаційної безпеки є *феноменологічний, політико-філософський* вимір даного явища. Сьогодні актуально не лише розробляти засоби забезпечення інформаційної захищеності суспільства і держави, але й вивчати світоглядно-аксіологічні проблеми забезпечення такої захищеності. Важливо, щоб кожний громадянин, кожний професіонал, кожний чиновник постійно усвідомлювали власну відповідальність на лінії інформаційної захищеності власної держави і народу. Це вкотре актуалізує *загальнофілософський зміст та методологію* нашого дослідження, коли інформаційна безпека осмислюється у тісному взаємозв'язку з можливостями і проблемами інформаційного суспільства.

Останнє, між тим, потребує також відповідної політико-правової культури, адже погодимося, що йдеться не лише про «нарощування технологічних можливостей здійснення інформаційного обміну», але й про, як помічає О. Бойченко, «глибоке усвідомлення необхідності здійснення всіх заходів щодо інформаційних ресурсів та забезпечення інформаційної безпеки держави» [30, с. 51]. *Правовий зміст* проблеми полягає щонайменше в тому, аби чітко окреслити та розмежувати права й обов'язки усіх зацікавлених суб'єктів у цьому просторі: виробників інформаційних технологій, креаторів інформаційних засобів, постачальників інформаційних послуг, власників інформації, користувачів інформації, зрештою держави як визначального регулятора інформаційного ринку.

Комплексність проблематики інформаційної безпеки держави, суспільства, людини, дозволяє віднаходити проблеми, що відзначаються особливою актуальністю та потребують перманентного концептуально-теоретичного аналізу із врахуванням нових інформаційно-технологічних здобутків та динамічних тенденцій і змін на міжнародній арені і в глобальному просторі інформаційної цивілізації.

У нашому дослідженні витоків та основних детермінантів проблеми інформаційної безпеки основна увага приділяється формуванню збалансованої безпекової системи, яка б максимально повно враховувала б комплексність зазначеної проблематики. В сучасному безпековому дискурсі, зокрема *теоріях соціальної комунікації* особливо актуально та виразно постає проблема цілісного та системного забезпечення інформаційної безпеки на державному, соціальному та індивідуальному рівнях. У вітчизняних роботах підкреслюється необхідність «збереження збалансованості інтересів особистості, суспільства і держави» [281, с. 352]. Враховуючи це, проводиться концептуально-теоретичний аналіз специфіки та взаємопов'язаності інтересів особистості, громади, суспільства, держави і міжнародної спільноти у сфері інформаційної захищеності і безпеки.

Відрізнити три виміри безпеки допомагає розуміння спільних та взаємодоповнюючих інтересів. Структурує цю проблематику зокрема

Ю. Нестеряк: інтереси особистості в інформаційному просторі – це, передусім, і захист персональних даних, і доступність інформаційних ресурсів, що гарантується Конституцією; інтереси суспільства – це досягнення «суспільної згоди й духовного розвитку» за допомогою в тому числі і сучасних інформаційних технологій, «зміцнення демократії та правової держави»; інтереси держави – це розбудова «національної інформаційної інфраструктури», а відтак і збереження суверенітету, територіальної цілісності, зміцнення соціальної, політичної, економічної стабільності [202, с. 41]. Таким чином, визначивши основні витоки та детермінанти проблематики інформаційної безпеки, їх багатовимірний і комплексний характер, а також необхідності системного, міждисциплінарного підходу до дослідження проблематики інформаційної безпеки особистості, суспільства і держави, звернемося до детальнішого аналізу самого категорії «інформаційна безпека», її політологічного змісту в контексті актуальних викликів суспільно-політичного розвитку.

Насамперед, звернемо увагу на найзагальніші визначення поняття «інформаційна безпека». Серед них вирізняються власне стратегічні, коли під інформаційною безпекою розуміють, як засвідчує А. Баранов, «стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій» [18, с. 72]. Як бачимо, такі визначення *концентруються на проблематиці запобігання* тим шкідливим наслідкам, що можуть принести різноманітні інформаційні загрози, а також усунення і подолання цих наслідків з якомога меншою шкодою для суспільства і людини.

Часто українські автори пишуть, власне, про інформаційні небезпеки (а не стан убезпеченості), та пропонують відповідні визначення складної категорії. Відтак, система інформаційної безпеки відрізняється, на думку В. Абакумова,

передусім тим, що мусить, попередити «негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій», «спеціальні інформаційні операції, акти зовнішньої інформаційної агресії та негласного зняття інформації» [1, с. 8], «інформаційний тероризм і комп'ютерні злочини», нестабільний розвиток інформаційної інфраструктури, збої у функціонуванні національного інформаційного простору тощо [1, с. 8].

Існують також і *ширші тлумачення*, коли інформаційна безпека є не просто окремим сегментом національної, не лише інструментом попередження загроз, але невід'ємною наскрізною, інтегральною, якісною характеристикою сучасного суспільства загалом та національної безпеки зокрема. Це своєрідний показник захищеності громадян, суспільства, держави, глобального співтовариства загалом.

Широкі категорії у методиках і технологіях дослідження передусім передбачають дотримання концептуально-теоретичного *принципу системності.* Відколи системний аналіз завоював значимі позиції у політичній науці, розвиток політичних та й без пекових шкіл набув помітної динаміки. Тож у дослідженні різних аспектів інформаційної безпеки, коли йдеться про держави, суспільства, окремих людей та їхні групи й спільноти, жодна складова не може бути осмислена поза рамками системних взаємодій, в тому числі й зумовленості та взаємозалежності з іншими; жоден вузький підхід до безпеки не може бути визнаний абсолютним; а жоден політичний феномен не може бути розглянутий поза контекстом сучасного інформаційного суспільства. Інформаційна безпека має виражену інклюзивно-інтегративну функцію, її системне розуміння пов'язане з глобалізаційними тенденціями, диджіталізацію політики, ситуативністю сучасних політичних відносин і процесів тощо. До того ж, це надважливе поняття у різних науках та різних сферах діяльності людей, що потребує комплексності й системності.

З цього приводу зауважимо, що чимало українських авторів, зокрема В. Ліпкан, схиляються до такого *інтегрального підходу*, «за якого інформаційна безпека визначатиметься за допомогою окреслення найбільш важливих її

сутнісних ознак з урахуванням постійної динаміки інформаційних систем і становлення не лише інформаційного суспільства а й інформаційної цивілізації» [168, с. 35].

У цьому зв'язку ми не могли оминути й російської теорії та практики забезпечення національної безпеки та різних вимірів. У РФ домінує саме таке широке розуміння проблеми, а інформаційна безпека у XXI ст. керівництвом країни визначена ключовим напрямком розвитку державної безпекової стратегії. Російські вчені переконують, що в інформаційній сфері існують серйозні внутрішні та зовнішні загрози, тож коли йдеться про безпеку, слід подбати і про збалансовану захищеність національних інтересів країни, життєво важливих інтересів особи, суспільства, держави в інформаційному полі [173, с. 79]. Загалом визнаємо, що агресивність, протиправність, конфронтаційність інформаційної політики РФ підкріплена як адміністративно-управлінським ресурсом, так і помітною увагою (псевдо)наукової спільноти. Це приносить свої політичні результати та владні ефекти країні, а також призводить до численних втрат демократичної спільноти.

Відтак активізація та актуалізація, постійна підтримка динаміки потужного науково-теоретичного дискурсу, який би інтегрував сучасне знання про інформаційну безпеку, розвивав його, сприяв новим структурно-функціональним дослідженням, їх практичному використанню – усе це особливо важливе завдання для всього цивілізованого світу, зокрема й України. Багатовимірна проблематика, до того ж, мусить бути максимально коректно, результативно «вписана» у загальні контексти повноцінного забезпечення національної, державної, міжнародної безпеки, коли інформаційна безпека мислиться невіддільно від освітніх, культурних, соціальних, економічних, політико-владних та інших відносин і процесів, політичних інституцій та позасистемних структур політики.

Насамперед важливо продовжувати вивчати існуючі напрацювання, розвивати та розширювати теоретико-методологічні засади дослідження проблеми інформаційної безпеки, загальноукраїнські, регіональні та міжнародні

її виміри. Існуючі загрози зобов'язують також орієнтуватися на всебічне забезпечення національних інтересів, яке потребує аналітичного матеріалу, експертної підтримки, наукових обґрунтувань. Розвинута методологія дослідження відтак мусила б органічно внести свої корективи у концептуально-теоретичні основи розуміння проблематики: збагатити словниковий апарат, категоріальну базу, комплексні політико-філософський та інформаційно-технологічний виміри обґрунтування безпеки.

У наших статтях [див. напр. 362] ми неодноразово наголошували на цій комплексності, у методологічному плані – поєднанні загальнофілософських, загальнонаукових та власне політологічних підходів і методів. Адже, наприклад, *філософсько-аксіологічний аналіз* категорії «інформаційна безпека» суттєво розширює наше розуміння політичних цінностей сучасного світу загалом. Сучасне вчення про філософсько-феноменологічні та соціально-психологічні детермінанти інформаційної безпеки людини і суспільства. Тут важливий індивідуальний вимір, на який слушно звертає увагу В. Богуш, що констатує, що «інформаційна безпека особистості – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо» [25, с. 41]. Лише через цей вимір – особистісний, психологічний – можливо далі розвивати систему безпеки громадянського суспільства, держави, нації. Цінність людського наповнення та значимості індивідуальної свободи тут визначальні, вони неминуче формують сучасні основи й відповідного політико-філософського дискурсу.

Це суттєве доповнення до сучасної аксіології політики, політичної науки у системі поведінкових дисциплін. Теоретичні праці, які розглядають основи інформаційної безпеки, навіть в межах окремих держав, локальних спільнот і навіть технологічних обставин певних суспільно-політичних проблем, увиразнюють наше розуміння принципів політичного життя і організації соціуму, глобальності інформаційного середовища, його системності, багатогранності, всеохопності, орієнтирів. Глобальний характер проблеми

інформаційної безпеки, поряд з глибоко інтуїтивним, ціннісно-психологічним відтак складає значимий інтерес у нашому дослідженні.

Звичайно, в рамках цієї роботи особлива увага приділяється також теоретико-методологічним принципам дослідження *структурно-функціональних* властивостей феномену інформаційної безпеки. Розуміння ключових інститутів, які функціонують у системі інформаційної безпеки, поза інституційних, стихійних та організованих структур, що зацікавлені у відповідній політиці, а також рольових місій кожного з них у фокусі уваги багатьох науковців. Ця дослідницька робота не може бути зроблена «раз і назавжди», адже сфера активно розвивається та поповнюється новими досвідами, практиками, моделями поведінки. Динаміку і статику вивчають через ключові потреби суб'єктів інформаційної політики, а також цілі, переконання та інтереси об'єктів інформаційного суспільства.

Структурно-функціональний аналіз для обраного предмету дослідження означає також розуміння того, що власне інформація, якою користуються різні суб'єкти і об'єкти політики, має бути повною та достовірною для прийняття ефективних і суспільно безпечних рішень. Ми погоджуємося з вченими, які відтак у межах інформаційної безпеки називають щонайменше три елементами: 1) забезпечення функціонування ефективних засобів інформаційної діяльності; 2) забезпечення можливості суб'єктів отримувати доступ до необхідних інформаційних ресурсів; 3) формування інформаційного ресурсу, що відповідає потребам суб'єктів [130, с. с. 271]. Загалом усі – від міжнародних організацій до кожного конкретного лідера громадської думки, від національної спільноти до територіальної громади, від держави до громадянина – кожен суб'єкт політики нині потребує інформаційної безпеки, а отже чіткіших теоретико-методологічних підстав для структурно-функціональної аналітики.

Абсолютизація чітко окреслених критеріїв політичних рішень та форм політики однак не дає повного розуміння категорій розвитку, змін, перетворень у суспільно-політичному житті. Тому поняття інформаційної безпеки доречно також осмислювати у контексті *теорії демократизації, транзитологічних*

моделей, розбудови *демократичної держави, розвитку громадянського суспільства*. У цьому баченні обрана проблема дослідження особливо актуальна для українського суспільства, де процеси зміцнення/забезпечення/оновлення національної інформаційної безпеки відбуваються паралельно з демократизаційними, де модернізація політичних інститутів означає також цілковиту відмову від частини з них та / або ж розбудову абсолютно нових. Тому інститути інформаційної безпеки в сучасних українських умовах часто постають також прискорювачами демократичних реформ, охорони державотворчих процесів, елементом прозорості правової держави, захисту й сприяння громадянському суспільству, платформою зрощування громадянської освіти і культури демократичної участі. Через таку парадигму політичної модернізації, на нашу думку, сьогодні важливо розвивати наше розуміння ролі інформаційної безпеки, теоретико-методологічних засад її дослідження в Україні.

Окремо нам йдеться про такі інтерпретації інформаційної безпеки, коли підкреслюється її *політико-правовий зміст*, тобто розглядаються системотворчі принципи нормального, безпечного, захищеного, та законодавчо окресленого функціонування соціуму як частини глобального інформаційного суспільства [див. 362]. У цьому ключі увагу привертають юридичні визначення, в тому числі ті, які стосуються конкретно української суспільно-політичної та правової реальності. Так, як зазначає В. Гурковський, «національна інформаційна безпека України – це суспільні відносини, пов’язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів» [63, с. 35]. Слушно визначає «комплекс питань інформаційної безпеки людини та суспільства» Б. Кормич, що під ним розуміє «забезпечення інформаційних прав і свобод людини і громадянина»; «захист людини від

неправомірного інформаційного втручання»; «забезпечення національної, культурної і духовної ідентичності від неправомірного втручання»; «забезпечення дієздатних правових та організаційних механізмів захисту відповідних прав тощо» [149, с. 17-18]. Не менш важливі, продовжує цей дослідник, і правові тлумачення питань інформаційної безпеки держави, яка позиціонується як «безпека розвитку інформаційної сфери держави»; «захист національного інформаційного ринку»; «забезпечення міжнародної інформаційної безпеки, зокрема, попередження: інформаційного тероризму, використання інформаційної зброї, інформаційної війни»; «захист та обмеження обігу інформації в цілях безпеки; захист інформаційної інфраструктури держави тощо» [149, с. 17-18].

Політико-правові підходи цінні також тим, що орієнтують на вивчення існуючої та потенційно можливої нормативно-правової бази для повноцінного функціонування сучасного інформаційного суспільства. Тут особливо важлива конкретика – досвід окремо взятих держав, правил, ситуацій, прецедентів тощо. У наших публікаціях [див. напр. 362; 363] детальніше аналізуються нормативно-правові документи в цій галузі в Україні, акцентується на їх фрагментарності, ситуативності, певній безсистемності. Подібні висновки робили й інші дослідники (В. Гурковський, Б. Кормич, Т. Субіна та ін.).

Серед базових документів зі створення та функціонування системи забезпечення інформаційної безпеки в Україні – Закон України «Про Національну програму інформатизації» від 04.02.1998 р. № 74/98, який прикметно зазнав змін у 2001, 2010, 2012, 2015 та 2020 рр. (очевидна залежність від виборчих циклів). Закон суттєво утвердив наше розуміння окремих політологічних категорій. До прикладу, серед основних понять визначено «інформаційний суверенітет держави», тобто, як окреслено в акті, її здатність «контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави» [102]. Документом передбачається формування правової бази інформатизації; розробка національних стандартів у цій галузі; формування

механізмів щодо здійснення практичних заходів забезпечення інформаційної безпеки [102]. Документ став етапним в налагодженні діалогу між державними управлінцями, громадськими активістами, науковцями, міжнародними експертами щодо назрілих проблем забезпечення інформаційної безпеки українського суспільства.

Окремі положення «Національної програми інформатизації» відображені та розвинуті пізніше Законом України «Про основні засади розвитку інформаційного суспільства в Україні 2007 – 2015 років» від 09.01.2007 р. № 537. Деякі проблеми, згадані у цьому документі, звучать досі актуально: «недоліки координації зусиль державного і приватного секторів економіки у розбудові інформаційного суспільства» [106]; «неефективне використання фінансових, матеріальних, кадрових ресурсів, спрямованих на інформатизацію, впровадження ІКТ у соціально-економічну сферу» [106]; поглиблення «інформаційної нерівності», відставання інформатизації окремих регіонів, галузей економіки, верств населення, технологій електронного бізнесу; недостатній розвиток відповідної інфраструктури та нормативно-правової бази; повільний розвиток комп'ютерної та інформаційної грамотності населення; брак інформаційної представленості України в інтернет-просторі, присутності україномовних ресурсів; захист авторських прав тощо [106]. Дійсно, погоджуємося з правознавцями, що документ формує цілісне уявлення про систему інформаційної безпеки, особливості її розвитку, зокрема наукової бази та передбачає удосконалення діяльності державних органів шляхом широкого застосування інформаційно-комунікаційних технологій [255, с. 3]. Зважаючи на гостру потребу формування нових принципів інформаційно-безпекової політики нашої держави, ми особливу увагу тут та у наших публікаціях приділяємо проблематиці інформаційної безпеки в системі інформаційної політики України. Увиразнює відповідний комплекс питань компаративний аналіз такої політики в нашій державі та у інших країнах світу.

Підкреслимо, що в умовах функціонування глобального інформаційного суспільства політичні ресурси, поряд з правовими механізмами захисту

інформаційної життя громадян та інформаційної безпеки держави є однаково актуальною проблемою, їх розуміння та взаємообумовленість формують новий порядок денний політичної теорії і практики. При чому треба погодитися з багаторічними застереженнями вчених щодо розбудови ефективної та дієвої, тристоронньої моделі системного забезпечення інформаційної безпеки – держави, суспільства, людини – про що йдеться й у конституційних нормах, і у теоретичних напрацюваннях, і у доповідях і звітах відповідальних органів влади:. Так, як констатує О. Косогов, «інформаційна безпека, захист якої відповідно до ст. 17 Конституції України, поряд із суверенітетом, територіальною цілісністю та економічною безпекою, є найважливішою функцією держави, досягається шляхом розробки сучасного законодавства, впровадження сучасних безпечних інформаційних технологій, побудовою функціонально повної національної інфраструктури, формуванням і розвитком інформаційних відносин тощо» [153, с. 163]. Отже, в Україні на конституційному рівні стверджується необхідність захисту інформаційної сфери держави та забезпечення інформаційної безпеки громадян.

Однак декларoване та фактично реалізоване у політичному житті суспільства часто не збігається, тож навіть при прийнятті низки важливих нормативних документів у цій галузі поки в Україні ще зарано говорити про цілісну, зрозумілу та ефективну систему захисту інформації. Суперечність інституційно закріпленого та фактично впровадженого є складною та багатогранною проблемою сучасної політичної науки, яку можемо простежити на прикладі інформаційної безпеки.

Зокрема розглянемо ситуацію зі законодавчо затвердженою декларацією – «Національною програмою інформатизації» – важливим орієнтиром розвитку системи інформаційної безпеки, що був визначений ще 1998 року. У документі йдеться про широкий набір проблем: від загального розуміння інформаційної безпеки як «невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки» [102], з означенням її ключових об'єктів («інформаційні ресурси, канали інформаційного обміну, телекомунікації,

механізми забезпечення функціонування телекомунікаційних систем і мереж, інші елементи інформаційної інфраструктури» [102]), до результатів Програми – «пакету нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації і профілактики вірусів, нові технології захисту інформації з використанням спектральних методів, високо надійні криптографічні методи захисту інформації» [102].

Відтак пошуки оптимальних механізмів забезпечення інформаційної безпеки для нашого суспільства не нові, вони відображені на законодавчому рівні в Україні, в офіційно проголошених доктринах і затверджених програмах. Це не спекулятивні політичні обіцянки чи маніпулятивні передвиборчі гасла, але цілком аргументовані та зважені позиції законотворця. Водночас прийняті норми поки не забезпечують послідовного і системного підходу в житті динамічного інформаційного суспільства, при чому ця тенденція має загальносвітовий характер, адже часто йдеться про абсолютно нові виклики. З іншого боку, реальні ресурси й можливості кожного конкретного суспільства відрізняються, й українське у цьому аспекті потребує повноцінної бази для реалізації проголошених норм і правил.

Водночас ідеалізувати законодавчі зусилля з унормування сфери інформаційної безпеки також не варто, адже незважаючи на тривалі дискусії, експертні рекомендації та наукові обґрунтування окремі норми і навіть базові поняття все ще не прописані належним чином, навіть за умови прийняття нових законів. Тривалий час у своїх публікаціях ми наголошували, що відчутним недоліком законодавства України щодо політичного забезпечення інформаційної безпеки є те, що все ще не виписана змістовна компонента, системотворча сутність власне інформаційної безпеки у контексті національної безпеки. У цьому зв’язку ми спостерігали лише загальні формулювання, що ускладнювало не тільки розуміння сутності, але й можливості реалізації ефективної

інформаційно-безпекової політики держави, тобто власне інтегративного елементу безпеки національної.

У Законі України «Про основи національної безпеки України» від 2003 р. не було запропоновано навіть елементарного визначення терміну «інформаційна безпека». Щоправда поняття згадується у контексті національної безпеки загалом, яка трактується у законі як «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, охорони дитинства, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та *інформаційної безпеки*, кібербезпеки та кіберзахисту, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, *захисту інформації,* ліцензування, промисловості та сільського господарства, транспорту та зв'язку, *інформаційних технологій*, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам» (ст. 1, виділено автором) [105].

Це широке розуміння подаємо у цьому розділі свідомо, що дозволить відстежити подальші зміни в категоріальному апараті сучасного дослідника інформаційних викликів та загроз у політичному житті суспільства. Власне у контексті загроз у законі й згадуються інформаційні, але це і вносить певні *суперечності*. Погоджуємося з численними дослідниками, зокрема з ідеєю, яку

висловлює В. Ліпкан, про те, що «перелік загроз, визначений законодавцем в цьому законі, дає можливість стверджувати про розуміння інформаційної безпеки, не як безпеки інформації в технічному аспекті, а більш широку категорію, що дещо суперечить розумінню інформаційної безпеки у Законі України «Про Концепцію Національної програми інформатизації»» [168, с. 27]. Сьогодні Закон втратив чинність, однак наявні суперечності у ключових визначеннях і категоріях в достатній мірі збереглися.

У 2018 р. у Законі України «Про національну безпеку України» знаходимо дещо коротше (порівняно з попереднім) трактування національної безпеки, зокрема як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» (ст. 1) [385; 386] – у якому водночас помічаємо певну відмову від конкретизації напрямів та, зокрема, й від інформаційного чинника [386]. У документі знову-таки не йдеться про операціоналізацію поняття «інформаційна безпека», водночас проблематика згадується у контексті напрямів державної політики у безпековій сфері, оскільки констатовано, що «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, *інформаційної,* екологічної безпеки, кібербезпеки України тощо» (ст. 3, виділено автором) [385; 386].

Отже, досі, навіть з оновленням нормативно-правових основ національної безпеки України, ключові поняття все ще залишають більше питань, аніж відповідей, потребують конкретизації та подальших наукових напрацювань. Визначальні суперечності тут вочевидь мають політичний зміст, тож існуючі документи лише певним чином відображають загальну динаміку потреб, інтересів, конфліктів у безпековій політиці держави в інформаційній сфері.

Зусилля науковців тут зосередженні не лише на обґрунтуванні, але й методичному повторенні доведених міжнародною практикою та аргументованими позиціями тез. Серед таких – теза про необхідність напрацювання цілісного кодифікаційного документу, що, на нашу думку,

«повноцінно охопив би різні аспекти формування державної політики в сфері національної безпеки, а також визначив би конкретний інструментарій забезпечення такої політики» [364, с. 113]. Ми неодноразово повторюємо [див. напр. 385], що відповідний документ мала би відрізняти 1) послідовність і системність; 2) прагматичність; 3) термінологічна чіткість; 4) орієнтованість на стратегічні пріоритети та принципи діяльності держави в інформаційно-безпековій сфері.

Досі важливо провадити усесторонню й узгоджену діяльність вчених, аналітиків, правознавців, державних діячів, політиків, стейкхолдерів з формування цілісного уявлення про інформаційну безпеку країни, в тому числі і як глобального гравця; з наукової позиції комплексно усвідомлювати пріоритети розвитку інформаційного суспільства; чітко розмежовувати ознаки та типи інформаційних комунікацій, зокрема їх вплив на політичні відносини; методологічно підходити до структурування інституційної системи інформаційної безпеки, зважаючи на динаміку сучасного політичного життя суспільства та специфічні геополітичні умови. Мають рацію дослідники, які інформаційно-аналітичне забезпечення державного управління чітко корелюють з процесом прийняття «виважених політико-управлінських рішень» на центральному і регіональному рівнях, а ігнорування такої залежності розцінюють як прямий шлях до конфліктів владних органів, комерційних структур, громад, до загальної непрогнозованості розвитку, що, як вважає Л. Євдоченко, «ускладнює планування (середньо і довгострокове) заходів національної безпеки, адекватних реаліям державного становлення та розвитку» [84, с. 13]. Ці та подібні тези обґрунтовувалися науковцями України у 1990-х рр., на початку 2000-х рр. та вочевидь знаходять свій відгук і в сучасних політологічних дослідженнях.

Реалізація стратегічних завдань зі забезпечення інформаційної безпеки та розвитку інформаційного суспільства потребує і концептуально-теоретичних, і законотворчих зусиль. При цьому черговим етапним документом для впорядкування політико-правового поля та, певною мірою, понятійного

простору інформаційно-безпекового життя України послугувала «Доктрина інформаційної безпеки України» 2017 р. [387]. Тут все ще немає визначення ключової категорії – інформаційної безпеки. Водночас з огляду на перелік основних «пріоритетів державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки» [265] можна виокремити ті складові, які законотворець вкладає у зміст цього складного феномену. Отже, йдеться про інтегровану систему оцінки інформаційних загроз та оперативного реагування на них; чітку систему повноважень відповідальних державних регуляторних органів; «прозорі механізми виявлення, фіксації, блокування та видалення з інформаційного простору держави інформації» [265], яка загрожує життю, здоров'ю громадян, пропагує війну, національну та релігійну ворожнечу, порушення територіальної цілісності тощо; зрозумілі механізми «регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації» [387]; роз'яснювальна робота серед військ та населення; повне покриття території України цифровим мовленням; дієва й ефективна система стратегічних комунікацій тощо [387]. Документ містить ще багато важливих для нашого дослідження положень, але у теоретико-методологічному розділі звертаємо увагу передусім на визначення.

Отже, у Доктрині поряд з категорією «інформаційна безпека» вживається також «інформаційно-психологічна безпека», а центральне місце зайняли поняття стратегічних, урядових і кризових комунікацій, а також стратегічного наративу як «спеціально підготовленого тексту, призначеного для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію» [265; 387]. Детальніший політологічний аналіз дозволяє стверджувати, що цей документ відрізняє саме таке розуміння інформаційної безпеки – не лише як інформаційної захищеності, декларованої раніше, але і як інформаційної впливовості, утвердження відповідальності, посилення спроможностей та комунікаційних можливостей сектору безпеки. Та Реальна

імплементація цього документу потребує особливої уваги та спільних зусиль усіх зацікавлених та відповідальних сторін, адже значний потенціал Доктрини закладає вже більш зрозумілі пріоритети і перспективи інформаційного суспільства майбутнього.

Зауважимо, що документ має історичних попередників. Зокрема «Доктрина інформаційної безпеки України», затверджена Указом Президента України від 8 липня 2009 р., у якій властиво центральна категорія – «інформаційна безпека» – визнана невід'ємною складовою кожної зі сфер національної безпеки, а також водночас «важливою самостійною сферою забезпечення національної безпеки» [79]. Тут також знаходимо багато інших точних формулювань, зокрема і чітке структурування важливих інтересів в інформаційній сфері. Тоді вчені й аналітики схвалювали й вітали такий документ, зокрема у контексті визначеності щодо правил гри у сфері інформаційної безпеки. Приміром, І. Малик звернув увагу, що «доктрина чітко визначила та окреслила основні засади інформаційної безпеки України, встановила місце інформаційної безпеки в системі забезпечення національної безпеки України, виокремила реальні та потенційні загрози інформаційній безпеці України, сформувала напрями державної політики у сфері інформаційної безпеки держави» [178, с. 81]. Проте в умовах відомої тогочасної політичної кон'юнктури реалізація відповідних положень затягувалась. У цьому вбачаємо ілюстративний приклад того, як політична воля та загалом позаінституційний чинник політики визначає реальний зміст та динаміку політичних явищ і процесів у окресленій сфері нашого дослідження, незважаючи на правові норми.

Загалом у поняттях і визначеннях не варто обмежуватися виключно національним законодавством, цього вочевидь недостатньо для комплексного розуміння проблематики, в тому числі і її теоретичного потенціалу, і практичного ефекту. Зокрема нашу увагу також привертають міжнародні практики і досвід провідних країн світу, які здійснюють ефективний інформаційний захист своїх держав, спільнот, громадян.

Зокрема у міжнародній Декларації принципів «Побудова інформаційного

суспільства – глобальне завдання у новому тисячолітті» [388] поняття інформаційної безпеки вперше згадується та визначається у контексті 11 ключових принципів інформаційного суспільства, коли йдеться про необхідність зміцнення довіри, також через безпеку мереж, аутентифікацію, захист і недоторканність приватного життя і прав споживачів. Тут також широко оперують поняттям «глобальна культура кібербезпеки». Загалом проблематика передбачає широке співробітництво з усіма зацікавленими сторонами, міжнародну співпрацю щодо захисту даних, боротьби зі спамом, врахування рівня соціально-економічного розвитку кожної країни, загального і недискримінаційного доступу до інформаційно-комунікаційних технологій, запобігання їх використання з метою нестабільності, в злочинних і терористичних цілях, тощо [388]. Отже, бачимо досить широкий як на початок тисячоліття спектр проблематики, який втім вже у наш час мусить деталізуватися.

З цією метою звернемося до досвіду провідних у галузі інформаційної безпеки країн, що задають темпи і динаміку відповідним змінам навіть на рівні розуміння та осмислення проблематики. Погоджуємося з українським дослідником О. Левченком, який вважає, що «розвинуті системи інформаційної безпеки функціонують у США, Великій Британії, Ізраїлі, ФРН, Російській Федерації, Китаї, тобто у тих країнах, які постійно знаходяться під потужним зовнішнім інформаційним впливом» [164, с. 168]. Такі національні системи інформаційної безпеки доводять ефективність на практиці, характеризуються *структурно-функціональним підходом*, також важливим і для нашого дослідження. Адже чітке розмежування важливих компонентів інформаційної безпеки, узгодження їх ролей та осмислення у комплексному взаємозв’язку дають повнішу картину розуміння політологічних явищ і процесів. Закордонний досвід найуспішніших у цьому аспекті країн, безумовно, з урахуванням національної специфіки, дозволяє системніше підійти до поняття політичних інститутів у структурі національної, зокрема й інформаційної безпеки у їх трансформації, модернізації, активному розвитку. Водночас напрацьовані у світі

за тривалий час механізми й моделі формування та функціонування дієвого інформаційного захисту національної безпеки й оборони потребують і геополітичного мислення, коли розвиток національної системи понять та положень мусить узгоджуватися зі світовими тенденціями та глобальними проблемами.

Власне глобальні тенденції можна простежити на прикладі великого геополітичного гравця – Сполучених Штатів Америки, де діє багатовимірна, функціонально складна та ефективна система інформаційної безпеки. Це ще й достатньо деталізована система, що поєднує стратегічні цілі та завдання федерального та місцевого рівнів. Логічно проблема заслуговує окремого дослідження, тож невипадково і в Україні з'явилися дисертації, що зосередженні виключно на цій тематиці [див. напр. 143]. Комплексний підхід до проблематики інформаційної безпеки в США передбачає охоплення широко спектру загальнонаціональних і специфічних, адміністративно-організаційних питань: свободи інформації, висвітлення діяльності влади до комп'ютерної безпеки, охорони особистих таємниць та ін. При цьому, як слушно зауважують дослідники, саме Президент США є головною відповідальною особою за забезпечення інформаційної безпеки та національної безпеки загалом [143, с. 9-10]. Законодавче унормування відповідних питань тут достатньо конкретизоване, як і визначеність у ключових поняттях. Цей досвід особливо цінний для українських законотворців, що водночас не можуть розраховувати на принаймні схожий за своїми масштабами матеріально-технологічний потенціал США у забезпеченні інформаційної безпеки. Однак саме універсальні, напрацьовані тут та ефективні на практиці методики означення та ідентифікації соціально-політичних проблем, що виникають у сфері національної безпеки, цілком можуть слугувати прикладом для наслідування.

Європейський досвід виявлення та боротьби з інформаційними загрозами також викликають широкий дослідницький інтерес. Окремо ми писали про це у статтях, присвячених проблемам всебічного забезпечення в рамках національної політики, економіки, культури інформаційного захисту в сучасному глобальному

суспільстві [368]. При цьому зауважуємо, що у більшості західних демократій поряд з економікою, політикою, культурою, енергетикою, транспортом, фінансами саме інформаційний сектор безпеки визнається визначальним для цивілізованого функціонування держави і суспільства. Зокрема, у Франції захист інформаційного середовища визнано одним із ключових напрямів забезпечення національної безпеки, аж до тієї міри, що дослідники, зокрема Б. Остроухой, Б. Петрик, М. Присяжнюк, вбачають у цьому «новий елемент у понятті сучасної багатовекторності геостратегії французької правлячої еліти, що безпосередньо впливає на особливості вибору способів використання оперативних можливостей національних спецслужб, ЗМІ та інших державних і неурядових структур, залучених до реалізації політики інформаційної безпеки французького суспільства і держави» [121, с. 343-344]. Тут велика увага приділяється такому поняттю як «національний інформаційний простір», що трактується центральним у стратегічній і тактичній системі безпеки, коли і її організаційна структура, і базові механізми реалізації, і навіть ситуативні розвідувальні чи підривні заходи спецслужб залежать та коригуються відповідно до основоположних засад національного інформаційного простору. Водночас важливі смисли цьому феномену задає громадянське суспільство, від якого залежить демократичність інформаційного простору. Відтак у Франції розроблено низку механізмів взаємодії (не)державних структур, які постійно проводять моніторингові заходи у цій галузі, чим увиразнюють сучасний зміст інформаційної безпеки вільних країн.

Загалом сучасні європейські трактування, норми та практики з інформаційної безпеки розглядають інформаційне поле серед пріоритетних об’єктів спеціального захисту, що здійснюється законотворчими, організаційно-управлінськими, силовими, інформаційно-технологічними засобами, але також передбачає громадський контроль, свободу слова та загалом дотримання демократичних прав і зобов’язань з боку усіх зацікавлених сторін.

Інший погляд на проблематику і в методологічному, і в прикладному аспектах спостерігаємо на прикладі системи інформаційної безпеки Китайської

Народної Республіки. Головні її відмінності можна сформулювати у таких поняттях як моноцентризм, наступальність й оборонність. Власне ця тема також не нова для політологічної спільноти та вже має низку самостійних напрацювань в Україні [див. напр. 275]. Саме інформаційна складова у багатьох відношеннях дозволяє цій державі вибудовувати стратегію регіонального і навіть міжнародного лідерства, адже осучаснює авторитарний режим, модернізує комуністичну ідеологію, розширює межі цільової аудиторії до молодіжної. Погодимося з тим, як вказує Хуан Цинь, що практично у КНР всі елементи «державної інформаційної політики зумовлені потребою забезпечення національних інтересів шляхом реалізації китайської моделі інформаційного суспільства та специфіки інтеграції КНР у глобальне інформаційне середовище» [275, с. 8-9]. Це також ілюстративний приклад трактування поняття «інформація» як збройного ресурсу, що майже у всіх випадках має як внутрішню, так зовнішню ціль. Безпека відтак розуміється не лише як активний захист, але і ефективна протидія зовнішнім інформаційним впливам, при цьому безпекові орієнтири та впливи охоплюють соціально-культурні, економічні, технологічно-інноваційні інтереси, розповсюджуються на локальні, загальнонаціональні, регіональні і міжнародні горизонти дії. Владні потужності КНР поступово та впевнено нарощують інформаційну впливовість у світі, що, з одного боку, ретранслює авторитарні цінності, з іншого – задає нові конкурентні виклики цього аспекту суспільно-політичного життя.

Отже, сучасні системи інформаційної безпеки, що налагоджені в світі, досить різні та вносять певну ясність у розуміння ключових категорій нашого дослідження. Пов’язано це і з традиціями встановлених політико-владних відносин, і з особливостями державно-адміністративного управління, і з політико-ідеологічними установками, що склалися у тому чи іншому соціумі. При цьому для розуміння інформаційної безпеки важлива і загальна суспільна згода, і консолідованість державних зусиль, і систематизованість нормативно-правової бази, і постійне нарощування матеріально-технологічних потужностей.

Аналізуючи досвід країн-лідерів у сфері інформаційної безпеки, слід також

зважати і на специфічні українські реалії, застереження, які природно передбачалися українськими дослідниками та гостро актуальні. Приміром, З. Коваль серед них виокремлює такі наступні, як: «відсутність організаційної системи розроблення й реалізації єдиної державної політики в галузі забезпечення інформаційно-психологічної безпеки; нерозуміння інформаційно-психологічної боротьби як механізму протидії експансії та агресії стосовно країни в будь-якій формі її прояву та забезпечення власних національних інтересів; недостатня розвиненість науково-методичної бази забезпечення інформаційно-психологічної безпеки, стратегії й тактики ведення інформаційно-психологічної боротьби; відсутність підготовки фахівців з комплексним баченням проблем інформаційно-психологічної безпеки країни, а також організації та ведення інформаційно-психологічної боротьби» [138, с. 11]. Тобто окрім загальних орієнтирів у теоретичних визначеннях, слід також пам’ятати і про важливий методологічний принцип політології – *соціальний детермінізм*. Адже умови і можливості для розбудови системи інформаційної безпеки нашої держави принципово відрізняються від тих, що успішно відбулися. Численні масовані зовнішні інформаційно-психологічні атаки вимагають комплексного бачення національних інтересів та цілісного розуміння системи їх забезпечення. Кризові суспільно-політичні явища та зовнішні впливи потребують системних теоретико-методологічних пошуків, широких діалогів політологів, соціологів, філософів, правознавців та інших науковців, аналітиків, стратегів, лідерів громадської думки тощо. При чому ця сфера не витримує відтермінувань чи несвідомих зволікань, адже відповідні потреби суспільства у ній лише зростають у динаміці сучасного глобалізованого світу.

Ми акцентуємо [див. 389], що особливої актуальності цій теоретико-прикладній проблемі додає також те, що перед українською державою і громадянським суспільством постійно наростають нові виклики. Вони мають щонайменше два виразні джерела походження: вже згадувану тут динамічну глобальну ситуацію, що змінюється у контексті бурхливого розвитку інформаційної цивілізації, а також агресивну політику РФ, яка також має суттєві

регіональні засоби інформаційного впливу. Відтак комплекс цих чинників і умов зобов'язує формувати таку візію інформаційної безпеки, що більше ситуативна, тобто не тільки стратегічно вибудована, але й сформована у відповідь на постійно зростаючі виклики та нові реакції. Авторитетні українські політологи, зокрема Л. Смола, слушно стверджують, що «інтереси України вимагають формування системи, що дозволить їй адекватно реагувати на негативні зовнішні та внутрішні впливи, зберігати цілісність суспільства та держави» [250, с. 3].

Чимало аналітиків тут сходяться на думці, що розвиток подібної системи передбачає: потужну аналітичну підготовку (що дозволить чітко визначитись із пріоритетами та орієнтирами інформаційної безпеки); постійні концептуально-теоретичні пошуки (визначення основних засад інформаційно-безпекової політики, системні дослідження питання, консолідація зусиль кращих дослідників у цій царині, налагодження академічних мережевих зв'язків тощо); підбір адекватних засобів інформаційного захисту (тобто достатньо ефективних у конкретний період часу, а також ресурсного та технологічно оптимальних, зокрема за структурою витрат).

Окремим, хоча й логічним продовженням відповідної роботи є напрацювання нормативно-правового підґрунтя в галузі інформаційної безпеки, де ключові концепти, теоретичні ідеї та підходи знаходять чітке юридичне визначення. Нами вже зазначалося, що питання систематизованого національного законодавства, яке б регулювало діяльність політичних суб'єктів (учасників та активних творців інформаційного суспільства), ані у нашій країні, ані у європейських суспільствах не нове. Однак тут пригадаємо ще деякі теоретичні дискусії, які вже багато років зберігають свою актуальність та не знаходять практичного вирішення.

До таких, наприклад, належить питання кодифікації інформаційного законодавства. Українські дослідники вже тривалий час наголошують, що прийняття інформаційного кодексу для нашої країни може суттєво змінити принципи функціонування політичної системи, внести корективи у важливі напрямки розвитку громадянського суспільства, сприяти безпековому простору

країни загалом. Йдеться про досить деталізований документ, що, на думку науковців, мав би містити: основи інформаційного розвитку країни; принципи забезпечення інформаційної безпеки людини, суспільства, держави; норми комп'ютерної етики, а також морально-етичні основи регулювання взаємовідносин між комп'ютером та людиною в мережі інтернет; основні засади інформаційного розвитку держави, діяльності її органів щодо забезпечення інформаційної безпеки, протидії інформаційним війнам; систему заходів з подальшого зміцнення інформаційної безпеки тощо [1, с. 12]. Загалом кодифікація в галузі інформаційної безпеки вносить визначеність, статусність, систематизованість у розуміння цієї проблеми. При цьому політико-правовий підхід у тематиці інституційних основ інформаційної безпеки лише посилює нашу думку про гостру необхідність наукового пошуку та структурно вибудуваних теоретико-методологічних засад дослідження, коли об'єктивно доведені факти та судження покладаються в основу напрацьованих норм права та політичних аргументів основних гравців інформаційного простору.

Якщо європейських досвід орієнтує саме на такий нормативний підхід до осмислення та регулювання назрілих проблем інформаційного суспільства, то сучасні автократії та їх агресивні інформаційні стратегії зобов'язують дивитися на ці ж проблеми ширше – у ключі сучасного політико-філософського дискурсу, у традиціях діалектичного підходу. Сьогодні ми, на підставі зауваження у наших інших працях, підкреслюємо, що саме інформація є тим «інклюзивним, інтегративним, наскрізним ресурсом, що дозволяє максимально ефективно управляти тією чи іншою спільнотою в рамках сучасної інформаційної цивілізації» [368, с. 104]. Погоджуємося з вченими, які, як О. Дзьобань, вважають, що «проблема забезпечення інформаційної безпеки увійшла до числа найбільш значущих і пріоритетних завдань, вирішення яких необхідне для існування й подальшого розвитку нашого суспільства» [74, с. 207]. Тому, продовжує вчений, «інформаційна безпека важлива тому, що ми захищаємо свій інформаційний простір, а отже, свої інформаційні ресурси, свою національну культуру … захищаємо себе, своє право на життя, своє місце в історії» [74, с.

207]. Тобто ані модернізація, ані трансформація інститутів державного та громадського управління не можуть сьогодні успішно тривати й завершитися без урахування інформаційної складової. При цьому слід врахувати, що сьогодні вона значно багатоаспектніша, а відтак і механізми демократизації ускладнюються, формують перед нами декілька порядків нових саме інформаційних викликів (поряд із суто політичними, економічними, соціальними, культурними, які традиційно враховували розробники теорії демократизації та політичного транзиту). Відтак проблема інформаційної безпеки у політико-філософській призмі означає повторну актуалізацію та перегляд таких ключових понять як глобальне об'єднання людства, шкідливі інформаційні впливи, ризики інформаційного співробітництва, нові цивілізаційні умови та можливості, національне і державотворчу будівництво та інші.

Безумовно проблематика не має вирішення без комплексного її розуміння, тобто також і через ціннісний, психологічний, економічний, соціальний її аспекти. Тому особливо імпонують наукові підходи, що враховують цю багатоскладовість, коли в інформаційній безпеці вбачається і геостратегічний інтерес країни, і шанс демократичного суспільного розвитку, і гарантія збереження цілісності та державного суверенітету. Це виразно помічаємо в зауваженні такого вченого, як Є. Кирильчук, що стверджує, що «практичне забезпечення національної інформаційної безпеки можливе за рахунок єдності усіх факторів – політичного, економічного, правового, організаційного та ін.» [134, с. 62]. Політологічне розуміння інформаційної безпеки дозволяє охопити інституційну й ціннісну складові проблеми, їх відображення у політичних відносинах і процесах.

Отже, сучасний розвиток демократичної, соціальної, правової держави, зростання громадянського суспільства відчутно залежить від використання інформаційних ресурсів повною мірою, від закріплення загальних основ та детальних механізмів державної інформаційної політики, від розбудови ефективної та адекватної часу системи національної інформаційної безпеки, від інформаційної культури окремих громадян та соціальних груп. Інформаційна

безпека держави, суспільства, громадянина, людини сьогодні є чинником міжцивілізаційного зближення, конкурентоспроможних комунікацій, правової культури, національної довіри, демократизаційних зрушень. Вона має локальні, національні, регіональні, міждержавні та глобальні виміри, але у всіх них потребує фахового концептуального розуміння та стратегічного консультування.

Сучасна політична наука орієнтує на вивчення динаміки і статики політичного життя, тож у питаннях інформаційної безпеки політологія розвиває наше бачення організованих суб'єктів та стихійних чинників, що впливають на цю сферу, дозволяє вивчати проблеми та суперечності, реалії та ризики, пріоритети і виклики. Міждисциплінарний підхід суттєво доповнює та розвиває сучасні теоретико-методологічні засади дослідження інформаційної безпеки. Через політико-правовий і феноменологічний змісти проблематики розпізнаємо повноту можливостей, які дозволяють сучасним державам захищати свій інформаційний простір від актуальних викликів глобалізованого світу. У теоріях соціальної комунікації та транзитологічних моделях вбачаємо численні позиції для поновлення теоретичних і прикладних дискусій про потенціал умовно нових і старих інститутів у розбудові інформаційного суспільства. При цьому структурно-функціональний аналіз окремих інститутів та загалом системи інформаційної безпеки у сучасному дослідженні видається не повним без врахування можливостей аксіологічної аналітики, тобто вивчення етичних, культурних, моральних, ціннісних суб'єктів і об'єктів політики, які задають динаміку та визначають загальні межі інформаційних перетворень у кожному конкретному суспільстві чи іноді навіть громаді.

Висновки до Розділу 1

Загалом у Розділі 1 розглянуто та систематизовано історіографічні та теоретико-методологічні й концептуальні особливості та параметри дослідження проблеми інформаційної безпеки в умовах політичної трансформації.

Для цього, по-перше, комплексно схарактеризовано стан дослідження й

історіографію тематики інформаційної безпеки в умовах політичної трансформації у зарубіжній і вітчизняній науці, в тому числі у контексті окреслення означеної проблематики в українському законодавстві. На підставі структуризації наукових джерел з досліджуваної теми виявлено, що джерельну базу потрібно поділяти на теоретико-методологічну та більшою мірою практично орієнтовану, в тому числі на кейс інформаційної безпеки в Україні. В цілому констатовано, що проблематика інформаційної безпеки дуже значною мірою пов'язана з дослідженням феноменів інформаційного суспільства, інформаційного простору, інформації як такої та національної безпеки держави тощо, однак й досі залишається недостатньою мірою систематизованою, головно в рамках розвитку сучасної політичної науки в Україні, навіть попри дуже значну практичну актуальність означеного питання в контексті розвитку нашої держави.

По-друге, у розділі проаналізовано ключові поняття, концептуальні та наукові підходи й правові означення як теоретико-методологічну основну дослідження інформаційної безпеки в умовах політичної трансформації. Встановлено, що категорія і феномен інформаційної безпеки, навіть теоретико-методологічно, є надзвичайно багатовимірними, складними та поліморфними, про що засвідчує той факт, що їх часто аналізують у рамках різних парадигм, підходів, концептуалізацій і вимірів, а також у широкому та вузькому розумінні. Подібного висновку досягнуто на підставі аналізу українського законодавства та практики, які також не є достатньо консолідованими. Відповідно, встановлено, що навіть теоретико-методологічно та регламентаційно означена проблематика потребує подальшого розвитку та систематизації, зокрема зважаючи на більш розвинений досвід країн Західної Європи, США, Китаю й інших впливових акторів міжнародної політики. На цьому тлі констатовано, що окремішній наголос у цьому контексті потрібно робити на розумінні й дослідженні інформаційної безпеки, в тому числі у нашій державі, завдяки інструментарію політичної науки.

РОЗДІЛ 2

ЗАКОНОДАВЧА БАЗА УКРАЇНИ ТА МІЖНАРОДНІ СТАНДАРТИ І ПРАКТИКА ЩОДО ФУНКЦІОНУВАННЯ ІНСТИТУТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Правове забезпечення інформаційної безпеки в Україні

З точки зору права інформаційна безпека базується на державній інформаційній політиці, відповідних законах, що врегульовують суперечності, гарантують інформаційну свободу громадян та їх доступ до інформації в національному інформаційному просторі. Низка питань, що виникає в цій галузі правничих наук, ще не отримала належного обґрунтування, а також політологічного осмислення. Зупинимось на них більш детально, однак із розумінням того, що саме сучасний інформаційний простір, а також відповідні ресурси, технології, інфраструктура та інформаційні все більше й більше визначають динаміку як соціально-економічного, науково-технічного розвитку суспільства, держави, громадянина, так і політико-культурного та правового.

Право й політика мають настільки тісні взаємозв’язки, а відповідна проблематика до того назріла для сучасної України, що академічна спільнота політологів до певної міри об’єдналася довкола відносно нової науково-пізнавальної системи, дослідницької парадигми, наукового напряму та навчальної дисципліни – правової політології. Характерно, що і проблематика політичного права, і завдання та цілі сучасної правової політики розглядаються як закономірна частина модернізаційного розвитку держави та суспільства. Ця тематика безпосередньо розвивається науковими співробітниками Інституту держави і права імені В.М. Корецького НАН України, знайшла відображення в низці статей, науково-практичних заходів, цілісній монографії [416], що привертає нашу увагу і з позиції сучасних проблем інформаційного суспільства та особливо близька у світлі українських його реалій та перспектив.

Проблематика інформаційного права в цілому та його безпекових аспектів зокрема набуває останнім часом неабиякої актуальності в контексті глобалізації та інформаційного суспільства, як нової ери існування людства, а також з огляду на появу нового типу відносин, що пов'язані із використанням та обігом інформації. Інформаційний простір, на думку численних дослідників є ареною зіткнень і боротьби різновекторних національних інтересів в умовах глобальної інтеграції та жорсткої міжнародної конкуренції головною. Погоджуємося з думкою, що при цьому сучасні інформаційні технології дають змогу досягти реалізації власних інтересів без застосування воєнного інструментарію, послабити або навіть зруйнувати конкуруючу державу, не застосовуючи сили, за умови якщо ця держава не усвідомить реальних та потенційних загроз негативних інформаційних впливів і не створить дієвої системи захисту і протидії цим загроза [197, с. 124].

Крім того, події в Україні протягом останніх років роблять тему інформаційної політики держави, її безпеки та протидії інформаційним загрозам не просто актуальною, а й життєво-значущою. Тому не дивно, що питання інформаційного права та безпеки стає об'єктом наукових розвідок вітчизняних та західних вчених, однак ця тематика залишає ще велике поле для аналізу, зважаючи на відносну новітність у політичній та правовій науці, постійну еволюцію правової регламентації, а також шалену швидкість практичних зміну у сфері інформаційних технологій. Важливим підґрунтям для розроблення та вивчення проблематики інформаційної, передусім державної, політики є доробки наукових шкіл з інформаційного права, представниками яких виступають, для прикладу, І. Арістова, О. Баранов, Л. Задорожня, Р. Калюжний В. Ліпкан, В. Олійник, А. Пазюк, І. Сопілко, В. Цимбалюк, та М. Швець. Вивченням ролі держави у формуванні інформаційного суспільства та забезпеченні інформаційної безпеки займаються такі вчені як, Г. Почепцов, Ф. Медвідь, О. Литвиненко, Д. Лук'яненко, І. Рамоне, О. Соснін та ін.

Виділення правових основ інформаційної безпеки (так само, як і їх вироблення та застосування) ґрунтується на правовому та науковому визначенні

самого цього поняття. Аналізуючи не лише дефініції, що відображенні у науковій, науково-методичній та енциклопедичній літературі, а й у правових документах (міжнародного та національного масштабів), ми побачимо величезну кількість визначень інформаційної безпеки, які відображають багатоаспектність та складність цього поняття. Одні правничі наукові школи зосередженні на розумінні та правозастосуванні інформаційної безпеки як частини інформаційних відносин, інший підхід апелює до безпекових студій та військової науки, розглядаючи інформаційну безпеку як частину загальної безпеки держави.

Представляючи перший підхід, В. Цимбалюк характеризує інформаційну безпеку як «стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації» [278, с. 204]. Доповнює розуміння Р. Калюжний, який вбачає у цій категорії «вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності» [124, с. 234-235].

Дослідники Л. Задорожня, М. Коваль В. Брижко, наголошуючи на актуальності проблеми законодавчого врегулювання питань інформаційної безпеки визначають: «Інформаційну безпеку можна розуміти, з одного боку, як безпосередньо захист інформації, і особливо – захист таємниці, комерційної інформації, інформації з обмеженим доступом, персональних даних тощо, з іншого – як захист інформаційних систем, які фактично є засобом передачі інформації» [89, с. 27].

На противагу ним, Л. Харченко, В. Ліпкан, О. Логінов визначають, що інформаційна безпека постає як «складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України» [272, с. 65]. Інформаційна безпека України, згідно тотожної позиції І. Громико та Т. Саханчук, також виступає, як захищеність державних інтересів, за якої забезпечується запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і безпечний

розвиток міжнародного інформаційного співробітництва [59, с. 130-134].

Прибічники широкого розуміння проблем інформаційної безпеки розглядають цю сферу діяльності не тільки крізь призму інформаційних відносин, а і через систему державно-управлінської діяльності. Так, В. Ліпкан в процесі аналізу системи забезпечення інформаційної безпеки констатує, що «основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які використовують систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління» [169, с. 219-220]. Дослідниця А. Нашинець-Наумова також зауважує, що «інформаційна безпека українського суспільства як важлива складова національної безпеки передбачає системну превентивну діяльність органів державної влади по наданню гарантій інформаційної безпеки особі, соціальним групам і суспільству в цілому і спрямована на досягнення достатнього для розвитку державності та соціального прогресу рівня духовного та інтелектуального потенціалу країни» [197].

М. Дмитренко, як і багато інших дослідників сучасної держави, звертає увагу на те, що нині жодна сфера життя не тільки окремих суспільств і держав, але і усього світового співтовариства не може функціонувати без розвинутої інформаційної структури, що в процесі формування інформаційного суспільства, яке є не тільки основою процвітання а також, що саме через інформаційне середовище генеруються та втілюються загрози національній безпеці держави. Зазначається, що ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян [76, с. 391].

Науково-правові дослідження не виробили загальноприйнятого механізму визначення та структуризації забезпечення інформаційної безпеки. У попередніх розділах ми вже зокрема зазначали, що у такій структурі могли би бути визначальними напрями, механізми та шляхи забезпечення. Однак, на

думку О. Тихомирова, «саме розуміння забезпечення інформаційної безпеки як комплексного виду діяльності дозволяє гармонізувати термінологію і здійснювати не лише структурний, а й глибокий змістовний аналіз, повною мірою застосовуючи потенціал діяльнісного підходу» [260, с. 165].

Юридична енциклопедія за редакцією Ю. Шемшученка представляє подібний агрегований синтетичний підхід до інформаційної безпеки. Так, дослідник визначає її «як один з різновидів національної безпеки і функцію держави, котрі сумарно означають: «законодавче формування державної інформаційної політики»; «створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об'єднаннями громадян, іншими суб'єктами права в Україні»; «гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України»; «всебічний розвиток інформаційної структури»; «підтримку розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України»; «створення і впровадження безпечних інформаційних технологій»; «захист права власності всіх учасників інформаційної діяльності в національному просторі України»; «збереження права власності держави на стратегічні об'єкти інформаційної інфраструктури України»; «охорону державної таємниці, а також інформації з обмеженим доступом»; «створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом»; «захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції»; «встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів з іноземними державами»; «законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України» [154, с. 714-715].

Отже, інформаційна безпека є феноменом, що одночасно належить до сфери правової регламентації державної інформаційної політики та сфери нормативного регулювання політики в галузі безпеки держави. Цілком виправданим видається і правове розуміння державної інформаційної політики України – на засадах правової держави, демократичного устрою, розробки та, як зазначає Л. Наливайко, «реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством» [194].

Тому інформаційна безпека як об'єкт правового регулювання та охорони конституційних прав і законних інтересів зазначених суб'єктів спрямована на одночасне забезпечення: конституційних прав і свобод людини, громадянина, єдності їх прав і обов'язків; і на захист духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства, його інформаційного і природного середовища; конституційного ладу, суверенітету, територіальної цілісності держави; політичної, економічної, соціокультурної, науково-технологічної, оборонної і державної безпеки, екологічної, власне інформаційної сфер тощо складових національної безпеки [205, с. 65]. Загалом кожен із вказаних напрямків потребує і організованої системи протидії інформаційним загрозам, і напрацювання системи власного інформаційного простору, і відповідної інфраструктури, тобто широких інформаційних ресурсів, доступних для держави, суспільства, громадян.

Необхідність забезпечення інформаційної безпеки вченими, такими як Л. Наливайко, цілком справедливо пов'язується з: 1) «потребою забезпечення національної безпеки України як цілісності, що передбачає й інформаційну складову»; 2) «існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам»; 3) «врахуванням того, що за допомогою інформації можна впливати на зміну свідомості людей, їх поведінкові моделі» [194].

Безумовно відповідний політологічний аналіз розпочинаємо з Основного Закону держави. Забезпечення інформаційної безпеки визначене нормами ч. 1 ст. 17 Конституції України як «найважливіша функція держави» і саме остання виступає

головним суб’єктом політики інформаційної безпеки [145]. Згідно зі ст. 2 Закону України «Про національну безпеку України», правову основу в сфері національної безпеки, окрім Конституції, визначають і «закони України, міжнародні договори, згода на обов’язковість яких надана ВРУ України» [386], а також видані на виконання Конституції та законів України інші нормативно-правові акти.

Серед міжнародних договорів варто навести такі приклади, які увиразнюють інформаційну складову навіть у складних міжнародних програмах співробітництва: Договір про безпеку і співробітництво у Європі (засновує структуру ОБСЄ, що опікується питаннями безпеки і співробітництва держав-учасників у галузі економіки, науки, технологій, довкілля, в гуманітарній сфері, а також питаннях прав людини, інформації, культури, освіти тощо); Угода про партнерство та співробітництво між Європейським співтовариством і Україною (започатковує таке партнерство, в тому числі з огляду на спільне бажання встановити культурне співробітництво, розширити доступ до інформації); Договір «Відкрите небо» (надає можливість сторонам здійснювати спостережні польоти над територіями одна одної для більшої відкритості у військовій діяльності, розширення миротворчих можливостей тощо), Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства (у якому сторони зобов'язуються обмінюватися інформацією щодо матеріального процесуального права та організації кримінального судочинства).

Ці та ряд інших договорів зобов'язують сучасні демократичні держави обмінюватися різноплановою інформацією, напрацьовувати дійові механізми її зберігання, спільно працювати у сфері сприяння загальній культурі споживання інформації людьми. Однак вони конкретизуються і в низці інших міжнародних документів. Наприклад, у прагненні об’єднати зусилля для боротьби з кіберзлочинністю і захисту законних інтересів у ході використання і розвитку інформаційних технологій країни-учасники підготували «Конвенцію Ради Європи про кіберзлочинність» [144].

Основні правила щодо здійснення діяльності в інформаційній сфері, тобто «створення, отримання, використання, поширення та зберігання інформації і

захисту прав суб'єктів інформаційних відносин», містяться у 32 і 34, а також низці інших (10, 15, 17, 23. 28, 29, 31, 32, 40, 50, 53, 54, 55, 57) статей Конституції України [145]. «Крім того, основу галузевого законодавства складають більш ніж п'ятнадцять базових законів і значний корпус пов'язаних нормативних актів. За підрахунками фахівців, кількість тільки Законів України, яких регулюються суспільні інформаційні відносини, досягла більш ніж 300» [82]. Серед найважливіших з них: «Про інформацію» [101], «Про доступ до публічної інформації» [95], «Про захист персональних даних» [98], «Про друковані засоби масової інформації (пресу) в Україні» [96], «Про телебачення і радіомовлення» [108], «Про звернення громадян» [100], «Про державну таємницю» [94], «Про засади запобігання і протидії корупції» [97] та деяких інших. Крім того, ціла низка нормативних актів у тій чи іншій частині розглядають питання конкретних дій при інформаційній діяльності в зазначеній сфері, наприклад, Податковий та Митний кодекси України, розглядають питання створення, збору, використання специфічної податкової, митної інформації, процеси окремі нюанси розповсюдження інформації та забезпечення безпеки регулюють адміністративне, карне та цивільне кодифіковане законодавство тощо.

Важливим правовим підґрунтям інформаційної безпеки виступають концептуальні державні документи – Концепції, Стратегії, Доктрини. Зокрема була розроблена Стратегія національної безпеки України, Доктрина інформаційної безпеки, Концепція розвитку інформаційного суспільства в Україні. В таких актах зазначаються базові пріоритети розвитку певної сфери, вони є підґрунтям для прийняття нових норм та усунення колій в існуючих.

Стосовно Доктрини інформаційної безпеки, то І. Сопілко зазначає, що такий документ покликаний окреслити концептуальні підходи реалізації державної інформаційної політики через ефективну реалізацію «політики національної безпеки в інформаційній сфері, або ж державної політики інформаційної безпеки» [253, с. 37]. Це, на думку вченого, своєрідна система офіційних позицій на мету, «функції, принципи та методи, основні напрями державної політики, заходи контролю у відповідній сфері» [253, с. 37]. Це також

той базовий категорійно-понятійний апарат, що повинен бути відображений і узгоджений у відповідних законах, а відтак і в компетенція і якостях конкретних суб'єктів реалізації такої політики. Ми також погоджуємося з думкою, що слідом за Доктриною мали би розроблятися документи наступного рівня: закони, конкретні програми тощо [253, с. 37].

Наш аналіз діючого вітчизняного законодавства, дозволяє зазначити, що в українській практиці часто складалась зворотна ситуація – спочатку розроблялись нормативні акти, які регулювали окремі дискретні сфери інформаційних та безпекових відносин (частіше, навіть, на рівні Постанов Уряду та Указів Президента, відомчих актів та інструкцій), а потім деякі з них змінювались законодавцем при актуалізації потреби у розробці та втіленні державної доктрини.

Фактично за великим рахунком лише закон України «Про інформацію» на початковому етапі існування української державності охоплював «глибокі пласти інформаційних відносин, регламентуючи їх на загальному, надгалузевому рівні» [101], та фактично регламентуючи і сферу інформаційних відносин, і сферу інформаційної безпеки. Закон був прийнятий 2 жовтня 1992 р. й відтоді є певним орієнтиром для розуміння основ у питаннях створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, тобто одним із перших важливих політико-правових рішень в організації безпечного інформаційного простору. Вітчизняні науковці високо оцінюють це тогочасне рішення, що вперше на вищому законодавчому рівні визначило ключові поняття інформації та її видів, державної інформаційної політики, режимів доступу до інформації, охорони інформації, гарантій інформаційного суверенітету України та багато інших [215, с. 65]. Зрештою Закон закріпив забезпечення інформаційної безпеки України серед головних напрямів державної інформаційної політики.

В ст. 14 Закону України «Про інформацію» безпосередньо визначені та розкриті види інформаційної діяльності, «а державна діяльність, що відповідає цим видам, згідно зі ст. 6 цього ж закону, складає основу державної інформаційної політики» [101]. За видами інформаційної діяльності у безпековому контексті виділяють: а) забезпечення одержання інформації у встановленому порядку;

б) забезпечення можливостей використання інформації; в) забезпечення законного поширення інформації; г) забезпечення належного зберігання інформації; д) захист інформації [101].

Водночас не варто й ідеалізувати Закон, що з часу прийняття вже більше п’ятнадцяти разів переглядався. Як вказує А. Петрицький, підсумовуючи правовий аналіз, що було здійснено і іншими правознавцями та практиками, прийнятті норми не охоплювали багатьох важливих аспектів інформаційної діяльності, призводили до чисельних правових колізій. Поза текстом значною мірою залишилася діяльності журналістів, ЗМІ та їх працівників, серйозні проблеми, пов’язанні з поширенням суспільно необхідної інформації з обмеженим доступом. Навіть вже згаданий понятійно-категоріальний апарат був достатньо суперечливим [215, с. 65].

Нова редакція Закону 2011 р. була покликана забезпечити оновлене правове підґрунтя для формування та реалізації державної інформаційної політики та зміцнення інформаційної безпеки. Після подій 2014 р. Закон знову зазнає часткових змін, пов’язаних передусім з уже згаданою гуманітарною складовою (питання мови інформації, історичних оцінок в ЗМІ, доступу до архівних документів тощо).

Ми погоджуємося з тими вченими, яким вдалося окреслити загальну тенденцію: зі здобуттям незалежності в Україні приймалися норми, що регулювали переважно питання технічного захисту інформації, структурні, організаційні відносини у сфері інформатизації, однак вже у процесі формування інформаційного суспільства, з розширенням гуманістичної візії на цю проблематику інформаційне законодавство також стало більше концентруватися на питаннях інформаційної безпеки [253]. Отже, наприкінці першого десятиріччя 2000-х рр. правова регламентація проблем інформаційної безпеки стала розвиватися активніше та охоплювати більш широке коло питань, зрештою прописуючи й ціннісно-смислові аспекти проблеми.

Однак, небезпечною реальністю України була і залишається несформованість системи забезпечення саме інформаційної безпеки, де панує

фрагментарний підхід. На концептуальному рівні у 1997 році Верховна Рада України в системі державної політики національної безпеки визначила лише власно інформаційну сферу, тобто сферу обігу інформації [146]. Закон України «Про основи національної безпеки», прийнятий у 2003 році закріплює підхід аналогічний концептуально визначеному в Концепції 1997 року. Також можемо констатувати відносну розмитість й неспівпадіння деяких норм та визначень, що надаються у різних правових актах. Серед недоліків вітчизняного законодавства з питань інформаційної безпеки Р. Алямкін та Н. Федорін також виділяють розпорошеність його правових норм у масиві інформаційного законодавства, а також те, що згадані норми носять, в основному, декларативний характер. Вони також зазначають, що на якість законодавчих приписів негативно впливає змістовна невизначеність деяких основних юридичних понять та порушення вимог принципу єдності термінології, що насамперед, стосується базового терміну «інформаційна безпека» [11, с. 94].

Зокрема у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» це поняття ототожнювалося з безпекою інформаційних ресурсів і трактується як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди державі через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [106]. Водночас у Законі «Про телекомунікації» та його визначенні інформаційної безпеки акцент робиться на безпеці телекомунікаційних мереж. Законом «Про основи національної безпеки України», що вже втратив чинність, інформаційну безпеку подано як невід’ємну складову національної безпеки без точного визначення його змісту. Замість цього поняття вживається термін «національна безпека в інформаційній сфері». У Законі ж «Про захист інформації в інформаційно-телекомунікаційних системах» воно також не визначено, хоча вжито у різних відтінках поняття «захист інформації» [11, с. 95].

Певною спробою створити стрижневий документ, що охоплював б сферу саме інформаційної безпеки було розроблення та прийняття Доктрини інформаційної безпеки протягом 2008-2009 рр. 23 квітня 2008 р. тодішній Президент України В. Ющенко наказом № 377/2008 ввів в дію рішення РНБО «Про невідкладні заходи щодо забезпечення інформаційної безпеки України». Серед результатів цього рішення власне і була підготовка «Доктрини інформаційної безпеки України» [263]. Треба відмітити колегіальний стиль напрацювання цього документу. В його підготовці і обговоренні взяли участь представники різних органів державної влади, академічні сили, громадські ініціативи; опрацьовано понад 200 конкретних пропозицій.

Відтак у Доктрині об'єктами інформаційної безпеки визначалися: забезпечення інформаційної безпеки особи, суспільства та держави. Спільні зусилля, покладені в часі підготовки, відобразилися у змісті, адже базовими напрямками у сфері забезпечення інформаційної безпеки України визнавались інформаційно-психологічний, технологічний та власне напрям зі захисту інформації, а перспектива реалізації таких напрямків вбачалася в тому числі у поєднанні діяльності держави, громадянського суспільства і усіх громадян [263].

Згідно Доктрини в інформаційній сфері України [263] вирізняються наступні життєво важливі інтереси держави: 1) «недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур»; 2) «ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері»; 3) «побудова та розвиток інформаційного суспільства»; 4) «забезпечення економічного та науково-технологічного розвитку України»; 5) «формування позитивного іміджу України»; 6) «інтеграція України у світовий інформаційний простір» [263].

В цьому ж документі було визначено наступні принципи забезпечення інформаційної безпеки України: 1) «свобода збирання, зберігання, використання та поширення інформації»; 2) «достовірність, повнота та

неупередженість інформації»; 3) «обмеження доступу до інформації виключно на підставі закону»; 4) «гармонізація особистих, суспільних і державних інтересів»; 5) «запобігання правопорушенням в інформаційній сфері»; 6) «економічна доцільність»; 7) «гармонізація українського законодавства в інформаційній сфері з міжнародним»; 8) «пріоритетність національної інформаційної продукції» [263].

Закон України «Про основи національної безпеки України» 2003 р. запропонував свого часу дещо інші візії напрямів «державної політики з питань національної безпеки в інформаційній сфері» [105]. Навіть у цьому формулюванні бачимо деяке зміщення акцентів. Зокрема серед центральних проблем названо гарантування інформаційного суверенітету України, національної інформаційної інфраструктури, новітніх технологій, інформація про Україну за її межами, боротьба з корупцією за допомогою сучасних інформаційних ресурсів, протидія монополізації інформаційної сфери України, недопущення переслідування журналістів за політичні позиції. Збереглися і традиційні установки стосовно дотримання права громадян на свободу слова, доступ до інформації, недопущення дискримінації в інформаційній сфері, захисту національного інформаційного простору загалом [105].

Багато вчених та практиків писали про неузгодженість Доктрини із безпековим законодавством, а також іншими нормативними актами, що регулюють інформаційні відносини держави [205, с. 66]. Прогалини правової системи забезпечення інформаційної безпек мали політичні наслідки та стали особливо відчутні після 2014 р.

У зв’язку з рішенням РНБО України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», уведеним у дію Указом Президента України від 1 травня 2014 року № 449 [264], Доктрина інформаційної безпеки 2009 р. втратила чинність. В цьому ж Указі зазначалось, що у тримісячний термін Уряд має розробити нову редакцію Доктрини національної інформаційної безпеки України, яка має враховувати актуалізовані інформаційні та військові загрози,

містити базу для протидії негативним інформаційним впливам, враховувати реалії «гібридної війни» та антитерористичних дій.

Також і в Рекомендаціях парламентських слухань «Законодавче забезпечення розвитку інформаційного суспільства в Україні» ще в липні 2014 р. вказувалось, що уряду необхідно «визначити пріоритетні напрями діяльності органів виконавчої влади з питань становлення і розвитку інформаційного суспільства в умовах інформаційної глобалізації та євроінтеграції України, а також інформаційної «війни»» [222]. Після тривалої підготовчої роботи була ухвалена нова «Доктрина інформаційної безпеки». Це було зроблено Указом Президента України №47/2017 від 25 лютого 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [265].

У цьому документі детальніше прописані пріоритети державної політики в інформаційній сфері, при цьому вони розподілені на чотири великі категорії, об'єднанні водночас спільними інтересами та цілями (які також сформульовані у Доктрині). Отже, серед пріоритетів зазначено, найперше, забезпечення інформаційної безпеки, що видається доволі широким за своїм охопленням проблем (тут передбачається і політико-культурна, і гуманітарна, і психологічна складові інформаційної безпеки, поряд – технологічна, військова, законодавча тощо). Відтак у наступному розділі йдеться про забезпечення розвитку інформаційного простору України, при чому право громадян на інформацію та його захист також включений у цей другий розділ пріоритетів. У цьому розділі питання суспільного мовника визначенні поряд з проблематикою масової медіа-грамотності, квотування, книговидання, інформування населення на окупованих територіях тощо. Третій розділ передбачає відкритість та прозорість державних органів перед громадськістю, тобто перспективи електронного урядування, відкритості публічної інформації, комунікацій зі ЗМІ та громадянами тощо. Він помітно менш конкретизований, аніж усі інші розділи. Зрештою четвертий, заключний розділ орієнтує на формування позитивного міжнародного іміджу України – це і розбудова інституцій публічної дипломатії, і моніторинг ворожої

пропаганди, і розвиток взаємовигідних відносин з українською діаспорою тощо [387]. Логіка окреслення пріоритетів у Доктрині цілком доречна в умовах війни, однак певна стихійність формулювань та їхня безвідносність до конкретних інститутів (що відтак поглиблює кризу політичної відповідальності) властиво зберігається.

Декларативність окремих положень, правові колізії, нестача наукових обґрунтувань – усі ці характеристики вже неодноразово повторювалися в історії розвитку інформаційної політики України загалом та системі забезпечення її інформаційної безпеки зокрема. Інституційне та правове забезпечення інформаційної безпеки досі залишається фрагментарним, при чому ці застереження вітчизняних науковців початку 2000-х рр. досі актуальні. Загальна система державно-управлінської діяльності та адміністративно-правового регулювання відносин у сфері забезпечення інформаційної безпеки, за тодішніми оцінками, була все ще не сформованою, а адміністративно-правові відносини – концептуально неузгодженими [205, с. 68]. Цікавим прикладом фрагментарності такого інституційного забезпечення інформаційної безпеки є створення у 2014 р. Інформаційно-аналітичного центру Ради національної безпеки та оборони, і при цьому ініціатива сформованого після виборів до ВРУ 2014 р. Уряду по створенню Міністерства інформаційної політики, яке не унормоване в існуючій законодавчій базі. Крім того, відсутність протягом довгого часу Положення про згадане міністерство, подальша тривала юридична та практична невизначеність його роботи означена ініціатива, на тлі економічної кризи та декларованого намагання Уряду знизити навантаження на бюджет країни, викликала певні зауваження з боку журналістської й експертної спільноти та громадських активістів.

Зважаючи на публічність як базову ознаку такого органу державної влади як міністерство, створення спеціального органу, що відповідатиме за контрпропаганду та контроль за інформаційними впливами саме в структурі кабінету міністрів, а не органів безпеки, призвело до певної конкуренції державних органів. Як зазначають фахівці інформаційно-аналітичного центру

РНБО, досвід інших держав показує, що управління інформаційними операціями, в тому числі і контрпропагандою, може бути покладено на окремий керівний підрозділ при Раді національної безпеки і оборони. До того ж буквально всі заходи з інформаційного аналізу, впливу або протидії планувалось доводити до дуже вузького кола осіб, інакше (коли про інформаційні операції будуть знати всі) – інформаційний вплив або контрзаходи будуть неефективними [64].

Отже, як зазначають фахівці Національного інституту стратегічних досліджень, зокрема С. Гнатюк, «в Україні сформувалася специфічна національна доктрина права, яка поєднує в собі елементи англо-американського й континентального підходів» [82] (двох найпоширеніших у світі). У контексті інформаційних відносин в суспільстві, протягом років незалежності напрацьовано, продовжують вчені, «багато спеціальних законів та підзаконних нормативних актів, що фрагментарно регулюють окремі аспекти та різновиди цих відносин, які водночас не вибудовують чіткої ієрархічної системи. З іншого боку – значний масив норм, що стосуються регулювання інформаційної сфери, міститься у кодифікованому законодавстві суміжних галузей права, наприклад – в цивільному, адміністративному, трудовому, кримінальному» [82]. Відтак, така змішана модель продукує реальні та потенційні системні труднощі

Нормативно це означено тим, що по-перше, «розпорошеність юридичних норм, що регулюють інформаційні відносини, по різних законах та підзаконних нормативних актах, ускладнює їх пошук, аналіз, а зрештою, – і практичне застосування» [82]. Прикладом цього можуть слугувати види державного забезпечення інформаційної безпеки та діяльності держави в інформаційній сфері, які регулюються різними нормативно-правовими актами: 1) «інформування – надання суб’єктам необхідної для функціонування та життєдіяльності якісної інформації» [95] (регулюється Законом «Про доступ до публічної інформації» [95]); 2) «інформатизація як цілеспрямована діяльність держави – створення політичних, економічних, технічних та інших умов для інформаційного розвитку суб’єктів, розвитку державного інформаційного

ресурсу та оптимізації обміну інформацією» [101] (здебільшого регулюється Законом «Про інформацію» [101]); 3) «унормування поведінки суб'єктів в інформаційній сфері – правова регламентація сфери інформаційних відносин» [79; 145] (регулюється Конституцією України та Доктриною інформаційної безпеки або кодифікації інформаційного законодавства); 4) боротьба з правопорушеннями в інформаційній сфері (регулюється нормами адміністративного, цивільного та кримінального кодексів).

По-друге, продовжують вчені, «кількість правових норм у сфері суспільних інформаційних відносин, визначених у законах і підзаконних актах, нині досягла вже критичної маси, що зумовлює необхідність їх впорядкування у рамках єдиної системи правових норм та понять, а також чіткої ієрархії законів» [82]. Гостро визріла потреба оновлення підходів та інтерпретацій, зрештою напрацювання єдиного концептуально цілісного розуміння державної інформаційної політики, яке би об'єднувало та визначало орієнтири елементом для усієї нормативної бази та відповідних положень. На противагу чисельним спробам дослідників та парламентарів «удосконалювати та ухвалювати ще більшу кількість нормативних актів, яка за деякими оцінками фахівців сягає» від декількох сотень до тисячі, іншою групою вчених, серед яких і І. Сопілко, «пропонується підхід формування єдиної несуперечливої ієрархічної системи нормативно-правових актів, що регулюють суспільні відносин у сфері державної інформаційної політики» [253, с. 36].

По-третє, зазначають вчені, «чимало встановлених навіть ключовими законами та підзаконними актами юридичних норм, які прямо або опосередковано регулюють сферу інформаційних відносин, виявилися концептуально не узгодженими між собою» [82]. Більше того, продовжують вони, «в інформаційному законодавстві використовується низка термінів, що недостатньо коректні, та/або не мають чіткого визначення свого змісту. Такими, зокрема, є: «інформація», «таємна інформація» і «таємниця», «документ» і «документована інформація», «інтелектуальна власність», «автоматизована система», «суб'єкт суспільних відносин» й «учасники

суспільних відносин», «система інформаційних відносин» тощо» [82].

Досі актуально звучать застереження про те, що ще багато термінів недостатньо коректні й чіткі як для політико-правового поля, тому довкола таких понять як, наприклад, «інформаційно-психологічна безпека», «інформаційно-психологічні впливи» тощо можливо чимало маніпуляцій [228]. Додамо до цього також, що потребують уваги і такі терміни як «державна інформаційна політика», «національний інформаційний простір», розмежування/узгодження таких категорій як «предмет інформаційних правовідносин» та «об'єкт інформаційного права» та інші. Усі ці напрямки актуалізують питання вдосконалення інформаційного законодавства України, зокрема у контексті його адекватності реальним загрозам, відповідності міжнародним стандартам, узгодженості у внутрішньому використанні понятійно-категоріального апарату.

Передусім варто відмовитися від суто декларативної законотворчості, переглянути існуючі положення на предмет їх актуальності, адже інформаційне суспільство дуже динамічно змінюється та привносить завжди нові сенси і виклики у політику. Від застарілих норм варто відмовлятися, але також і системно відстежувати дієвість оновлених чи нещодавно прийнятих. Правове регулювання суспільних інформаційних відносин, на думку Л. Наливайко, могла би суттєво писилити систематизація норм права в цій сфері, зокрема: «визначення ієрархічної системи та структури інформаційного законодавства на рівні правової доктрини»; «відокремлення в системі законодавства інформаційної галузі та розміщення її у зводі законів України як окремого розділу «Інформаційне законодавство»»; «кодифікація, тобто розробка й прийняття Верховною Радою України окремого Кодексу України про інформацію» [194].

Ідея систематизації у цій галузі періодично резонується в українському суспільстві, і найчастіше пов'язується саме зі створенням Інформаційного кодексу України. Його необхідність визнають багато суб'єктів політики, але сперечаються про зміст, окремі положення тощо. При цьому окреслилися відмінні підходи.

Детальніше ці підходи вже розглядали аналітики, ми ж лише наведемо окремі тези. 1) Своє бачення Інформаційного кодексу пропонував Державний

комітет телебачення і радіомовлення України, який основою цього документу передбачав «Концепцію національної інформаційної політики» та змінені відповідно до неї інші закони та нормативно-правові акти України. Однак ідея Концепції так і не була реалізована. 2) Вчені Інституту держави і права ім. В. Корецького ґрунтовно розписали структуру майбутнього Кодексу: базова частина (системо-утворюючі норми у сфері інформації та інформатизації); галузева частина (регулятори інформаційних відносин в окремих сферах життя особи, держави, суспільства); видові норми (регулятори інформаційних відносин «у сфері створення, пошуку, одержання, використання, зберігання та поширення окремих видів інформаційної продукції або в окремих складових інформаційного процесу» [228]); спеціальні норми (регулятори інформаційних відносин щодо створення і використання інформаційних технологій та телекомунікаційних систем). 3) Урядова комісія з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади вивела дискусію у ширше русло загальної систематизації інформаційного законодавства, при чому на трьох стадіях: стадії інкорпорації законодавства («ієрархічної системи та структури інформаційного законодавства на рівні правової доктрини» [228]); етапі виокремлення в системі законодавства галузі та її закріплення у Зводі законів України як розділу – «Інформаційне законодавство»; власне стадії кодифікації. Ці ідеї Комісією висунуті в проекті «Концепції реформування законодавства України у сфері суспільних інформаційних відносин» [147; 228].

Відсутність системності в підходах до кодифікації інформаційного законодавства є, на думку І. Березовської, однією з важливих проблем реформування законодавства в сфері забезпечення інформаційної безпеки України. В той же час, варто зазначити, що формування нових суспільних відносин в інформаційному суспільстві передбачає створення відповідного комплексу правового забезпечення. В усьому світі ведеться робота над реформуванням (удосконаленням) чинного законодавства, розробленням нових нормативно-правових актів у сфері регулювання інформаційних відносин і забезпечення інформаційної безпеки держави [20, с. 310].

Крім того, зазначають вчені, «українське законодавство у низці аспектів «відстає» від динаміки змін, що виникають у процесі розвитку інформаційного суспільства в Україні та світі», через що «багато елементів останнього існують поза правовим полем, не регулюються нормативними актами, що стримує його повноцінний розвиток» [82]. Як вказують фахівці Національного інституту стратегічних досліджень, «досі відсутня значна частина підзаконних нормативно-правових актів, розробка та затвердження яких передбачена чинним законодавством. Запропоновані відповідними державними органами проекти таких актів є здебільшого недосконалими і некоректними з точки зору відповідності діючому законодавству» [82].

На практичні проблеми в галузі інформаційної політики вказується і в Рекомендаціях парламентських слухань від 3 липня 2014 р. «Законодавче забезпечення розвитку інформаційного суспільства в Україні», де констатується, що «за часів незалежності України галузь інформаційних технологій розвивалася практично без підтримки з боку держави, роль якої переважно зводилася до збору статистичних відомостей, які часто не відображали реального стану справ» [222]. Водночас продовжується, що «в Україні сформувалися досить потужний інтелектуальний потенціал та високі темпи зростання у сфері програмної продукції» [222]. Загалом у головному представницькому органі влади України неодноразово підіймалися питання про дієвість та контрольованість інформаційної політики, налагодження її громадської і державної підтримки, співробітництва у цій галузі, а в умовах інформаційної агресії все гостріше – про цілісність системи забезпечення інформаційної безпеки країни, суспільного мовника, українське мовлення за межами країни, про інформаційно-аналітичну, кіно- та медіа продукцію вітчизняного виробника тощо.

Аналізуючи проблемні питання інформаційної безпеки, що залишаються поза правовою регламентацією або врегульовані недостатньо, варто також пам’ятати і про кращі світові практики забезпечення інформаційної безпеки. Зокрема йдеться про виокремлення у цій системі двох основних підсистем: інформаційно-технічної (комп’ютерні пристрої, інформаційні мережі, програми) та інформаційно-

психологічної (ЗМІ, громадські організації, дипломатія). При цьому фахівці відносно єдині у думці, що інформаційно-технічна підсистема в Україні функціонує достатньо успішно, однак інформаційно-психологічна за рівнем та кількістю проблем іноді навіть може негативно впливати на першу. Відтак загалом система інформаційної безпеки України характеризується як розбалансована, зі зміщеними акцентами на її технічній складовій [64].

З цього приводу О. Тихомиров зауважує, що «результати аналізу різноманітних джерел свідчать про недостатню розробленість та систематизованість структурних складових практичного забезпечення інформаційної безпеки» [260, с. 165]. Ми солідаризуємося з цим вченим, який вказує, що «на нормативно-правовому рівні практично безальтернативним залишається підхід, у межах якого, залежно від пріоритетних загроз, визначаються напрями забезпечення інформаційної безпеки, об'єднані за традиційними сферами життєдіяльності» [260, с. 165]. Доктрина інформаційної безпеки України 2009 р. [263], а також деякі інші «фундаментальні» та базові правові акти для забезпечення національної безпеки використовують саме подібний підхід. У наукових дослідженнях пріоритет надається класифікації загроз як чинників, що зумовлюють основні напрями або шляхи забезпечення інформаційної безпеки. Однак, на нашу думку, при нормотворенні важливо не лише діагностувати, у якій саме сфері життя (економічній, соціальній чи культурній) існують загрози, а описати та класифікувати їхню сутність та механізми запобігання та знищення.

Вже тривалий час держава визнає існуючі загрози інформаційній безпеці України – намагання маніпулювати суспільною свідомістю громадян, загрози для свободи слова, доступу до інформації, пропагування насильства, жорстокості, порнографії, злочинність та тероризм, що пов`язані з використанням сучасних інформаційних технологій і глобальних мереж, розголошення державних таємниць, конфіденційної інформації, персональних даних тощо – цей комплекс проблем був достатньо детально прописаний на найвищому законодавчому рівні, навіть до дізнання реалій інформаційної агресії [див. напр.105].

Як вважають фахівці, зокрема І. Боднар, «головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни» [26, с. 69], спроба втрутитися у інформаційні ресурси суспільства, деформувати свідомість особистості, заради нав’язування власних цінностей, поглядів, інтересів у життєво важливих сферах, заради управління поведінкою, рішеннями і розвитком тощо. Власне йдеться про комплекс загроз суверенітету країни на інформаційному рівні з використанням окремого, стратегічного та принципово нового виду протистояння – інформаційного, що без застосування зброї у класичному її розумінні, досягає потрібних цілей у сучасних конфліктах і війнах.

Крім того, в жодному з нормативних актів, що регулюють інформаційні відносини в нашій державі, ми не можемо зустріти поняття «інформаційної зброї», що дійсно ускладнює правозастосовну діяльність судів за її використання та є перепоною для правоохоронних, оборонних, безпекових структур у попередженні та вирішенні конфліктних ситуацій, встановлення складу злочину проти територіальної цілісності та державного ладу. Серед таких засобів інформаційної зброї є ті, що вже апробовані часом (наприклад, спеціальні психологічні операції), а також відносно нові (наприклад, специфічні комп'ютерні засоби боротьби), водночас вчені помічають у них спільну ознаку – «усі вони засновані на ідеї опосередкованого впливу на матеріальний світ через світ інформаційний» [26; 194].

Інформаційну зброю часто розуміють як деяку сукупність технічних, політичних, організаційних і інших засобів, за допомогою яких реалізуються інформаційні загрози. О. Литвиненко, підсумовуючи напрацювання американських фахівців, вказує, що існує багато видів інформаційної зброї, які можна об'єднати в чотири основні типи: 1) «засоби впливу на інформаційну інфраструктуру»; 2) «засоби розвідки, отримання інформації з інформаційних, телекомунікаційних і подібних систем»; 3) «засоби впливу на інформацію, яка обробляється в інформаційних системах, наприклад, на програмно-математичне забезпечення цих систем»; 4) «засоби впливу на суспільну свідомість» [165, с. 47].

Чимало засобів реалізації загроз для інформаційної безпеки, про які ми писали раніше, відтак можна розглядати як прояви використання інформаційної зброї, адже йдеться і про дезінформування, приховування інформації, порушення чинного порядку та перевірених каналів інформаційного обміну, і про несанкціонований доступ до інформаційних ресурсів держави й суспільства, і про чи необґрунтоване обмеження доступу до суспільно важливих джерел інформації, і про крайні прояви інформаційного тероризму, зумисне ушкодження інформаційного простору держави, розповсюдження комп'ютерних вірусів тощо. За давніми пересторогами Г. Лазарева, дійсним результатом негативних інформаційних впливів є деформація інформації, що відтак спотворює інформаційне середовище держави, соціуму, їхніх інформаційних ресурсів, ускладнює та заплутує функціонування важливих державних, виробничих, наукових, фінансових систем, зрештою порушує національний інформаційний суверенітет [161, с. 81].

Мусимо також констатувати, що законодавством фактично не класифікуються та не пояснюються ані самі загрози інформаційній безпеці, що допомогло б завадити негативним інформаційним впливам, ані регламентуються правові легітимні механізми протидії ним. Водночас протидія загрозам в інформаційній сфері мала би передбачати: 1) моніторинг інформаційної сфери, тобто системний аналіз чинників і агентів впливу на інформаційну сферу; 2) ранжування загроз, тобто встановлення пріоритетності загроз, реальних і потенційних небезпек; 3) профілактика і попередження негативного впливу загроз; 4) безпосередня протидія загрозам.

Тут не зайвим буде звернутися і до енциклопедичних визначень, перевірених численними теоріями і підходами практик, що доводять – для захисту національного інформаційного простору та важливо залучати адекватні методи і засоби з огляду на актуальні інформаційні та інформаційно-аналітичні технології, зокрема: 1) правове регулювання та контроль; 2) економічне (податкове, тарифне, митне тощо) регулювання та контроль; 3) державне ліцензування, сертифікація суб'єктів національного інформаційного простору та об'єктів інформаційної інфраструктури;

4) технічний та програмний захист; 5) криптографічний захист; 6) цілеспрямована протидія засобам ведення інформаційної війни [154, с. 714].

В Рекомендаціях парламентських слухань «Законодавче забезпечення розвитку інформаційного суспільства в Україні» [222], що відбулись в липні 2014 р., було зазначено проблемні сфери, в яких існують нормативні та практичні прогалини, деталізувались методи по забезпеченню інформаційної безпеки та рекомендувалось здійснити наступні конкретні кроки: 1) «сформувати ефективну систему забезпечення інформаційної та кібернетичної безпеки»; 2) «утворити координаційний орган для здійснення контролю та регуляції відповідної політики»; 3) «розробити проект Закону України про кібернетичну безпеку» [222]; 4) «напрацювати нормативну базу та здійснити організаційно-технічні заходи, необхідні для фіксування та використання у цивільному і кримінальному процесі даних, що були отримані за допомогою засобів ІКТ»; 5) «з'ясувати структуру власності компанії «Зеонбуд», «Київстар», «МТС», потенційні загрози у зв'язку з монопольним становищем цих компаній»; 6) «забезпечити координацію діяльності органів державної влади, їх ефективну взаємодію із засобами масової інформації та інститутами громадянського суспільства щодо розвитку вітчизняного інформаційного простору» [222]; 7) «впровадити програмне забезпечення вітчизняного виробництва в органах влади з метою забезпечення кібернетичної безпеки в Україні»; 8) «розвивати сучасну систему оперативного зв'язку між державними органами влади та органами місцевого самоврядування»; 9) «спростити запровадження комплексної системи захисту інформації в державних органах влади та органах місцевого самоврядування»; 10) «забезпечити захист від кіберзагроз критично важливих об'єктів національної інфраструктури, шляхом проведення аудиту інформаційної безпеки і запровадження відповідних вимог для підприємств усіх форм власності» [222]; 11) «створити єдиний національний ІТ-депозитарій (резервну копію «бекапу» критично важливих інформаційних ресурсів для держави)»; 12) «адаптувати системи захисту державних інформаційних ресурсів до вимог та стандартів ЄС з проведенням

тестів на проникнення критично важливих об’єктів національної інфраструктури тощо» [222].

Варто зауважити, що окремі зі згаданих напрямів реалізовані, інші перебувають на стадії реалізації, наприклад, у жовтні 2017 р. прийнятий Закон України «Про основні засади забезпечення кібербезпеки України», що «у системній кореляції з вирішенням питань захисту та забезпечення прав і свобод громадян, конституційних засад української держави, визначає необхідні основи безпеки України у кіберпросторі, а також державної політики у сфері кібербезпеки, координацію державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері» [419].

Проблемними все ж залишаються питання, пов’язані із науково-освітнім забезпеченням інформаційної безпеки. Це те інтелектуальне підґрунтя успішного розвитку національних інформаційних систем, без якого неможливо ані вирішити складних конкретних завдань у цій сфері, ані впровадити їх комплексне бачення. «Професійна освіта та організація наукових досліджень у галузі інформаційної діяльності», що визначена ст.15 та ст.16 Закону України «Про інформацію» [101], могла би суттєво посилити відповідну галузь. За напрямами пізнавального процесу в інформаційній сфері цей Закон називає: 1) професійну інформаційну освіту; 2) наукові дослідження інформаційної сфери; 3) просвітницько-інформаційне виховання [101].

Проте, на практиці ми бачимо, що медіа-грамотність, яка стала частиною освітніх програм на рівні середньої освіти західних країн, часто залишається об’єктом уваги та дій громадянського суспільства, а вітчизняні освітні інституції, державні установи недостатньо у минулі роки приділяли увагу цій галузі просвітницької роботи. Саме тому серед Рекомендацій вище згаданих парламентських слухань «Законодавче забезпечення розвитку інформаційного суспільства в Україні» наявні і такі: 1) «забезпечити оновлення матеріальної бази закладів освіти і наукових установ, що здійснюють дослідження і готують фахівців інформаційної сфери»; 2) «сприяти розвитку та впровадженню, зокрема в освітні процеси, новітніх комп’ютерних технологій» [222]; 3) «забезпечити викладення у

середніх загальноосвітніх школах правил роботи в соціальних мережах, участі у форумах, захисту персональних даних та мережевої етики з урахуванням сучасного стану розвитку ІКТ»; 4) «визначити пріоритети наукових і науково-технічних досліджень та розробок щодо становлення і розвитку інформаційного суспільства із соціогуманітарних, технологічних та інноваційних проблем» [222]; 5) «розвивати співробітництво суб'єктів господарювання з науковими установами та закладами освіти щодо розробки і впровадження інформаційних технологій, ресурсів, продукції і послуг»; 6) «забезпечити, з урахуванням рішень Національної академії правових наук України, виокремлення інформаційного права і права інтелектуальної власності в окрему наукову спеціальність тощо» [222].

Окрім новітніх викликів та реалій, що не врегульовані або не передбачені існуючим законодавством, не одне десятиріччя існують проблеми інформаційного простору, що потенційно становлять ризики і для інформаційної безпеки нашої держави. Серед них ми можемо виділити: 1) проблеми створення суспільного мовлення та приналежності засобів масової інформації фінансово-промисловим олігархічним групам; 2) проблеми законодавчого регулювання інформаційної діяльності в мережі Інтернет та поширення інформації у соціальних Інтернет-мережах; 3) проблеми авторського права за умов поширення Інтернет-технологій та ідентифікації джерел.

Питання професійної компетентності та моральної відповідальності журналістів також є на часі для інформаційного суспільства загалом та системи національної безпеки зокрема. При чому на проблему звертають увагу як незалежні аналітики, так і Національна спілка журналістів України. Фахівці стверджують, що сьогодні порушення етичних стандартів практично не мають жодних серйозних наслідків для відповідного ЗМІ чи журналіста/ів. З більшою ймовірністю такі вчинки нададуться до громадського розголосу і/або громадському осуду, розглядатимуться на зборах редакційних колективів, але не змінять загальну ситуацію безвідповідальності журналістів. Тут особливо відчутна нестача узгодженого Кодексу журналістської етики, а також ефективних механізмів контролю за його виконанням. Водночас навіть наявність такого кодексу, як

вказують експерти, не є гарантією його виконання. Адже спроб розробити такі документи вже налічується чимало, зокрема: Національною спілкою журналістів України у 1992, 1997, 2002 рр.; Національно експертною комісією з питань захисту суспільної моралі у 2010 р. Проте жоден такий кодекс не передбачає обов'язкового характеру та механізмів контролю за його додержанням. З боку держави, в чинному законодавстві теж фактично відсутні визначення відповідальності журналістів за порушення професійних приписів [228; 238].

2.2. Міжнародні норми та практика забезпечення інформаційної безпеки

Сьогодні основні для розуміння забезпечення міжнародної інформаційної безпеки міжнародно-правові норми закріплені у Статуті ООН, а також інших міжнародних нормативно-правових актах, що формують правовий базис для розв'язання збройних конфліктів, визначають засади міжнародного гуманітарного права, а також регулюють процес упередження та боротьби з міжнародним тероризмом. Таким чином, серед основних правових принципів, що пов'язані з міжнародними інформаційними відносинами в частині гарантування інформаційної безпеки називають такі: «принцип суверенної рівності держав у сфері використання інформаційних ресурсів, забезпечення інформаційного суверенітету держави та рівноправної участі в переговорних процесах щодо встановлення і кодифікації міжнародно-правових документів у сфері інформаційної безпеки»; «принцип невтручання у внутрішні справи інших держав, неприпустимість інформаційної інтервенції з метою проведення спеціальних інформаційних кампаній, ворожої пропаганди та поширення деструктивної чи спеціально спрямованої інформації» [269, с. 111; 439, с. 18]; «принцип заборони застосування сили або загрози силою, який забороняє використання інструментів інформаційного впливу проти територіальної цілісності чи політичної незалежності будь-якої держави»; «принцип мирного врегулювання міжнародних спорів, який зобов'язує держави до превентивної дипломатії або переведення збройного конфлікту на переговорний рівень за

допомогою інструментів інформаційного впливу» [269, с. 111; 439, с. 18]; «принцип територіальної цілісності та непорушності кордонів, який стосується визначення меж національного інформаційного простору та заходів захисту від несанкціонованого втручання ззовні»; «принцип дотримання фундаментальних прав і свобод людини, який визначає конституційні та спеціальні норми, а також норми міжнародних договорів щодо свободи слова та вільного обігу інформації, незалежності і плюралізму міжнародних мас-медіа, свободи вираження, заборони цензури та захисту конфіденційності інформаційних ресурсів» [269, с. 111; 439, с. 18]; «принцип самовизначення народів і націй, який встановлює права національних меншин на культурну самобутність та інформаційну діяльність; принцип міжнародного співробітництва, який зобов'язує держави співпрацювати задля зміцнення миру та міжнародного взаєморозуміння, розвитку глобальної інфраструктури з метою досягнення інтересів людства» [269, с. 111; 439, с. 18]. Отже, це комплекс політичних, економічних і соціокультурних принципів, важливих для міжнародного порозуміння.

Відповідна тенденція закріпилася і у резолюціях Генеральної асамблеї ООН, а саме Резолюція ГА ООН 53/576 (1998 р.) «Роль науки і техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим сфер»; Резолюція ГА ООН 54/49 (1999 р.) «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки»; Резолюція ГА ООН 55/28 (2000 р.) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки»; Резолюція ГА ООН 60/45 (2005 р.) «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» та багато інших [137, с. 11].

В резолюції 1989 р. № 44/21 Генеральна Асамблея ООН звернулась до всіх держав із закликом сприяти міжнародній співпраці «в усіх напрямах забезпечення міжнародної безпеки, підтвердила дієвість і значення Статуту ООН, необхідність дотримання основних його принципів, висловилась за співробітництво в рамках Організації та її основних структур» [268] з метою

знайти різноманітні «підходи до зміцнення принципів і систем міжнародної безпеки на основі нормативних документів ООН» [268].

У 1999 році на 54-ій сесії ГА ООН було прийнято оновлений проект резолюції (A/RES/54/49) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», який вперше вказав на загрози міжнародної інформаційної безпеки відносно не тільки до цивільної, але і до військової сфер. Поряд із зазначеним, за результатами роботи сесії було опубліковано проект «Принципів, що стосуються міжнародної інформаційної безпеки» (A/55/140У). Принципи є свого роду робочим варіантом кодексу поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов'язання, що також закладають основу для широких міжнародних переговорів під егідою ООН і інших міжнародних організацій з проблем міжнародної інформаційної безпеки (МІБ). У них міститься необхідна понятійна база з предмету МІБ, наводяться основні визначення: міжнародної інформаційної безпеки, погроз інформаційній безпеці, інформаційної зброї, інформаційної війни, міжнародного інформаційного тероризму та злочинності [28].

Фактично на рівні цих резолюцій йдеться про незастосування сили, але одночасно й небезпеки нового покоління інформаційної зброї, коли вкрай необхідна якісна система міжнародного контролю за інформаційними озброєннями. Передбачалося узгодити позиції світового співтовариства щодо проблеми потенційного воєнного використання інформаційно-комунікаційних технологій [269, с. 111], вдосконалення існуючих і нових систем озброєнь. У таких резолюціях помітно, як міжнародна спільнота шукає і нових методів для гарантій невтручання у внутрішні справи держав, що ускладнюється з розвитком власне інформаційних впливів. Тому розглядаються усі доступні можливості для створення міжнародної системи моніторингу інформаційних загроз, для забезпечення фундаментальних прав і свобод в інформаційній сфері, але й попередження випадків використання високих технологій з протиправною метою. Цей специфічний міжнародно-правовий режим інформаційної безпеки

відтак мусить передбачити оновлене міжнародно-правове регулювання інформаційної безпеки. Безпосередньо на рівні ООН це також кодифікація спеціальних принципів і норм, які склалися на основі Статуту ООН, а також оновлення існуючих і укладання нових угод у сфері інформаційної безпеки.

Упорядкування і стабілізація міжнародного співробітництва держав в інформаційній сфері – складне та багатогранне питання, що потребує окремого дослідження. Сучасні технології мають транскордонний характер, відтак і злочини стосуються міжнародної безпеки та стабільності в цілому, а не лише окремих систем права. І. Забара, наприклад, констатує функціонування двох провідних напрямів міжнародно-правового регулювання використання інформаційно-комунікаційних технологій: інформаційний («змістовний») та комунікаційний («технічний»). У міжнародно-правовій проблематиці інформаційної безпеки вони розглядаються з позицій протидії використанню ІКТ, що спрямовані на шкоду 1) основним правам і свободам людини та 2) критично важливим структурам держав [87].

Інформаційний напрям передбачає протидію транскордонному поширенню за допомогою інформаційно-комунікаційних технологій матеріалів, що суперечить принципам і нормам міжнародного права, розпалюють міжнаціональну, міжрасову, міжконфесійну ворожнечу, поширюють расистські, ксенофобські ідеї. Це письмові матеріали чи зображення або будь-яка демонстрація положень, які підбурюють до ненависті, дискримінації, насилля проти будь-якої особи або групи осіб. Такі дії, як слушно зауважують фахівці, можуть відбуватися і через використання інформаційної інфраструктури для пропаганди насильства, залякування, пригнічення, нав’язування певних моделей поведінки; для екстремістських та терористичних актів; повалення державного ладу тощо [86, с. 66]. Комунікаційний напрям передусім орієнтований на боротьбу зі зловмисним використанням комунікаційних систем та інформаційних ресурсів, що має негативний вплив на політичну, фінансову, соціально-економічну та інші сфери життя сучасного людства.

Відтак вчені і практики нині звертають увагу на охоронні та забезпечувальні норми як частину міжнародного інформаційного права, що розвиваю сучасну кібер-стабільність і кібер-мир (зокрема, окремі норми в Резолюціях ГА ООН «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур» №57/239 (2002), № 58/199 (2003), № 64/211 (2009), Декларації Еріче про принципи кібер-стабільності та кібер-миру (2009), Глобальній програмі кібербезпеки Міжнародного союзу електрозв'язку (2007) тощо [212, с. 48]. Безумовно проблематика потребує більш системного підходу.

Відтак, усвідомлюючи ті зміни суспільно-політичного життя, що спричиняє сучасне цифрове середовище, високі технології у сукупності з глобалізаційними процесами, Радою Європи підготовлено Конвенцію про кіберзлочинність. Вона відкрита до підписання у листопаді 2001 року, набула чинності 1 липня 2004 року, підписана Україною у квітні 2005 року та ратифікована у грудні 2006 року. Через цей документ міжнародна спільнота наголошує, що держави мають вжити усіх заходів, «для встановлення кримінальної відповідальності відповідно до їх внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це» (ст. 2) [144]. Зокрема йдеться про кримінальну відповідальність за правопорушення, пов'язані з незаконним доступом, нелегальним перехопленням і втручанням у комп'ютерні дані чи систему; також кіберзлочинами названо зловживання пристроями, підробку та шахрайство, пов'язані з комп'ютерами, дитяча порнографія, порушення авторських прав та деякі інші [144].

Відзначимо, що зрештою сьогодні співзвучна цим проблемам і нормотворчість в Україні. Вітчизняним законодавством визнано і достатньо точно визначено сутність таких небезпек як кіберзлочин (суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [418]); кібератака

(навмисні дії, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки і режиму функціонування комунікаційних і технологічних систем тощо [418]); кібершпигунство (шпигунство, що здійснюється у кіберпросторі або з його використанням); кібертероризм; кіберзагроза та багато інших пов'язаних явищ [418; 419].

У міжнародній площині, не лише ООН та Рада Європи займаються питаннями правового забезпечення інформаційної безпеки. До проблематики активно долучається все більше число міжнародних організацій. Наприклад, з ініціативи так званої «Великої вісімки» (на той час G8) у 2000 р. ухвалено «Окінавську хартію глобального інформаційного суспільства» [204]. У документі передусім сформульовано прагнення солідарними зусиллями (в державному і приватному секторах) ліквідувати міжнародний розрив в галузі інформації і знань, наблизити прогрес, «раціональний розвиток інформаційного суспільства» через політичне співробітництво. Хартія містить змістовні розділи щодо 1) використання можливостей цифрових технологій; 2) подолання електронно-цифрового розриву; 3) сприяння загальній участі у використанні сучасних технологій для досягнення взаємодоповнюючих цілей зі стійкого економічного зростання, підвищення суспільного добробуту, стимулювання соціальної злагоди, зміцнення демократії, транспарентного і відповідального управління, прав людини, розвитку культурного різноманіття, зміцнення міжнародного миру [204]; 4) подальшому розвитку зі створення безпечного і вільного від злочинності кіберпростору [204].

Глави держав і урядів 56 держав-учасниць ОБСЄ на саміті 2010 р. також приділили певну увагу проблемам інформаційного суспільства. Зокрема заради розвитку вільного, демократичного, загального і неподільного євроатлантичного і євразійського співтовариства безпеки, вони вкотре задекларували актуальність низи транснаціональних загроз. Відтак серед таких проблем як – тероризм, організована злочинність, нелегальна міграція,

поширення зброї масового ураження, незаконний оборот легкої і стрілецької зброї, наркотиків і торгівля людьми – на рівні виокремлено і кіберзагрози. Для протистояння їм, так само як і іншим небезпекам в військово-політичній, економіко-екологічній сферах, у галузі прав людини і основних свобод, необхідна все більша міжнародна єдність цілей і дій [420].

Водночас багато держав у розбудові власної систем інформаційної безпеки враховують не лише спільні орієнтири глобального розвитку, але також (а іноді й передусім): національні інтереси; накопичений досвід інформаційних протистоянь і захисту інформаційного суверенітету; реальні та потенційні загрози для конкретного суспільства, національної безпеки та безпеки держави; національні культурні й духовні цінності, традиції тощо. Не варто забувати й про об'єктивні фактори, які також унеможливлюють однакові підходи до проблеми у всіх країнах світу. Такими зокрема є рівень інформаційного розвитку країни, її технологічні потужності, підготовка до інформаційних викликів широких верств, суспільства, державних службовців, комунікаційні можливості тощо. Попередні застереження, висловленні світовими лідерами галузі про цифрову нерівність тут як ніколи доречні.

Демократичні держави, і тут ми цілком погоджуємося з дослідниками, справді володіють ширшими можливостями, розвинутішими правовими механізмами реалізації національних інтересів, в тому числі й в інформаційній сфері. На думку вчених, такі країни вигідно відрізняє: 1) чітке визначення пріоритетів національних інтересів в інформаційній сфері, 2) гарантування інформаційного суверенітету держави, 3) регламентація порядку використання національних інформаційних ресурсів, 4) створення загальної системи охорони та захисту інформації з обмеженим доступом, 5) поширення духовних та культурних цінностей на населення інших країн, 6) обмеження спроб зовнішньої інформаційної та духовної експансії. [11, с. 92].

Стратегії та тактики інформаційної політики та інформаційної безпеки держав у політико-правовому полі можуть відрізнятися. Часто науковці, як приклад у цьому зв'язку, наводять сучасний досвід Великій Британії.

Продумана, деталізована система забезпечення інформаційної безпеки цієї держави реалізується через дієві механізми захисту прав та свобод громадян у інформаційній сфері, гарантії діяльності медіа, громадських організацій. Водночас пріоритет національної безпеки тут також дуже виразний, тому в національних інтересах згадані вище суб'єкти за законом мають і чітко окреслені межі діяльності. Законодавчо регулюються питання захисту інформації, збереження державної таємниці, мереж і телекомунікацій, окремий Кодекс визначає практики доступу до урядової інформації [78].

Спільний європейський простір також зобов'язує держави-члени ЄС адаптовувати нормативно-правові положення до спільних вимог, які встановлені і в інформаційній сфері, а також готовність співпрацювати над розробкою спільних, в тому числі й ширших міжнародних стратегій (документів, інституцій, механізмів), які б зміцнювали довіру, прозорість й безпечність глобального інформаційного простору, узгоджували діяльність держав у спільному кіберпросторі. Україна також орієнтується на ці високі стандарти інформаційної безпеки.

Прикладом для наслідування в окремих аспектах інформаційної політики може слугувати й досвід ФРН. Тут ще у 2011 р. прийнята Стратегія кібербезпеки, створено Центр кіберреагування, узгоджена інформаційно-безпекова політика уряду та державного секретаріату, а також інших органів влади, активно розвиваються механізми захисту інфраструктури стратегічного значення, налагоджується двостороння співпраця державного сектору з приватним у боротьбі проти кіберзлочинності. Комплексний підхід, на думку фахівців, дозволяє федеративному уряду ФРН забезпечити оперативне виявлення, реагування та локалізацію інформаційних атак, системно захищати суспільство від деструктивних кібервпливів та небезпечних інцидентів, запроваджувати кращі інформаційні технології у всіх сферах суспільного життя, зокрема й розвивати електронну демократію тощо [78].

Нерідко у контексті осмислення різних досвідів становлення політико-правових відносин в інформаційній сфері вчені з пострадянського простору

наводять і приклад Франції. У цій країні велика відповідальність щодо регулювання відповідних проблем покладається на узгоджену діяльність Міністерства внутрішніх справ та Міністерства оборони, тобто є комплексна візія внутрішніх та зовнішніх інформаційних загроз, розуміння їх взаємозв'язаності. Політико правові механізми закладені в основу достатньо дієвої системи безпеки інформації та попередження комп'ютерних злочинів. Законодавчо окремо врегульовано питання про електронні комунікації, зокрема нормами забезпечується контроль за передачею інформації в радіочастотному просторі. Вчені загалом вирізняють два головні акценти у правовому забезпеченні інформаційної безпеки Франції: 1) захист національного інформаційного простору, в тому числі й обмеження іноземної присутності в інформаційній сфері; 2) культурна дипломатія інформаційними засобами, зокрема поширення національних інтересів у франкомовних країнах Африки, Азії та Латинської Америки [11, с. 93].

Сполучені Штати Америки спрямовують свою інформаційну політику на впорядкування інформаційних потоків у політичній, економічній та військовій галузях задля забезпечення збалансованості між державним контролем і свободою інформаційної діяльності. Сформовано законодавчу базу забезпечення інформаційної безпеки. Зокрема, йдеться про регламентацію основ такого забезпечення (закони «Про удосконалення інформаційної безпеки», «Про комп'ютерну безпеку», «Про комп'ютерне шахрайство і зловживання»); регулювання інформаційних відносин та порядок доступу до закритої інформації (закони «Про свободу інформації», «Про таємницю», «Про право на фінансову таємницю», «Про охорону особистих таємниць» «Про висвітлення діяльності уряду»). Наведені вище закони формують правову основу для прийняття підзаконних нормативно-правових актів, націлених на реалізацію єдиної державної політики у сфері інформаційної безпеки [11, с. 94].

Важливим інститутом забезпечення спільного стратегічного бачення у цій сфері є Департамент внутрішньої безпеки США (Department of Homeland Security), що в цілому реалізує координацію діяльності державних органів,

громадських і всіх приватних структур, які покликані до захисту інформаційного простору федерації та поширення цінностей інформаційної політики цієї наддержави за її межами. Особливо слід наголосити на позиції Сполучених Штатів стосовно ворожих дій в кіберсередовищі. Це – право використовувати будь-які засоби: дипломатичні, політичні, воєнні та економічні, які є адекватними і не суперечать міжнародному законодавству для захисту країни, союзників, партнерів та інтересів США.

Отже, говорячи про формування правових основ і гарантій міжнародної інформаційної безпеки, слід визнати, що наразі можна засвідчити різні позиції провідних держав сучасності щодо розуміння потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства. Зважаючи на це, на 54-й сесії Генеральної Асамблеї ООН було ухвалено оновлену резолюцію 54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», на підставі якої концепція світової інформаційної безпеки набула визнання як глобальна проблема сучасності. Мотивацією для прийняття резолюції стало усвідомлення принципово нових потенційних загроз для міжнародного миру під впливом науково-технологічного прогресу та глобальної взаємозалежності усіх сфер життєдіяльності міжнародного співтовариства. У цій резолюції державам-членам було запропоновано висловитися щодо проблем інформаційної безпеки, дослідити технології загроз у цій сфері, у тому числі протиправне застосування інформаційних і комунікаційних систем та ресурсів, розробити загальноприйнятні принципи, спрямовані на зміцнення безпеки та посилення боротьби з інформаційним тероризмом і злочинністю [81].

Втім питання на цьому вочевидь не було вичерпаним, а в нових інформаційних реаліях ще гостріше постало перед світовою спільнотою. Уніфіковані норми щодо правового регулювання міжнародної інформаційної безпеки стають необхідністю нашого часу, що характеризується всеохоплюючою глобалізацією і потужними антиглобалізаційними рухами, зростанням гострих протистоянь між ними, в тому числі й в інформаційному

просторі; порушенням територіальної цілісності і інформаційного суверенітету держав, поєднанням конвенційних і не конвенційних засобів сучасної війни; зрештою дрібними кіберзлочинами та масштабними хакерськими атаками, масованим інтелектуальним піратством тощо Тому вже 69-а сесія Генеральної Асамблеї ООН 2014 р. «вітає початок роботи» Групи урядових експертів з досягнень в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки, але також закликає усі держави-члени приймати до уваги її оцінки і рекомендації; вчасно інформувати про загальну ситуацію у сфері інформаційної безпеки, національні зусилля для її зміцнення, усіляко сприяти збереженню вільного потоку інформації, відповідально ставитися до використання інформаційно-комунікаційних технологій в конфліктах, політичних взаємодіях тощо [421].

Висновки до Розділу 2

Для нормативно-правового регулювання інформаційної безпеки України властива певна дезорієнтованість, фрагментарність, розпливчастість, недосконаліть чинного законодавства, що яскраво виявили анексія Криму Російською Федерацією у 2014 р. та стимуляція розвитку сепаратизму, пряма агресія на сході України і тривала війна України з маріонетковими структурами ЛНР та ДНР, фінансованими та підтримуваними Росією.

Складність законодавчого регулювання у інформаційній сфері пов’язана також з тим, що об’єктами такого забезпечення одночасно є особистість, суспільство та держава. Їхні інтереси збігаються лише частково. При чому забезпечення інформаційної безпеки особистості під контролем і державних органів, і правозахисних організацій, і міжнародних структур, натомість регламентація державної безпеки в інформаційній сфері переважно самої лише держави [11]. Тому захист інформаційної безпеки держави так потребує внутрішньої консолідації, об’єднання різних політичних сил, соціальних груп, окремих громадян для спільного позиціонування на міжнародній арені.

Проблеми правового регулювання інформаційних відносин в Україні пов’язанні як з інформаційною безпекою держави, так і з можливостями її швидкої подальшої інтеграції у міжнародну спільноту демократичних, модернізованих країн. Загалом правова політика України в інформаційній сфері ще за багатьма ознаками залишається декларативною, розпорошеною, змістовно невизначеною, несистемною, бюрократизованою. Великий вплив на неї мають закріплена система фінансово-промислових інтересів, застарілих комунікацій, інерційних суспільних мас. Однак на шляху до демократії, європейської інтеграції, у боротьбі з російською агресією, ця політика зазнає помітних реформ. На цьому складному шляху часто вирішення складних тактичних завдань, необхідність швидкого реагування на вкрай небезпечні інформаційні виклики, що загрожують навіть цілісності країни та суб’єктності держави, збагачує безцінним досвідом наше суспільство, консолідує довкола спільних цілей та стратегічних орієнтирів, які потенційно стануть важливою основою якісного політико-правового забезпечення інформаційної безпеки українських громадян, соціуму, держави. Такий досвід унікальний, він може скласти важливу частину загальноєвропейського, тож не варто також і недооцінювати потенціал вітчизняної політико-правової системи.

РОЗДІЛ 3

ГЛОБАЛЬНИЙ ХАРАКТЕР ТА СУБ'ЄКТ-ОБ'ЄКТНІ ВИМІРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Глобальний характер інформаційної безпеки: інституційні можливості та ризики

У визначенні поняття «інформаційної безпеки як різновиду безпеки національної, який орієнтований на забезпечення прав і свобод людини, зокрема в питаннях вільного доступу до інформації, на створення і запровадження безпечних інформаційних технологій, на захист права власності всіх учасників інформаційної діяльності», слід мати на увазі, що означена категорія має глобальний характер, а тому й потребує розгляду в системі глобального (світового) інформаційного простору. Зупинимось на цьому детальніше.

Сучасна цивілізація характеризується специфічним основним ресурсом її глобального розвитку – інформацією. Це, з одного боку, надає людству, окремим спільнотам та індивіду нові можливості для розвитку й творчості, але з іншого − формує нові виклики та ризики, подолання яких вимагає від усіх суб'єктів загальноцивілізаційного, національного, державного, громадського розвитку докладання додаткових зусиль, спрямованих на посилення ефективності саме інформаційного виміру безпеки. У наших інших розвідках ми констатували, що наскрізна інформатизація всіх «сфер життєдіяльності суспільства і людини вимагає сьогодні особливо уважного ставлення з боку філософів, політологів, науковців до специфіки глобального характеру проблеми інформаційної безпеки» [371, с. 87]. Ми погоджуємося з дослідниками, які вбачають на межі століть зміни в самому сприйнятті інформації сучасним суспільством, коли соціальне значення комунікаційних технологій суттєво оновило наше розуміння світового розвитку, а

«всепроникаюча у всі сторони життєдіяльності інформація» буквально трансформувала наші колишні уявлення про безпеку та пріоритети політичного життя. Це, приміром, знаходимо у зауваженні В. Ананьїна, який стверджує, що «в умовах тотальної інформатизації суспільства значну роль відіграють питання інформаційної безпеки» [12, с. 194].

Відтак досліджуючи політико-філософські аспекти інформаційної безпеки, важливо проаналізувати це питання, як зауважено в наших працях, «з точки зору глобального характеру функціонування сучасного цивілізаційного простору» [371, с. 88]. Річ у тому, що «глобалізований світ ставить перед національними спільнотами, державами і людиною нові виклики та загрози, які інтенсифікуються через активізацію глобальних інформаційних обмінів» [371, с. 88].

Цікаво, що «перед сучасною людиною і суспільством постає в цьому аспекті складна дилема: з одного боку, інформатизація та глобальний інформаційний простір дають нам безліч нових можливостей до подальшого розвитку в різних сферах суспільної життєдіяльності, а з іншого − через інтенсивність самих інформаційних потоків та бурхливий розвиток технологій інформаційного обміну постійно виникають нові загрози безпеці людини і суспільства» [371, с. 88]. Відповідно, виникає запитання про те, «як вирішувати цю дилему за умов, коли ми вже не можемо відмовитися від процесів інформатизації та глобалізації?» [371, с. 88]. До того ж це вочевидь різні рівні осмислення проблематики для молодих демократій і тих, що вже утвердили свій демократичний вибір та орієнтацію на плідну міжнародну співпрацю (європейську інтеграцію, економічне співробітництво, культурний обмін тощо). Якісне й ефективне забезпечення інформаційної безпеки держави залежить від низки факторів, які часто походять зі зовнішніх і навіть багатосторонніх джерел, тож тут складно говорити про рівні можливості чи універсальні правила політичної гри.

Питання гостро постало й для дослідників сучасних соціальних і політичних комунікацій, які також вивчають процеси глобалізації, що

супроводжуються інтенсивним використанням у економіці, культурі, політиці сучасних досягнень високих технологій. Науковці, наприклад О. Ющук, зазначають, що саме «розвиток інформаційних технологій призвів до зростання відносної важливості окремих аспектів суспільного життя» [287, с. 224]. Річ у тому, що «внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси» [287, с. 224]. Тому, продовжує вчений, «організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками, зросла впливовість засобів масової інформації» [287, с. 224].

Згадані фактори, як ми констатуємо в інших працях, «зумовлюють актуальність концептуально-теоретичного аналізу глобального характеру проблеми інформаційної безпеки» [371, с. 88]. Так, «з одного боку, такий характер дозволяє розробляти певні універсальні форми та механізми захисту конкретного інформаційного простору. З іншого − саме глобальний інформаційний простір, що схильний до надвисокої динаміки розвитку, дуже часто ставить перед національними системами безпеки виклики, на які важко відповідати таким локальним та регіональним суб’єктам, як держави, соціуми, місцеві громади» [371, с. 88].

Саме тому, продовжено у наших дослідженнях, «актуальність і висока значимість поставленої нами проблематики визначається тим, що сьогодні на всіх рівнях суспільного функціонування необхідно проводити постійний пошук доволі хиткого балансу між тими можливостями, що надає нам глобальна інформаційна цивілізація, і тими ризиками, що з’являються через неможливість контролювати тенденції і процеси інформаційно-соціального та інформаційно-технологічного розвитку» [371, с. 89]. Тобто сьогодні важливо розуміти як позитивні, так і негативні прояви цифрового світу, постійно розширювати горизонти залучення високих технологій в політичний процес, але прогнозувати і попереджати потенційні небезпеки, які можуть паралельно змінювати політичну картину світу.

На цю ж особливість, але у правовому аспекті звертають увагу вітчизняні правознавці, коли безумовно згадують сучасні переваги, наприклад, швидшої передачі інформації, збільшення її обсягів, можливостей для оперативного її опрацювання. Однак паралельно з тим, коли вони, зокрема Ю. Максименко, висловлюють тривогу з приводу «поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо» [177, с. 3]. Відповідно, продовжуємо ми у своїх дослідженнях, «глобальний характер таких загроз ускладнює вироблення механізмів їх нівелювання, адже сьогодні щодня виникають нові технологічні виклики, на які не можна відреагувати за допомогою застарілих методів захисту» [371, с. 89]. І зазначаємо, що «саме тому глобальний характер проблеми інформаційної безпеки постійно актуалізує дослідження різних вимірів даної проблематики» [371, с. 89], а тому і в нашому дослідженні доцільно детальніше проаналізувати «переваги та ризики переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції» [371, с. 89].

Ми вважаємо, що «насамперед, необхідно підкреслити абсолютно новий статус, що отримала інформація в рамках нової глобальної цивілізації» [371, с. 89]. Адже «інформаційний простір сьогодні не є виключно технологічним, віртуальним, контрольованим», а в сучасній цивілізації «перетворився на прості форми реальної суспільної життєдіяльності» [371, с. 89]. Причому «ми не використовуємо інформаційний простір, а живемо в ньому, підпорядковуючись абсолютно новим закономірностям розвитку, новим правилам поведінки, новим принципам виробництва і управління [371, с. 89]. В даний час особливо цінним є політико-філософський погляд на проблему, зокрема у форматі зауваження, яке робить С. Ягодзінський, що «інформаційні простори за своїми властивостями

вже не збігаються з просторами віртуальної реальності», адже «їх не можна вимкнути, вийти з них» [288, с. 77]. Тому, продовжує вчений, «інформаційний простір − це частина соціальної реальності, а отже він визначає параметри соціального простору і соціального часу» й «у такому розрізі феномен інформаційної реальності є предметом філософського та політологічного аналізу» [288, с. 77]. При цьому, ми вважаємо, що «такий аналіз також має проводитися з врахуванням нових реалій, виявляючи абсолютно нові за своєю сутністю можливості, ризики і суперечності, що визначають тенденції світового, національного і особистісного розвитку» [371, с. 90].

Переваги інформаційного суспільства сьогодні відчутні у більшості сфер суспільного життя, у політичному сенсу це шлях до прозорості урядів, демократичності рішень, полілогічності політичних дискусій тощо. Сучасні вчені, зокрема О. Золотар, навіть вбачають «своєрідну трансформацію інформації, яка в наш час ототожнюється з простором реальної взаємодії суб'єктів соціальної життєдіяльності» [117, с. 106]. В той же час, ми констатуємо, що «непристосованість до нових реалій несе в собі безліч ризиків, що призводять до складних суперечностей як в житті окремої людини, так і у життєдіяльності цілих соціальних спільнот, включаючи нації та держави, політичні утворення різного рівня, а також глобальну людську цивілізацію в цілому» [371, с. 90].

Як наслідок цього, ми аналітично констатуємо, що «саме через різноманітність та динамічну змінність тих викликів і суперечностей, що постійно виникають внаслідок розвитку інформаційного суспільства, сьогодні надзвичайно актуалізується концептуально-теоретичний аналіз глобального характеру проблеми інформаційної безпеки» [371, с. 90]. Відповідно, винятково «в такому її вимірі, з нашої точки зору, уможливлюється реальний пошук дієвих механізмів її забезпечення» [371, с. 90]. Новітні інформаційні та телекомунікаційні технології у сфері політики загалом та міжнародних відносин зокрема знову ж тісно пов'язують політичний і правовий контексти. Це одночасно формування нового глобального інформаційного середовища, та

збереження вже встановлених ціннісних орієнтирів, загальнолюдських сенсів і норм, підважування яких руйнує основи світової стабільності.

Тому для політології тут також важливі чіткі правові означення, які у системі інформаційної безпеки вбачають можливість для налагодження широкого міжнародного співробітництва, але також і протидію активізації раніше невідомих видів злочинності, попередження інформаційного протиборства між країнами. Тобто у контексті міжнародної безпеки та розвитку науковці, зокрема Р. Алямкін, пишуть «про розв'язання проблеми захисту інформаційних ресурсів, а також підвищення надійності та стабільності функціонування електронних засобів зв'язку, передовсім мережі Інтернет» [11, с. 91].

Саме внаслідок цього ми стверджуємо, що «при дослідженні проблеми інформаційної безпеки важливо враховувати її міжнародний і глобальний характер» [371, с. 90]. Окрім того, ми наполягаємо, що «варто говорити про можливості формування ефективної системи державної чи національної інформаційної безпеки без партнерства в цій сфері з іншими суб'єктами міжнародних відносин, державами, транснаціональними корпораціями, міжнародними організаціями» [371, с. 90].

Отже, нормативно-правові аспекти також збагачують власне політологічні візії проблематики. У цьому розрізі в одній із наших праць зазначено, що «сьогодні ключові геополітичні гравці глобального світу всіляко намагаються виробити ефективні правила співробітництва і партнерства з метою повноцінного використання переваг та нівелювання ризиків, що створюються завдяки переміщенню інформації у глобальному інформаційному просторі, що формується та розвивається під впливом інформаційної революції» [371, с. 91]. Політологічний аналіз орієнтує на інституційне забезпечення, регулятивне розмежування, а також загалом геополітичне, концептуальне розуміння основ міжнародного співробітництва під впливом сучасного інформаційного простору. Політологи пишуть про потребу «якісно нового бачення архітектури міжнародної безпеки», що у сьогочасних реаліях зазнає інформаційних спотворень і

маніпуляцій, деструктивних комунікаційних атак, інформаційного тероризму, та й загалом перебуває у полі невизначеності, перманентних змін, подвійних стандартів [240, с. 3].

Ці реалії міжнародної інформаційної безпеки безумовно позначаються й на потенціалі та межах національних систем, коли розвиток технологій випереджає державні потужності і ресурси для адекватного реагування на них, а міжнародні стандарти часто лише формуються та мають здебільшого декларативний характер. Водночас ми констатуємо, що «для України особливо актуальною проблемою є те, що в глобальному інформаційному просторі особливо підсилюється роль глобальних гравців, а менш впливові суб'єкти міжнародних відносин просто потрапляють в поле їх інформаційних впливів, перетворюючись на об'єкти» [371, с. 91]. Відповідно, ми постулюємо питання в аспекті національної інформаційної безпеки України про те «чи існує можливість запобігання цьому негативному виміру глобального інформаційного простору?» [371, с. 91].

Шукаючи відповідь на нього, зазначаємо, що «одним з ключових викликів і ризиків, що постають перед Україною в контексті глобального характеру проблеми інформаційної безпеки, є втрата власної національної ідентичності, державного суверенітету, особливо інформаційного суверенітету, який визнається сьогодні ключовою ознакою державної самостійності та правосуб'єктності» [371, с. 91]. З цього приводу погоджуємося з О. Дубасом, який «всебічне вивчення можливостей, потреб і специфіки інформаційного розвитку в сучасному світі та в Україні» [83, с. 3] бачить дійсним і важливим напрямком для збереження національних культурних і політичних особливостей, інструментом зміцнення діалогу культур, більше того – вагомим підготовчим етапом національної держави для «адекватної відповіді викликам і соціальним небезпекам, які таїть у собі глобалізація» [83, с. 3]. Науковий потенціал у забезпеченні національної системи інформаційної безпеки сьогодні несправедливо недооцінюється.

Таким чином ми констатуємо, що «одним з ключових вимірів проблематики інформаційної безпеки сьогодні є пошук адекватного балансу між впливами глобального характеру, що ґрунтуються на інтенсифікації

переміщення інформації в глобальному інформаційному середовищі, та потребами окремих людей та соціальних спільнот, в тому числі держав і націй, що не є провідними суб'єктами, здатними впливати на глобальні цивілізаційні тенденції та процеси» [371, с. 91]. Причому ми продовжуємо, що «не можна відкидати і переваги, що створюються завдяки більш вільному та швидкому переміщенню інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції» [371, с. 92]. Річ у тому, що «одна з таких переваг полягає в тому, що гарна поінформованість розвиває громадянські якості, що сприяє інтенсифікації розвитку громадянського суспільства в різних країнах і регіонах світу» [371, с. 92]. Вчені пишуть, що так звані «громадяни цифрового світу» порівняно менш байдужі у соціальних і політичних справах, вони не відсторонюються від інших, усвідомлюють значимість ефективних інститутів і функціональної системи; вони є частиною онлайн-світу, і саме його здатність поєднувати пасивних абсентеїстів і політично активних громадян дозволяє долати прояви неуцтва [37, с. 25]. Ми ж продовжуємо, що «в Україні також необхідно повноцінно використати «громадянський» ресурс глобальної інформаційної цивілізації», адже «такий ресурс може бути дуже корисний при реалізації різноманітних громадянсько-просвітницьких та освітніх проектів» [371, с. 92]. Особливо на тлі того факту, що «саме розвиток громадянських якостей людей, однією з яких є вміння фільтрувати складні інформаційні потоки, може стати в пригоді при протидії ризикам інформаційних впливів і агресивних дій» [371, с. 92].

В той же час, ми помічаємо, що «на фоні активізації громадянської активності, що відбувається завдяки простішому переміщенню інформації, створюються передумови і для значних негативних ефектів, одним з яких є загроза втрати національно-культурної ідентифікації» [371, с. 92]. Відповідно, «користуючись новітніми інформаційними технологіями, людина отримує безліч можливостей занурюватися в глобальне середовище цінностей і смислів, що повністю втратили національно-культурне коріння» [371, с. 92]. Соціологи в Україні, приміром Т. Рудницька, вже застерігають, що «користувачі Інтернету

становлять модернізовану групу, яка за своїми соціокультурними характеристиками значно ближча до представників інших культур у глобальному інформаційному просторі, ніж до українського населення, не охопленого Інтернетом» [243, с. 38]. Таким чином, ми аргументуємо, що «важливо в будь-якому аспекті дослідження проблематики інформаційної безпеки звертати увагу на такий подвійний вплив інформаційної революції, коли люди, отримуючи нові корисні можливості, втрачають важливий зв'язок з традиціями, що визначають їх національну, суспільно-групову, особистісно-духовну ідентичність» [371, с. 92].

Продовжуючи цю логіку, ми зазначаємо, що «в аспекті переваг та ризиків переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції, проблематика інформаційної безпеки має розглядатися в якості концептуального ядра, навколо якого вибудовується вся система сучасних соціальних, економічних, політичних, національно-безпекових відносин» [371, с. 92-93]. Суголосні нашим є міркування вчених, які в інформаційній безпеці вбачають елемент, з якого по суті вибудовується цілісна система національної безпеки. Так, Н. Крилова стверджує, що «в інформаційному суспільстві канали, мережі і системи інформації та комунікації стають, так би мовити, і нервовою, і серцево-судинною системою суспільства водночас», а тому «розробка та поширення інформаційних засобів впливу та мирні моменти співіснування відбуваються одночасно у межах інформаційної протидії» [156, с. 427]. Саме через це, продовжує вчена, «збереження стану рівноваги у стосунках, скоріше за все, і буде визначником інформаційної безпеки» [156, с. 427]. Завдячуючи цьому висновку, ми помічаємо, що «в умовах глобального характеру сучасних безпекових механізмів неможливо виносити інформаційну безпеку людини, соціуму, держави за межі глобально-цивілізаційних тенденцій», адже «ті суб'єкти, які готують інформаційні загрози, операції, війни, повноцінно використовують глобальний характер сучасного інформаційного середовища, застосовуючи всі можливі інформаційно-технологічні та психологічні можливості впливу» [371, с. 93].

Підсумовуючи, ми наполягаємо, що «важливо розуміти, що всі переваги та ризики переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції, безпосередньо пов’язані між собою» [371, с. 93]. Відповідно, для того «щоб скористатися перевагами, яких дійсно багато, необхідно вибудовувати таку систему інформаційної безпеки, яка б дозволила максимально нівелювати всі можливі ризики, реальні загрози та суперечності» [371, с. 93]. Причому серед переваг глобалізованого інформаційного простору традиційно, як вважає Н. Глебова, називають «науково-технічний і суспільний прогрес, міжкультурне співробітництво, підвищення рівня життя» [50, с. 26], кожна з цих позицій заслуговує окремого напрямку політичної активності, самостійного урядового порядку денного, розгорнутих і багатосторонніх суспільних комунікацій, які суттєво збагачують якість та зміст національної політики. Часто ми недооцінюємо або ж навпаки переоцінюємо наслідки інформаційних здобутків, коли ж натомість найефективнішим видається збалансований та максимально об’єктивний погляд на комплекс проблем.

Важливо, що тут не завжди доречним виглядають спроби масштабування цих проблем аж до загроз «втрати національної та соціальної автентичності», позбавлення свободи, «нової форми тоталітаризму», але цілком виправданими видаються вимоги виробляти спільні позиції, оновити підходи, напрацювати організаційно-правові, суспільно-економічні і комунікаційно-технологічні норми регулювання інформаційної сфери як у планетарному, так і в національному масштабах [50, с. 26]. У цьому процесі особливо цінними є такі політичні принципи та засоби як оперативність, розмежування рівнів комунікаційного контролю, чітке маркування джерел інформації, відкритість, але також і усування вразливостей до ворожих інформаційних потоків, стратегічна орієнтованість, організованість та координованість дій і взаємодій з глобальним інформаційним простором.

Враховуючи все це, Україна має затвердитися в глобальному цивілізаційному середовищі в якості конкурентоспроможного суб’єкта. Ми наполягаємо, що «для

цього дуже важливо використовувати всі інструменти ефективного розвитку, що надаються технологічним простором інформаційного суспільства» [371, с. 94]. Водночас ми стверджуємо, що «необхідно облаштувати надійну національну систему інформаційного захисту від безлічі інформаційних загроз, що йдуть від внутрішніх і зовнішніх впливів, а також з боку глобальних факторів небезпеки, притаманних самій структурі інформаційної цивілізації» [371, с. 94].

Все це дозволило нам аргументувати, що «перед українською державою на сучасному етапі державотворчих трансформацій постає складне завдання: максимально використати інформаційно-технологічні, соціально-структуруючі, масово-інформаційні можливості, що надаються інформаційної цивілізацією, і при цьому захистити власних громадян та державний організм від ураження з боку руйнівних і загрозливих зовнішніх і внутрішніх інформаційних впливів» [371, с. 94]. Ми погоджуємося з вченими, які серед обов'язків кожної держави називають і забезпечення вільного та незалежного функціонування засобів масової комунікації, і, як помічає Ю. Горбань, «дотримання стандартів свободи слова, інформаційних прав і свобод громадян» [51, с. 40], і захист національних інформаційних ресурсів, і створення розвинутого та сучасного інформаційного простору, конкурентоспроможного на світовому та національному ринках [263; 265]. Таким чином, ми з впевненістю наполягаємо, що «успішність та конкурентоспроможність нашої держави безпосередньо залежить від того, наскільки ефективну систему інформаційної безпеки вона вибудує на фоні значного зростання переваг та ризиків інтенсифікації циркуляції інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції та глобалізованої цивілізації» [371, с. 94].

Значну увагу у своїх публікаціях [375] ми відводимо питанню співвідношення контрольованих та неконтрольованих інформаційних обмінів, що відчутною мірою визначають можливості системи інформаційної безпеки ефективно функціонувати та динамічно розвиватися. Розмежування цих проявів пов'язуємо не лише зі сучасними специфічними українськими реаліями, але й зі загальною логікою та експлозивною природою інформаційної революції у світі,

коли інформація раптово стала невід'ємним елементом політичних, соціальних, економічних, освітніх, технологічних та інших структур. Навіть у сучасних підручниках зі соціально-поведінкових та правових наук зафіксована подібна думка. Її, приміром, ретранслюють Б. Остроухой, Б. Петрик, М. Присяжнюк, які констатують, що «постійне зростання впливу інформаційної сфери характерне для сучасного етапу розвитку суспільства» і «до структури цієї сфери входять: сукупність інформації, інформаційних зв'язків та інформаційних систем, об'єктів, які готують інформацію, зберігають, розповсюджують і використовують її, а також система регулювання інформаційних відносин» [121, с. 11].

Сучасні політологи розвивають цю думку, тож вже поряд з поняттям інформаційної революції з'являється неологізм – «блогерна революція», якій вже в новому поколінні політологічних словників Г. Шипунов дає таке означення: «організація за допомогою соціальних мереж та інших Інтернет-ресурсів (блоги, Facebook, Twitter, YouTube та ін.) масових антиурядових виступів, які можуть призвести до повалення чинного політичного режиму» [361, с. 28-29]. Водночас науковці також наголошують, що потенціал подібних явищ у перспективі не варто переоцінювати, адже і владні структури все частіше переходять на сучасні методики комунікації та поступово знаходять можливості для встановлення власного контролю у мережі інтернет.

Отже, не залежно від того, розглядаємо ми сьогодні проблеми державного функціонування, чи розподілу владних повноважень, чи партійного будівництва тощо – увесь традиційний комплекс політологічних питань потребує врахування глобального інформаційного фактору. Більш того йдеться про певну стійку залежність національної безпеки від інформаційної, при чому з постійним нарощуванням потенціалу останньої.

У цьому ж зв'язку майже недосяжною видається орієнтація на цілковиту контрольованість процесів інформатизації у суспільства. Глобалізація та технологічний прогрес постійно вносять корективи у будь-які форми сучасного держаного контролю, одним із найскладніших із яких видається саме інформаційний. Тому сучасні національні програми, стратегії політики у окремих

сферах, доктрини та декларації, якщо і орієнтують нас на певні основи інформаційної безпеки, все ж повинні передбачати можливість появи неконтрольованих, стихійних, несподіваних інформаційних загроз. Антикризові сценарії політики вже не проста формальність, але необхідний запобіжник руйнуванню цілісності систем, певна гарантія забезпечення життєдіяльності держави, суспільства, громадян.

По-справжньому важливо тут і держслужбовцям, і виборним політикам, і громадським активістам та аналітикам усвідомлювати тотальність інформатизації життя сучасних людей (але й не забувати про фактор цифрової нерівності). Тобто йдеться про «чинник, який присутній у кожній сфері життєдіяльності суспільства», а відтак й про інформаційну безпеку «як одну з провідних» у системі національного розвитку [7, с. 227]. Збалансувати контрольовані та неконтрольовані інформаційні обміни, передбачати останні, запобігати їх шкідливим слідам у політичному житті – необхідна вимога інформатизованого суспільства. У політичній сфері на різних рівнях гостро постає питання кадрового забезпечення відповідної вимоги, тобто підготовки та збереження у системі високопрофесійних спеціалістів, яких би відрізняли вузькоспеціалізовані та загальні компетенції. Однак всеохопність та глобальний характер інформатизації ускладнює навіть саму можливість пошуку таких фахівців. Системи, які перебувають під постійним впливом неконтрольованих інформаційних посилів, імпульсів й обмінів, навіть за високого ступеня захисту від вразливостей, вочевидь не можуть передбачити всього розмаїття можливих проблем. Самі ж фахівці не завжди оперативно, точно і компетентно можуть відповісти на всі ті виклики, на які наражаються інститути інформаційної безпеки, тож тут як ніколи важлива вдумлива кадрова, освітня політика та захист наукового знання.

(Не)контрольованість інформаційних потоків є досить неоднозначним явищем, що характеризує загалом сучасне глобальне середовище. Протидія неконтрольованим інформаційним потокам може іноді розцінюватися як загалом протидія глобалізації та знищення демократичного устрою. Адже глобалізація є

одним із можливих чинників запобігання авторитаризму в окремих державах, обмеження тотальної узурпації інформаційного життя громадян окремих суспільств. У своїй сукупності і взаємодії вони складають основи сучасного, прогресивного глобального інформаційного простору, але розцінюють цей простір не всі наукові однаково. Так, Н. Глебова стверджує, що «соціальний зріз глобального інформаційного простору характеризує соціальне спрямування економічних, політичних, культурних й інших процесів, що відбуваються у відкритому суспільстві» [50, с. 24]. Тому, продовжує вчена, «об'єднуючись на міжнародній арені із системою міждержавних відносин, глобальний інформаційний простір є, з одного боку, самостійною сферою зіткнення зовнішньополітичних інтересів держав у сфері міжнародних відносин, а з іншого – об'єктом і засобом реалізації цих інтересів у системі міждержавних відносин» [50, с. 24]. Тут майже завжди науковою та експертною громадськістю підіймається питання суверенітету. Адже тонка межа між власними інтересами держави, певним інформаційним суверенітетом, з одного боку, та необхідністю вступати в міжнародні інформаційні обміни (часто неконтрольовані, непередбачувані, загрозливі), з іншого, зобов'язує все глибше аналізувати політичні проблеми крізь цю суперечливу візію. Все це означає, що прийняття політичних рішень тепер залежить від вміння віднаходження власної ніші у контексті інформаційної прозорості та відкритості, однієї сторони, та безпеки, з іншої сторони.

Однак не слід гіперболізувати і практику балансування як універсальну можливість життєдіяльності суспільства та держави у глобальному світі. Важливо зважати й на інші політичні інструменти і техніки, які довели свою ефективність на практиці. Однією з таких є активізація, тобто максимально активна позиція, якою провідні країни світу фактично формують нині порядок денний глобального інформаційного простору. Такий підхід дозволяє наповнювати навіть неконтрольовані інформаційні потоки корисними і зручними сенсами, а контрольовані – очолювати та модерувати. Активізація власної інформаційної позиції є важливим напрямком розвитку України як самостійного і впливового

геополітичного гравця, який швидко інтегрується у цивілізовані форми міжнародного співробітництва. Політологи у цьому питанні бувають досить однозначними. Зокрема О. Проскуріна ще задовго до подій 2014 р. писала, що «настав час відмовитися від ролі «губки», котра пасивно споживає інформацію, яка подається розвиненими країнами і далеко не завжди прийнятна для внутрішнього використання в країні» [230, с. 141]. Власні правила гри, конкурентоспроможні стратегії та політичні пропозиції, напрацьовані канали комунікації, виразні інформаційні матеріали – ці та інші інструменти політики України в рамках глобального інформаційного простору лише посилять державу серед суб'єктів регіональної і міжнародної діяльності. Це один із дієвих та перевірених шляхів унезалежнення від непередбачуваних впливів і неконтрольованих інформаційних обмінів.

Загалом сьогодні активізація позицій на міжнародній арені передусім передбачає розробку стратегії інформаційної безпеки держави. Йдеться про комплексне бачення, що поряд з існуючими нормами та встановленими закономірностями інформаційного розвитку сучасного світу, передбачає також неконтрольовані, емерджентні фактори, потенційні виклики і загрози. Ця глибока та багатоскладова аналітична розробка повинна зрештою зважувати два важливі чинники, на які вказують вчені. Серед них, як констатує Н. Глебова, треба виокремлювати такі положення-питання, згідно з якими: 1) поза глобальним інформаційним простором Україна не зможе існувати як повноправний суб'єкт міжнародних відносин, тому вагомим орієнтиром інформаційної стратегії України повинне слугувати «просування через інтеграцію в цей простір» [50, с. 24]; 2) втрата ж культурної та національної самобутності в процесі інтеграції є особливо загрозливою, тому не менш значимий напрям стратегії – прагнення зберегти цю самобутність, «цивілізаційну та культурну ідентичність у процесі соціально-економічної й політичної модернізації, яка має тенденцію до універсалізації» [50, с. 24].

Детальніший погляд на проблему свідчить про суперечливість та взаємозалежність цих орієнтирів, адже глобальний характер проблеми

інформаційної безпеки хоч і ускладнює механізми інформаційного захисту окремих спільнот і держав, але також допомагає вийти на новий рівень боротьби з існуючими загрозами, переймати кращі практики, а відтак й розвивати кращі національні традиції, пропагувати історичні надбання, інтелектуальні й культурні здобутки вже за допомогою сучасних технологій. До того ж і контрольовані, і неконтрольовані інформаційні потоки часто тісно пов’язані між собою, серед них буває складно відрізнити національні, локальні та зовнішні, ворожі атаки, тож без спільних та узгоджених дій демократичного світу напрацювати та навіть просто зафіксувати в національних законодавствах відповіді проблеми досить складно. Тут потрібні спільні та взаємно вигідні стратегії інформаційного спротиву.

Попри це формулювання стратегії інформаційної безпеки держави дійсно залежить від активності держави стосовно напрацювання контрольованих нею інформаційних потоків. Саме активність державних організацій у справі створення власного конкурентоспроможного інформаційного продукту визначає здатність досягати своїх цілей у глобальному інформаційному середовищі. Вчені наголошують, що визначальним у сучасній «інформаційній і комунікаційній ері» є медіа, а також більш широка проблематика виробництва, поширення, володіння, маніпулювання інформаційними технологіями. Саме з цього приводу О. Зернецька стверджує, що питання «хто, з якою метою, з якими намірами володіє каналами комунікації, контролює їх − відіграє вирішальну роль у трансформації розвитку суспільства, забезпечення миру та справедливості в сучасну епоху» [116, с. 26]. Заміщувати неконтрольовані інформаційні виклики, витісняти шкідливі впливи, випереджати загрозливі атаки – усе це комплекс реакційних тактичних заходів і завдань зі стратегічного бачення інформаційної безпеки, натомість заповнювати інформаційне середовище щонайбільшою кількістю контрольованих та суспільно важливих обмінів – ознака максимально збалансованої та продуманої стратегії держави у цій галузі. Активна позиція відрізняє лідерів інформаційного простору на міжнародному ринку, а також успішні держави у глобалізованому світі.

Успішні стратегії у цій галузі відрізняє розуміння інформації як управлінського ресурсу, як корисного інструменту взаємодії (при чому як у глобальному світі, так і на внутрішньому суспільно-політичному ринку). Таке розуміння, а найголовніше – його практичне втілення у політиці передбачає, що інформація має відповідно збиратися, аналізуватися, продукуватися та зрештою організовуватися. Структурована та функціонально розподілена вона стає потужним статусним інструментом політичної влади та державної безпеки, вона унормовує відносини і процеси в політиці, збагачує політичний світогляд та політико-правову культуру суспільства. Сучасне державне управління, місцеве самоврядування, політичне адміністрування складно організувати без здійснення впорядкованої, системної, чітко орієнтованої політики, що базується на принципах грамотної роботи з інформацією та інформаційної безпеки. До того на рівні держави і громадянського суспільства це система розгалужена, коли контрольовані інформаційні обміни додають ефективності, взаємної користі та стабільності партнерським відносинам.

Ось як про це пишуть такі авторитетні вчені, як А. Марущак: «Рух інформації в системі управління, як правило, характеризується складністю і розгалуженістю […] Жодна з функцій управління не може забезпечувати підтримки заданих параметрів системи без налагоджених і постійних потоків інформації. Організаційна структура інформації являє собою невід'ємну, органічну частину системи управління, що забезпечує комплексну та ефективну взаємодію всіх її елементів» [185, с. 15]. Втім не кожна держава здатна ефективно використати такий важливий інструмент політики як інформацію. Передусім це (а не тільки рівень економічного розвитку) залишає не лише існуючі державні інститути, але часто й усе суспільство за межами сучасного цивілізаційного й культурного контекстів, поза основних тенденцій соціального, технологічного, політичного розвитку. Пасивний суб'єкт глобальної та регіональної міжнародної політики та економіки вирізняє передусім невміння комунікувати й контактувати, відсутність ініціативи, неспроможність до партнерства, відстороненість від глобальних проблем.

Державна неспроможність позначається і на світогляді людей та ефективності окремих громадських ініціатив. Ми неодноразово наголошуємо, що саме «через нездатність держави здійснювати власний інформаційний суверенітет, контролювати основні інформаційні потоки, що впливають на внутрішню і зовнішню політику та інші сфери соціального функціонування, значних втрат зазнають її громадяни» [375, с. 131]. У цьому зв'язку дуже доречно згадати соціально-поведінкові та власне психологічні підходи до цієї проблематики, зокрема зауваження такого вченого, як А. Лазаревич, згідно з яким «у рефлексивну природу свідомості дедалі активніше втручаються елементи штучного мисленнєвого конструювання неіснуючої у природі дійсності. Свідомість працює не з образами об'єктивного світу, а з образами образів, зумовлених у кращому випадку певними інформаційними блоками, а в інших – просто уявленням, відчуттям реального чи очікуваного задоволення, навмисними або ненавмисними оманами і т. ін.» [162, с. 300].

Підміна реального бажаним чи нав'язаним здійснюється через агресивний і безперервний інформаційний вплив. Таким впливам свідомість окремої людини може протистояти за рідкісними випадками. Здебільшого ж системні інформаційні атаки ворога формують некритичне сприйняття дійсності, байдуже або й конфронтаційне до власної державності суспільство. Саме тому інформаційний захист громадян належить до відповідальності держави. Безумовно йдеться про комплекс заходів у сфері освіти, культури, науки, зовнішньої політики, та загалом у системі контрольованості інформаційного простору. Окрім внутрішніх ризиків тут варто враховувати й позасистемні впливи, ворожі інформаційні загрози, специфіку глобального інформаційного простору, що значною мірою визначає світоглядні орієнтири нашого сучасника.

Навіть з метою здобуття і збереження впливових та авторитетних позицій в очах власних громадян будь-якій державі важливо вибудовувати продуктивні відносини та ініціювати комплексні рішення на міжнародній арені. Проблематика активної діяльності держави в сфері міжнародної інформаційної безпеки актуалізована у праці дослідниці відповідних політичних відносин і

процесів Є. Макаренко [174]. У ній питання презентується у складному зв'язку нормативної впорядкованості та контрольованості значних інформаційних потоків, громадської безпеки та суб'єктності держави на міжнародній арені, адже вчена стверджує, що «взаємозалежність […] інтегрованого світу приводить до необхідності забезпечення його інформаційної єдності і транскордонного переміщення зростаючих потоків інформації» [174, с. 17]. Тому, продовжує вона, «в інформаційну епоху закономірно зростає значення політики правового регулювання міжнародного обміну інформацією, яка є могутнім інститутом формування громадської думки і впливає через нього на зовнішню і внутрішню політику держав» [174, с. 17].

Отже, самої лише вдало прописаної стратегії не достатньо для забезпечення інформаційної безпеки. Велике значення відіграє процесуальний, діяльнісний аспект політики. Держава як член впливових міжнародних структур і організацій, як захисник інтересів власних громадян, як регулятор інформаційних потоків і відносин на управлінському, нормативному та адміністративному рівнях дозволяє говорити про чіткі орієнтири та саме активницьку (підкріплену конкретними діями і послідовними заходами) стратегію інформаційного захисту. Активницька стратегія не допускає формалізму, узурпації, ізоляціонізму, вона створена для громадян та інститутів, що забезпечують повноцінний розвиток суспільства, вона окреслена у практиці конкретних політичних дій та обмежена зрозумілими і прозорими правилами політичної взаємодії. Така стратегія глобалізована та орієнтована на національний інтерес одночасно.

У нашій роботі ми невипадково актуалізуємо поняття демократичної трансформації та політичної модернізації, адже описані вище прагнення та орієнтири щодо подальшого регулювання інформаційних потоків і обмінів видаються неможливими без достатнього рівня демократії у державних органах та суспільних організаціях. Інституційний вимір забезпечення інформаційної безпеки мислиться невіддільно від світоглядного, коли існуючі політичні відносини, процеси, цінності, вибудовані умовно за «демократичними

мірками». Натомість сучасні автократичні, закриті, бюрократизовані, неопатримоніальні, кланові, корупційні політичні системи містять додаткові вразливі елементи, що надаються інформаційним впливам. У своїх роботах на цьому наголошує, наприклад, дослідник спеціальних інформаційних операцій О. Литвиненко, який стверджує, що «захист від інформаційних впливів та спеціальних інформаційних операцій може забезпечити лише відкрита ідейна система, тобто така, що не концентрується на собі, а прагне до найбільшого поширення, доки вона не втрачає привабливості для оточуючих» [166, с. 131]. Причому, продовжує вчений, «альтернативою цьому може бути тільки застосування найжорсткіших, майже тоталітарних методів контролю, які до того ж дають доволі короткотривалий або обмежений ефект» [166, с. 131]. Демократичний політичний режим відтак мислиться як надійна основа ефективної та довгострокової системи інформаційної безпеки.

В Україні контрольованість інформаційних обмінів відчутною *мірою залежить від успішності демократизаційних перетворень*, від встановлення та збереження таких політичних інститутів, механізмів і соціально-політичних відносин, які характерні для правової держави, від громадянської ініціативності та партнерства, від солідаристських прагнень та численних діалогічних платформ. Реалістична, дієва, адекватна викликам сучасності та потребам суспільства стратегія інформаційної безпеки у будь-якому разі повинна захищати однаково як державний суверенітет, так і права громадян. Ці змісти не можуть бути лише декларативними, вони взаємодоповнюють один одного на практиці, передбачають людські та інституційні виміри.

Тут варто знову повернутися до завдання сучасної держави захищати права і свободи своїх громадян. Вочевидь це завдання прямо чи опосередковано пов’язане і зі суверенітетом, і з державною незалежністю, і з дієвою стратегією міжнародного позиціонування. Адже сучасні загрозливі інформаційні впливи передусім спрямовані на свідомість та психічне здоров’я конкретного індивіда, при чому сучасні технології таргетування цільових аудиторій аж до конкретної людини дозволяють відносно легко та недорого маніпулювати навіть

освіченими людьми. Неконтрольовані інформаційні потоки є часто причиною неконтрольованих дій людей, їх поганого самопочуття, безініціативності, репресивності, байдужості до суспільно-політичного життя. Однак через багатоаспектність цього чинника відповідні причино-наслідкові зв'язки оперативно довести досить складно.

У цьому контексті привертають увагу сучасні дослідження проблем інформаційного насильства, тобто цілеспрямованого впливу на (під)свідомість людини, зокрема через застосування інформаційних атак, розповсюдження вигадок, неправди, напівправди, пліток, дестабілізуючої інформації. Це часто повторювані дії, тобто шокуючі інформаційні впливи, що мають багаторазовий ефект – в момент первинного споживання інформації, пізніше через її активне обговорення, численні інтерпретації, масові дискусії. Ось як про це пишуть фахівці, зокрема О. Дзьобань і В. Пилипчук: «Сучасна людина піддається інформаційному насильству за день сотні разів. Нас умовляють, зазивають, наполегливо намагаючись переконати: що потрібно одягати, на чому смажити, чим лікувати... Радіо, телебачення, газети, журнали нав'язують своє розуміння життя. Звичайно, ці продукти сертифіковані, але небезпечний не сам продукт, а реклама. Вона створює імідж, образ, стереотип мислення. Ми купуємо не певний продукт, а шматочок «іншого життя». Реклама не є логічною, і саме ця алогічність і створює маніпулятивний ефект, що загрожує нашому психологічному здоров'ю» [74, с. 73]. Зауважимо лише, що сучасні маркетингові прийоми все активніше використовують у політичних цілях, а інформаційне насилля стало буденним інструментом політики окремих урядів та політичних сил. Контроль держави над подібними інформаційними обмінами є безумовним пріоритетом національної безпеки.

У своїх дослідженнях ми часто акцентуємо, що подібного характеру індивідуальні стреси, невротичні розлади окремих людей дуже швидко екстраполюються на громадський, державний, національний рівень. У сучасному глобалізованому та інформатизованому світі це більше не проблема особистісна чи сімейна, якщо вона спровокована масованими інформаційними атаками (тобто

має чітко виражене соціальне походження). Цілеспрямовані впливи на (під)свідомість людини загрожують реальній безпеці суспільства, держави, громадянських структур, це атаки моральних та ціннісних основ демократичного співжиття. Відтак і формується гостра необхідність такої політики, за якої критичне число контрольованих інформаційних обмінів в державі переважало над кількістю інформаційних потоків і каналів, які не піддаються жодному контролю.

Безумовно успішні політичні практики у цій галузі засвідчують, що така державна політика має забезпечуватися симетрично – високими інформаційними технологіями, продуманими стратегіями, комплексом оборонних та запобіжних заходів. Зазвичай це дороговартісні, ресурсозатратні, комплексні механізми та програми, про які варто подбати заздалегідь, при цьому враховувати їх вплив на індивідуальну, групову, масову свідомість. Для цього науковці пропонують розрізняти джерела, канали, технології впливу на психологію і поведінку людей, які використовують ворожі сили, щоб адекватніше реагувати на них або й випереджати загрози. Серед таких О. Юдін і В. Богуш, приміром, називають: «засоби масової інформації і спеціальні засоби інформаційно-пропагандистської спрямованості»; «глобальні комп'ютерні мережі і програмні засоби швидкого поширення в мережах інформаційних і пропагандистських матеріалів»; «засоби і технології, що нелегально модифікують інформаційне середовище, на підставі якої людина приймає рішення»; «засоби створення віртуальної реальності»; «чутки, міфи і легенди»; «засоби підпорогового семантичного впливу»; «засоби генерування акустичних і електромагнітних полів» [285, с. 178]. Ідентифікація проблем та їх джерел у політиці – важлива і концептуально-теоретична, і практична мета. Тому інформаційна безпека держави залежить від розуміння стратегій і тактичних дій різних суб'єктів у цій сфері, розпізнавання внутрішніх і зовнішніх деструктивних впливів, а також від загального означення ключових понять.

У глобалізованому світі, визначаючи поняття «інформаційного впливу», важливо окреслити його суб'єктну складову, основні діяльнісні сили. Тобто

важливо не безособлювати відповідні напади, розпорошуючи відповідальність за деструктивні дії. Вплив інформацією у кожному конкретному випадку здійснюється конкретним суб'єктом політики, керується його цілями та інтересами. Цілком ймовірно, що результати інформаційного впливу можуть бути непередбачуваними чи диверсифікованими, але це не спростовує суб'єктивного фактору та персональної відповідальності за такі рішення/програму/вчинок.

У сучасних дослідженнях інформаційний вплив дослідники, як приміром Є. Скулиша, трактують як «організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини» [123, с. 10]. При цьому вже традиційно розрізняють інформаційно-технічні та інформаційно-психологічні впливи, які щоправда однаково потребують і компетентних суб'єктів дії, і відповідних ресурсів. Для політичної системи загалом та для держави зокрема це не означає виключно пошук винних, тобто відповідальних за інформаційні атаки суб'єктів. Окрема відповідальність природно лежить на державних органах, покликаних випереджати загрози та формувати стійку до чужорідних інформаційних впливів систему національної безпеки.

Однак розбудова такої системи все ж мусить виходити з індивідуальних особливостей людини. Численні приклади інформаційних атак беруть початок з технічної помилки всього однієї людини чи з прояву вразливості психіки однієї особистості. Людський фактор політики тут дуже виразний, а відповідна закономірність політології вкотре доведена в нових інформаційних умовах. Попри те, що людство покладало великі надії на високі технології як рушій прогресу, як чинник утвердження цивілізованих форм політики, саме людина (з її потребами, ідейними переконаннями, психологічними особливостями, рівнем освіти, віруваннями, традиціями, здатностями інтелекту) залишається визначальним рушієм суспільно-політичних змін. Тож доки сучасні технології

не освоєнні достатньою мірою пересічним споживачем інформації, доти деструктивного елементу в політиці від інформаційних впливів не уникнути.

Співзвучні нашим міркуваннями зауваги В. Отрешко, яка детальніше розглядає ці особливості політичної свідомості громадян, різні моделі поведінки людей, які відрізняють їх за схильністю до різних інформаційних впливів, за спроможністю здобувати, аналізувати та давати оцінки. Зокрема, дослідниця зазначає, що «загальним джерелом зовнішніх загроз інформаційній безпеці особистості є та частина інформаційного середовища суспільства, яка через різні причини неадекватно відображає дійсність», а тому «інформація, що вводить людей в оману, не дає можливості адекватно сприймати своє оточення і себе» [210, с. 320]. Вчена продовжує, що «внутрішні джерела загроз інформаційній безпеці особистості закладені в самій біосоціальній природі психіки людини, в особливостях її формування та функціонування, в індивідуально-особистісних характеристиках індивіда, механізмах сприйняття та переробки інформації» [210, с. 320].

Отже, «людиновимірний» рівень інформаційної безпеки вкотре орієнтує нас на значимість освітніх і просвітницьких систем та заходів, (не)формальних структур, що діють у просторі науки, культури, особистісного розвитку. При чому все ж особливу роль у протистоянні деструктивним зовнішнім та негативним внутрішнім інформаційним впливам відіграє саме державна система освіти. Своєчасно незасвоєні уроки демократії, громадянської культури, конституціоналізму, правосвідомості серед населення формують вразливе до інформаційних атак середовище, що може становити сьогодні загрозу не лише для певного режиму чи устрою, не тільки для конкретного суспільства, але й для глобалізованого світу загалом.

Втім варто також конкретизувати зовнішні інформаційні загрози, що свідомо формують одні суб’єкти інформаційних відносин щодо інших; тобто у контексті проблем глобалізації доречно увиразнити ті інформаційні впливи, що виходять з різних форм інформаційної експансії. У політичній науці вирізняють декілька класифікацій таких деструктивних впливів. Нашу ж увагу привернули окреслені

вітчизняними вченими зовнішні джерела інформаційної небезпеки, зокрема, як зазначають Я. Малик і О. Береза: «діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері»; «політика домінування деяких країн в інформаційній сфері»; «діяльність міжнародних терористичних груп»; «розробка концепцій інформаційних війн будь-якими структурами»; «культурна експансія у відношенні до конкретної країни» [179, с. 24]. Кожна з цих форм достатньо глибоко вивчена сучасними аналітиками, зокрема західними, адже йдеться про напрацювання дієвих інструментів протидії реальним загрозам безпеці. З іншого боку, деякі зовнішні інформаційні впливи з часом дещо деформуються, змінюють впізнаванні параметри, через що їх складніше ідентифікувати, а отже й важливо продовжувати аналізувати усіма доступними засобами. Не виключено, що навіть напрацьовані кращі стратегії запобігання інформаційним загрозам не можуть бути удосконаленими, зокрема із залученням тих же високих технологій у процес аналітики.

Національна стратегія інформаційної безпеки України вочевидь мусить враховувати ці зовнішні фактори, їх гнучкість та періодичне оновлення. Модернізація у цьому сенсі означає постійний моніторинг та звірення проголошених орієнтирів з реальністю, це також збереження та нарощування засобів інформаційного впливу всередині суспільства і за його межами, це ефективне регулювання інформаційної сфери з використанням кращих інструментів і останніх доведених практикою дієвих технологій. Політична модернізація інформаційної сфери мусить не лише наздоганяти визнані й зразкові світові моделі, але й паралельно випереджати загрозливі інформаційні атаки, що часто потужніші у своєму технологічному потенціалі за наявні в перехідному суспільстві ресурси політики.

В умовах зовнішньої агресії нерідко навіть продукування українського інформаційного продукту може перебувати під активним впливом закордонних чинників, що вносить стихійність у модернізаційні плани та стратегії. Вчені, зокрема О. Гіда, зауважують, що і «постійні зовнішні вимоги щодо забезпечення відкритості інформаційного простору України для інформаційних потоків з-за

кордону часто переростають в активне втручання окремих іноземних держав у внутрішнє життя країни» [48, с. 334-335]. З цього приводу О. Ф. Гіда продовжує, що «нерідко інформаційні атаки мають на меті дискредитацію національних традицій і цінностей українського суспільства, посягають на культурне надбання народу, нав'язують країні чужі пріоритети та ідеологію, розпалюють протестні настрої серед населення» [48, с. 334-335]. Можливість протистояти подібним загрозам передбачає потужні ресурсні витрати, ефективну систему менеджменту, найновіші технології. Серед країн-лідерів у цій сфері складно змагатися, водночас вибудовування національних систем інформаційної безпеки є беззаперечною цінністю демократичного транзиту. Визначаючись з пріоритетами та перспективами, навіть молодим демократіям сьогодні варто особливо вкладатися у цю галузь, що має довгострокові орієнтири.

Поряд із цим чимало дослідників наполягають, що сучасні реалії фактично зобов'язують українське суспільство максимально переорієнтуватися лише на боротьбу з деструктивними впливами, зовнішніми інформаційними загрозами, і саме у такий оборонний спосіб вибудовувати стратегію національної системи інформаційної безпеки. З цього приводу В. Гурковський зазначає, «за умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір» [62, с. 28]. Водночас незайвим тут також буде додати, про чий саме інформаційний простір йдеться, адже найчастіше навіть великі геополітичні протистояння ведуться не на полі головних супротивників, а у просторі вразливих суспільств та нестабільних держав. Неспроможність давати адекватні інформаційні відповіді для багатьох сусідніх держав ідентифікується як знак до інформаційної експансії та поступового поглинання, навіть без очевидного застосування воєнної сили. В умовах жорсткої інформаційної конкуренції, посилення глобалізаційних тенденцій дуже важливо реалізувати власні національні інтереси, використовувати сучасні інформаційні технології, формувати власний порядок денний інформаційної політики. Чіткі стратегічні пріоритети у системі інформаційної безпеки, серед низки зовнішніх

інформаційних загроз, дозволять державі не тільки втримати позиції на міжнародній арені та зберегти власну інституційну спроможність, але й ефективніше вибудовувати комунікації зі суспільством, та й загалом розширити можливості громадян до саморозвитку, професійного, культурного зростання тощо.

Сценаріїв розгортання інформаційних протистоянь та їх можливих наслідків для сучасного світу опубліковано чимало. Серед них критичні, песимістичні, і навіть дестабілізаційні (коли сам факт представлення такого сценарію використовується для деморалізації супротивника). Сучасна цивілізація фактично визнала інформаційний ресурс головною зброєю міждержавного, міжнаціонального, міжрегіонального протистояння. Інформаційне маніпулювання та деструктивні впливи застосовуються і щодо великих соціальних спільнот, держав, народів, націй, і стосовно конкретних людей, їх цінностей, норм, установок тощо. Руйнацій, миттєвих чи сповільнених, можуть зазнавати суб'єкти і об'єкти політики різного рівня, однак часто через саме інформаційні канали, що складно відстежити у звичних для безпекової справи способи.

Українська політолог Л. Смола, по сучасному розвиваючи ідеї інформаційного суспільства, все ж застерігає і від відповідних маніпуляцій. Це зрозуміло з її зауваження: «Змінюючи поведінкові стандарти та ціннісні орієнтації людини можна дестабілізувати соціально-політичну обстановку в тій чи іншій країні. Відповідно, суспільство з низькою політичною культурою, несформованими соціокультурними цінностями та загальноприйнятими правилами соціальної взаємодії завжди буде піддаватися маніпулюванню як зі сторони окремих осіб, так і різних структур, а інформаційні технології зроблять такі дії більш ефективними» [250, с. 3]. Тут варто справді конкретизувати ці ключові власне політологічні орієнтири, від яких залежить можливість держави і суспільства протистояти зовнішній інформаційній агресії: 1) проведені демократизаційні реформи, 2) зріле громадянське суспільство, 3) стабільна правова держава, 4) демократична політична та активістська громадянська культура населення. Цей перелік можна продовжувати та деталізувати, однак і у

такому обсязі він викликає сумніви щодо потенціалу України у протистоянні деструктивним зовнішнім впливам.

Умови глобалізованого світу змінили сутність і характерний принцип дії зовнішньої загрози. У наш час її складніше відрізнити від внутрішньої. Сучасні технології суттєво скоротили час, який раніше був потрібен для трансформації зовнішньої інформаційної загрози у внутрішню. Цей динамічний процес досить швидко перетворює одиничний факт, привнесений ззовні, у тривалий, постійний виклик, що потрапляє та стрімко вкорінюється у межах вже національного інформаційного культурного, соціального, політичного життя суспільства. Межа між зовнішніми та внутрішніми загрозами інформаційній безпеці стає все менш помітною, адже у цьому просторі активно функціонують сучасні засоби масової інформації, соціальні мережі та інші зацікавлені в інформаційних сенсаціях актори.

Серед науковців чимало критичних оцінок процесу медіа-комерціалізації, яку характеризують навіть як «несанкціонований доступ до свідомості», адже, як вважає В. Григор'єв, через «панування принципу «рекламної паузи» на телебаченні є вплив на психіку мільйонів людей. Тому в сучасний період інформаційні ресурси та інформаційні системи відносяться до числа основних елементів об'єктів безпеки в усіх сферах життєдіяльності держави» [58, с. 54]. Число споживачів медіа-інформації постійно зростає, а її виробники нерідко зловживають цим ресурсом вже як інструментом політичного впливу, боротьби за владу, зовнішньої агресії. Через ЗМІ та мережеві інформаційні засоби досяжність вразливих об'єктів та цілей фактично зводиться до мінімуму, тобто завдати шкоди інформаційній безпеці окремої особистості чи цілого суспільства стає простіше. Глобальний характер сучасного інформаційного суспільства одночасно скоротив відстань між нападником та жертвою навіть міжнародних протистоянь, не кажучи про регіональні чи локальні.

У світі глобальних інформаційних потоків інформаційні впливи можуть проникати та залишати свій слід у всіх сферах життєдіяльності суспільства. Тобто зовнішні й внутрішні загрози не тільки легко переносяться з однієї в іншу площину, але й цілком можуть своїм деструктивним впливом пронизувати

усі аспекти функціонування державних інститутів, громадських структур, людських спільнот і окремого індивіда. Ця всеохопність і тотальність інформаційних впливів часто нагадує тоталітарні практики, що викликає у політологів стійкі аналогії окремих проявів сучасного інформаційного суспільства з найжорстокішими практиками державного управління або колоніалізму в історії людства. Тож, ще задовго до фактичної анексії та проявленої інформаційної агресії проти України з боку РФ, вітчизняні політологи, зокрема О. Морозов, застерігали про існуючі загрози інформаційній безпеці та навіть вирізняли специфічні види таких загроз, зокрема: «1) загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України; 2) загрози інформаційному забезпеченню державної політики України; 3) загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікації і зв'язку; 4) загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються» [190, с. 24].

Перелічені деструктивні впливи і загрози достатньо тісно зв'язані між собою. Наприклад, порушення прав громадян, в тому числі й інформаційних, навіть виключно зовнішніми агентами, як наслідок знижує довіру до державних інституцій, покликаних гарантувати відповідні права. Взаємна недовіра лише поглиблюватиметься засобами масової інформації, для яких така тематика викликає особливий інтерес. Усе це лише посилюватиме вразливість системи до геополітичних загроз та гальмуватиме розвиток сучасних державницьких і громадянських структур, динаміку демократизаційних процесів тощо. З іншого боку, якщо інформаційних атак зазнає державний апарат, це не може також не відобразитися на конкретних можливостях громадян та на загальній атмосфері у суспільстві. Соціально-економічний прогрес країни та її культурний розвиток напряму залежить від спроможності спільними політичними зусиллями держави і громадян, медіа та технічної інфраструктури формувати безпечне інформаційне середовище, конкурентне, насичене, суспільно корисне, яке інтегроване у

глобальне, але захищене від його негативних проявів. Політичні домовленості, партнерство, широкі дискусії та консенсусні рішення, взаємний контроль та моніторингові заходи – усе це ті сучасні методики політики, що відрізняють демократичні починання у розбудові безпечного інформаційного простору.

Проте, звичайно, йдеться не лише про широкі політичні засоби та механізми в освоєнні глобального інформаційного простору, але й про дуже конкретні безпекові інструменти, що в часі динамічного становлення останнього потребують висококваліфікованих підходів та практик. Особливої гостроти набуває проблема інформаційно-психологічних протистоянь, тобто досить прицільний та точковий вплив на великі соціальні групи, що вчиняється з метою реалізації конкретних (гео)політичних інтересів. Фахівці з безпекознавства сьогодні наголошують, що провідні держави у боротьбі за збереження власних позицій і їх масштабування активно розвивають так звані «нелетальні системи ураження супротивника», це зокрема інтелектуально й технологічно потужні системи своєрідної зброї – спеціальних сил і засобів інформаційно-психологічного впливу, у різноманітних модифікаціях. З цього приводу В. Петров зазначає, що «звичною стала практика інформаційно-психологічного протиборства (боротьби і/або війни), яка по суті перетворилася у самостійний напрям зовнішньої політики розвинених держав» [216, с. 3]. Досвідчила подібного впливу і Україна в особі як пересічних громадян, так і окремих державних службовців, політиків, військових, інтелектуалів, що мало серйозні та багатоскладові наслідки.

Відрізнити ознаки та вчасно розв’язати початки інформаційно-психологічного протиборства односторонніми зусиллями досить складно. Тут українські позиції могли би посилити зарубіжні партнери, а аргументацією збагатити самі цілі глобального розвитку. Адже на умовному ідеологічно-цивілізаційному та інформаційному «фронті» велика кількість суб’єктів глобальної політики, які керуються власними стратегіями та ситуативними інтересами. Чимало з таких інтересів пов’язанні з Україною, відтак наше суспільство зазнає багатосторонніх інтенсивних впливів, в тому числі й агресивних інформаційно-психологічних, яким можливо протиставити лише

масштабніші, технологічно потужніші та спільні дії. Ця політика мала би приваблювати не лише своїм консолідуючим характером, але й ціннісним потенціалом, коли хоча й вразливі, але все ж правові й демократичні за своєю сутністю інститути та відносини знаходять потужну підтримку міжнародної спільноти у боротьбі з інформаційними нападами агресорів.

На шляху вибудовування такого не тільки декларативного, але й дієвого, ефективного, адекватного часу міжнародного партнерства, державі ще й варто розробляти чіткі механізми ідентифікації різних форм інформаційно-психологічного та інформаційно-технологічного впливу. Часто труднощі при налагодженні глобальних мереж комунікації щодо питань безпеки викликає саме невміння означувати та класифікувати існуючі загрози. У цьому суттєво допомагають наукові напрацювання, зокрема нашу увагу привертають визначення В. Ліпкан, Ю. Максименко, В. Желіховського. Їх класифікація деструктивних інформаційних впливів за ознаками інтенсивності й масштабності видається досить точною: 1) інформаційна експансія (діяльність з досягнення конкретних інтересів методом безконфліктного проникнення в інформаційну сферу); 2) інформаційна агресія (незаконні дії однієї зі сторін в інформаційній сфері, обмежене і локальне застосування сили, для завдання супротивнику відчутної шкоди в окремих областях його діяльності); 3) інформаційна війна (вищий ступінь інформаційного протиборства, інформаційне насильство над державами, народами, націями, класами, соціальними групами, спрямоване на розв’язання суспільних, політичних, ідеологічних, національних, територіальних та інших конфліктів через широкомасштабне застосування інформаційної зброї) [168, с. 129-130].

У межах названих вище трьох форм вчені розрізняють безліч технологій і методів інформаційної агресії/насильства/експансії, кожен з яких потребує адекватних основ інформаційного захисту, відображення у стратегії і тактиці безпеки. Нерідко один і той самий суб’єкт політики (держава чи їх співдружність, політична партія чи партійна система загалом, передвиборчий штаб чи поле виборчої кампанії в цілому, правозахисна організація чи громадянське суспільство,

соціальна група, окремий індивід тощо) може зазнавати багатосторонніх і багаторівневих інформаційних агресій. Глобальність сучасного світу сприяє цьому. Стратегічне бачення Україною інформаційних загроз сьогодні залежить і від наукових, фундаментальних визначень пріоритетів у цій політиці, і від фактичних дій та практик, які застосовує держава в умовах ведення справжньої інформаційної війни, в якій постійно перебуває. Те саме стосується й інших суб'єктів політики, які окремо поза державною стратегією інформаційної безпеки ризикують втратити і власну суб'єктність у політичному житті суспільства, і навіть цілковито увесь цей простір незалежного функціонування.

Глобалізація інформаційного середовища стосується не лише держави, адже цей всеохопний процес привносить та змінює більшість суб'єктів і об'єктів сучасної політики, серед яких важливу рол відіграють засоби масової інформації. Проблема, безумовно, міждисциплінарного характеру, тож нашу увагу привернуло дослідження А. Юричка, який вивчає інформаційні маніпуляції у світовій періодичній пресі з позицій сучасної журналістики. Зокрема він зазначає, що такі маніпулювання (через ЗМІ) набули сьогодні масового характеру, більше того, коли медіа використовують сучасні технології інформаційно-психологічного впливу – це найчастіше пов'язано з утвердженням певного політичного впливу та виконанням конкретних політичних завдань. Це очевидно з його позиції про те, що «політичне маніпулювання інформацією, що реалізується через зарубіжні ЗМІ, зокрема, в Україні, є серйозною загрозою, як головним засадам розбудови демократичного суспільства і зміцненню незалежності України, так і особистій інформаційно-психологічній безпеці громадян» [286, с. 3].

Небезпека зовнішніх деструктивних інформаційних впливів відтак походить не лише від офіційних державних агентів з закордону, але й від окремих медіа-корпорацій, комерційних структур, неформалізованих об'єднань, що активно функціонують у всесвітній мережі, добре вивчили закономірності функціонування інформаційного суспільства та готові використовувати його вразливості на власну користь. Увесь масив інформаційних потоків контролювати за допомогою державних інструментів досить складно, тому таким важливим є налагодження

міжнародного співробітництва зі залученням громадського сектору, наукової та освітянської спільноти, експертного середовища, професійних спілок тощо. Боротьба з інформаційними маніпулюваннями суспільною свідомістю найефективніша, коли відбувається на різних рівнях, з розвитком багатосторонніх каналів комунікації та загалом зі встановленням довірливих відносин між партнерами.

Суб'єкт-об'єктний вимір інформаційної безпеки заслуговує окремої уваги, але у контексті глобалізації варто також акцентувати на політичних процесах, що відбуваються одночасно та не можуть власне повноцінно відбутися без один одного. В українських реаліях йдеться передусім про щонайменше такі паралельні у політичному житті суспільства процеси як 1) налагодження та розвиток міжкультурних і міжнародних комунікацій, 2) модернізація і зміцнення демократичних інститутів 3) розбудова інфраструктури інформаційного суспільства як рушійної сили прогресивних державно-політичних змін. Для ворожої інформаційної агресії кожен із цих важливих напрямків національного розвитку є потенційною ціллю для дестабілізації.

Політологи, які вивчають проблеми вироблення ефективної стратегії національної інформаційної безпеки України, досить часто вказують серед можливих засобів протидії інформаційній війні багатокомпонентні, такі, що корелюються з трьома згаданими вище процесами. Це засоби, які б враховували і подальшу інтеграцію в сучасний західний цивілізаційний простір (подолання цифрової нерівності, сприяння академічній мобільності, культурні обміни та діалоги народів через сучасні високотехнологічні здобутки), і демократичні трансформації (проведення чіткої інформаційної політики, розбудова її прозорих інститутів і механізмів, забезпечення державою права громадян на інформацію, свободу слова тощо), і цифрові зрушення у сучасному світі (вирішення проблем власності в сфері інформації, чіткі правила гри в інформаційній сфері, визначена роль держави в її регулюванні тощо). Політологи нерідко звертають увагу і на технічний та технологічний аспекти

проблематики. Так, Г. Несвіт стверджує: «З огляду на існуючі у світі процеси глобалізації телекомунікаційних мереж, можна припустити, що саме інформаційним видам агресії буде відданий пріоритет у майбутньому. Держава повинна постійно удосконалювати технічні засоби протидії інформаційній війні [...] Ці засоби повинні розроблятися власними силами, повинні бути вітчизняні наукові розробки, з тим, щоб виключити можливість технічного контролю за їх функціонуванням» [198, с. 13]. Отже, зовнішні та внутрішні деструктивні впливи в інформаційному суспільстві повинні максимально нівелюватися асиметричними міжнародними та національними заходами, локальними й регіональними проектами, а головно – послідовною стратегією та практикою інформаційної безпеки.

В часі інтенсивних інформаційних протистоянь, фактичних інформаційно-психологічних і мережевих воєн відповідна стратегія є необхідністю, що визначає здатність держави зберігати та утверджувати суб'єктність у глобальному світі. Тут принагідним є досвід США, який детально аналізують і вітчизняні дослідники. Зокрема утверджується необхідність дослідження, напрацювання та перманентного оновлення підходів до врегулювання інформаційно-психологічної складової діяльності держави – «інформаційне забезпечення тих чи інших дій влади». Підкреслюється, що сучасні збройні конфлікти містять дуже виразні ознаки їх інформаційного та психологічного забезпечення. Відтак таке забезпечення мусить бути пролонговане у часі, тобто це далеко не разовий захід, а складний їх комплекс до, під час та після початку розгортання бойових дій [85, с. 3].

Класифікація інформаційних впливів зайняла чільне місце і у наших дослідженнях [див. напр. 374], але тут лише коротко вкажемо на окремі типи, що характеризують глобальний характер інформаційної напруги та конфліктогенності. Отже, інформаційна складова властиво, органічно та все послідовніше виявляється в усталених системах міжнародних, міжнаціональних, соціально-політичних відносин. Сучасний інформаційний конфлікт став невід'ємною частиною збройного протистояння і вже у такій формації виокремлюється в окремий тип. У його структурі можна вирізнити інформаційні

агресії, диверсії, війни. Інформаційні протистояння сьогодні співіснують з реальним війнами, а за своєю інтенсивністю та загрозливістю вражають навіть стійкі системи та інститути. Тому державна програма, яка покликана протидіяти інформаційним загрозам, передусім чітко такі загрози ідентифікує, з наукових позицій розрізняє сутність та ключові етапи інформаційних операцій, інформаційних агресій, інформаційного тероризму, комп'ютерної злочинності, інформаційних воєн тощо. Цілі та тактичні завдання їх можуть відрізнятися: від дезінформації громадян; пропаганди і поширення конкретних ідей і поглядів; ослаблення визначених політичних позицій і переконань аж до точкових маніпуляцій свідомістю окремих людей; дезорієнтації цілих груп чи класів; розхитування інституційних основ суспільства; залякування мас. Вирізняючи основні види, цілі та напрями збудження інформаційної небезпеки, можна деталізувати й конкретні заходи боротьби з ними.

Інформаційні операції вже традиційно розглядають серед розповсюджених видів інформаційних протистоянь або навіть інформаційної агресії, що спостерігається в глобалізованому світі. Визнані наковці, зокрема В. Горбулін, О. Додонов і Д. Ланде, вважають, що у цій категорії потрібно вбачати «реалізацію попередньо спланованих інформаційно-психологічних впливів на ворожу, дружню або нейтральну аудиторію шляхом впливу на установки та поведінку для досягнення заздалегідь визначених цілей» [52, с. 8]. Отже, інформаційні операції передбачають залучення та активізацію таких технологій, які допускають можливість маніпулятивно-агресивного впливу на індивідуальну та суспільну свідомість. Можна також стверджувати, що доступ до таких технологій сьогодні мають не лише провідні світові держави, але й приватні компанії, власники засобів масової комунікації, лідери ринку соціальних мереж. Очевидно цей факт мають враховувати і безпекові інституції держав, які захищаються від інформаційних операцій.

Враховуючи увесь спектр можливих видів та напрямів збудження інформаційної небезпеки, особливо у боротьбі з інформаційними операціями вважливо зважати на їх миттєвість, раптовість, ефект несподіванки. Таким

характеристикам можливо впевнено протиставити лише попередньо підготовлене населення, тобто такого споживача інформації, якому властивий високий рівень медіа-грамотності, політичної і правової культури, соціальної відповідальності, патріотизму, громадянської згуртованості. Національні системи освіти та виховання у провідних країнах світу досить успішно інтегрують відповідні складові у свої програми, що забезпечуватимуть інформаційну безпеку держави і суспільства у глобалізованому майбутньому.

Найбільш вразливе ж середовище до інформаційних операцій агресивного характеру формується з людей, що апатичні до політики, пасивні у соціальних справах, нігілістичні, замкнені рамками мінімальних знань та вузьких світоглядних орієнтирів. Позбавлене ключових культурних, громадянських, національних патернів мислення і поведінки суспільство втрачає не лише додаткові опції демократичного розвитку, але й досягнуті (поза)інституційні реформи. Тому додатковим фактором вразливості є також перехідний етап у суспільно-політичному розвитку, тривалий транзит осучаснених форм та засобів політики, що ще на шляху донесення та утвердження можуть зазнавати нищівних інформаційних атак. Масові навіювання та масові маніпулювання свідомістю часто готуються саме для таких цільових груп, для незрілих структур та незакріплених механізмів і норм.

Сприятливі для проведення інформаційного впливу умови часто лише апробуються одиничними інформаційними операціями, але нерідко приносять за собою значно масштабніші дії агресора. Тому будь-яка короткочасна інформаційна атака чи разове пошкодження інформаційних мереж з боку супротивника може і повинно розцінюватися як попереднє випробовування системи та суспільства на стійкість. Такі дії цілком ймовірно переростають у повномасштабні інформаційні конфлікти, у розв’язання інформаційної війни та/або зрештою і в реальне збройне протистояння, хоча й умовно локальне за географією, однак глобальне за наслідками впливу на політичний світогляд та міжнародну політику.

Сучасна наукова література приділила чимало місця пошуку відповідей

на питання про сутність та роль інформаційних воєн у процесі глобалізації. Погоджуємося з авторами, зокрема з В. Абакумовим, які дають наступне означення: «Інформаційна війна − це сукупність методів та способів цілеспрямованого впливу суб'єктів-агресорів в умовах інформаційної відкритості на соціальні відносини (відносини людей між собою, відносини в суспільстві та державі), інформаційні ресурси, інформаційно-аналітичні та інформаційно-технічні системи, системи формування масової свідомості та психіки окремої людини з обов'язковим використанням інформаційної зброї (властивостей інформації, інформаційних ресурсів та новітніх інформаційно-телекомунікаційних технологій) з метою штучного створення факторів гальмування розвитку людини, суспільства та держави, встановлення контролю над інформаційними ресурсами потенційного противника задля отримання переваг у пріоритетних сферах суспільного життя» [1, с. 9]. Це, написане до подій 2014 р. визначення, достатньо формалізовано, однак чітко структуроване.

Існують також визначення, що конкретизують власне безпековий, суб'єкт-об'єктний та важливий для нашого дослідження глобальний виміри проблематики. Он з них передбачає, що «інформаційна війна – 1) вплив на цивільне населення і (або) військовослужбовців іноземної держави шляхом поширення певної інформації; 2) цілеспрямовані дії, розпочаті для досягнення інформаційної переваги шляхом заподіяння шкоди інформаційним процесам та системам супротивника при одночасному захисті власних інформаційних процесів та систем» [361, с. 119]. Друге визначення вигідно відрізняє розуміння проблематики вже власне в умовах інформаційної війни, коли український дослідник акцентує на широких (прихованих і відритих) засобах такої війни, а також можливих її результатах (поразкові настрої, державна зрада, колабораціонізм тощо).

Загалом йдеться про жорстокі інформаційні протистояння, коли контроль і максимальне використання потенціалу власного інформаційного простору і військової інформації посилюють послідовні та системні атаки на інформаційні канали супротивника. Серед складових інформаційної війни дослідники

називають: дезінформацію, психологічні операції, електронну боротьбу, антипропаганду, заходи по забезпеченню безпеки та супротиву, інформаційні атаки у відкритій формі, фізичний вплив на інформаційні ресурси та інші дії зі заохочення супротивника до здійснення хибних кроків й досягнення переваги над ним [180, с. 594]. За цих умов державі-жертві агресії варто оптимізувати ресурсні витрати, узгодити всередині країни субординацію і підходи, шукати однодумців і партнерів у глобальному інформаційному просторі, а також чітко ідентифікувати реальних і потенційних суб'єктів загрози. Не менш важливо мінімізувати зовнішній доступ до політичної, військової, економічної, інтелектуальної, соціально-психологічної та власне інформаційної сфер суспільства, скоротити можливості для колективних і персональних помилок у безпековому просторі з боку відповідальних структур. Різноманітні методи інформаційного впливу часто потребують ще більшого розмаїття реакційних заходів, при чому як передбачених національною стратегією інформаційної безпеки, так і цілком інноваційних підходів, яких може потребувати в конкретний момент часу суспільство. Тож, часто ініціювати інформаційне протистояння видається значно легшим завданням, ніж протистояти йому.

Глобалізаційні процеси однаково вражають у якості об'єктів інформаційної війни як великі держави, нації, міжнародні організації та їх союзи, так і комерційні компанії, громадські організації локального рівня, партійні осередки чи просто авторитетних і впливових політичних діячів. Провокують подібні акти інформаційної агресії зазвичай технологічно та ресурсно потужні структури, серед яких і транснаціональні корпорації, і держави-лідери, що водночас зрідка прямо визнають свою суб'єктність у започаткуванні інформаційних воєн, але активно діють через посередників, беруть участь у відповідних публічних дискусіях, прийнятті рішень тощо.

Нові технології в інформаційній війні пов'язанні не лише зі збільшенням швидкості та обсягів передачі інформації, це також осучаснення та пристосування маркетингових заходів до цілей інформаційної агресії. Якщо фізичне насильство засуджується усією цивілізованою глобальною спільнотою,

то можливості та прояви насильства інформаційного, яке часто пов’язане з технологіями агресивного маркетингу, поки ще мало вивченні, слабко контрольовані та майже не надаються офіційним оцінкам. Ініціатори інформаційних воєн часто користуються можливостями сучасного відкритого глобального інформаційного простору, тією відносно легкою доступністю до свідомості пересічних громадян та активних політиків. У цьому контексті загальна переконливість, емоційність інформаційних повідомлень, першість у їх донесенні, технології самопозиціонування і рекламування ваговитіші за аргументовані та підкріплені раціональним фактажем відомості. Сучасні споживачі інформації мають можливість (хоча далеко не завжди нею користуються) отримувати повідомлення з різних джерел, від кожної сторони-супротивника інформаційної війни. Це може призводити і до різних наслідків: від перетворення споживача інформації у войовничого прихильника однієї зі сторін конфлікту до цілковитого розчарування, сумнівів, аполітичності людей тощо. У будь-якому разі йдеться про боротьбу за громадську думку, яка є важливим об’єктом інформаційної війни.

Співзвучні цим тезам і міркування Т. Поди, яка доводить сьогочасну значущість інформаційно-комунікаційних технологій у сфері міжнародних відносин, у політичних відносинах і процесах, адже зазначає, що: «в сучасній інформаційній війні принципове значення набула іміджева або «брендова» індоктринація, сенс якої полягає у впливі на суспільну свідомість еталонними стандартами життя» [218, с. 60]. Вчена продовжує, що «дійовими особами іміджевої індоктринації є не політики і політтехнологи, а актори шоу-бізнесу, які за популярністю та частотою появи у ЗМІ випередили багатьох державних діячів» [218, с. 60]. Відтак перелік активних суб’єктів та ефективних інструментів інформаційного впливу (ззовні чи зсередини) постійно зростає. Важливу роль у інформаційних війнах відіграють медіа-персони. І хоча питання їх суб’єкт-об’єктності дискусійне, позаяк у глобальних масштабах, на яких акцентуємо у цьому розділі, світові селебріті (з англ. celebrity – знаментість) мають очевидні переваги над локально відомими персонами. Охоплення

популярною особистістю великої кількості послідовників і фанатів є потенційною цільовою аудиторією для розробників нових стратегій і тактичних задумів інформаційних агресій. Відтак інформаційна війна може мати виразний вимір у сфері масової культури, яка також мало надається контролю і регулюванню.

Отже, можливості вибудовування національної стратегії інформаційної безпеки залежать від низки факторів. У цій сфері потрібно враховувати контрольовані і неконтрольовані обміни інформацією, визначати основні форми, рівні та механізми інформаційного протистояння, відрізняти деструктивні інформаційні впливи зовнішнього і внутрішнього характеру, розуміти їх пов’язаність, всеохопність, маніпулятивність.

3.2. Суб’єкт-об’єктні виміри інформаційної безпеки у контексті впливовості та партнерства політичних інститутів

Проаналізувавши основні причини та види інформаційних загроз, що виникають під тиском інформаційної революції та визначивши потребу впровадження засобів (механізмів, технологій) інформаційної безпеки, слід більш детально вивчити її суб’єкт-об’єктні виміри − характеристики об’єктів, на яких спрямована безпекова діяльність, та її суб’єктів − людей та соціальних інститутів, які її забезпечують.

У сучасній політичній науці питання про суб’єкт політичної дії та об’єкт, що формується під впливом такої дії, є одним із центральних. Детальніше визначення подає О. Бабкіна, означуючи ці «рефлективні поняття» у політологічній енциклопедії. Політичну суб’єктність дослідниця називає передусім властивістю великих соціальних груп, і вже потім – їх інститутів, політичних організацій, ідеологів, лідерів, активних членів, що здійснюють важливі ролі в політиці. Об’єкт в політиці трактується як частина політичної реальності (політичної системи, політичних відносини, політичних процесів, інститутів, соціальних груп та особистостей), на яку спрямована діяльність

суб'єкта [360, с. 695-696]. Важливо підкреслити, що саме розуміння специфіки суб'єктів і об'єктів сучасної інформаційної політики дозволяє стверджувати думку про цю сферу політики як відносно самостійну, вагому, властиво і якісно відмінну від інших (з комплексом окремих інтересів, суспільних запитів, конфліктів, що потребують політичного вирішення, стратегій та орієнтирів).

Суб'єкта політики традиційно вирізняє діяльна позиція, впливовість, певний набір ресурсів, можливостей, достатній для активної практики рівень легітимності. Аналізувати суб'єктів інформаційної політики означає передусім розпізнати максимально можливе коло таких суб'єктів, тобто враховувати явні і приховані можливості різних інституцій, організацій, окремих людей чи їх груп в реалізації власних чи загальних інтересів у інформаційному просторі країни. Природно, що початок для відповідного аналізу могли би задати наші міркування про роль держави як базового політичного інституту, визначального суб'єкта політики, а відповідні завдання вже частково реалізовані нами у низці публікацій, присвячених особливостям формування ефективної державної інформаційної політики [380].

Суб'єкт-об'єктні відносини у системі інформаційної безпеки, на наш погляд, великою мірою залежать від діяльності державних структур загалом, а у контексті пропонованої проблематики – від інститутів інформаційної безпеки, які функціонують в системі державного управління й адміністрування**.** Держава задає загальну динаміку та правила роботи на інформаційному ринку країни, встановлює норми та обмеження для розвитку інформаційної демократії, захищає інформаційний простір не лише від загалом атак, але й конкретних суб'єктів інформаційного маніпулювання. У державній системі координат інформаційної безпеки кожен суб'єкт політики має знайти своє місце та функцію, якщо дбає про збереження цілісності країни, суверенітету держави, соціально-політичного розвитку суспільства, до якого належить.

Набути суб'єктності у сучасному світі означає також свідомо та цілеспрямовано розвивати державні інститути, структури, мережі зв'язків між ними. У системі інформаційної безпеки варто враховувати ще й чимало

напрямків (міжнародний і внутрішній, інформаційно-психологічний, кібернетичний та ін.) для організації ефективної діяльності відповідних структур. Науковці зауважують, що загальне керівництво системою інформаційної безпеки зазвичай здійснюється очільником виконавчої гілки влади. Йдеться про відповідний робочий орган, що відповідальний за розробку державної інформаційної політики, за координацію її елементів, прийняття ключових рішень. Законодавчо визначені державні структури, на думку сучасних науковців, варто розглядати як такі, що складають підсистеми інформаційної безпеки (міністерства і відомства), що також формують у своїх межах деякі підрозділи, відповідальні за виявлення, аналіз, протидію інформаційним загрозам [237, с. 39].

У першому розділі ми вже частково зверталися до досвіду США, європейських країн, Китаю, де достатньо ефективно функціонують системи інформаційної безпеки, що дають нам розуміння ключових понять та теоретико-прикладних проблем у відповідній сфері суспільно-політичного життя. У цьому ж розділі зауважимо, що кращі безпекові стратегії та практики, які успішно захищають сучасний інформаційний простір, побудовані на трьох визначальних принципах: ієрархічності; державної координованості; взаємодії. Ці три принципи мають виражений суб'єкт-об'єктний характер, адже йдеться про необхідність побудови системи інформаційної безпеки з керівними і дорадчо-консультативними органами, відповідальне здійснення управління такою системою, координування діяльності та взаємодії її структурних підрозділів. Сучасна країна, що стає об'єктом постійного зовнішнього інформаційного впливу, в контексті самозбереження та розвитку має відповідно й постійно працювати над власною суб'єктністю. У цьому вбачається одна з головних закономірностей політичного життя. В одному й тому ж інституті може бути закладена як діяльнісна активність у світі політики, так і пасивна, виконавська функція. Однак ефективність державних органів від поєднання таких суперечливих початків не повинна втрачатися, адже ці структури мають бути наділені відповідними функціями та засобами для реалізації спільних

цілей та дуже конкретних завдань.

Ієрархія державних структур, тобто найчастіше визначальних суб’єктів у системі інформаційної безпеки, перебуває у центрі уваги численних дослідників, які вивчають тенденції і закономірності у цій сфері. Ця традиція перенесена зі сфери національної безпеки загалом, яка не може функціонувати без належного забезпечення суворого порядку, системи підлеглих та вищих чинів, без чітких і зрозумілих відносин субординації та вертикальних зв'язків. У зарубіжних країнах, де налагоджено ефективну і функціональну ієрархію системи інформаційної безпеки, її зазвичай очолює глава держави або нерідко керівник виконавчої влади. Вагомим є орган управління з питань інформаційної безпеки, який створюється при главі та опирається у своїй діяльності на відповідну структуру в уряді. Такою структурою може бути відповідний департамент (управління) інформаційної безпеки. Крім того очільнику цієї системи напряму підпорядковуються відповідні інфраструктурні інституції міністерств і відомств. Зокрема такі органи, як правило, функціонують при міністерстві, що відповідає за зовнішню політику держави, при міністерстві внутрішніх справ (наприклад, структури реагування на інформаційну злочинність, комп’ютерні інциденти тощо). Низка таких структур діє і при міністерстві оборони (генеральний штаб з підрозділами – зі захисту та безпеки інформації, виявлення, аналізу та протидії інформаційним загрозам, кібернетичних операцій та ін.) [237, с. 40].

В Україні система інформаційної безпеки працює за схожою моделлю центральних суб’єктів, серед яких також варто враховувати діяльність Служби безпеки України, Служби зовнішньої розвідки, інших міністерств і відомств (Міністерства культури та інформаційної, політики, Міністерства освіти та науки України, та ін.). Очевидно, що такі державні структури, які задають напрям та динаміку сфери інформаційної безпеки, мають вибудовувати свою діяльність за принципами координованості, в межах встановлених норм, загальних програм, стратегій та планів, не повторювати повноважень, уникати невластивих функцій та надміру концентрації владного контролю. Вітчизняний законотворець

підкреслює також як засадничі принципи інформаційної політики, зокрема «додержання прав і свобод людини і громадянина», «повагу до гідності особи, захист її законних інтересів, а також законних інтересів суспільства та держави», «забезпечення суверенітету і територіальної цілісності України», про які йдеться у відповідному указі президента [265]. У поєднанні принципів інформаційної політики демократичної системи та принципів інформаційної безпеки суб'єкта цивілізованих міжнародних відносин вбачаємо дійсний шлях розвитку сучасних політичних інститутів. І у розробці стратегій, і у процесі реалізації запланованих програм саме держава дбає про необхідні матеріальні ресурси, кадрове забезпечення, міжнародне співробітництво у сфері інформаційної безпеки.

Традиційно ефективна система інформаційної безпеки передбачає налагоджену інфраструктуру і взаємодію цілої низки державних органів, а також наявність безпекового сегменту (підрозділу, сектору, відділу тощо) у складі кожного державного органу. Тобто умовно не лише на військові чи правоохоронні формування, утворені відповідно до законів, покладається функція забезпечення національної безпеки. З розвитком сучасного поняття безпеки як багатокомпонентного феномену, що також передбачає інформаційну складову, сучасна держава інтегрує інформаційно-безпековий зміст до діяльності фактично кожного свого структурного елементу. Більше того – практично кожен сучасний державний службовець є потенційною ціллю інформаційних атак, тож державні інституції мусять постійно дбати про підвищення кваліфікації, інформаційних компетентностей, комп'ютерної та медіаграмотності своїх співробітників тощо.

Безумовно основою ефективного функціонування державних органів у сучасному інформаційному просторі є підготовлені до актуальних викликів і загроз фахівці. Таких професійних державних службовців, які значною мірою визначають суб'єктність відповідних структур держави, потребують сучасні офіси глав держави, очільників законодавчих органів, міністерства та інші центральні органи виконавчої влади, суди, прокуратура, національні, місцеві державні адміністрації, органи місцевого самоврядування, прикордонні служби,

збройні сили, служби національної безпеки тощо. При цьому нерідко окремо створюються й спеціальні державні органи, які покликані займатися виключно проблемами вироблення ефективної інформаційної політики та певною мірою інформаційною безпекою держави. Їх заснування часто пов’язують з особливо загрозливими в історії країни періодами (громадянськими протистояннями, міждержавними конфліктами, а тепер й інформаційними війнами), коли і внутрішній споживач, і міжнародна спільнота потребують вчасного, оперативного, достовірного інформування про перебіг подій та їх об’єктивне трактування.

Перелік важливих та життєво необхідних для суспільства та політичної системи функцій, які покладаються на державу як суб’єкта інформаційної політики, є досить великим. Це і збереження інформаційного суверенітету держави, і попередження безконтрольного впливу на інформаційний простір, і захист та гарантії усім суб’єктам інформаційних відносин, і забезпечення прав людини та громадянина. Однак, незважаючи на цей перелік, роль держави в інформаційному просторі часто викликає помітні дискусії в експертному та науковому середовищі, вона нерідко зазнає критики і з боку медіа-спільноти, і від громадських та політичних діячів.

Державна система інформаційної безпеки містить багато вразливих елементів, що часто через прогалини в організації окремих з них переноситься на усю площину захисту інформаційних прав і свобод громадян. Наприклад, помилка одного державного службовця (відкриття фішинг-листа з корпоративного акаунта або необережне поводження з інформацією, що віднесена до державної таємниці, тощо) потенційно небезпечна для всього сектору політики або й суспільства загалом. Втрачаючи контроль над державною інформацією через необережність чи злий умисел одного з посадовців, держава поступово втрачає свою суб’єктність, покладенні на неї обов’язки встановлювати, виконувати та підтримувати політико-владні відносини, в тому числі й в інформаційній сфері.

Людський фактор не єдиний, що може викликати певні труднощі в організації державної системи інформаційної безпеки. Недоліки законодавчої бази такої системи також можуть провокувати певні непорозуміння, суперечності й навіть конфлікти у цій сфері. Визначальними у цьому аспекті є принципи системності, справедливості, правової визначеності, свободи, гласності, без яких держава втрачає підтримку людей. Часто через правові неточності функції зі забезпечення інформаційної політики та безпеки держави «розпорошені» між різними структурами, відтак втрачається центральний відповідальний суб'єкт та підпорядковані йому органи.

Дії окремих державних органів чи посадовців можуть мати негативний інформаційний вплив на суспільство; шкоди завдає і неповна, невчасна, недостовірна комунікація державних діячів зі суспільством; поширене і явище нераціонального застосування інформаційних технологій, порушення конфіденційності в держструктурах тощо. Раціональне та адекватне позиціонування держави на інформаційному ринку також може бути ускладнене відсутністю стратегічних пріоритетів і визначень у цій сфері, зрощуванням приватних інтересів окремих зацікавлених сторін із державними, надмірною електоральною залежністю (популізмом) високопосадовців, або ж навпаки – ігноруванням зв'язків з громадськістю, залежністю від іноземних суб'єктів тощо. Тобто йдеться на загал про комплекс проблем, пов'язаних з виробленням політики і її виконанням, що впливає на стан захищеності суспільства.

Як зазнає М. Зайцев, непослідовність державної політики забезпечення інформаційної безпеки, недоліки спеціального законодавства, яким передбачено напрямки її реалізації, зумовлює відсутність чіткої та узгодженої системи суб'єктів забезпечення інформаційної безпеки. Подібні обставини потребують, на думку дослідника, таких першочергових дій: по-перше, оптимізація кількості елементів системи забезпечення інформаційної безпеки (їх збільшення ускладнює функціонування й ефективність системи загалом); по-друге, утвердження ролі єдиного суб'єкту управління забезпеченням

інформаційної безпеки (тобто наділеного владними повноваженнями стосовно інших структур цієї системи та спрямованого на сучасні механізми взаємодії з ними); по-третє, розмежування повноважень та функцій суб'єктів забезпечення інформаційної безпеки (уникнення дублювань, конкуренції в діяльності цих суб'єктів) та одночасне охоплення всіх аспектів життя інформаційного суспільства цими суб'єктами; по-четверте, громадський контроль, коли до складу системи забезпечення інформаційної безпеки входять не тільки органи державної влади, а й інституції громадянського суспільства [90, с. 231-238].

Важливі доктринальні напрямки організації діяльності органів влади у системі інформаційної безпеки визначені і в українському законодавстві. Серед них у таких нормативно-правових актах, як «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та «Про Доктрину інформаційної безпеки України», згадується про «створення повнофункціональної інформаційної інфраструктури держави, забезпечення захисту її критичних елементів»; «підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань»; «вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері»; «розгортання та розвитку системи конфіденційного зв'язку як сучасної захищеної транспортної основи» [106; 265]; а в умовах гібридної війни окремо наголошується на реалізації суб'єктами державної інформаційної політики, насамперед, завдань з протидії руйнівному інформаційному впливу Російської Федерації [265]. Тобто ефективна інформаційна політика державних структур національної безпеки часто вимірюється не лише міжнародними стандартами і правилами, але й спроможністю захищати специфічні національні інтереси, приймати найактуальніші виклики та долати гострі загрози.

Однак суб'єктність у сучасній політиці втримує не лише держава та її органи, але й громадський сектор, який все активніше розвиває власну участь,

впливовість, можливості, в тому числі й у інформаційній сфері. Сьогодні це доволі широкий спектр політичних, економічних, правозахисних, культурно-просвітницьких, професійних, безпекових, волонтерських, трудових, мережевих, творчих, самоврядних та інших організацій. Водночас масштабність та змістовна наповненість такого сектору відрізняється у різних країнах, що залежить від встановлених соціально-політичних традицій, типу політичного режиму та загалом світогляду громадян. Оскільки у системі національної інформаційної безпеки йдеться про необхідність протидії не лише внутрішнім, але й зовнішнім загрозам, то на можливості інститутів громадянського суспільства нерідко впливає ще й геополітична розстановка сил. Отже, сучасне суспільство та його інститути в інформаційній сфері можуть проявлятися по-різному – і як суб'єкти, і як об'єкти відповідної політики, що залежить від низки чинників.

Інститут громадянського суспільства як форма організації та засіб здійснення спільної волі громадян, зокрема й у політиці, не претендує на здобуття владних повноважень у міністерствах чи відомствах, але орієнтований на захист прав та інтересів громадян, що апріорі визначає його безпекову сутність. Разом з тим, оцінки участі інститутів громадянського суспільства у безпековому просторі також розділилися поміж науковцями.

Дослідники В. Крутов та Г. Новицький стверджують, що фактично вся сукупність недержавного сектору залишається поза процесом єдиної політики у сфері забезпечення національної безпеки [157, с. 162]. Інституціональна структура суб'єктів забезпечення національної безпеки достатньо складна, однак вона також не може залишатися самоціллю, тобто створюватися виключно заради держави чи відірвано від політичної реальності й людей загалом. Нерідко стихійність, протестність суб'єктів політики від небайдужої громадськості викликає дискусії щодо спроможності їх ефективної участі в політиці. Тому вже згадані правознавці і в законодавстві, і у практиці забезпечення національної безпеки відстежили необхідність чіткого визначення функціонального місця недержавного сектору безпеки [157, с. 166].

Натомість багато вчених також вбачають великий потенціал у діяльності інститутів громадянського суспільства у системі захисту інформаційної безпеки. Наголошується, що і через формальні, й через неформальні об'єднання громадян забезпечується участь громадськості у прийнятті рішень з питань інформаційної політики, а також окреслюється ініціатива, усвідомлена й активна позиція громадянського суспільства з розв'язання проблем інформаційної безпеки тощо [див. напр.170, с. 110]. Додамо, що така участь не може узагальнюватися, адже йдеться про дуже різноманітні організації та формати, іноді й взаємовиключні. Кожен конкретний випадок громадянської активності в інформаційному просторі потребує окремої уваги і дослідника, і відповідального державного посадовця. Найпевнішим тут видається шлях продуктивної співпраці державних та недержавних суб'єктів заради досягнення результатів у сфері захисту національних інтересів та громадських прав, суспільного інформаційно-культурного простору загалом.

В інформаційній сфері загалом та у системі забезпечення інформаційної безпеки зокрема недержавні суб'єкти мають можливість проявляти себе в ролі різних структурних елементів. Відповідні основні форми участі на прикладі українських реалій відрізняють і вітчизняні вчені, зокрема називають такі громадські практики в інформаційній сфері: громадський контроль за діяльністю органів державного управління та дотриманням законності в інформаційній сфері; участь у роботі тематичних консультативно-дорадчих структурах при державних органах; залучення до публічних громадських обговорень, що проводяться органами державного управління; вивчення громадської думки спільно з державними органами; надсилання органам державного управління інформаційних запитів, звернень, скарг, заяв про інформаційні правопорушення; направлення державним органам заяв і клопотань про задоволення прав та законних інтересів у цій сфері тощо [34, с. 34].

Сучасна демократія, як і рух до демократичних змін вбачаються нам мало можливими без названих форм громадських активностей, адже громадські й релігійні організації, політичні партії і організації роботодавців, творчі та

професійні спілки, благодійні фонди, самоврядні територіальні громади, трудові й навчальні колективи організації – усі ці структури громадянського суспільства можуть розвиватися лише активно задіяними в інформаційному житті країни. Вони формують інформаційне суспільство та одночасно залежать від його можливостей та небезпек. І події Революція Гідності в Україні, і сьогочасна російсько-українська війна засвідчили потужний потенціал недержавних суб'єктів інформаційної безпеки. Водночас цей період особливо виразно показав необхідність відрізняти власне громадські від імітаційних, псевдогромадських ініціатив, тобто тих, що інспіровані ззовні та не відображають суб'єктності громадян у сфері інформаційної безпеки, а швидше самі складають загрозу для суспільного розвитку.

Серед впливових недержавних суб'єктів інформаційної безпеки часто називають неурядові аналітичні центри як незалежні у своїх дослідженнях та висновках осередки прогресивного знання. На перехідних етапах політичної модернізації та демократизації організації, на зразок західних «think tanks», зазвичай лише починають свій розвиток, але їх роль в генеруванні ідей, альтернативних візій, оновлених підходів до проблем політики фактично незамінна. Члени аналітичних організацій є фактичними розробниками цілей політичного розвитку, ретрансляторами прогресивних цінностей суспільства. Актуальні для країни питання, порядок денний політики формуються в тому числі й у цих осередках громадсько-політичної думки. В останні роки аналіз проблем та перспектив розвитку інформаційного суспільства тут займає важливе місце, а нерідко й окремий напрям діяльності низки організацій з політичної аналітики.

У демократичних країнах аналітичні центри часто беруться за надскладні завдання інформаційної безпеки, а їх тісна співпраця з державними структурами досить стабільна, що відображається і на практично-політичному, і на законодавчому рівні. Відповідний досвід особливо цікавий українським дослідникам, які звертають увагу на те, що, до прикладу у США ще в 2003 р. ухвалено закон «Про внутрішню безпеку» («Home Security Act»). Завдяки цьому затверджується Національна стратегія із забезпечення безпеки у

кіберпросторі; Національна стратегія фізичного захисту об’єктів життєзабезпечення населення; створено Міністерство внутрішньої безпеки, що координує діяльність державних органів і всіх приватних структур з питань забезпечення інформаційної безпеки. Загалом ці рішення заклали основи для єдиної національної системи протидії кібернетичному тероризму, створення територіальних, відомчих і приватних центрів протидії, чіткого визначення їхніх функції та порядку взаємодії [11, с. 93-94]. «Мозкові» центри США традиційно вважаються потужними осередками продукування відповідних важливих стратегій для інформаційної безпеки людей.

Водночас це не єдиний приклад для наслідування досвіду утвердження суб’єктності аналітичних організацій у системі інформаційної політики. Зокрема варто виокремити і політичні практики європейських країн, наприклад уряд Нідерландів у 2011 р. ухвалив Національну стратегію кібербезпеки «Сила через співпрацю». Цей досвід обговорювався на авторитетних міжнародних конференціях. Зокрема йшлося про створення Національної ради з кібербезпеки, що відповідальна за власне забезпечення реалізації підходу з максимального співробітництва державного та приватного секторів, зокрема й активне доручення до співпраці наукових центрів країни. Окремо започаткував діяльність і Національний центр з питань кібербезпеки (відповідальний за виявлення тенденцій та загроз інформаційній безпеці, сприяння подоланню пов’язаних з нею наслідків інцидентів і кризових ситуацій) [78, с. 30-31]. Отже, тут також незалежний громадський, науково-методичний, аналітичний супровід вважається невід’ємною частиною успішної діяльності безпекових інституцій.

Демократії, які відбулися, високо цінують експертне фахове знання, а звіти та рекомендації авторитетних центрів нерідко покладаються в основу держаних рішень. У країнах же, де відбуваються глибокі трансформації політичної системи та ціннісних основ суспільства, особливо важливою є роль неурядових аналітичних центрів також і як інструментів громадського контролю. У своїх публікаціях [369; 370; 384] ми відводимо цьому питанню особливу роль, адже йдеться не лише про цілісну державницьку стратегію, а й про зворотній бік

проблематики – моніторинг державних рішень та контроль за діями влади. У сфері інформаційної безпеки зокрема такі центри політичної аналітики до певної міри є зв'язковою ланкою між владою та громадою, посередником та ефективним каналом зв'язку між інтелектуальним середовищем і державними органами. Неурядові аналітичні центри у демократичній країні системно представлені у медіа-просторі країни, серед їх спеціалістів чимало медіа-персоналій, коментаторів суспільно важливих питань, кризових менеджерів, прогнозистів та консультантів з політичних питань, в тому числі й політико-інформаційних.

Однак громадські об'єднання у ролі інститутів, що формують суспільну думку, можуть виконувати досить суперечливі завдання порядку денного інформаційної політики. Налаштовані на співпрацю з державою, такі ініціативи дійсно можуть і вже приносять ефективні результати. Однак можливі й інші варіанти, коли неурядові центри є прихованим інструментом захоплення влади, а іноді й реалізації протиправних рішень. Прикметно, що саме корпус відповідальних аналітиків найчастіше й виявляє подібних об'єктів політики (які позаяк імітують власну суб'єктність і самостійність). Наприклад, про проблему «поширення проявів загрозливого впливу неурядових громадських організацій на стан національної безпеки України через дестабілізацію внутрішньополітичної ситуації» [211, с. 213] К. Павлюк попереджав ще задовго до 2014 р. Зокрема, вчений наводив приклад діяльності об'єднання «Народний фронт «Севастополь-Крим-Росія», що «проводило публічну агітацію і розповсюджувало матеріали із закликами до дій щодо зміни державного кордону, конституційного ладу України, реалізації силового сценарію возз'єднання Криму з Росією» [53; 211, с. 213]. Організації, що діють в інтересах позасистемної опозиції, іноземних урядів, потребують особливої уваги правоохоронних органів і однозначно не можуть розглядатися державою на рівні з громадським сектором.

Отже, не всі неурядові організації, які навіть діють легально, можна вважати повноцінними суб'єктами інформаційної політики, а тим більш

потенційними партнерами держави у справі забезпечення національної безпеки. Таке застереження має високу актуальність в умовах інформаційної війни загалом, а також під час важливих для країни подій: проведення виборів, референдумів, прийняття важливих законів, укладання багатосторонніх договорів, міжнародних заходів тощо. Уряди країн, які системно зазнають інформаційної агресії, вимушені здійснювати посилений контроль за діяльністю політично активних структур. Небезпечних акторів можна розпізнати за провокаціями у формі інформаційних приводів, дестабілізуючих публічних акцій (пікетів, перфоменсів, мітингів тощо), розповсюдженням антидержавної інформаційної продукції, загалом за руйнівною, такою, що підриває основи національної державності, діяльністю, в тому числі й в інформаційному просторі.

Безумовно, подібні застереження щодо боротьби з екстремістськими об'єднаннями і рухами у жодному разі не повинні руйнувати взаємної довіри суспільства та держави. Активізація громадських організацій у інформаційному полі є певним індикатором демократії, тож у демократичних країнах держава створює правові, організаційні, соціально-економічні умови для розвитку недержавних суб'єктів інформаційної безпеки. До того ж усіляке сприяння з боку державних структур всебічній співпраці з громадським сектором навпаки лише посилює позиції у боротьбі з псевдоекспертами, сепаратистами, терористами, що нерідко видають себе за лідерів думок.

Суб'єктність у інформаційні безпеці не вичерпується згаданими вище інститутами, їх ми детальніше опишемо в наступних розділах. Однак тут вибір держави та недержавного сектору в якості ключових суб'єктів здійснений невипадково, з акцентом не на протиставлення, а саме тісну взаємозалежність та взаємодоповнюваність. У сучасній теорії політики держава і громадянське суспільство більше не можуть розглядатися як протилежні категорії, і саме на прикладі інформаційної сфери це дуже показово. Партнерство, взаємна підтримка, спільні дії та цілі політичної модернізації і широкої демократизації – усі ці ознаки власне й вирізняють впливових і діяльних суб'єктів інформаційної

політики від вдаваних. Останні ж можуть траплятися як у громадському секторі, так і державному.

Відтак від суб'єктів інформаційної безпеки доречно перейти до питання її об'єктів. Якщо сучасний політико-владний ресурс зосереджений переважно в суб'єктів інформаційної політики, то виконавська культура реалізації владних рішень – у об'єктів, коло яких природно значно ширше. У цьому контексті ми знову зосередимося на особистості, організаціях, колективах, суспільстві, нації, народові, державі, але вже не як діяльних акторів, а з позицій їх чутливості та сприйняття актуальних проблем інформаційного простору та пріоритетних напрямків інформаційної політики.

Об'єкт у сучасній політології вважається тим, на кого спрямована діяльність суб'єкта. Вчені справедливо зауважують, що це підлеглий, пасивний елемент влади, від нього вимагається лояльність, готовність підкоритися суб'єкту [360, с. 695-696]. За аналогією з прийнятими у сучасних енциклопедіях підходами, серед об'єктів інформаційної політики виокремимо такі дві важливі групи як організовані канали суспільно-політичного життя та процеси політичного розвитку. Втім у сучасних дискусіях про об'єкт політики центральними залишаються категорії потреб, інтересів, запитів. Система інформаційної безпеки, як частина загальнонаціональної та міжнародної, повинна орієнтуватися на захист життєво важливих інтересів суспільства та держави, потреби громадян та їх легальних об'єднань, запити особистості та нації.

Отже, система інформаційної безпеки повинна бути спрямована на захист вищеперерахованих інтересів через різні форми і методи реалізації політики, а також власність, владу, морально-етичні норми як визначальні об'єкти політичного впливу та авторитету. Тому науковці відрізняють різні пріоритети в інформаційній сфері, зокрема й за визначальними інтересами об'єкта політики.

Відтак серед інтересів особистісних такі вчені, як Л. Борисова та В. Тулупов, як правило, називають «забезпечення конституційних прав і свобод людини на

збирання, зберігання, використання та поширення інформації», «недопущення несанкціонованого втручання у зміст, процеси обробки, передавання та використання персональних даних», а також «захищеність від негативного інформаційно-психологічного впливу та інші» [32, с. 41]. Людський вимір інформаційної політики, про який ми писали у попередніх розділах, зобов'язує особливу увагу приділяти інтересам особистості і при плануванні стратегії інформаційної політки, і під час її реалізації. Саме з особистості бере початок як політична ініціатива, та і здатність її реалізовувати, тобто суб'єктна й об'єктна сутність політики.

На колективи як об'єкт інформаційної безпеки зобов'язують звернути увагу ряд чинників. Передусім покликання на саме колективні інтереси містять чимало сучасних визначень національної та інформаційної безпеки. Нерідко науковці розуміють ці феномени як різновиди суспільних відносин, які складаються між людьми і саме їх колективами, а вже результатом такої стихійної чи цілеспрямованої діяльності вважають певний рівень функціонування і розвитку громадянського суспільства, правової держави, демократичного режиму, міжнародного співробітництва тощо [див. напр.267, с. 14]. У трудових, педагогічних, студентських та інших колективах формується свідомість, культура, переймаються поведінкові моделі, тож цілком виправданим видається їх осмислення у системі суб'єкт-об'єктних відносин національної та інформаційної безпеки.

По-друге, об'єктивні соціально-політичні реалії у країнах, що здійснюють демократичний транзит, зокрема і пострадянських, демонструють досить потужні позиції колективів, в тому числі і в контексті політичної соціалізації. Поза політичними контекстами оволодіння інформаційними навиками видається неповним, тож колективи, особливо у посткомуністичних системах залишаються важливим елементом інформаційної безпеки. В сучасних колективах дискутуються найактуальніші події зі світу політики, по-різному прочитуються поточні інформаційні повідомлення, а в умовах досі слабкої участі членів перехідних суспільств в роботі консультативних органів, партій чи громадських об'єднань, саме колективи зміцнюють ціннісні політичні орієнтири людей як підґрунтя

інформаційної безпеки нестабільних систем.

На рівні держави, області, району, міста тощо функціонують різні за масштабами колективи, що сприймають та інтерпретують інформацію у доступній їм формі та спосіб. Це може навіть загрожувати розколами у загальнонаціональному вимірі. Однак саме розуміння таких колективів як об'єктів інформаційної безпеки, впровадження адекватних цільових програм, орієнтованих на консолідацію та спільні завдання, і дозволяють вибудовувати захищений простір сучасного інформаційного суспільства. Професійні чи освітні колективи дійсно є тим організованим каналом, злагодженим механізмом, який цілком доречно використовувати для ефективного протистояння різноманітним інформаційним загрозам, а також для демократизації суспільно-політичного життя в країні загалом.

Зрештою суспільство як об'єкт інформаційної безпеки аналізувати у політологічному дослідженні досить відповідально, адже складна структура, гетерогенність присутніх у ньому інтересів практично унеможливлює всеохопність такого дослідження. Тут цілком погоджуємося з К. Поппером, який у концепцію «відкритого суспільства» вкладав велику перспективу, однак також зі застереженнями про небезпеки для його існування. Останніми він вважав усе, «що заперечує існування системи» [221, с. 448]. Тож інтереси суспільства складно відокремити від хоча б однієї з його складових. Усі сфери життєдіяльності та відповідні інтереси різних соціальних груп зазнають певних загроз, а отже й усі аспекти суспільно-політичного життя певною мірою мали би бути представлені у системі інформаційної безпеки.

Тут варто було б вирізнити лідерів думок, агентів змін та середньостатистичних членів суспільства, настрої, активність та лояльність яких вочевидь буде відрізнятися (як і міра участі у суб'єкт-об'єктних відносинах у політиці). Потужним чинником формування світогляду суспільства є не лише держава, але сучасні комерційні проекти та особливості ринкової економіки загалом. Вони привносять елемент конкурентності, пошуку нових ідей, прагнення модернізації у різні соціальні прошарки. З іншого боку, комерціалізація ЗМІ містить і деякі елементи, що загрозливі для системи інформаційної безпеки, і особливо

позначаються на свідомості суспільства: від пропаганди насильства до антидержавницьких закликів. Наслідком панування принципу «рекламної паузи» на телебаченні є вплив на психіку мільйонів людей, що легко перетворюються в об'єктів інформаційної політики інших держав, корпорацій тощо.

Сьогодні дослідники й дещо ширше ставлять питання щодо різних об'єктів у системі інформаційної безпеки, а саме у контексті феномену культури безпеки. При цьому культура інформаційної безпеки може бути увиразнена у тому ж таки особистісному, колективно-груповому та суспільному вимірах, але кожен з них осмислюється не як організований канал чи процес (як у пропонованих вище підходах), а саме як певний політико-культурний простір. Поняття культури безпеки трактується як рівень розвитку людини й суспільства, що характеризується значимістю забезпечення безпеки життєдіяльності в системі особистісних і соціальних цінностей, безпечної поведінки в повсякденному житті й в умовах небезпечних та надзвичайних ситуацій, рівнем захищеності від загроз і небезпек в усіх сферах життєдіяльності. На індивідуальному рівні культура безпеки проявляється у світогляді, нормах поведінки, підготовленості людини у сфері безпеки. У колективах діють деякі корпоративні цінності, професійна етика, мораль, і та ж (не)готовність до актуальних викликів інформаційного суспільства. Водночас на рівні власне суспільному йдеться про традиції безпечної поведінки, суспільні цінності, безпекові вразливості тощо [67, с. 42].

Все ж аналіз об'єктів інформаційної безпеки та інформаційної агресії через інституційну призму повертає нас до різних сфер життя власне суспільства, зокрема інформаційно-культурної, яка зазнає у наш час стихійних провокацій, нападів, а на стадії системних трансформацій та в умовах нових геополітичних реалій може піддаватися й руйнівним впливам, деструктивним інформаційним атакам. Увесь цей комплекс проблем виводить нас також на наступний рівень аналізу об'єктів інформаційної безпеки – дослідження у цьому контексті нації. Осмислюючи сутність суб'єкт-об'єктних відносин у системі інформаційної безпеки важливо враховувати її етнонаціональний вимір загалом, базові характеристики нації та народу в інформаційному просторі. Негативні інформаційні впливи, котрих зазнає

цей об’єкт політики, накопичуються, чимало з них пов’язані з тією ж культурною сферою і особливо виразні з вибором демократичного шляху розвитку.

Слушно зауважує О. Дзьобань про те, що сучасні методи інформаційної війни поширюються на всі сфери життя суспільства, а в транзитивній реальності часто проявляються у таких специфічних явищах як інформаційна релігійна експансія, переписування сторінок історії, свідоме перекручування норм національних мов у бік їх збідніння, введення ненормативної лексики тощо. Дослідник наголошує, що загроза поширення псевдокультурних знань і цінностей сприяє створенню фіктивного людського і соціального капіталу, а зрештою і деградації суспільства (низькому професіоналізмі, зниженню значущості моральних норм, створенню культу помилкових цінностей тощо) [72, с. 251]. Нам видається, що такі загрози ще більшою мірою позначаються на можливостях нації розвивати свій потенціал у суспільно-політичному житті. Адже саме націю з поміж інших суб’єктів/об’єктів політики вирізняє політична спільність, проживання на певній території, власна мова, культура, державність (або прагнення її створити).

Розглядаючи націю як об’єкт інформаційної безпеки, підтримуємо прийняту у сучасних наукових дослідженнях традицію розрізняти поняття «національна безпека» та «безпека нації». Зокрема Я. Лантінов зауважує, що доцільно розрізняти «національну безпеку» у широкому та вузькому сенсах. У широкому – це система «безпек» як усіх складових нації (ієрархічне поєднання безпеки держави, безпеки недержавних об’єднань (громад) та безпеки фізичних осіб), так і поєднання усіх аспектів безпеки (безпеки військово-політичної, економічної, енергетичної, екологічної, інформаційної тощо). При цьому національна безпека у широкому сенсі співпадає з суспільною безпекою (не плутати з громадською безпекою). Національна безпека у вузькому сенсі – це вищий, найзагальніший рівень безпеки, який не може бути зведений до жодного з окремих аспектів. Змістом національної безпеки у вузькому сенсі є забезпечення «життя» нації, її самобутньої життєдіяльності [163, с. 572].

У своїх публікаціях [див. напр. 370] ми послуговуємося визначенням національної безпеки у вузькому сенсі. Підкреслюємо, що самобутність будь-якої

нації проявляється, передусім, в її культурі, мові, традиціях, здатності сформулювати й реалізувати національну ідею. Відтак й інформаційна безпека нації – це також захист неповторних національно-культурних цінностей, історичних традицій, історичної пам'яті, мови, унікальних субкультур тощо.

Єдність культурного й інформаційного факторів особливо позначається на безпеці нації. Ми погоджуємося з дослідниками, які вважають, що перехід до демократичного устрою може мати деякі культурні наслідки та інформаційні загрози. В усталені періоди культура нації характеризується деякою єдністю, впорядкованістю, ієрархічністю, взаємопов'язаністю, водночас культура перехідного суспільства дещо мозаїчна, іноді й небезпечно вразлива, позбавлена спільної ідентичності, надзвичайно чутлива до зовнішніх загроз. До такого стану, на думку сучасних вчених, причетна одночасна дія декількох чинників: і внутрішні пошуки нацією свого місця в нових суспільно-політичних реаліях, специфічних умовах соціокультурного транзиту, і розвиток глобальних інформаційних й комунікаційних технологій, і геополітичні зміни, яких зазнає сучасний світ. Усе це сприяє руйнуванню системи цінностей традиційних спільнот, певній планетарній уніфікації культури, суспільної думки, політичної поведінки, запозичення окремих рис сторонніх культур [72, с. 248-249].

Інформаційна безпека повинна враховувати вищеозначені виклики та зменшувати їх негативний вплив шляхом сприяння відтворенню у суспільстві національно-культурних норм, при чому вочевидь спектр доступних для цього засобів варто розширювати, не обмежуючись лише системою освіти, але й зокрема розвиваючи ефективне співробітництво зі засобами масової інформації. Не випадково значної популярності набувають сьогодні також практики культурної дипломатії, їх використовують великі та успішні демократії, в тому числі й в цілях інформаційної безпеки – чим більше людей на планеті розумітиме національні традиції, культуру, історію, здобутки їхнього народу, тим більша ймовірність розвитку ефективних міжнародних відносин у сфері економіки, екології, високих технологій та у інших сферах суспільного життя.

Поліетнічні нації, серед яких і українська, мають додаткові переваги та

ризики на цьому шляху. Саме тому доречно говорити про політичну націю у контексті інформаційної політики, а також розглядати народ як об'єкт інформаційної безпеки. Дослідники переконливо доводять, що етнічна структура українського суспільства характеризується беззаперечним кількісним переважанням корінного автохтонного українського етносу, а також палітрою різних національних й етнічних меншин і груп, які репрезентують основні етномовні сім'ї у світі. Це одночасно розцінюється вченими і як постійний фактор збагачення політичної нації різноманітними досвідами, культурами, історіями, а також як чинник додаткових взаємних зобов'язань з гармонізації міжетнічних взаємин, з розбудови спільних ціннісних орієнтирів, культурних та інформаційних практик [54, с. 489]. Очевидно, що серед визначальних заходів інформаційної безпеки щодо окремих народів та етнонаціональних груп, мають бути ті, що засновані на принципах толерантності, плюралізму, віротерпимості, гуманізму, соціального детермінізму.

Етнонаціональні утворення закономірно також вразливі до зовнішніх інформаційних загроз, адже етнічні, культурні, релігійні, мовні відмінності легше надаються до використання у політичних маніпуляціях. Суб'єкти дестабілізації ситуації в поліетнічній країні часто орієнтуються саме на ці маркери розпалювання ворожнечі та протистоянь. Ці відмінності часто максимілізуються у інформаційному просторі, а досвід мирного та продуктивного співжиття фактично нівелюється. Держава мусить проводити системну роботу для того, щоб подібні зовнішні інформаційні атаки руйнувалися на фактичних реаліях суспільно-політичного життя, коли в країні встановлені рівні і чіткі правила етнонаціональних відносин, зрозумілі механізми та доступні канали комунікації між представниками різних громад, відкриті можливості для розвитку та взаємного обміну ідеями.

Зважаючи на велику кількість національних меншин й етнічних груп як об'єктів інформаційної політики, держава повинна дбати про їх захист, в тому числі й на інтегральній світоглядній основі, якою є українська національна ідея. Поняття це дуже дискусійне, резонансне у суспільстві, однак дослідникам вдалося

напрацювати низку визначальних характеристик, з якими суспільство зростає до рівня політичної нації, що керується національною ідеєю у своєму розвитку. Йдеться, як зауважують Л. Герасіна, О. Данильян, О. Дзьобань та інші: по-перше, і про «поліетнічну, консолідовану інститутом громадянства, приналежністю до країни як спільної Батьківщини»; по-друге, «про свідому своєї політичної мети спільноту, що прагне побудови незалежної, економічно міцної та соціальної, демократичної, правової держави»; по-третє, «про об'єднання спільністю історичної долі, мовою, культурними традиціями, толерантністю корінного українського етносу щодо численних етнічних груп» [224, с. 96-97]. Як мінімум ці три складові національної ідеї якісно наповнюють зміст суб'єкт-об'єктних відносин в інформаційній політиці, коли здатність і бажання виконувати покладені державою обов'язки з інформаційної безпеки обумовлені не стільки примусом, не лише існуючими загрозами, але й спільними прагненнями.

Держава власне також може розглядатися як об'єкт інформаційної політики, про що вже частково йшлося вище. При чому серед національних прагнень часто створення та утвердження у геополітичному просторі власної держави є достатньо потужною основою для забезпечення в тому числі й інформаційної безпеки. Отже, всебічний розвиток та історичний поступ цього базового політичного інституту не лише впливає на можливості інформаційного захисту, але сам по собі у сучасній політології розглядається як системоутворюючий об'єкт інформаційної безпеки.

Однак центральним є питання, яким чином може забезпечуватися інформаційний захист такої доволі потужної інституції як держава, і вочевидь тут на перший план виходять ключові політологічні правила та закономірності: поділу і розподілу влади, соціального детермінізму політики, демократизації суспільно-політичного життя, балансування інтересів, ресурсів, витрат і можливостей тощо. У широкому розумінні, яке подають сучасні науковці, інформаційна безпека держави − це захист вітчизняного інформаційно-культурного поля та національних інформаційних ресурсів. При цьому наголошується, що інформаційна безпека національних ресурсів, складовим елементом якої є державні інформаційні ресурси, забезпечується їх власниками

(для державних інформаційних ресурсів власником є державні органи управління) шляхом створення комплексної системи захисту інформації щодо несанкціонованого доступу та дотримання належного рівня їх захисту [284, с. 300].

Очевидно, коли ведемо мову про державу як об’єкт інформаційної безпеки, не можемо обмежуватися лише її ресурсами, доречно також увиразнити її інституційний, процесуальний, діяльнісний та інші аспекти, які детальніше розглянемо у інших розділах. Узагальнюючи різноманітні підходи щодо захисту держави як об’єкту інформаційної безпеки, наприклад, правознавці називають такі ключові параметри для постійного моніторингу та аналітики: кількість і види реально існуючих джерел загроз; імовірність реалізації кожної із загроз і нападу в цілому; розмір збитку, що завдається у результаті реалізації кожної загрози; ступінь стійкості об’єкта безпеки до деструктивних впливів (імунітет); здатність об’єкта уникати нападу (реалізації загроз); ступінь надійності системи захисту; здатність об’єкта безпеки до самовідновлювання і розміри витрат, необхідних для ліквідації наслідків нападу [133, с. 20]. Державні органи потребують комплексного аналізу та оцінки відповідних загроз, від яких залежить можливість не лише прийняття поточних рішень, але й стратегічних завдань.

Аналізуючи суб’єкт-об’єктні взаємодії у сфері інформаційної безпеки, на нашу думку, необхідно зосередити увагу на сутнісних характеристиках ідеологічних (внутрішніх і зовнішніх) суб’єктів інформаційної безпеки.

В залежності від типу політичної системи роль ідеологічних суб’єктів інформаційної безпеки, а саме партій, громадських рухів тощо, може бути багатоаспектною за формами прояву та силі впливу на загальнодержавну систему інформаційної безпеки. Так, у тоталітарних країнах ідеологічні суб’єкти інформаційної безпеки (партії, державний апарат) не допускають інших суб’єктів − колективи, етнонаціональні групи, до діяльності у цій сфері. Інформаційна безпека при тоталітаризмі спрямована, перш за все, на захист інтересів держави. Інформаційні потреби людини й суспільства в таких системах мають другорядний характер. Необхідно зазначити, що інформаційна

політика у тоталітарній країні передбачає захист «провладних» ідеологічних постулатів та критику інших ідеологій, які характеризуються як реакційні. Відповідно, у тоталітарних країнах всі засоби масової інформації знаходяться під жорстким контролем держави і являють собою систему не тільки агітації й пропаганди, а є також знаряддям маніпулювання суспільною свідомістю.

Як відомо, у демократичних політичних системах не існує однієї державницької ідеології. Держава забезпечує конкуренцію ідеологій, які є ненасильницькими за своєю суттю, на відміну, скажімо, від фашизму або комунізму. Інформаційна безпека у демократичних країнах спрямована на захист інтересів і громадянина, і держави, і суспільства як рівноправних об'єктів. У системі забезпечення інформаційної безпеки демократичної країни гармонізуються інтереси та відносини у трикутнику людина-держава-суспільство. Відтак ідеологічні суб'єкти інформаційної безпеки, а це перш за все, партії та їх представники в органах влади всіх рівнів й громадських організаціях впливають на вироблення інформаційної політики держави. В контексті нашого дослідження важливо з'ясувати як вибудовуються відносини між партійними структурами, мас-медіа та державою, оскільки саме за допомогою ЗМІ ідеологічні суб'єкти впливають на інформаційну безпеку країни.

Засоби масової інформації у полі уваги науковців різних галузей сьогодні невипадково, від якості та частотності медіа-супроводу залежить успішність численних політичних програм, заходів, суспільно важливих реформ тощо. Роль медіа у здійсненні інформаційної політики держави, як і у забезпеченні її інформаційної безпеки складно переоцінити. Одна й та ж подія, факт, явище суспільно-політичного життя через державницьку, ідеологічну чи партійно ангажовану призму медіа може набути абсолютно різного спрямування. ЗМІ мають доступ до світогляду сучасних людей, відтак стратегічного значення набуває захист національних інформаційних інтересів за їх допомогою.

Однак способів співпраці з медіа сьогодні чимало, а різні держави демонструють різні досвіди налагодження відносин з журналістською спільнотою як об'єктом та суб'єктом інформаційної безпеки. Не останню роль

тут відіграє структура власності на ЗМІ, а відтак і їх ідеологічна чи партійна приналежність. У західному дослідженні «Чотири теорії преси» Д. Галлін та П. Манчіні визначають щонайменше три такі моделі, які вказують на можливі шляхи взаємодії ЗМІ та держави: 1) модель «Поляризованого плюралізму» «з низьким рівнем тиражів газет, низькою фактичною професіоналізацією медіа-спільноти, високим рівнем її пов'язаності з політичними партіями та фінансово-промисловими групами, зокрема й регіональними (Іспанія, Італія, Греція, Португалія)»; 2) модель «Демократичного корпоративізму» «з високим рівнем розвитку масової преси, політичного паралелізму, журналістської професіоналізації, втручання держави у діяльність ЗМІ, визначальною роллю стабільних корпорацій (Німеччина, Австрія, Швейцарія, Бельгія, Голландія, Данія, Фінляндія, Норвегія, Швеція)»; 3) модель «Ліберальна» з високим ступенем журналістської професіоналізації, «середнім рівнем тиражів масових газет, низьким рівнем політичного паралелізму і втручання держави у діяльність медіа (Великобританія, Канада, США)» [46].

Вчені припускають, що сучасна українська модель може бути у цій системі координат означена як модель «Поляризованого плюралізму», при цьому аналізують дані відповідних державних установ та органів (Державної статистичної служби України, Книжкової палати ім. І. Федорова, Державного комітету телебачення і радіомовлення, Національної ради України з питань телебачення і радіомовлення ті ін.). Ті констатують, що в країні, наприклад, газети користуються відносно низькою популярністю, але при цьому достатньо тісно пов'язані з політичними партіями та фінансово-промисловими групами [39, с. 105]. Додамо, що очевидна ангажованість на інтереси окремих політичних сил, крім того, може бути обумовлена недостатнім державним контролем за галуззю, а також браком підтримки журналістської освіти, та системи вищої освіти в країні загалом, коли журналісти мало пов'язують виконання своїх професійних обов'язків з громадянськими зобов'язаннями та відповідальністю перед суспільством. У такий спосіб медіа-персона часто перетворюється з активного члена інформаційного простору в об'єкт чи навіть інструмент інформаційного

впливу зацікавлених сторін.

Загалом політичні сили (у демократичних країнах сформовані традиціями політичні партії) як ідеологічні суб'єкти інформаційної безпеки мали би бути зацікавлені у забезпеченні загальнонаціональних інтересів, в тому числі і через медіа-діяльність. Формування безпечного інформаційного простору дозволяє формувати власне електоральне поле, розвивати прозорі канали політичної комунікації, ефективніше проводити політичні стратегії тощо. Конкурентна боротьба політичних партій можлива лише в умовах незалежних ЗМІ, відтак інформаційно-просвітницька діяльність, популяризація демократичних цінностей мусить бути невід'ємною частиною партійних активностей. Збереження ж владних позицій за партіями також залежить від цілісності держави та єдності народу, тому політичним силам варто відмовитись від технологій протиставлення у суспільстві, розколів різних соціальних груп. Партії та їх лідери у демократичній системі усвідомлюють свою ідеологічну суб'єктність, в тому числі й відповідальність за захист національних інтересів, за інформаційної безпеку суспільства та держави.

Сучасні науковці та практики у політичній сфері переконливо доводять, що окрім внутрішніх ідеологічних суб'єктів інформаційної безпеки, варто аналізувати вплив на неї й зовнішніх ідеологічних суб'єктів. Вищеозначені суб'єкти можуть чинити на національну інформаційну безпеку як позитивний, так і негативний вплив. Позитивні наслідки проявляються тоді, коли зовнішні ідеологічні суб'єкти (партії, громадські організації, наднаціональні структури) підтримують ідеологічні настанови певної країни, наприклад, сприяють утвердженню ліберальних (демократичних) цінностей в Україні, діляться досвідом проведення певних реформ та ін. Негативний вплив зовнішніх ідеологічних суб'єктів проявляється у нав'язуванні тим або іншим країнам ціннісно-світоглядних настанов не сумісних з їх культурою, політичними традиціями, правовою системою тощо.

Серед зовнішніх джерел інформаційної безпеки дослідники традиційно згадують як широкі означення (наприклад, політику домінування окремих країн

в інформаційній сфері; культурну експансію щодо конкретної країни; напрацювання комплексних концепцій інформаційних війн та нападів), так і цілком конкретні (діяльність іноземних політичних, військових, економічних, розвідувальних структур в інформаційній сфері, а також міжнародних терористичних груп) [179, с. 24]. Зовнішній суб'єкт інформаційно-ідеологічного впливу вирізняється особливою небезпечністю, його складніше контролювати чи обмежувати національними засобами політики, він потребує міжнародної співпраці дієвих суб'єктів-партнерів.

Зовнішні ідеологічні суб'єкти достатньо активні в продукуванні деструктивних інформаційних впливів і розпалюванні інформаційних воєн. Їх об'єктом може стати окремий політичний інститут, певна соціальна група, суспільство загалом. Однак доступність цих об'єктів для інформаційних маніпуляцій найбільшою мірою залежить від держави, хоча й остання може надаватися цільовим інформаційним атакам. Найвразливішими для інформаційно-психологічної експансії, за визначенням вчених, є ті держави, яким властиві: а) відносна політична відкритість та стихійна включеність у глобальні процеси обміну капіталами й інформацією; б) етнічна, конфесійна, ідеологічна строкатість, травматичне минуле; в) відносно слабкі політичні інститути й вразливі інститути сектору безпеки [241, с. 6]. Часто саме вразливість однієї з цих складових максимально масштабується противником у світових масштабах за допомогою сучасних інформаційних засобів, й відтак поступово поширюється думка про так звану «failed state» (неспроможну державу) або й «government failure» (державне фіаско).

В наш час Україна постає типовим об'єктом впливу зовнішніх інформаційно-ідеологічних суб'єктів. Предметом цих впливів є національна єдність, територіальна цілісність, мова, культура, релігія, зовнішньополітичний вектор розвитку української держави. Проте зовнішні руйнівні дії певних суб'єктів не мали б значного впливу на суспільну свідомість та громадську думку, якби їх не підтримували політичні сили або окремі політики всередині України.

Таким чином, чим розвиненішими є внутрішні ідеологічні суб'єкти

інформаційної безпеки та структури, що з ними взаємодіють, тим меншим є вплив зовнішніх ідеологічних суб'єктів. Основне завдання внутрішніх ідеологічних суб'єктів інформаційної безпеки полягає у захисті національних інтересів та пріоритетів, а також у чіткому розумінні політико-ідеологічних цілей зовнішніх ідеологічних суб'єктів.

Наступний вимір проблематики актуалізують численні сучасні політичні мислителі, що аналізують виклики і проблеми глобалізації. Зокрема у праці В. Шахова та В. Мадіссона відстежуємо, як зміщуються акценти у розуміння національного інтересу під впливом глобалізованого світу та як посилюється «втручання міжнародних організацій у внутрішні справи країни, яка прагне взяти участь в тих чи інших інтеграційних проектах» [282, с. 48]. Ми погоджуємося з авторами, що в умовах тотального «розвитку інтеграційних процесів, подальшої інтернаціоналізації політики і зростання ролі міжнародних організацій, об'єктивно відбувається процес звуження національно-державного суверенітету» [282, с. 48]. Однак про межі та нові можливості такого звуження політологи та політики досі дискутують.

Інтеграційні процеси, розвиток ринкової економіки та інтернаціоналізація ринку капіталу й праці актуалізують проблему ролі суб'єкта комерційної діяльності як агента інформаційної безпеки (небезпеки) суспільства (якщо комерційна мета суперечить інтересам держави і суспільства, можливі його деструктивні інформаційні впливи на суспільство).

Суб'єкт комерційної діяльності у XXI сторіччі не може обійтись без застосування інформаційних технологій у різний спосіб: рекламна компанія, збереження та обробка інформації, продаж певної інформації іншим комерційним структурам, захист персональних даних співробітників, захист новітніх технологічних розробок тощо. Разом з тим, існує постійна небезпека несанкціонованого втручання у інформаційні ресурси комерційних суб'єктів з боку інших держав, іноземних комерційних структур (промисловий та комерційний шпіонаж, знищення баз даних задля перемоги у конкурентній боротьбі тощо).

Саме тому від якісного захисту власних інформаційних ресурсів суб'єктами

комерційної діяльності залежить і загальносуспільна та загальнодержавна інформаційна безпека, перш за все, у сфері економічної діяльності. Вищеозначені суб'єкти повинні дбати про власну інформаційну безпеку, прогнозуючи та нівелюючи можливі загрози, оскільки захист комерційної інформації є важливим чинником безпеки суспільства та держави загалом, та інформаційної зокрема.

У сфері інформаційної безпеки комерційних структур вчені пов'язують основні загрози з проблемами доступності, тобто порушення досяжної можливості використання комп'ютерних систем або оброблюваної інформації. При цьому Ю. Нестеряк зазначає, що «ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереження й керованості» [200, с. 64]. При цьому, продовжує науковець, інформаційні системи, як правило, розглядають через три визначальні аспекти: технічних засобів, програмного забезпечення і комунікацій «для ідентифікування і застосування промислових стандартів інформаційної безпеки (як механізми захисту і запобігання на трьох рівнях: фізичному, особистому і організаційному)» [200, с. 64].

З нашої точки зору, особливу роль у забезпеченні інформаційної безпеки суспільства та держави відіграють такі комерційні суб'єкти як ІТ-компанії. Вкрай важливе їх співробітництво з державою у розробці нового програмного продукту для всіх сфер життєдіяльності суспільства, розробка систем захисту інформаційних ресурсів держави, участь у створенні загальнодержавних стратегій та програм розвитку інформаційної сфери, протидії кіберзлочиності тощо.

В інформаційному суспільстві й комерційні структури, і держава, і громадський сектор повинні об'єднати зусилля щодо подолання небезпек у інформаційній сфері: комп'ютерні злочини, кіберзлочинність, кібертероризм тощо. Найбільшою проблемою сьогодення в діяльності правоохоронних органів щодо протидії злочинності є суттєве зростання комп'ютерних злочинів в наслідок широкого розповсюдження комп'ютерних систем і технологій у всіх сферах життєдіяльності суспільства. При цьому кіберзлочинність за своєю суттю набагато ширша за комп'ютерну злочинність і включає цілий спектр протиправних діянь.

Відповідно, у сучасній літературі, як констатує О. Бойченко, кіберзлочинність

тлумачиться як «сукупність злочинів, що здійснюються в кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних» [29, с. 57-58]. Також зі слів автора очевидно, що швидке зростання кіберзлочинності для сучасних фахівців очевидне, а відтак йдеться про можливість спричинення цими злочинами значного фінансового збитку громадянам, організаціям, державі при мінімальному ризику для злочинця, а також про зростання взаємозв'язку кіберзлочинності з організованою злочинністю [29, с. 57-58].

З метою забезпечення інформаційної безпеки держави важливо також прийняти правові норми для тих комерційних суб'єктів, які надають інформаційні послуги та працюють на ринку телекомунікаційних технологій. Зокрема, необхідно чітко прописати на законодавчому рівні не тільки права, але й обов'язки операторів та провайдерів телекомунікацій, які б відповідали положенням Декларації про свободу комунікацій в мережі Інтернет, затвердженої Комітетом Міністрів на засіданні заступників міністрів Ради Європи 2003 р. в м. Страсбурзі (Франція) [122], Конвенції Ради Європи про кіберзлочинність [144].

На нашу думку, для посилення відповідальності комерційних суб'єктів у галузі інформаційної безпеки варто імплементувати положення Конвенції Ради Європи про кіберзлочинність: надання органам дізнання та слідства повноважень щодо видачі обов'язкових до виконання приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які необхідні для розкриття злочину (ч. 1 ст. 16 та ст. 17 Конвенції про кіберзлочинність); збереження провайдерськими установами даних про трафік інформації на термін до 90 днів з можливістю подальшого продовження цього строку (ч. 2 ст. 16 Конвенції про кіберзлочинність); встановлення для суб'єктів, які зберігають комп'ютерні дані, зобов'язань не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом періоду, який визначається законодавством держави (ч. 3 ст. 16, ч. 3 ст. 20, ч. 3 ст. 21 Конвенції про кіберзлочинність); розкриття провайдером в інтересах органу дізнання або слідства технічної інформації, достатньої для ідентифікації

підприємств чи фізичних осіб, що надавали послуги, та шлях, яким інформація передавалась (ч. 1 ст. 17 Конвенції про кіберзлочинність); надання органам дізнання та слідства права терміново здійснити обшук (огляд, виїмку) комп'ютерної інформації [144].

Таким чином, суб'єкти комерційної діяльності можуть співробітничати з державними структурами у сфері інформаційної безпеки за такими напрямками як технологічний, консультативний, безпековий, науковий, інформаційно-аналітичний та ін.

Разом з тим, суб'єкти комерційної діяльності можуть створювати певні небезпеки для інформаційної сфери суспільства та держави. Яскравим прикладом вищеозначеного явища є діяльність певних ЗМК (засобів масової комунікації), зокрема окремих каналів комерційного телебачення. Так, нажаль, певні телеканали можуть демонструвати низькопробну продукцію, яка руйнує морально-психологічний клімат у суспільстві, пропагує насильство та нездоровий спосіб життя. Як справедливо підкреслюють фахівці, основний потік телематеріалів прямує з великих промислово розвинених країн Заходу (США, Англія, Франція, ФРН) у менш розвинені. Тільки США щорічно продають телевізійним організаціям інших країн телематеріалів на 100-200 тис. годин показу. Другий найбільший експортер телепрограм Велика Британія реалізує таких матеріалів на порядок менше (на 20-30 тис. годин відповідно), далі слідують Франція (15-20 тис. годин) і ФРН (5-6 тис. годин). У 1980-х рр. чимало європейських газет почали писати про «культурний геноцид» і «американський телевізійний десант в Європі». Тоді ж у Франції та інших європейських країнах, стала складатися протекціоністська політика щодо національного кіно та телебачення [73, с. 190-191]. Водночас такі звинувачення також є досить дискусійними, можуть мати змовницький характер, а сьогодні потребують максимально об'єктивного, критичного аналізу.

У будь-якому разі кожна країна покликана захищати національний інформаційний простір від закордонного інформаційного впливу, який забезпечується місцевими комерційними структурами задля отримання прибутку. Необхідно напрацювати чіткі критерії для визначення характеру діяльності

комерційних суб'єктів різного ґатунку згідно з якими можна визначати їхній позитивний або негативний вплив на інформаційну безпеку держави та суспільства.

Підводячи підсумки щодо суб'єкт-об'єктних характеристик у сфері інформаційної безпеки, варто проаналізувати проблему консолідації суб'єктів задля підвищення ефективності інформаційної політики та інформаційної безпеки загалом.

Консолідація суб'єктів інформаційної безпеки є нагальною потребою в Україні, від вирішення якої в наш час залежить не тільки захист національно-культурної ідентичності, але й збереження та розвиток держави. В умовах розв'язаної проти України інформаційної війни консолідація суб'єктів інформаційної безпеки повинна відбуватися навколо єдиної стратегії розвитку інформаційної сфери, ціннісних констант, виваженої та ефективної інформаційної політики.

На думку О. Гіда, інформаційна безпека нерозривно пов'язана з необхідністю зміцнення ідеологічної платформи держави. Іншими словами, щоб бути захищеними інформаційно, необхідно мати контрольовану державою медійну структуру (інтернет-ресурси, ЗМІ, телебачення), власну систему пропаганди для здійснення інформаційних атак і контратак стосовно спроб посилення зовнішніх впливів на суспільно-політичну обстановку в країні [47, с. 232; 383].

Не сприяє консолідації суб'єктів інформаційної безпеки той факт, що за роки незалежності Україна не виробила сталої стратегії національної безпеки в питаннях захисту її інформаційного суверенітету від деструктивних впливів. Недостатньо чітко прописані повноваження основних державних структур – МВС, СБУ, Державної служби спеціального зв'язку та захисту інформації щодо протидії викликам в інформаційній сфері. Багато проблем виникає і через незнання користувачами основ мережевої безпеки та відсутність в органах державної влади і місцевого самоврядування спеціально підготовлених кадрів, здатних оперативно та ефективно вирішувати ці проблеми. Сучасні дослідники також підкреслюють гостру потребу роботи з громадською думкою, утвердження розуміння того, що інформаційна безпека не є виключно віданням держави, але й кожної організації,

колективу, громадянина. Часткове розв'язання проблеми вбачається й поглибленні партнерства держави з приватним сектором, адже в нових ринкових умовах інформаційна безпека значною мірою залежить від останнього [47, с. 233].

Серед ключових суб'єктів забезпечення інформаційної безпеки та інформаційної політики вже традиційно згадуємо різноманітні ЗМІ та ЗМК, але в умовах інформаційної війни їх роль зростає на порядок вище. Відповідальність медіа-спільноти у реалізації інформаційної політики держави залежить і від ступеня її залучення до обговорення відповідних проблем. Тобто така суб'єктність не може бути односторонньою, лише у співпраці держави з медіа обоє набувають затребуваної сьогодні суспільної впливовості та користі. Ресурсність ЗМІ найчастіше полягає у доступі до первинних джерел інформації, відтак це їх співпраця – це можливість для державних структур та органів місцевого врядування бути максимально обізнаними у актуальних подіях і їх контекстах, оперативно реагувати на виклики, а також це вагома платформа для зворотного – системного інформування населення про ситуацію в країні, запроваджені реформи, очікувані результати політики тощо.

Дослідники зазначають, що державна інформаційна політика, зі свого боку, мала би передбачити максимально безпечне середовище функціонування ЗМІ та ЗМК, в тому числі орієнтувати сучасних журналістів, ведучих, блогерів на нейтралізацію негативних впливів з боку різного роду деструктивних сил, уникати спроб маніпулювання свідомістю людей через інформаційний ресурс. Не менш вагомим вчені називають і створення національних медіа-ресурсів – для відстоювання інтересів держави в глобальному інформаційному просторі, для аргументованого доведення до широких громадських кіл та світової спільноти значущих країні повідомлень про соціально-політичні події, історію, культуру народу [48, с. 337]. Отже, пов'язані, передусім комунікативними каналами, державні структури та медіа-платформи у такій взаємодії є особливо взаємокорисними та можуть формувати потужні проекти для спільного успішного позиціонування у світових інформаційних процесах.

Ідеологічна компонента суб'єкт-об'єктних відносин у сфері інформаційної

безпеки видається неповною без належної уваги закладам освіти та науки. Їх діяльність в інформаційному просторі зазвичай мало помітна, адже йдеться передусім про підготовку професійних кадрів, а також напрацювання стратегічно важливих знань, результати чого не одразу очевидні. Однак бездіяльність чи суттєве обмеження діяльності цих інституцій у системі інформаційної безпеки має незворотні негативні наслідки, адже без інтелектуальних спроможностей суспільству поступово стають недоступними більшість сучасних технологій.

Ми погоджуємося з дослідниками, які підкреслюють значущість закладів освіти у формуванні соціокультурного, об'єднуючого підґрунтя суб'єктів інформаційної політики та безпеки. При цьому вирізняють такі важливі напрямки освітньо-інформаційної політики: забезпечення єдності процесів управління освітою за допомогою автоматизованих засобів управління і пов'язаних з ними комплексів із використанням технічних і програмних засобів нових поколінь; створення інформаційних систем профільного міністерства на користь забезпечення процесів (у тому числі й інтелектуальних) освітньої діяльності; використання сучасних інформаційних технологій для досліджень і запровадження якісно нових засобів інформаційних технологій та форм їх застосування та ін. [290, с. 127]. Безумовно, це не вичерпний перелік, а проблема заслуговує окремого дослідження.

Загалом партнерство різних суб'єктів і об'єктів інформаційної безпеки, налагодження системних зв'язків, обмін важливими даними, стратегічна візія і виконавська культура у цій сфері – усе це цілком досяжне завдання, з огляду на сучасний етап розвитку інформаційного суспільства. Тут особливо цінними залишаються спільні демократичні орієнтири, прагнення соціально-політичної модернізації, утвердження незалежності, цілі сталого розвитку.

Вчені, зокрема Л. Борисова, В. Тулупов і Г. Красноступ, також слушно зауважують, що якісна консолідація всіх суб'єктів інформаційної безпеки передбачає: «зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності»; «забезпечення доступу громадян до інформації та забезпечення ефективного її використання; створення національних систем і мереж інформації»; «сприяння постійному оновленню,

збагаченню та зберіганню національних інформаційних ресурсів»; «створення загальної системи охорони інформації»; «сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету держави тощо» [33, с. 38-40; 431].

Висновки до Розділу 3

По-перше, визначивши основні переваги та ризики інтенсифікації трансферу та руху інформації у глобалізованому комунікативному просторі та в умовах інформаційної революційності, доведено неможливість повноцінного використання нових переваг, що з'являються в інформаційному суспільстві, без забезпечення адекватного рівня інформаційної безпеки. Можливості швидких інформаційних обмінів, отримання завдяки новим інформаційним технологіям нових знань, розвиток соціальних та індивідуальних форм творчості на основі оперування великими масивами інформації можуть бути нівельованими через некоректне або ж злочинне використання нових технологій навіювання, маніпулювання та інформаційних диверсій. Таким чином, можна стверджувати, що одним з ключових завдань сучасної науки є пошук адекватних шляхів утворення стійкого балансу між розвитком інформаційних технологій та вдосконаленням механізмів інформаційного захисту. При цьому, важливо враховувати глобальний характер інформаційної цивілізації, через який перед людиною і суспільством постають додаткові виклики та загрози інформаційній безпеці.

По-друге, класифікувавши контрольовані та неконтрольовані інформаційні обміни, визначено декілька принципів побудови ефективної системи державної інформаційної безпеки. Зокрема, держава має розробити нормативно-правову базу та задіяти управлінсько-адміністративні механізми для реалізації певної програми контролю за інформацією, що переміщається в національному інформаційному просторі. Тільки тоді коли контрольовані обміни будуть превалювати над неконтрольованими, можна буде говорити про

досягнення певного рівня інформаційної безпеки держави, суспільства і людини. При цьому, державний контроль за інформаційною сферою не повинен порушувати ключові права і свободи громадян. Більше того, як показує практика саме демократичне забезпечення прав громадян на отримання і передачу інформації може бути надійним підґрунтям для системи державного контролю над інформаційною сферою. Таким чином, стратегію забезпечення інформаційної безпеки в нашій країні треба розпочинати з широких демократизаційних перетворень, а також з розвитку та активізації реального і дієвого громадянського суспільства, яке не може існувати без сильної правової держави.

По-третє, розглянувши ключові деструктивні зовнішні та внутрішні інформаційні впливи як основні джерела загострення інформаційної небезпеки, доведено їх особливу гостроту в умовах глобальної цивілізації. Сьогодні жодна держава чи національне суспільство не в змозі адекватно відповісти на ті виклики, що породжує глобальний інформаційний простір. Проте, якщо держави-лідери здатні займати в цьому просторі активницьку позицію, то такі трансформаційні суспільства як Україна, автоматично перетворюються на об’єкти інформаційної агресії з боку могутніх суб’єктів глобалізованого світопорядку. Саме із врахуванням такої специфіки глобальних інформаційних реалій, на нашу думку, має відбуватися вибудовування стратегії інформаційної національної безпеки України. В умовах, коли в країні все ще розвиваються основи демократично-правової державності, громадянського суспільства, протистояти зовнішнім і внутрішнім деструктивним інформаційним впливам можна виключно спираючись на досвід та ресурсно-технологічну допомогу більш значних суб’єктів сучасного глобального геополітично-інформаційного простору.

По-четверте, проаналізувавши основні види та напрями збудження інформаційної небезпеки, серед яких особливо підкреслені спеціальні інформаційні операції, інформаційна агресія, інформаційна війна тощо, проілюстровано складність протистояння таким агресивним діям в умовах

сучасного глобалізованого світу. Технологічна сфера глобально-інформаційної цивілізації забезпечує високий рівень транспарентності інформаційного простору, що дозволяє потенційним суб'єктам інформаційної агресії вільно використовувати свою перевагу в технологічному та ресурсному потенціалі. Саме тому суб'єктами інформаційної агресії зазвичай є країни-лідери, що ставлять перед собою глобальні геополітичні завдання, або ж величезні транснаціональні корпорації, успіх яких залежить від маніпулювань з глобальним інформаційним полем. Для тих же держав та соціальних спільнот, що стають об'єктами інформаційної агресії, найефективніше, з нашої точки зору, діяти на упередження і профілактично. На рівні держави це означає необхідність підняття рівня освіченості та громадянської активності населення. Тільки освічені громадяни, що міцно спираються на демократично-правові державні інституції, здатні ефективно протистояти інформаційно-психологічним впливам, що чиняться під час інформаційних операцій чи воєн.

По-п'яте, суб'єкт-об'єктні характеристики інформаційної безпеки мають багатоплановий й різнорівневий характер, який варто враховувати при оцінках впливовості різних інститутів та визначенні стратегічних орієнтирів ефективного партнерства між ними. Системоутворюючим суб'єктом інформаційної безпеки є держава, але її діяльність у демократичних країнах не може повною мірою забезпечити багатоаспектні інтереси й потреби об'єктів у цій сфері. Саме тому виникає необхідність залучення до забезпечення інформаційної безпеки країни недержавних суб'єктів, а також різноманітних колективів, етнонаціональних утворень, комерційних структур тощо.

РОЗДІЛ 4

ІНФОРМАЦІЙНО-БЕЗПЕКОВА ДІЯЛЬНІСТЬ ДЕРЖАВНИХ ІНСТИТУТІВ ТА ПОЛІТИЧНИХ ПАРТІЙ

4.1. Інформаційно-безпекова діяльність державних інститутів: єдність культурного та політичного факторів

Від загального означення глобального та внутрішнього вимірів системи інформаційної безпеки, окреслених у попередніх розділах, перейдемо до осмислення проблеми у конкретному суспільстві. Актуальні часові ти просторові рамки незалежної України формують особливу політичну реальність, складну у своїй сукупності інститутів, норм, механізмів політичної дії, неоднорідну в інформаційному просторі, сповнену низки можливостей, викликів та небезпек. Конкретизуючи діяльність політичних інститутів інформаційної безпеки варто розпочати з ролі державного сектору як визначального у конструюванні відповідних правил, норм, орієнтирів розвитку.

Дійсно, погоджуємося з науковцями, які в інформації вбачають не лише знання, але й сучасне джерело влади. Соціальне значення інформації, тобто можливість за її допомогою здійснювати управління соціальними й економічними процесами, розширюється і набуває політичного характеру. Інформаційні ресурси сьогодні важливі і для демократизації та стабільності держави, і для оновлення продуктивних та організаційних сил суспільства, і для розвитку самої людини [273, с. 127]. Тому дискусійним все ще залишається питання першості за певним інститутом у структурі інформаційної безпеки, особливо у суспільствах, що як і українське, переживають черговий важливий етап політичної трансформації.

Водночас варто зауважити, що рівень цивілізаційного розвитку сучасної держави значною мірою залежить від інформаційного простору загалом, тобто існує деяка взаємообумовленість, про яку частково ми писали раніше. Україна як

демократична, правова держава не може відокремлювати свою інформаційно-безпекову діяльність від інших політичних та соціальних інститутів, поза межами соціо-культурного простору і глобальних контекстів загалом. На це передусім орієнтує стаття 17 Конституції України, в якій регламентовано: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [145]. Доречними будуть і застереження науковців про те, що при усіх перевагах інформатизації (оптимізація політичних механізмів, швидшому державному реагуванні на соціальні виклики, налагодження соціо-економічних процесів, вдосконалення основ взаємодії влади та суспільства), існує і її зворотний бік, пов'язаний передусім із розширенням кола зацікавлених у деструктивних інформаційних впливах суб'єктів політики, з маніпулятивним використанням інформаційних технологій, злочинними діями в інформаційному просторі тощо [152, с. 88]. Саме тому визначення та класифікація ключових політичних інститутів – агентів інформаційної безпеки – постає основою нашого дослідження, а інформаційно-безпекова діяльність державних інститутів у цій класифікації видається все ж первинною, хоча й тісно пов'язаною з іншими структурними компонентами.

Отже, якщо повернутися до розуміння інформації як джерела політичної влади, то безпекова система мала би передбачити усі необхідні механізми та структури для мирного та конкурентного її здобуття, демократичних процедур отримання і утримання влади, впровадження владних реформ та реалізації владних функцій, нарешті цивілізованих способів передачі владних ресурсів демократично обраним наступникам. Тут закладено безліч ризиків, відтак система інформаційної безпеки держави дбає про безперешкодну діяльність Центральної виборчої комісії, дотримання Виборчого кодексу України, ефективне функціонування інститутів законодавчої, виконавчої та судової гілок влади, розподіл влади з територіальними громадами, незалежну роботу ЗМІ тощо. Очевидно, що у кожній з названих структур реалізується загальнонаціональна та структурна компонента стратегії інформаційної безпеки.

Водночас, якщо розуміти інформацію як засіб політичної боротьби і навіть міжнародної війни, то державні інститути, що дбають про інформаційну безпеку, та їх спрямованість суттєво розширюються. Значення інформації у безпеці сучасного світу коротко окреслив М. Маклуен: «Істинно тотальна війна – це війна за допомогою інформації» [227, с. 43]. Тобто за допомогою застосування сучасних інформаційних технологій сьогодні розгортаються, підтримуються та згортаються збройні конфлікти, економічні й культурні експансії, терористичні акти та інші види агресивних впливів. Державні структури, серед яких Офіс Президента, Міністерство закордонних справ, постійні делегації Верховної Ради України та багато інших, тут також мають виступити єдиним «фронтом». Якщо у питаннях внутрішньої боротьби за владу важливе дотримання принципу стримувань і противаг, в тому числі й в інформаційній політиці, то глобальні протистояння сьогодні як ніколи провокують до розвитку консолідованих, довірливих, партнерських взаємин між усіма органами влади задля спільної дії та протистояння зовнішній агресії.

Для сучасної України інформаційна політика зберігає цю багатозадачність, а отже, й потребує множини взаємопов’язаних інституцій та органів з оптимально розділеними функціями та адекватною часу стратегією розвитку. При чому, цілком погоджуємося з вченими, які вважають, що саме інформаційну безпеку для такої, як наша, країни яка здійснює перехід до демократії та ринкових відносин, можна вважати пріоритетною, адже йдеться і про рівень захищеності, стабільності основних сфер життєдіяльності суспільства щодо небезпечного інформаційного впливу, і загалом про інтенсивність розвитку суспільства в тій чи іншій сфері за рахунок ефективного використання накопичених людством знань [25, с. 41].

Інформаційна безпека для незалежної України вбачається не лише у повторенні досвіду демократичних країн, яким вдається поєднувати різні її напрямки за допомогою стабільних інститутів. Специфіка українських реалій ще й у тому, що налагоджувати таку систему потрібно у цілковито відкритому дискурсі, коли силові методи утвердження державної влади неприйнятні, а

ідеологічний плюралізм звужує можливості для політичного переконання громадян. При цьому ключові завдання та зобов’язання держави не зменшуються, а до певної міри навіть ускладнюються з розвитком інформаційного суспільства і особливо з розгортанням масштабної інформаційної війни проти неї. Система повинна протистояти стихійним і зумисним, внутрішнім та зовнішнім загрозам, захистити суспільство й громадян від негативного інформаційного впливу, тобто вона насамперед пов'язана з діяльністю держави (встановленням правових норм, контролем за їх дотриманням, їх оновленням відповідно до актуальних суспільних потреб та інтересів тощо). Відтак сучасні засоби державної політики потребують інноваційного погляду, модернізації в часі, коли вимоги та загрози для такої політики постійно зростають.

Однак перш ніж шукати відповідей на питання «Яким чином модернізувати інформаційну політику України?», варто також окреслити «Хто саме відповідальний за здійснення державної інформаційної політики України?». Ми вже згадували, що статтею 7 Конституції України [145] забезпечення інформаційної безпеки України віднесено саме до найважливіших функцій держави. Держава здійснює свою діяльність через відповідні органи державної влади. Зокрема, ч. 3 ст. 7 Конституції України визначає коло суб’єктів, на які покладається забезпечення державної безпеки та виконання комплексу інших заходів, пов’язаних із забезпеченням національної безпеки, а саме у регламентації про «відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом» [145]. Вочевидь перелік цей неповний, особливо у контексті сучасного розуміння феномену інформаційної безпеки.

Агентами інформаційної безпеки прийнято вважати державу, державні органи та структури, що займаються виробленням відповідних орієнтирів, постановкою цілей і тактичних завдань політики, її забезпеченням на найвищому рівні. Важливо підкреслити, що це не тільки структури виконавчої гілки влади, а й законодавчої та судової. Важливу роль у інформаційній політиці відіграють і

органи місцевого самоврядування, державного адміністрування на місцях, що потребує окремої уваги у світлі сучасної реформи децентралізації та проведення перших місцевих виборів 2020 р. за новими правилами. Загалом будь-які інституціоналізовані форми вироблення та захисту конкурентоспроможного інформаційного продукту, боротьби з ворожими інформаційними атаками можуть розглядатися у цьому зв'язку, адже сучасна політика мережева за свою сутністю, з властивими горизонтальними й вертикальними зв'язками.

Водночас дуже слушно українські дослідники вирізняють власне політичні інститути у цій сфері. Політична складова забезпечення національної безпеки, за такого підходу і як стверджує М. Зайцев, покладається на таких агентів, як: «1) Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України, які здійснюють загальне керівництво, координацію та контроль за реалізацією заходів у сфері національної безпеки» [90, с. 231-238]; «2) Міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України, на які безпосередньо покладається виконання заходів у сфері національної безпеки» [90, с. 231-238].

Зауважимо, що центральні інститути держави, що проявляють посилену активність в інформаційному полі, потребують постійного моніторингу аналітиків та науковців. Можемо також прогнозувати, що у суспільстві, яке зазнає відчутних внутрішніх політичних трансформацій, а також потужних зовнішній інформаційних і військових атак, ця сфера ще довго характеризуватиметься деякою нестабільністю. Ці органи часто реорганізовуються, змінюють структуру, керівництво.

Зокрема ще відносно нещодавно ми, як і багато інших вітчизняних політологів, відстежували діяльність новоствореного Міністерства інформаційної політики України [див. 380]. Цей спеціальний державний орган

став до певної міри знаковим в історії інформаційно-безпекової діяльності нашої держави. Він був покликаний займатися виключно проблемами вироблення ефективної інформаційної політики та певною мірою інформаційною безпекою держави. Поява інституту викликала дискусії, неоднозначні оцінки, резонансні суперечки у ЗМІ. Водночас керівник цього відомства Ю. Стець окреслював у рамках діяльності Міністерства необхідність напрацювання Концепції інформаційної політики і стратегії її впровадження, у чому вбачалася згадана нами в попередніх розділах, затребувана стратегічна візія держави. Окремий департамент передбачався задля налагодження системної роботи щодо відображення інформаційних загроз з боку РФ і країн-лобістів. Ще один департамент мав на меті налагодження комунікації між органами влади стосовно дотримання єдиної позиції, формуванням ключових інформаційних послань України до світової громадськості. При цьому Міністр зазначав, що у діяльності його структура керується досвідом Великобританії, Франції, США, де такі органи існували під час Першої світової війни і були відновлені у 1938 році [120]. Отже, Міністерство інформаційної політики засновувалось в Україні саме з огляду на реалії війни, у відповідь на них.

Питання про профільне міністерство широко обговорювалося у політичному дискурсі України ще в 2014 р. 14 січня 2015 р. Кабінет Міністрів України ухвалив постанову «Питання діяльності Міністерства інформаційної політики України» [432], «відповідно до якої й було засновано цей орган як головний у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету та інформаційної безпеки України, серед основних напрямків діяльності якого: поширення суспільно важливої інформації в Україні та за її межами, забезпечення функціонування державних інформаційних ресурсів, розбудова в країні системи державних стратегічних комунікацій, забезпечення здійснення реформ засобів масової інформації» [391; 432].

Міністерство, як засвідчує офіційний сайт, провадило діяльність під гаслом «Найкраща пропаганда – це правда», та принаймні декларативно визначало цілком справедливі пріоритети роботи: розвиток інформаційного простору

України загалом через його дерегуляцію, демонополізацію, деолігархізацію; реформа урядових комунікацій та загальна комунікаційна підтримка проведення реформ; інформаційна реінтеграція тимчасово окупованої території АР Крим та м. Севастополь, а також тимчасово окупованих територій Луганської та Донецької областей; популяризація України у світі через соціальні кампанії й оновлення системи іномовлення [392]. Однак орган постійно піддавався критиці, що цілком очікувано для такої інституції стратегічного значення в країні, що зазнає системної інформаційної агресії. Прописані в Положенні [391] завдання далеко не повною мірою відображалися у звітності Міністерства [391], відтак на хвилі чергової зміни влади в країні самостійний орган припиняє діяльність, точніше зазнає фактично двох реорганізацій у 2019 та 2020 р.

Подальші зміни у цій системі ЦОВВ щодо інформаційної політики та інформаційної безпеки розглянемо трохи згодом, а тут варто зауважити, що увесь час функціонування незалежного державного управління інформаційною інфраструктурою України її було дещо розпорошено за різними інституціями. Відносно самостійну діяльність у цій сфері провадили Національна рада з питань телебачення і радіомовлення [103], Державне агентство з питань електронного урядування України [396], Державний комітет телебачення і радіомовлення України [397], Адміністрація Державної служби спеціального зв’язку та захисту інформації України [398], Національна комісія, що здійснює державне регулювання у сфері зв`язку та інформатизації [399], Служба Безпеки України [400], зрештою вже згадане Міністерство інформаційної політики. Лише простий перелік зазначених державних інституцій говорить про доцільність їх функціонального та структурного об’єднання. Головна мета їх діяльності – стимулювання розвитку галузі. Принципово, головним завданням усіх перелічених інституцій – захистити інформацію від неправомірного доступу чи поширення. Інституціям бракувало та досі не вистачає координації.

На нашу думку, провідну роль серед державних органів у забезпеченні ефективності інформаційно-безпекової діяльності держави тривалий час все ж відігравало Міністерство культури України (раніше ліквідоване, реорганізоване і

зрештою сьогодні перейменоване). Це Міністерство є центральним органом виконавчої влади України, функціонування якого координується урядом України. Згідно Положення, затвердженого постановою Кабінету Міністрів України у 2014 р., Міністерство культури України забезпечувало формування та реалізовувало «державну політику у сферах культури та мистецтв, охорони культурної спадщини, вивезення, ввезення і повернення культурних цінностей, державної мовної політики, а також забезпечувало формування та реалізацію державної політики у сфері кінематографії» [401]. Прямої вказівки на функції Міністерств у системі інформаційної політики у цьому документі ще не прописані, окрім необхідності широко висвітлення питань, що належать до компетенції Мінкультури.

Така функціональна сторона діяльності цього політичного інституту вже за 5 років буде увиразнена, і в цьому вбачаємо певну логіку. Тут погодимося з авторами, які вважають, що ще до недавнього часу зростання економіки асоціювалося переважно з розвитком у технічних галузях індустріального суспільства, але з опцією руху України до інформаційного суспільства сфера культури виходить на якісно новий рівень розуміння і сприйняття у системі державної політики. Культура сприяє наданню новітніх послуг, виробництву специфічних товарів, стимулюванню творчості, відродженню та розвитку унікальних традицій, локальних звичаїв, інноваціям у широкому розумінні цього слова [195].

Фактично ж від Міністерства культури України тривалий час залежали: достовірність і повнота інформації у суспільстві, зокрема через забезпечення документування історико-культурного процесу; збереження інформації (матеріальних носіїв культурно-історичної інформації, а також емоційно-образної складової культурної спадщини); якість та ефективність культурно-історичної інформації, утвердження місця культурної спадщини та культурних цінностей в масовій свідомості; забезпечення відповідності об'єктів культурної спадщини та їх атрибуції (неприпустимість спотворення в комерційних та інших цілях); збереження історико-культурного контексту та інформації, що

представляється різними установами культури та освіти (неприпустимість її спотворення в ідеологічних цілях); обмін і співробітництво між установами культури, освіти, ЗМІ з метою більш повного та достовірного представлення існуючої культурно-історичної спадщини [9, с. 48]. Усі ці напрямки дуже резонують з інформаційно-безпековою діяльністю держави загалом.

Стратегічне значення мають і структурні елементи цього Міністерства: з державної мовної політики; у справах релігій та національностей; з охорони культурної спадщини; зі сценічного і візуального мистецтва; з питань мовної політики та літератури; з питань музейної справи; з питань переміщення культурних цінностей; мистецької і художньої освіти; з питань мобілізаційної роботи; з відновлення та збереження національної пам'яті Українського народу та інші. Досить важливою функцією Міністерства вважалося регулювання порядку розповсюдження і демонстрування всіх видів вітчизняних й іноземних фільмів на території України.

Загалом на Міністерство великою мірою покладається відповідальність за стимулювання виробництва українського контенту державними та недержавними суб’єктами, за обмеження маніпулятивних та неправдивих повідомлень, потенційно небезпечного та аморального продукту в національному інформаційному просторі. Це безумовно входить до сфери інформаційної безпеки, втім тривалий час законодавчо не унормовувалося. З іншого боку, досяжність такої мети викликає чимало дискусій загалом, адже, як зазначають аналітики, виконавець у такому разі цілком прогнозовано стане «цензором» та «придушувачем свободи слова в Україні» для представників ЗМІ та громадських організацій [219]. Втім в умовах, коли ЗМІ чинять найпотужнішим вплив на свідомість сучасника, пошуки дієвих форм державних структур в інформаційній сфері продовжуються, як і способи забезпечення і підтримки якісного національного інформаційного продукту.

Однією з головних функцій Міністерства було і залишається забезпечення суспільної моралі та сприяння виконанню закону «Про захист суспільної моралі». Стаття 5 цього закону регламентує, що «змістом державної політики у

сфері захисту суспільної моралі є створення необхідних правових, економічних та організаційних умов, які сприяють реалізації права на інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному, інтелектуальному, морально-психологічному стану населення» [99]. Втім очікування та реальні результати у цьому питанні також розбіжні. Міністерство практично позбавлене відповідних можливостей, не контролює продукт, що надходить до споживача через ЗМІ, адже їх монополізація закриває доступ до таких питань.

Від Міністерства культури у системі забезпечення інформаційної безпеки України свого часу очікували численних заходів. Спільно з іншими міністерствами та відомствами воно мало б забезпечити виконання програми розвитку національного книговидання та преси, державне фінансування реконструкції та розвитку поліграфічної бази; створити умови для підвищення конкурентоспроможності українських ЗМІ, їх якості, технічної оснащеності, фінансової спроможності; підвищити рівень соціального захисту працівників ЗМІ; збільшити кількість інформаційно-пошукових каталогів та систем, які б були здатні повноцінно працювати українською мовою, мовно адаптованих програмних продуктів; посилити боротьбу з контрабандою іноземних друкованих видань та книг, аудіо-, відео-, кіно- та іншої інформаційної продукції; запровадити цільові програми «Світові зірки України»; максимально інтегрувати Україну до світового інформаційного простору тощо [79]. Цей перелік ще з 2009 р. є одночасно критерієм (не)спроможності державних інститутів України у системі інформаційної політики, але також і орієнтиром для подальших змін у цьому напрямку. При цьому інформаційні та культурна складова державної політики тривалий час осмислювалися паралельно.

У вересні 2019 р. у процесі чергової оптимізації системи центральних органів виконавчої влади акцент на інформаційній складовій з назв таких органів в Україні на певний час зник. При реорганізації шляхом перетворення Міністерства інформаційної політики утворено Міністерство культури, молоді та спорту України, на який покладено також завдання та функції ліквідованих Міністерства культури і Міністерства молоді та спорту [393]. Вже у березні 2020

р. через зміни до постанов уряду України новостворений орган перейменовано у Міністерство культури та інформаційної політики України, відновило свою окрему діяльність Міністерство молоді та спорту України [394]. Відтак інформаційну складову у системі урядової політики повторно увиразнено, хоча цього разу поряд і після культурної. Зміни настільки динамічно торкнулися цієї сфери, що спрогнозувати подальший інституційний розвиток системи інформаційної безпеки досить складно. Цілком ймовірно, що така ситуація невпевненості не заохочує й до відповідних активностей у самій цій державній структурі. З іншого боку, зближення гуманітарної та інформаційної політики держави через такий оновлений формат інституції видається досить перспективним.

Після обрання главою держави В. Зеленського і дострокових парламентських виборів 2019 р. формується Міністерство цифрової трансформації України. Як зазначено у відповідній постанові уряду «Питання Міністерства цифрової трансформації» від 18 вересня 2019 р. № 856 [433], це «головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сферах впровадження електронного документообігу, розвитку цифрових навичок та цифрових прав громадян, відкритих даних, національних електронних інформаційних ресурсів та інтероперабельності, інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу, надання електронних та адміністративних послуг, електронних довірчих послуг та електронної ідентифікації, розвитку ІТ-індустрії» [402; 433]. У вигляді двох відносно самостійних структур КМУ фактично розділяє інформаційну політику держави, водночас лише подальший аналіз відповідних політичних практик і державних рішень дозволить оцінити ефективність та доцільність такого розрізнення, а також його наслідки для інформаційної безпеки держави та українського суспільства.

Втім інформація на всіх етапах історичного розвитку людства була об'єктом політичної боротьби. Сьогодні правомірно стверджувати: чим більшими інформаційними можливостями володіє держава, тим вірніше вона домагається стратегічних геополітичних переваг та розвитку. Відтак стає зрозумілим, чому багато держав розглядають інформацію як стратегічний ресурс. Саме тому в Україні існує безліч інституцій, що опікуються тим чи іншим чином інформаційною безпекою, серед них згадаємо і ту роль, що її відіграють у безпековій діяльності також такі інститути як Державний комітет телебачення та радіомовлення України, Національна рада з питань телебачення та радіомовлення, Служба Безпеки України та інші.

Важливе місце у цій системі посідає Державний комітет телебачення і радіомовлення України, який бере участь у забезпеченні формування та реалізація державної політики у сфері телебачення і радіомовлення, інформаційній та видавничій сфері. Серед центральних органів виконавчої влади із спеціальним статусом він має достатньо довгу історію функціонування. Його попередники діяли ще у 1990-х рр., тоді ж на певний час комітет навіть було реорганізовано у Міністерство України у справах преси та інформації. Втім повноваження Держкомтелерадіо з тих пір зазнали численних трансформацій: від головного в системі органів виконавчої влади щодо забезпечення інформаційної безпеки до такого, що «виконує за дорученням Міністра культури та інформаційної політики за участю інших державних органів завдання щодо забезпечення інформаційної безпеки» [397].

Зазначимо, що навіть на офіційному сайті органу поки відображені не всі актуальні зміни [411]. Адже й чинне від 2014 р. Положення про цей комітет [396; 397] вже 5 разів змінювалося. Ним зокрема на Держкомтелерадіо покладаються нині такі завдання: «готувати пропозиції щодо вдосконалення системи державного управління у сфері телебачення і радіомовлення, інформаційній, видавничій сфері та поліграфії»; «узагальнювати практику застосування законодавства з питань, що належать до його компетенції, розробляти пропозиції щодо вдосконалення зазначеного законодавства в Україні»; «сприяти розвитку

вітчизняних ЗМІ»; «забезпечувати дотримання державної мовної політики у згаданих сферах»; «сприяти діяльності Суспільного телебачення і радіомовлення»; «забезпечувати єдність вимірювань, здійснення метрологічного контролю та нагляду у сфері»; «вживати заходів щодо обмеження доступу до видавничої продукції, що має походження або виготовлена та/або ввозиться з території держави-агресора»; «вести Державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції»; «забезпечувати підготовку пропозицій щодо призначення премій і стипендій в інформаційній та видавничій сфері» [396; 397]. Крім того, визначено багато іншого – загалом майже сорок завдань, що прямо чи опосередковано стосуються інформаційного простору.

Особливу увагу в системі інформаційно-безпекової діяльності держави привертають колегіальні інституції. Зокрема з 1990-х рр. намагається зберегти вплив на розвиток телерадіоінформаційної галузі та інформаційної політики сучасної України й Національна рада України з питань телебачення і радіомовлення – конституційний, колегіальний, постійно діючий орган. Цю раду з 8 членів фактично формують Верховна Рада України і Президент (по чотири члени кожен інститут, причому терміном на п’ять років). Згідно з Законом України «Про Національну раду України з питань телебачення і радіомовлення» [103], прямо про інформаційну безпеку серед визначальних функцій цього органу не йдеться (його метою визначено «нагляд за дотриманням законів України у сфері телерадіомовлення, а також здійснення відповідних регуляторних повноважень» [103]). Водночас сьогочасні члени Ради артикулюють достатньо амбітні цілі, тісно пов’язанні з необхідністю розв’язання назрілих політичних протистоянь, в тому числі і в сфері інформаційної безпеки. «Відповідальна журналістика – захист від зовнішньої агресії» – у такий спосіб сформульована на офіційному сайті місія Національної ради України з питань телебачення і радіомовлення, що зокрема передбачає захист інформаційного простору, розвиток мовлення на тимчасово окупованих територіях, перехід до цифрового стандарту мовлення, сприяння конкуренції на інформаційному ринку, суспільному мовнику, відстоюванню інтересів України на міжнародному рівні

тощо [412].

У політологічному дослідженні інститутів інформаційної безпеки складним видається рішення окреслити пріоритетні питання. Окремі питання забезпечення інформаційної безпеки законодавством покладено на інші державні органи. Окремі питання варто хоча б у загальних рисах окреслити, оскільки, як вже йшлося раніше, об'єктом негативних інформаційних впливів можуть бути різні аспекти суспільного життя, які прямо чи опосередковано впливають на політичну систему. Серед таких і суспільна мораль.

Законом України «Про захист суспільної моралі» 2004 р. [99] було передбачено заходи щодо захисту суспільства від подібного негативного інформаційного впливу, який спричиняє розповсюдження продукції, й відтак заборонено «виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні, а також продукції, яка пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України; пропагує фашизм та неофашизм»; «принижує або ображає націю чи особистість за національною ознакою»; «пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святинь»; «принижує особистість, є проявом знущання з приводу фізичних вад»; «пропагує невігластво, неповагу до батьків»; «пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички» [99] тощо. В інституційному плані також було передбачено створення спеціального органу, на який покладалася реалізація та додержання вимог чинного законодавства у сфері захисту суспільної моралі – Національної експертної комісії України з питань захисту суспільної моралі. Втім і цей постійний державний експертний і контролюючий орган викликав чимало дискусій у суспільстві, і відтак вже у 2015 р. був ліквідований.

Разом з тим, визначені законодавством напрями державного регулювання обігу інформаційної продукції, контроль у сфері захисту суспільної моралі покладено на вищі органи державної влади України, а також такі інституції як Міністерство внутрішніх справ України, Національну поліція, центральні органи

виконавчої влади, що реалізують державну політику у сферах культури, кінематографії, реалізують державну податкову і митну політику, а також на вже згадані вище Державний комітет телебачення і радіомовлення України, Національну раду України з питань телебачення і радіомовлення. На ці інституції покладається, як регламентовано в законі «Про захист суспільної моралі», відповідальність за створення в Україні «необхідних правових, економічних та організаційних умов, які сприяють реалізації права на інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному, інтелектуальному, морально-психологічному стану населення» [99].

Окремі питання забезпечення інформаційної безпеки також визначені в Законі України «Про оборону України» від 1991 р. (остання редакція станом на момент дослідження від 17.09.2020) [104]. Безумовно, оборона України серед центральних пріоритетів державної інформаційної політики, яка, за визначення ст. 1 цього Закону, передбачає систему політичних, економічних, соціальних, воєнних, наукових, науково-технічних, правових, організаційних, власне інформаційних та інших заходів держави. При цьому цілком доречно до її сфери залучені практично усі органи державної влади, військового управління, місцевих державних адміністрацій, органи місцевого самоврядування, підприємств, установ і організацій України у сфері оборони. Інформаційна складова у цьому законі окреслена достатньо чітко, зокрема як «проведення розвідувальної та інформаційно-аналітичної діяльності в інтересах підготовки держави до оборони; захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвинутої інфраструктури в інформаційній сфері тощо» [104]. У цій системі узгодження та координації спільних дій Міністерство оборони України, до прикладу, «провадить розвідувальну та інформаційно-аналітичну діяльність в інтересах національної безпеки та оборони держави, бере участь в аналізі воєнно-політичної обстановки, прогнозуванні» [104]; Генеральний штаб Збройних Сил України – визначає потреби в матеріально-технічних, інформаційних ресурсах, комунікаціях тощо, необхідних для ЗСУ та інших військових формувань, бере участь в організації

використання та контролю за інформаційним простором держави, проводить інформаційно-аналітичну діяльність в інтересах застосування ЗСУ; міністерства, центральні та інші органи виконавчої влади – також узгоджують з Генеральним штабом питання використання інформаційного простору держави.

Загалом система підготовки до збройного захисту та захисту України у разі збройної агресії або конфлікту, дійсно, повинна передбачити дуже чіткі правила взаємодії, зокрема й між ключовими політичними інститутами, що суттєво впливають на інформаційний простір країни. Не менш вагому роль у цій системі відіграє Служба зовнішньої розвідки України, діяльність якої регулюється Законом України «Про Службу зовнішньої розвідки України» від 2006 р. (зі змінами 17.07.2020 р.) [107]. Цей розвідувальним окремий державний орган України не належить до системи органів виконавчої влади та здійснює діяльність під загальним керівництвом Президента України, а також демократичним цивільним контролем. Орган відповідальний за добування, аналітичну обробку та надання інформації визначеним законодавством України керівникам вищих органів державної влади; здійснення спеціальних заходів впливу в інформаційній сфері з позицій державної політики України; забезпечення безпечного функціонування установ України за кордоном, захисту відомостей, що становлять державну таємницю; протидію зовнішнім, в тому числі й інформаційним загрозам національній безпеці України.

Велику кількість зобов’язань зі забезпечення інформаційної безпеки держави покладено на Державну спеціальну службу зв’язку та захисту інформації України, діяльність якої регулюється Законом України «Про Державну службу спеціального зв’язку та захисту інформації України» від 2006 р. (з останніми змінами 16.10.2020 р.) [93]. Ст. 2 Закону передбачає, що цей державний орган «призначений для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення,

урядового фельд'єгерського зв'язку, а також інших завдань» [93]. Зауважимо, що діяльність Служби спрямовується урядом, але вона також підконтрольна українському парламенту (адже звітує про додержання законів, прав і свобод людини та громадянина тощо) та президентові (адже звітує з питань, які пов'язані із забезпеченням національної безпеки України). Діяльність цієї інституції зосереджена на захисті держави як суб'єкта інформаційних процесів і відносин.

Неповним був би огляд державних інституцій, що функціонують у системі інформаційної політики, без звернення до досвіду Служби Безпеки України. На офіційному сайті цього державного органу спеціального призначення з правоохоронними функціями, чітко окреслені 5 ключових пріоритетів діяльності, серед яких чільне місце відведене захисту інформаційної безпеки [413]. Служба дбає про захищеність інформаційного та кіберпростору України, зокрема запобігає кібертероризму, кібершпигунству, блокує хакерські атаки, спростовує неправдиві повідомлення, викриває псевдопатріотичних та сепаратистських агітаторів, «ботоферми» тощо. У цьому ж напрямку розвиває діяльність підрозділ інформаційної контррозвідки у структурі СБУ, через який налагоджено також міжнародну співпрацю зі забезпечення інформаційної безпеки людей. Широкі повноваження та відповідальні завдання зобов'язують Голову СБУ до підзвітності перед ВРУ, Президентом, широкого інформування громадськості про свою діяльність; підрозділи органу також перебувають під наглядом прокурора.

Президент країни також дбає про забезпечення інформаційної безпеки держави, в тому числі й через ряд спеціально створених структур, через консультативно-дорадчі органи і служби. Тож, у системі інститутів формування та здійснення державної інформаційної політики варто окреслити й діяльність такого важливого консультативно-дорадчого органну як Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України. Вона покликана передусім налагоджувати порозуміння між різними структурами у цій сфері, зокрема здійснювати: аналіз

стану і загроз національній безпеці України в інформаційній сфері та узагальнювати відповідний міжнародний досвід; аналіз галузевих програм і виконання заходів, пов'язаних із реалізацією міністерствами та іншими ЦОВВ державної політики в інформаційній сфері; розробку пропозицій Президентові України та РНБО України щодо: визначення національних інтересів України в інформаційній сфері, концептуальних підходів до формування і вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки держави; реалізацію державної стратегії захисту національного інформаційного простору та входження України у світовий інформаційний простір [406]; удосконалення системи правового та наукового забезпечення інформаційної безпеки України; організації та порядку міжвідомчої взаємодії міністерств, інших ЦОВВ у сфері забезпечення інформаційної безпеки тощо [406].

Втім поки ще рано вести мову про інституційну зрілість структур, що сформовані при главі держави України та орієнтовані на інформаційну політику. Певний період за Наказом Президента України від 12 квітня 2014 року «Про Інформаційно-аналітичний центр» був створений та розгорнув активну діяльність такий інститут при Раді Національної безпеки і оборони України. [414]. У складі РНБО, що має суттєві переваги оперативного реагування на актуальні виклики та легітимації відповідних державних рішень, Центр інформував про ситуацію на Сході України, системно моніторив проблеми інформаційної безпеки. Вже сьогодні ця інформаційно-аналітична установа не є державним органом

Загалом спостерігаємо певну нестабільність консультативних і дорадчих органів та служб при Президентові. Деякий час у цій сфері діяла Рада з питань інформаційної політики при Президентові України Л. Кучмі (передусім відповідала за аналіз ситуації, що склалася в інформаційному просторі України) [407]. Пізніше, за президентства В. Ющенка, – Національна комісія з утвердження свободи слова та розвитку інформаційної галузі (була покликана до підготовки пропозицій з приводу виконання зобов'язань нашою державою як члена Ради Європи, ОБСЄ, а також досягнення Україною відповідності щодо

набуття членства в ЄС, зокрема у контексті ефективності й стабільності її відповідних інститутів та інститутів забезпечення свободи ЗМІ та слова) [408]. При Президентові України П. Порошенку була створена Рада з питань захисту професійної діяльності журналістів та свободи (зокрема для сприяння дотриманню конституції, слободи ЗМІ, слова, думки, дієвого взаємозв'язку держави та ЗМІ, а також громадянського суспільства) [409].

Схожі завдання має й новостворена у 2019 р. Указом Президента України В. Зеленського Рада з питань свободи слова та захисту журналістів: аналіз законодавства в інформаційній сфері, пропозиції щодо його вдосконалення; моніторинг стану забезпечення захисту професійної діяльності журналістів, додержання журналістських стандартів, пропозиції щодо посилення відповідних гарантій; напрацювання заходів щодо взаємодії держави, громадянського суспільства, ЗМІ з питань свободи слова; моніторинг інформаційного простору, пропозиції щодо вирішення актуальних питань захисту інформаційної безпеки України тощо [410]. Зауважимо, що діяльність подібних органів завжди перебуває під уважним наглядом журналістської спільноти, яка прямо належить до відповідної цільової аудиторії, відтак будь-які недоліки у роботі цих структур мають широкий резонанс у суспільстві.

Навіть побіжний огляд джерел з проблем інформаційної безпеки держави [90; 181; 220; 223] вказує на те, що головні зауваження дослідників зосередженні переважно довкола названих вище інститутів, зокрема тих, що діють у структурі виконавчої гілки влади. Проте у парламентсько-президентських республіках важливо звернути окрему увагу і на роботу законодавчого органу як інституту інформаційної безпеки. Саме через прийняті тут законопроекти надається поштовх роботі більшості згаданих вище інституцій, як і вносяться зміни у подібні структури, їх функції, повноваження в інформаційному полі країни тощо. Підкреслимо, що колегіальність, відкритість і гласність роботи Верховної Ради України є також однією із засадничих основ сучасної інформаційно-безпекової діяльності держави, коли доступ до її ключових матеріалів, можливість спостерігати за гострими політичними суперечками і погодженням політичних

рішень на головній політичній «сцені» країни відкрито практично для будь-яких осіб, журналістів, аналітиків. Сьогодні важливо зберегти цю транспарентність ВРУ та шукати нових форм її забезпечення, зокрема і в умовах карантину. У цьому питанні велика відповідальність покладена на Апарат ВРУ, який є розпорядником публічної інформації, потрібної в ході функціонування парламенту.

У структурі ВРУ також функціонує декілька важливих профільних комітетів, прямо причетних до інформаційної політики держави. Зокрема Парламент України дев'ятого скликання постановив утворити 23 комітети, серед яких у контексті нашого дослідження, увагу привертають три: Комітет ВРУ з питань свободи слова, Комітет ВРУ з питань гуманітарної та інформаційної політики, а також Комітет ВРУ з питань цифрової трансформації.

Перший зосереджений на таких важливих для сучасного суспільства і держави питаннях як забезпечення свободи слова, а також права громадян на інформацію, захист прав та свобод журналістів, працівників ЗМІ, гарантіях діяльності медіа. Комітет вже має свою історію у структурі ВРУ різних склакань, а його діяльність та звітність за попередні роки (зокрема з 2002 р.) доступна до загального ознайомлення [404].

Комітет з питань гуманітарної та інформаційної політики охоплює зримо ширше коло питань, які стосуються багатьох сфер суспільного життя та держави, зокрема: культурно-просвітницької та мистецької діяльностей; медійної індустрії, національної кіноіндустрії; аудіовізуального ринку; туристичної та рекреаційної діяльностей; охорони історико-культурної спадщини; рекламної та благодійної діяльності; діяльності друкованих і електронних ЗМІ; політики у сферах використання державної мови та мов національних меншин, а також свободи совісті та релігійних організацій; державна політика у сфері сімейно-шлюбних відносин, а також демографічна політика; висвітлення діяльності парламенту. За винятком питань, що належать до сфери національної безпеки та оборони, предметом відання саме цього комітету визначено державну політику у сфері інформації та інформаційної безпеки [403]. Комітет за заявленим

спрямуванням та назвою відображає закладену й в реорганізації відповідного Міністерства ідею щодо поєднання гуманітарної (культурної) та інформаційної політик. Про таку доцільність і ми часто писали у своїх публікаціях. Попередниками цього комітету слугували такі Комітети Верховної Ради України восьмого скликання: 1) з питань культури і духовності та 2) з питань свободи слова та інформаційної політики.

Зрештою кількісно найширший, деталізований предмет відання цей парламент визначив для новоствореного Комітету ВРУ з питань цифрової трансформації. Серед його орієнтирів: правові засади цифровізації та цифрового суспільства, зокрема й відповідні Національна, державні, міжнародні програми цифрового співробітництва; електронна демократія та урядування; державні інформаційно-аналітичні системи; державні інформаційні ресурси та сфера «відкритих даних»; смарт-інфраструктура міст і громад; інновації у сфері цифрового підприємництва, електронної комерції; стартапи й дослідницько-аналітичні центри у сфері цифрових технологій; електронна індустрія та теле- і радіокомунікації; віртуальні активи, блокчейни та токенізація тощо; розвиток орбітальної економіки; кібербезпека, технічний та криптографічний захист інформації; цифрові компетентності та права громадян, та ще багато іншого [405]. Очевидно, що логіка заснування Комітету так само, як і у вище згаданому випадку, відображає урядові візії, ця інституція навіть має спільну офіційну сторінку з однойменним Міністерством.

Загалом в Україні досить складна мережа державних інститутів, що визначають, реалізують та контролюють сферу інформаційної безпеки. Між ними не завжди узгодженні повноваження, налагоджена співпраця та збережена інституційна пам’ять. Водночас намічені й деякі позитивні зрушення у напрямку модернізації та демократизації. Комплекс здобутків та недоліків в організації роботи державних інститутів, відповідальних за інформаційну безпеку в Україні, спробуємо об’єднати, відповідаючи на питання про те «Які проблеми визначають спрямованість інформаційно-безпекової політики держави?»

Зокрема можемо відмітити, що сьогодні практично кожна така інституція в

Україні, окреслюючи власні завдання та пріоритети роботи, враховує зовнішньополітичний вплив на національну інформаційну безпеку, а також роль міжнародного співробітництва для інформаційного захисту і розвитку суспільства. Це співзвучно застереженням дослідників, які багато років наголошували, що країни з нерозвиненим інформаційним простором можуть бути лише споживачами інформаційних продуктів, однак останні далеко не завжди відповідають національним інтересам. Для незалежної України окремим значущим напрямком інформаційної політики завжди було формування і підтримка її позитивного іміджу в світі. Однак аналітики стверджували, що загальний обсяг інформації закордоном про Україну та її зовнішню політику незначний (порівняно з потенціалом), а в деяких секторах міжнародної політики, регіонах планети, ділових колах тощо і зовсім відсутній. До того ж ця інформація часто тенденційна, не відповідає дійсності, неактуальна [273, с. 131]. Не можна стверджувати, що сьогодні ситуація у цій сфері збалансована. Інформаційна активність зовнішніх акторів щодо України як і раніше велика, а після 2014 р. в рази посилилася. Важливо, що саме державні інституції налагоджують сьогодні роботу з вчасного, доступного, багатостороннього, об’єктивного інформування про події в Україні, її історію, культуру, традиції, здобутки тощо.

Водночас державні інститути України, які працюють зокрема й з міжнародними викликами, могли би чіткіше вирізняти функції та повноваження, зважаючи на достатньо конкретні та напрацьовані багаторічними дослідженнями вектори інформаційної безпеки. Зокрема вчені вказують на таку структуру: 1. Глобальна інформаційна безпека (безпека розвитку міжнародної інформаційної сфери; захист міжнародного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин; захист та обмеження обігу інформації в цілях глобальної інформаційної безпеки; захист міжнародної інформаційної інфраструктури; захист міжнародних інформаційних ресурсів; побудова глобального інформаційного суспільства тощо) [137, с. 16]; 2. Інформаційна безпека окремих держав у міжнародному інформаційному просторі (безпека інформаційного простору держави від інформаційних загроз,

інформаційних операцій, інформаційного тиску та інформаційних війн з боку інших акторів міжнародних інформаційних відносин; захист державного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин; захист та обмеження міжнародного обігу інформації в цілях державної інформаційної безпеки; побудова та забезпечення належного функціонування інформаційного суспільства; захист своїх приватних осіб від незаконних посягань акторів міжнародних інформаційних відносин тощо) [137, с. 16]; 3. Інформаційна безпека установ у міжнародному інформаційному просторі: захист інформації з обмеженим доступом, яка належить установі, від несанкціонованих дій з боку інших акторів міжнародної інформаційної сфери; доступ до загальнодоступної інформації та інформації, доступ до якої не може бути обмежено; захист від випадкового чи навмисного втручання в нормальний процес функціонування автоматизованої інформаційної системи організації з боку інших акторів міжнародної інформаційної сфери тощо) [137, с. 16]; 4. Інформаційна безпека людини в міжнародному інформаційному просторі (захист інформаційної і комунікаційної приватності, персональних даних; вільний доступ до масової та суспільно-значущої інформації; захист від негативного інформаційного впливу; захист інформаційних і комунікаційних прав на міжнародному рівні тощо) [137, с. 16].

Безумовно, окреслене питання має доктринальний характер та може розв’язуватися лише спільними зусиллями державних і громадських інститутів усіх країн світу. Невипадково, науковці знаковою вважають Резолюцію 54/49 «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки», прийняту на 54-та сесії ГА ООН, коли логіку і потребу міжнародної інформаційної безпеки концептуалізовано глобальною справою сучасності та людства [175, с. 46]. Міжнародні організації сьогодні сприяють, всілякими способами заохочують увагу урядів та громадськості до концепції стратегічної стабільності людства у XXI ст., яка б передбачала обов’язково й інформаційну складову. Така стабільність зазнає сьогодні негативних та суперечливих впливів, при чому не лише у контексті політичних, економічних, етнічних, соціальних та

інших конфліктів, але й у світлі світових (дез)інтеграційних процесів. Інформаційна безпека як умова підтримки міжнародного миру визнається і авторитетними світовими вченими, і дипломатами, і сучасними політичними візіонерами. Система глобальної безпеки еволюціонує та змінюється, а перехідні суспільства у цій системі можуть розглядатися і як особливо вразливі до інформаційних загроз об'єкти, і як середовища, що швидше інших пізнали сутність гібридних атак, а отже й здобули цінний досвід спільного протистояння інформаційним агресіям.

Важливим напрямком розвитку інститутів системи інформаційної безпеки в Україні є також розуміння як державних інтересів, так і загальнолюдських цінностей у цій галузі. Дійсно, про це пишуть і багато сучасних дослідників, адже об'єктами інформаційної безпеки є передусім люди, з одного боку, та держава, з іншого, як певна цілісність. Тобто для інститутів, що відповідальні за безпеку та оборону, важливо дбати і про захист свідомості, орієнтирів, психіки людей та їх спільнот, і про державний інформаційний суверенітет загалом (виняткове право держави на формування й використання усіх інформаційних засобів, створених за державний кошт; належне володіння й розповсюдження всією спільнотою у державі відповідних національних інформаційних ресурсів) [135, с. 60]. Тому дуже часто у сучасних положеннях про відповідні органи влади ми бачимо цілком доречне збалансування цих аспектів: прав і свобод людини, а також захисту державного суверенітету, що видаються вкрай пов'язаними та взаємозумовленими у країні, яка прагне демократії.

Загалом погоджуємося з вченими, які виокремлюють конкретні напрями регулювання інформаційної сфери державою як визначальним агентом інформаційної безпеки: забезпечення права й можливостей людей для доступу до інформації й інформаційних ресурсів; забезпечення інформаційної безпеки індивіда, спільнот, держави; заохочення конкуренції, боротьба з монополізмом, зокрема державний контроль за концентрацією ЗМІ в руках фінансово-промислових груп; дотримання свободи слова; захист інтересів різних соціальних груп (національних меншин, молоді, професійних спільнот тощо) в

інформаційній сфері; охорона національної культурної спадщини, мови, протистояння ідеологічній експансії інших країн; захист інтелектуальної власності; впровадження переваг електронної демократії та електронного уряду; боротьба з кіберзлочинами; правове регулювання інтернету та інші [179, с. 22]. Відмітимо, що у змісті діяльності різних державних органів України ці напрями часто повторюються.

При цьому важливо враховувати, що рівень інформаційної безпеки визначає стан розвитку політичної, соціально-економічної, оборонної, закордонної та інших компонентів національної безпеки в нашій державі, а відповідні деструктивні інформаційні впливи проявляються фактично у всіх сферах життя суспільства. Тому інформаційна складова логічно повинна бути присутня у структурі функцій кожного державного органу, однак їх розосередження часто загрожує фактичною бездіяльністю. Деякі вчені навіть вважають, що в Україні немає реальних гарантів її інформаційної безпеки, відсутній необхідний комплекс нормативно-правових актів, а весь процес інформатизації має стихійний, некерований характер, зрештою переважає використання іноземних інформаційних продуктів [220, с. 798-801].

У Законі України «Про основи національної безпеки України», який втратив чинність у 2018 р. [105], визначалися «основні напрями державної політики з питань національної безпеки в інформаційній сфері»: «забезпечення інформаційного суверенітету України»; «вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну»; «активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України»; «забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів

державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції»; «вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України» [105].

За окремі напрямки, а також у комплексі назрілих проблем ще чимало аналітиків та науковці гостро критикують державні органи, що функціонують у сфері інформаційної політики. Виходячи з вищевикладеного треба зазначити, що в Україні склалася ситуація, коли кількість відповідних установ, що зобов'язані відповідати за інформаційну безпеку все ще не переходить в якість їх діяльності. Число державних органів в інформаційній сфері та відцентрові інтереси різних зацікавлених сторін ускладнює можливості порозуміння та максимальної політичної ефективності. На це нерідко вказують і самі державні службовці: громіздка та неефективна система національної інформаційної безпеки України часто лише безпідставно поглинає ресурси, натомість потребує оптимізації, взаємоузгодженості довкола спільної мети [219].

Щодо ролі державних інститутів у гарантуванні «безпечного інформаційного простору» для людини і суспільства, то дослідники наголошують, що в нашій країні відсутня ієрархічно побудована організаційна структура державних органів. Це зауваження стосується і вищих ланок гілок влади, і самоорганізації громадян, тобто йдеться про необхідність чіткішого визначення уповноважених органів, їх організації, функцій, координації у сфері інформаційної безпеки [207, с. 63].

Значною мірою, на прикладі українських політичних інститутів, бачимо, як змінюється їх структура та місце в ієрархічній системі залежно від викликів і загроз, що постають перед сучасним інформаційним суспільством. Тому осмислюючи актуальні проблеми інформаційно-безпекової діяльності держави, важливо передусім окреслити ті проблеми, які постійно або періодично впливають на інституційну спроможність та ефективність держави.

У цьому питанні також можна використати декілька наукових підходів.

Зокрема доречно розрізняти реальні та потенційні небезпеки безпеці України в інформаційній і комунікаційно-технологічній сфері, які досить часто на практиці тісно пов'язані. Нерідко реально назріла проблема разом із собою також приносить низку додаткових потенційних загроз. Відтак розуміння різних сценаріїв розвитку політичних подій складає важливу частину роботи державного апарату. Зважаючи на чинне законодавство, сьогодні серед викликів стабільності українського суспільства в інформаційній сфері: окремі випадки обмеження свободи слова; проблеми з доступом громадян до інформації; різні форми поширення у медіа-просторі культу насильства; масова комп'ютерна неграмотність і відповідно висока комп'ютерна злочинність; випадки розголошення таємної державної, а також конфіденційної інформації; численні приклади політичних маніпулювань суспільною свідомістю через поширення недостовірних, неповних або упереджених повідомлень [105]. Особливо варто наголосити на небезпеці посягання на державний, зокрема й інформаційний суверенітет України. Усвідомлення потенційних та реальних загроз, пошук дієвих механізмів протидії їм може суттєво розвинути існуючу систему інформаційної безпеки держави.

З дещо інших позицій науковці розрізняють також внутрішні та зовнішні джерела інформаційної безпеки держави, при цьому не можна недооцінювати жодну із цих груп ризику. У внутрішніх викликах важливо враховувати згадану раніше гуманітарну складову, адже серед джерел внутрішніх загроз – і відсутність історичних традицій, і прогалини політичного досвіду та інституційної пам'яті, і деформовані уявлення про основи демократичного співжиття, функціонування правової держави тощо. Усі ці, по суті аксіологічні позиції відображаються і в інформаційній сфері, зокрема зростанням числа комп'ютерних злочинів, зниженням рівня освіченості громадян, нестачею кадрового потенціалу для роботи з сучасними високими технологіями. Інституційно внутрішні джерела небезпек також дуже відчутно позначаються на спроможності держави запроваджувати механізми електронного врядування, кіберзахисту органів влади та державних підприємств, основи електронної

демократії тощо

Про зовнішні джерела інформаційної безпеки вже частково йшлося раніше, однак тут окремо підкреслимо, що описані науковцями зовнішні загрози для України (зокрема, як зазначає Я. Малик: «діяльність іноземних політичних, військових, економічних, розвідувальних структур в інформаційній сфері»; «політика домінування деяких країн в інформаційній сфері»; «діяльність міжнародних терористичних груп»; «розробка концепцій інформаційних війн іноземними структурами»; «культурна експансія щодо конкретної країни та інші» [179, с. 25]) – повинні спровокувати перегляд і державної інформаційної політики. При чому не лише інформаційно-безпекової, адже діалектика внутрішнього та зовнішнього факторів найчастіше вже як наслідок має інформаційний резонанс, але корінням своїм сягає значно складніших соціальних, економічних та інших аспектів життя суспільства.

Відтак ми погоджуємося з дослідниками, які виокремлюють два головні напрямами забезпечення інформаційної безпеки держави: 1) у сфері міжнародної співпраці – інтеграція в міжнародну систему забезпечення інформаційної безпеки і співпраця по запобіганню протиправних дій в інформаційній сфері; 2) у сфері оборони – вдосконалення системи моніторингу загроз та їх джерел, своєчасне інформування відповідних суб’єктів влади про стан інформаційного ресурсу, про інформаційні системи оборонної сфери; засобів, методів і способів здійснення, спеціальних заходів і заходів інформаційного впливу; системи підбору і спеціальної підготовки користувачів тощо [227, с. 45]. Водночас наголошуємо на необхідності тісного взаємозв’язку державних інститутів, відповідальних за кожен із цих напрямів, вибудовуванні відносин за демократичними принципами стримувань і противаг.

Погляд на державні інститути з позиції актуальних загроз та проблем у інформаційній сфері допомагає з’ясувати загальний рівень їх ефективності, виявити недійові механізми, зайві/законсервовані елементи системи, накреслити план тактичних завдань та стратегічні програми модернізації, реорганізації тощо.

Зрештою повернемося до окресленого на початку розділу питання: «Яким

чином модернізувати інформаційну політику України?». Вчені, які тривалий час аналізують особливості інформаційної політики держави, зокрема й українські контексти інформаційної безпеки, стверджують, що можливості інформаційного захисту сьогодні суттєво урізноманітнилися і їх варто вивчати окремо. При чому теорія політичної модернізації та демократичного транзиту тут особливо доречна і навіть дозволяє осмислити цю проблематику, як мінімум, у трьох різних підходах.

Перший підхід головний акцент робить на сучасних реаліях інформаційного суспільства як принципово відмінного від попередніх і за ступенем розвитку держави, і за інтелектуальною зрілістю окремих людей та їх спільнот, до чого не завжди готові слабші країни, їх інститути та широкі суспільні маси. Відтак, до прикладу, у державному управлінні для запобігання чи/та нейтралізації загроз інформаційній безпеці пропонується, зокрема В. Григор'єв, застосовувати такі три базові групи методів: 1) правові (розробка комплексу нормативно-правових актів та положень, що «регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки») [58, с. 54-55], «2) програмно-технічні (наповнення національного інформаційного простору новітніми технологіями, що здатні істотно підвищити адекватне відображення реальності, продуктивність інформаційної діяльності в суспільстві, захист національних інтересів)» [58, с. 54-55] та 3) організаційно-економічні методи (безпека інформаційної революції для суспільства через коректне управління соціально-економічними процесами).

Для України цей тріадний комплекс методів дуже важливий. Адже поки ми маємо справу з недостатнім розвитком політичної і правової культури суспільства, низькою обізнаністю в сучасних технологіях, цифровою нерівністю та її економічними, соціальними і навіть політико-психологічними наслідками для країни. Відтак держава мусить здійснювати визначальні заходи у всіх трьох напрямках та стимулювати до таких активностей усе суспільство, що зрештою може сприяти демократичному переходові.

У організаційній частині, на думку ряду дослідників, система забезпечення інформаційної безпеки України не виконує окремих важливих функцій: неефективне управління її діяльністю; несистемний характер організаційних змін та реформ; відсутність аналітичної підтримки, прогностичних оцінок щодо функціонального змісту та напрямків розвитку органів державної влади тощо [220]. Недоліки організації можуть бути тимчасовими, але є й такі, що набули негативної тенденційності або законсервованості, що, як результат, може призвести до чергового кризового стану національного інформаційного простору, загроз державному суверенітету, демократії і безпеці людей. Соціально-економічні труднощі часто пов’язанні з обмеженнями прав і свобод людей, закритістю інформації, перешкоджаннями роботі незалежних журналістів. Ескалація інформаційних загроз фактично відображає системне недоопрацювання з боку органів влади, що не змогли завчасно передбачити конфлікт, розробити можливі сценарії реагування на нього, оперативно впровадити адекватні механізми протидії інформаційній агресії. Організаційно-економічні методи забезпечення інформаційної безпеки попереджають значні втрати політичного, економічного, воєнного та іншого характеру для країни, яка зазнала інформаційної атаки; мінімізують шкоду, яку юридичним особам і громадянам завдають деструктивні інформаційні впливи.

Як невід'ємна частина буття людини, суспільства і держави, інформація є одним з найважливіших об'єктів правового регулювання. Відтак стан правового забезпечення цих процесів багато визначає в діяльності держаних та інших інститутів у країні. Проте у цьому контексті йдеться не лише про національне законодавство, але й про міжнародні норми, сучасні стандарти регіонального, транскордонного, європейського співробітництва, впровадження яких значною мірою залежить від зусиль державних органів. Детальніше про правові механізми забезпечення інформаційної безпеки, правовий супровід сучасного інформаційного суспільства напишемо пізніше, у окремому розділі, оскільки питання особливо важливе для сучасної України.

Налагодження правових механізмів, розвиток сучасних технологій,

організаційні та економічні зрушення можуть сприяти поступовому вирішенню тих проблем інформаційної безпеки, які пов’язанні з недостатньою підготовленістю вищого державного керівництва, органів влади та військових формувань до сучасних цифрових реалій, а також зі загрозами, спричиненими відставанням нашої країни від розвинутих за рівнем інформатизації держави, промисловості тощо. Однак у питаннях щодо координації роботи владних інститутів, балансування суспільних інтересів, ефективного урядування в сучасних інформаційних умовах лише вказаних методів недостатньо. Відтак виокремимо *другий підхід*, який основний наголос робить саме на політичних заходах як ключових для держави у забезпеченні інформаційної безпеки.

У пошуках інноваційних засобів та ресурсів, за допомогою яких державні інститути можуть здійснювати максимально ефективне планування та реалізацію інформаційної політики, не менш важливою є згадана на початку нашого дослідження ще одна тріада – налагодження оптимальних взаємодій базових соціальних інститутів – громадянина, суспільства, держави, – що й визначають соціально-політичну сутність безпеки. Показово, що ще задовго до прямого розгортання Російською Федерацією інформаційної агресії проти України, вітчизняні науковці робили особливий наголос на гострій необхідності розбудови системи інформаційної безпеки на основі вказаних інститутів [див. напр. 214; 245]. Адже державний інтерес у системі інформаційної безпеки (збереження державного суверенітету й конституційного устрою, ефективне функціонування політичної системи) мало можливий поза розвитком визначальних цінностей суспільства, його консолідаційних прагнень та організованих ініціатив, як і немимислимий без гарантування і забезпечення індивідуальних прав та свобод громадян в інформаційній сфері.

Відзначав складну і важливу роль, яку відіграє категорія прав та свобод людини і громадянина в інформаційній безпеці і Б. Кормич. Він, зокрема, зауважив, що по-перше, «в демократичному суспільстві загальновизнані права людини і громадянина в сфері інформації виступають основним критерієм, що характеризує стан інформаційної безпеки конкретної особи і суспільства в

цілому» [148, с. 133], а по-друге, «норми, що закріплюють права і свободи людини в сфері інформації, є стримуючим фактором свавілля держави, по-третє, самі права і свободи людини у сфері інформації можуть реалізуватися за наявності цілеспрямованої підтримки політичними рішеннями керівництва держави» [148, с. 133]. Ця політична складова визначальна для концепції нашого дослідження.

Які б інструменти та засоби інформаційної політики не обирала держава через свої інститути та органи, важливо завжди враховувати взаємопов'язаність трьох об'єктів інформаційної безпеки. Для окремого індивіда інформаційна безпека можлива у реалізації конституційних прав і свобод, зокрема з одержання, використання, поширення, зберігання інформації; у захищеності здоров'я та психіки від деструктивних інформаційних впливів, від маніпуляцій свідомістю; у захисті авторських прав тощо. Для суспільства інформаційна безпека вбачається також в безперешкодних можливостях реалізовувати згадані конституційні права, але крім того кожне модерне суспільство прагне до рівня інформаційного, у якому підтримується і високо цінується інтелектуальний потенціал, розвивається критичне мислення, плюралізм ідей, зберігаються культурні, моральні, історичні основи ідентичності нації тощо. Нарешті для держави інформаційна безпека передбачає забезпечення інформаційного суверенітету; розвиток науково-технологічного потенціалу; інтеграцію в прогресивний інформаційний простір; створення конкурентоспроможних інформаційних продуктів і технологій; захищеність від монополій, спеціальних інформаційних операцій, інформаційної злочинності, інформаційного тероризму та інших деструктивних інформаційних впливів, що завдають шкоди національним інтересам [214, с. 124; 245, с. 115-116].

Перехід до демократії часто ускладнений загальним нерозумінням тісного зв'язку усіх трьох цих вимірів інформаційної безпеки та відповідно заходів, що вони їх потребують. Тобто в українському суспільстві все ще поширені думки про те, що захист інформаційного простору залежить виключно від держави, і навпаки – серед державних службовців нерідко побутує недооцінка громадських

ініціатив чи навіть сміливих авторських задумів окремих науковців й аналітиків, які можуть розвивати досить інноваційні підходи до розв'язання назрілих інформаційних конфліктів. Державні органи цілком можуть зайняти у цих комунікаціях діалогічну позицію, відкрити нові канали комунікації, сприяти демократичній дискусії, розвивати соціальні ліфти, що у своїй сукупності модернізуватимуть систему інформаційної безпеки в цілому. Окремі сюжети для такої співпраці вже намічені і навіть успішно реалізовані в Україні, а от стратегічного та системного бачення політичними елітами країни все ще бракує.

Цілком співзвучний цьому окреслений підхід до проблеми вибору Україною як державою методів інформаційної політики, який варто особливо підкреслити у контексті нашого дослідження. Адже вітчизняні дослідники серед заходів інформаційної безпеки досить слушно виділяють власне політичні, зважаючи на особливе предметне поле такої діяльності та ключову роль держави в узгодженні правлячих і опозиційних, системних та стихійних, зовнішніх і внутрішніх сил у політичному житті суспільства. Це зокрема заходи зі з'ясування односторонніх і багатосторонніх інтересів у суспільстві шляхом обміну інформацією, проведення переговорів, налагодження контактів; якісний інформаційний супровід визначальних політичних процесів (виборів, референдумів, реформ тощо); об'єктивне висвітлення сутності існуючих проблем, конфліктів, криз у ЗМК, а також створення відповідних умов для їх професійної діяльності; залучення максимальних можливостей для інформування населення у зонах напруженості, а також для донесення державницької позиції до міжнародного співтовариства; відкритість до незалежних моніторингів за дотриманням основних прав і свобод людини тощо [175, с. 47]. До кожного із названих пунктів особливо вразлива система інформаційної безпеки України.

Усі ці політичні заходи не виключають необхідності здійснення державними інститутами інших важливих функцій, передбачених законодавством. Тобто власне політичні методи забезпечення інформаційної безпеки варто і потрібно підсилювати згаданими раніше правовими,

економічними, технологічними. Комплексно науковці, зокрема О. Федорук, вбачають у системі забезпечення державної інформаційної безпеки такі функції: нормативно-правове забезпечення системи управління національними інформаційними ресурсами; розробка й реалізація фінансово-економічних засад регулювання процесів формування і використання інформаційних ресурсів; здійснення державної реєстрації таких ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів; забезпечення ефективного використання інформаційних ресурсів у діяльності органів державної влади; оптимізація державної політики інформатизації щодо забезпечення науково-технічних, «виробничо-технологічних й організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури» [270, с. 183]; забезпечення розробки та застосування правових, організаційних й економічних механізмів стосовно форм і засобів обігу інформаційних ресурсів держави; «регулювання інформаційного співробітництва для забезпечення рівноправного та взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну; здійснення єдиної державної політики наукової підтримки системи державного управління формуванням, розвитком і використанням національних інформаційних ресурсів»; кадрове забезпечення функціонування системи державного управління національними інформаційними ресурсами»; «інформаційно-аналітичне забезпечення прийняття рішень у сфері управління інформаційними ресурсами» [270, с. 183]. Не складно помітити, що вагоме місце у цьому підході займають такі категорії сучасної політології як соціально-політичні інтереси, ресурси, засоби, інструменти влади.

Ще одну не менш важливу групу заходів могли би скласти *ціннісно-культурні,* які варто розглянути у контексті *третього підходу* до розуміння методів інформаційно-безпекової діяльності сучасної держави. Вони передбачають не лише залучення органів державної влади, місцевого самоврядування чи державних підприємств до вирішення назрілих проблем інформаційного простору. Тут ми солідарні з вченими, які не бачать можливим

вирішення проблем інформаційної безпеки без впровадження нових ідей, нових знань, загалом нової філософії політики [див. напр. 390], в тому числі й у сфері інформатизації. Концептуальними є пропозиції щодо широкого залучення саме вітчизняних науковців, мислителів, моральних авторитетів, інтелектуалів до обговорення безпекових викликів і перспектив. Ці люди є певними гарантами високої якості прийнятих стратегій і рішень, найважливіших політичних, економічних, соціальних, військових концептів. Гостро відчувається і потреба у фахівцях, відповідальних за сучасну систему сертифікації програмних і технічних засобів, впровадження стандартизації, створення національних баз даних, систем телекомунікації, безпечність роботи в світовому інформаційному просторі [220, с. 798-801].

Це стратегічне розуміння значення закладів освіти, інститутів культури, наукових установ, які перебувають у віданні держави, задля збереження духовного багатства, історичних надбань, примноження інтелектуальних здобутків і підтримки творчих талантів країни. Всяка система інформаційної безпеки видається беззмістовною, якщо не сповнена конкретних ціннісних змістів та чітких смислових орієнтирів, сутність яких великою мірою залежить від інституційної спроможності названих осередків. Однак часто у дискусіях про політичні цінності і стратегії головний акцент зміщується у бік політичних ідеологій, а визначальними акторами виступають не стільки культурні чи наукові заклади, скільки конкурентні зовнішні й внутрішні політичні сили. Така ситуація особливо потребує концентрації політичної волі держави, покликаної захищати інформаційну та гуманітарну сферу життя суспільств.

Суспільна сфера у найзагальніших рисах, як і цей конкретний її вимір, залишається дуже вразливою для інформаційних впливів, оскільки охоплює системи формування громадської думки, структури ЗМІ, інформаційно-організаційні структури політичних партій, громадських рухів, національно-культурних та релігійних інституцій, структури забезпечення основних прав і свобод, плюралізму і незалежності виявлення поглядів, вільного обміну ідеями та інформацією. Серед головних причин, що впливають на ціннісно-культурний

розвиток та стан морально-ідеологічної стабільності та безпеки в Україні, вчені, зокрема В. Петрик, називають: «відсутність цілісної системи інформаційно-аналітичного забезпечення органів державної влади та управління; руйнування інтелектуального потенціалу, неготовність наявної системи освіти до підтримання процесів випереджувального розвитку держави»; [214, с. 126; 379] «повільність процесів усвідомлення прошарком колишньої радянської партійно-господарчої номенклатури, наукової й творчої інтелігенції, паростками нової буржуазії свого місця в суспільстві та формування власно української еліти, що призводить до неможливості сформувати керівними колами зрозумілої і привабливої для суспільства національної ідеї»; [214, с. 126; 379] «низький загальний рівень розвитку інформаційної інфраструктури, що не виключає ймовірність експансії іноземних компаній на ринку інформаційних послуг»; «руйнування національного інформаційного простору та виникнення можливості його використання в антидержавних інтересах»; «недостатній професійний, інтелектуальний і творчий рівень вітчизняних виробників інформаційного продукту та послуг, їхня неконкурентоспроможність на світовому інформаційному ринку»; «інформаційна експансія провідних іноземних держав» [214, с. 126; 379]; «розроблення і використання ними, міжнародними чи вітчизняними злочинними організаціями різних сучасних способів безпосереднього підриву» [214, с. 126; 379]; мало контрольована діяльність окремих політичних сил, ЗМІ та осіб, котра «спрямована на руйнування моральних цінностей, свідомості, підрив морального й фізичного здоров’я нації»; «використання засобів масової інформації з позицій, протилежних інтересам громадян, політичних і громадських організацій, держави»; «утрата довіри до влади з боку значної частини населення через застосування «брудних» політичних технологій, особливо під час виборчих кампаній»; «конкурентна боротьба за володіння ЗМІ, процес їхньої монополізації та концентрація в межах їх інформаційної та політичної влади»; «маніпулювання громадською думкою (шляхом дезінформації, перекручування фактів і даних, замовчування правдивих відомостей тощо)» [214, с. 126; 379].

Суспільство і держава не готові адекватно реагувати на прояви цих негативних для України явищ сучасності. Пануючі в суспільстві та на рівні державної влади погляди на інформаційну безпеку як лише безпеку в інформаційній сфері, тобто сфери обігу інформації, дезорієнтують і дезінформують людину і громадянина, суспільні та державні інституції. Проблеми інформаційної безпеки стають усе гострішими і непередбачуваними. Однією із важливих проблем як формування інформаційного суспільства, так і забезпечення інформаційної безпеки є базова основа, на якій здійснюється досягнення визначених цілей [206, с. 321]. Визначення національних інтересів, яким загрожує інформаційна небезпека, є основою для розробки і вдосконалення державної політики у сфері інформаційної безпеки. В умовах невизначеності національної ідеї, коли суспільство розколоте за політичними, економічними, соціальними, територіальними, етнічними, релігійними, екологічними параметрами, система національних інтересів має включати зрозумілі для широких верств населення, несуперечливі, взаємоузгоджені, життєво важливі матеріальні, інтелектуальні, духовні цінності. Національні інтереси в умовах сучасної України не можуть бути джерелом політичного, ідеологічного протистояння, економічної нестабільності та інших негативних процесів і явищ.

Часто у публічному просторі недооцінюють або навпаки переоцінюють значення державних інститутів у підтримці й розвитку національної ідеї, спільних цінностей, стратегічних орієнтирів, як і її роль у захисті від деструктивних ідеологічних впливів, що використовують інформаційне середовище. Держава забезпечує безпеку кожного громадянина як на території України, так і за її межами, дбає про суспільний економічний, культурний, духовний розвиток. З цією метою для підтримки належного рівня захисту національних інтересів, а також об’єктів безпеки України розробляється система та мережа політико-правових норм, що врегульовують суспільно-політичні відносини у сфері національної безпеки нашої держави, визначаються основні напрямки діяльності органів державної влади та управління, створюються чи перетворюються органи та сили забезпечення національної безпеки,

виробляється стратегія взаємодії суб'єктів забезпечення національної безпеки, розробляється механізм демократичного цивільного контролю за системою управління національною безпекою [244, с. 147].

Проте жорсткі методи захисту з боку держави хоча і є доступними та найзрозумілішими, однак далеко не завжди влаштовують громадськість, часто не відповідають демократичним засадам, та й загалом не сприяють формуванню консолідуючих смислів та ідеології національного розвитку. У інформаційній сфері у цьому контексті прийнято вирізняти дві основних форми державного контролю (цензури): прямий та опосередкований. У прямому контролі (цензурі) розрізняють попередній і наступний контроль. Попередній контроль історично активно використовувався, але зараз здійснюється лише у диктатурах та під час надзвичайного чи воєнного стану. Йдеться про системи, у яких відповідний урядовець (цензор) переглядає інформацію ще до її виходу у світ та (не)дозволяє її розповсюдження. Прямий наступний контроль з використанням засобів судового переслідування (і не тільки) застосовується у багатьох сучасних державах. Журналіст в авторитарному суспільстві перетворюється на джерело небезпеки та перебуває під постійним контролем з боку правлячої влади (еліти, ідеології тощо), в інтересах забезпечення існуючого статус-кво, тобто авторитаризму. Опосередкований контроль передбачає застосування економічних важелів щодо ЗМІ з метою коригування їхньої політичної лінії. Ця форма контролю вважається найпоширенішою у сучасних демократичних суспільствах [178, с. 78]. Контроль хоч і складає важливу частину діяльності державних структур, які прагнуть захистити від негативних інформаційних (в тому числі й ідеологічних) впливів на суспільство, однак мало ефективний у питаннях вибудовування та підтримки власних ціннісних орієнтирів.

У цьому аспекті досить перспективним вбачаємо поєднання комплексу методів державної політики, особливо доповнення правових і політичних – ціннісно-культурними. З аналізу чинного законодавства видається, що саме в означеному напрямку (за винятком періодів демократичних реверсів) рухається сучасне українське суспільство на шляху до демократії. Наприклад, якщо

критично осмислити зміст Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9 січня 2007 р. [106], то у ньому достатньо чітко окреслені шляхи забезпечення інформаційної безпеки держави («створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів»; «підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань»; «вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері»; «розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація тощо» [106]). Проте спільні цілі та цінності прописані досить розмито й універсально (за винятком посилань на власну історію інформатизації в Україні, діяльність відомої школи кібернетики тощо), поза реальними інформаційними загрозами і небезпеками того часу, поза консолідуючою національною ідеєю.

Ускладнили рух до цифрового суспільства подальші політичні процеси зі згортання демократії. Так, О. Олійник вважає, що Доктрина інформаційної безпеки України, затверджена Президентом України у 2009 р., не тільки порушила чинне законодавство, а й дезінформувала і дезорієнтувала суспільство та державні інституції. Законодавчі і нормативно-правові акти, прийняті у 2010-2011 роках, в тому числі щодо адміністративної реформи не наближали наше суспільство до системного і комплексного вирішення проблем забезпечення інформаційної безпеки. Фрагментарність та несформованість – такими називали найбільш характерні прояви як інституційного забезпечення, так і управлінської та адміністративної діяльності держави у сфері інформаційної безпеки [205, с. 66]. Отже, для суспільства та громадянина дуже важливо, аби задекларовані

орієнтири та цінності мали політичну підтримку, правове визначення, стратегічну оцінку. Національна ідея та її інформаційна підтримка потребує узгодженої співпраці інтелектуальних осередків, державних органів, медіа, активної громадськості та кожного громадянина зокрема. Оновлення Доктрини було надзвичайно актуальною справою, адже попередній документ не витримував жодної критики.

Натомість знаковим для інформаційно-безпекового простору країни стало вже частково згадане вище рішення РНБО України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», введене в дію Указом Президента України №47/2017 від 25 лютого 2017 року [265], що безумовно пов'язано з новими, особливо небезпечними реаліями гібридної війни. Зокрема, у новій Доктрині національними інтересами України в інформаційній сфері визначено життєво важливі інтереси як особи, так і суспільства та держави – це дуже важливо з позиції раніше описаного нами тріадного підходу до розуміння без пекового простору та його суб'єкт-об'єктних складових. У Доктрині стосовно інтересів особи вказані три вже традиційно окреслені міжнародними нормами та сучасною наукою позиції, зокрема: «права і свободи людини на збирання, зберігання, використання та поширення інформації»; «захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів» [265]. Натомість державні і суспільні інтереси в інформаційній сфері Доктриною об'єднанні та складає двадцять позицій – від протистояння агресивному впливу деструктивної пропаганди, передусім з боку Російської Федерації до розбудови системи іномовлення України. Зауважимо, що у документі достатньо місця відводиться проблемам ідентичності, культури, національному і релігійному порозумінню, позитивному іміджу України у світі, що є важливим показником окреслення ціннісно-культурних пріоритетів інформаційної сфери у правовому полі. Прямо у Доктрині йдеться також про необхідність «збереження і примноження духовних, культурних і моральних цінностей Українського народу» [265], розвитку і функціонування української мови, захист мов національних меншин, вивчення мов міжнародного спілкування – усі ці

напрямки суттєво доповнюють правові, організаційні та технологічні методи забезпечення інформаційної безпеки і фактично наповнюють їх змістом.

4.2. Роль політичних партій на шляху розвитку стратегії інформаційної безпеки у демократичному суспільстві

Визначивши та проаналізувавши зміст та логіко-гносеологічну функцію категорії «інформаційна безпека», зокрема як різновиду національної безпеки, котра націлена на забезпечення прав та свобод людини й громадянина стосовно вільного доступу до інформації, «створення і впровадження безпечних інформаційних технологій» та «захисту права власності всіх учасників інформаційної діяльності» [434, с. 14], важливо осмислити (вивчити) місце та роль у цьому процесі політичних партій.

Необхідно зазначити, що політичні партії, популяризуючи певну ідеологію, здійснюючи агітаційно-просвітницьку роботу, беручи участь у діяльності органів влади активно впливають на інформаційний простір країни і як наслідок стають активними суб'єктами інформаційної безпеки. Саме тому, з нашої точки зору, важливо проаналізувати специфіку позиціювання політичної партії у інформаційному просторі держави і суспільства. Як правило таке позиціювання відбувається за допомогою різноманітних ЗМІ й обумовлено тим, що будь-яка політична партія повинна бути зв'язуючою ланкою між владою та громадянським суспільством.

На сьогодні ми часто можемо спостерігати певну заполітизованість українського інформаційного простору. Значний доступ української політичної еліти до засобів масової інформації дозволяє політичним настроям проникати практично в усі сфери суспільного буття. Можемо припустити, що представники політичних кіл України розглядають питання розвитку на наших теренах громадянського суспільства також у політичному контексті. Звичайно, політика значною мірою присутня в процесах розбудови громадянського суспільства, зокрема через важливу роль у цьому політичних партій. Власне і політичні партії,

і громадські організації покликані виконувати роль посередника між громадою і державою, тим самим створюючи умови для розвитку громадянських ініціатив, проте спрямованість цих ініціатив у кожного із названих соціальних інститутів своя [19].

Коли мова йде про сучасну політику та інформаційні технології, сучасні дослідники формулюють чимало важливих і дискусійних питань, вирішення яких залежить і від рівня розвитку партійної системи в країні. Наприклад, нові соціальні мережі формують специфічне середовище для здійснення політики, у якому при виборі кар’єри політика велику цінність має зворотній зв'язок, соціальне схвалення аудиторії віртуальних мереж. З такою ціллю сучасні політики часто вдаються до використання «ботоферм» задля отримання та утримання особистої чи партійної рейтинговості в соціальних мережах, з іншого ж боку, викриття таких «брудних» кампаній для політичної сили нерідко позначається втратою суспільної довіри [415, с. 91]. У цьому ключі партійна змагальність певною мірою перетворюється у змагання технологій: та партія, що має доступ до кращих технологій, здійснила якісніший кадровий відбір фахівців, що здатні вирішувати складні завдання сучасного цифрового суспільства, цілком може сподіватися на електоральну підтримку. Сучасні технології цілком спроможні розвивати та сприяти як демократичним партійним ідеологіям, так і популістським передвиборчим обіцянкам. Тож майбутнє політики, оснащеної кращими інформаційно-комунікаційними можливостям, не обов’язково гарантує соціальну збалансований, демократичний, мирний вектор розвитку. Воно великою мірою залежатиме від конкретних інтересів та можливостей їх реалізації, в тому числі й від партійних орієнтирів.

Вочевидь, політичні партії позиціонують себе у інформаційному просторі як носії певної ідеології, як суб’єкти владних повноважень (парламентські партії), як захисники суспільних інтересів тощо. Завданням партій, у цьому контексті, є встановлення комунікації з електоратом з метою впливу на їх свідомість: популяризація партійної програми, забезпечення підтримки серед населення і як наслідок перемога на виборах.

Колективний характер більшості реалізованих у політиці цілей передбачає використання спеціальних засобів шляхом трансляції бажаної інформації, здатних забезпечити єдину спрямованість дій великої кількості людей, тобто мобілізувати їх на масові дії. Саме мас-медіа і виявляються єдиним таким засобом, враховуючи їх функцію формування інформаційного аналога суспільства, а наслідком такого становища є особлива роль ЗМІ в сучасному політичному процесі та їх величезний вплив на політичне життя. Свідченням цього є виникле порівняно недавно для опису цієї нової ситуації поняття «медіаполітика» [248].

На думку дослідниці С. Бодрунової, поняття «медіаполітика», тобто політика через посередника, в ролі якого виступають ЗМІ, з'явилося не так давно в рамках теорії політичного маркетингу, згідно з якою виборці виступають як цільові групи з певними потребами, а політики, політичні партії, запропоновані ними моделі розвитку та програми управління державою – як замінник споживчого продукту, який повинен відповідати інтересам електоральної аудиторії [189]. Тобто позиціонуючи себе у інформаційному просторі політичні партії та їх лідери повинні враховувати інтереси громадян й соціальних груп задля встановлення з ними позитивної комунікації, створення атмосфери довіри та підтримки з боку електорату.

На сьогоднішній день, у науковій літературі існує низка теорій, які пояснюють природу вдалого чи навпаки неефективного позиціювання політичної партії у інформаційному просторі: теорія «когнітивного дисонансу» Л. Фестінгера, а також теорія «корисності і задоволення потреб» Е. Каца. У теорії «когнітивного дисонансу» підкреслювалося таке: коли нав'язують певні думки та ідеї, то люди потрапляють у певний психологічний дискомфорт. Тому індивід, бажаючи уникнути дискомфорту, обирає та сприймає лише ті зовнішні повідомлення, які не суперечать його усталеним переконанням. В свою чергу теорія «корисності і задоволення потреб» пояснює основну причину відбору людиною того чи іншого повідомлення за принципом задоволення її власних інтересів. Людина робить свій вибір, виходячи з користі, яку несе для неї та чи інша інформація. Наприклад, як зазначає С. Бодрунова, «у період виборчої

кампанії людина може звернути увагу на повідомлення, яке не лише виявиться корисним при голосуванні на майбутніх виборах, але і викличе відчуття його власної політичної компетентності» [27, с. 45]. Виходячи з вищенаведеного, зазначимо, що політичні партії позиціонують себе у інформаційному просторі, вивчаючи психологію електорату, аналізуючи результати соціологічних досліджень щодо сподівань та прагнень громадян. Фактично вдале позиціювання політичної партії у інформаційному просторі держави й суспільства базується на ефективній та багатоканальній політичній комунікації.

У цьому аспекті достатньо цікавими є дослідження політичної комунікації, що відомі, як стверджують О. Карчевська й Г. Агафонова, під назвами «теорії чарівної кулі» і «теорії підшкірної голки» [435]. Ці концепції, продовжують вчені, «виходили з припущення про величезні, практично необмежені можливості інформаційно-пропагандистської дії на масову аудиторію, яка в плані відбору повідомлень поводиться досить пасивно і, по суті, нагадує пацієнта, чий стан починає змінюватися після отримання дози лікарського препарату у вигляді ін'єкції» [435]. Одним із засновків цих теоретичних моделей прийнято вважати Г. Лассуела, який у своїй роботі, присвяченій аналізу механізмів пропагандистської дії на маси, дав класичне визначення масової пропаганди як «молота і ковадла громадської солідарності», що зливає мільйони атомізованих індивідів в єдину «амальгамовану масу ненависті, віри і надії» [56].

Одним з важливих механізмів позиціювання політичної партії у інформаційному просторі є політична реклама, яка виконує низку функцій: просвітницьку, пропагандистську, агітаційну, комунікативну та навіть маніпулятивну.

Сутність політичної реклами як комунікативної технології й механізму позиціювання у інформаційно-політичному просторі полягає, на думку дослідників, у такому: 1) політична реклама формує комунікативний простір взаємодії між політичними акторами та громадянами; 2) реклама здійснює прямий цілеспрямований вплив на масову аудиторію; 3) використовує загальновизнані символи та смисли, що легко сприймаються; 4) транслює політичні ідеї, образи,

створює міфи; 5) виконує інформаційну, ідеологічну, соціально-орієнтувальну, освітню, естетичну, пропагандистську, мобілізаційну функції; 6) політична реклама поєднує апеляцію до раціональної аргументації та потужний емоційний заряд; 7) виражає у концентрованому вигляді програму політичного актора (державного діяча, партії, політичного лідера); 8) політична реклама − це елемент маркетингової стратегії позиціонування актора у політичному просторі [16].

Політична реклама дозволяє певній партії найбільш рельєфно показати свої програмні відмінності, ідеологічні переваги щодо іншої партії, позиціонуючи себе у певному сегменті інформаційного та політичного просторів. Як зазначає І. Шовкун, «політична реклама − це форма політичної комунікації в умовах вибору, що здійснює адресний вплив на групи людей та електоральні групи в лаконічній, оригінальній, легко запам’ятовуваній формі» [283]. Причому, продовжує вчений, «політична реклама відображає суть політичної платформи певних політичних сил, налаштовує виборців на їхню підтримку, формує і впроваджує в масову свідомість певні уявлення про характер цих політичних сил, створює бажану психологічну установку на голосування» [283].

З нашої точки зору, при всій специфіці кожної політичної партії можна виокремити низку загальних етапів її позиціонування у інформаційному просторі суспільства й держави. На першому етапі, як правило шляхом соціологічного опитування, визначаються провідні теми та етапи майбутньої рекламно-пропагандистської кампанії (стратегія позиціювання політичної партії), визначається пакет найбільш виграшних характеристик політичної партії та цільова аудиторія у інформаційно-політичному просторі − групи електорату, які підтримують дану партію (або потенційно можуть підтримати).

На другому етапі, відбувається формування, коригування або зміна політичного іміджу партії, створюються рекламні повідомлення, які позитивно характеризують дану політичну силу, напрацьовуються аргументи щодо її переваг над іншими політичними акторами, пропонується бачення майбутнього та шляхи вирішення існуючих у країні проблем. В той же час, на цьому ж етапі здійснюється відокремлення даної політичної сили від інших шляхом наведення

аргументів щодо негативних властивостей політичних опонентів. Відповідно всі вищеозначені кроки здійснюються за допомогою ЗМІ та всіх існуючих каналів комунікативного впливу на масову аудиторію.

На третьому етапі здійснюється тестування вищеозначених заходів позиціювання партії у інформаційному просторі шляхом проведення фокус-груп та інших соціологічних досліджень, які повинні показати рівень популярності партії у суспільстві та особливості сприйняття масовою свідомістю світоглядно-політичних меседжів конкретної політичної сили.

На наступному етапі позиціювання політичної партії відбувається корекція обраної на першому етапі стратегії (відповідно за необхідністю) шляхом розповсюдження різноманітної інформації у мас-медіа.

У подальшому позиціювання політичної сили у інформаційному просторі базується на даних моніторингу соціально-економічної, політичної, зовнішньополітичної ситуації у країні та світі. Відповідно, результати такого моніторингу можуть призвести до корекції або зміни тактики й стратегії позиціювання політичної сили у інформаційному просторі.

У процесі позиціювання політичної партії у інформаційному просторі активно використовуються прямі та непрямі форми політичної реклами, агітації та пропаганди. До першої форми належать повідомлення, що поширюються в умовах міжособистісного контакту суб’єкта реклами (партії) і об’єкта рекламного впливу. Друга форма передбачає використання мас-медіа: преси, телебачення та радіо. Нові можливості для поширення рекламних повідомлень відкриває розвиток мережі Інтернет. Це відбувається завдяки поєднанню у мережі аудіовізуальної та текстової інформації, інтерактивності та комплексному використанню електронної пошти, соціальних мереж, сайтів, форумів та ін.

Останнім часом світовим трендом щодо позиціювання політичних партій у інформаційному просторі є активне використання мережі Інтернет. Мережа Інтернет має деякі переваги як інструмент політичних комунікацій та засіб позиціювання політичних партій у інформаційному просторі. Базовими характеристиками Інтернет-простору як підсистеми інформаційного простору є

такі: оперативність, гіпертекстуальність, мультимедійність, інтерактивність; необмежений обсяг інформації, тривалий термін її зберігання, постійна актуалізація, можливість тематичного моніторингу інформації; глобальність, відсутність просторових та часових меж; анонімність користувачів Інтернет-простору; висока рентабельність використання технологій Інтернету та деяке зниження витрат на отримання інформації [41, с. 33]. У сучасних умовах політична партія, що піклується про свій рейтинг повинна обов'язково бути представлена у «світовій павутині», яка охоплює все більшу кількість громадян та поступово стає провідним комунікативним засобом у інформаційному просторі.

Як зазначають дослідники М. Грачов і А. Мадатов, можна виокремити наступні переваги використання Інтернет-комунікацій у діяльності політичних партій. По-перше − це значне зниження витрат на передачу інформації від керівних органів до місцевих відділень та у зворотному порядку, що позитивно впливає на істотне підвищення ролі первинних організацій та рядових членів у внутрішньопартійному житті. По-друге − застосування Інтернет-комунікацій значно розширює можливості всіх членів партії у формуванні політики партії, зокрема через публічне обговорення проектів рішень, що приймаються, у режимі реального часу. Вищеозначені дослідники також наголошують, що Інтернет-форуми, які мають у силу власної інтерактивності та оперативності очевидну перевагу перед традиційними друкованими виданнями, слід розглядати в якості перспективного засобу забезпечення ефективного зворотного зв'язку та прямого діалогу партій із власними прихильниками, особливо у періоди підготовки та проведення виборчих кампаній. Разом з тим М. Грачов та А. Мадатов формулюють, з нашої точки зору, досить суперечливий висновок про те, що Інтернет у недалекому майбутньому дозволить партіям відмовитися від традиційної форми проведення конференцій та з'їздів шляхом залучення інтерактивної комунікації представників регіональних партійних відділень, віддалених один від одного у просторовому відношенні [55, с. 94-95]. Суперечливість вищеозначеної тези полягає в абсолютизації Інтернет-технологій як засобу комунікації, оскільки низка важливих питань у політиці вирішуються

під час особистого спілкування та на закритих зустрічах керівників політичних партій.

Разом з тим, позиціювання політичних партій у інформаційному просторі за допомогою мережі Інтернет відкриває для них низку можливостей: швидкісне розповсюдження інформації, залучення нових симпатиків, вплив на різноманітні суспільні групи, здійснення мобілізаційних та агітаційних заходів тощо. Необхідно зазначити, що застосування Інтернет-комунікацій змінює і внутрішньопартійне життя, роблячи його більш динамічним та інформаційно насиченим.

З нашої точки зору, специфіка позиціювання політичної партії у інформаційному просторі залежить не тільки від її матеріально-технічного, інтелектуально-креативного та фінансового забезпечення, а й від ідеології та цінностей, які вона пропагує. Саме ідеологічні та програмні постулати партії визначають характер її позиціювання у політичному, а відповідно й в інформаційному просторі держави та суспільства. Разом з тим, у сучасному світі можна спостерігати деідеологізацію політичних партій: програма партії не базується на одній системі принципів, а є міксом з різних за ідеологічною природою постулатів.

На думку українського дослідника М. Примуша, в нашій країні фіксується стійка тенденція до гібридизація політичної ідеології, що є ознакою ідеологічної кризи політичних партій [226, с. 201]. Такий стан справ призводить до того, що позиціювання політичних сил у інформаційному просторі має популістський, не стійкий характер за своїми змістовними характеристиками. Лідери політичних партій з легкістю змінюють свої погляди, а їх представники у владі активно мігрують з однієї політичної сили до іншої, що дезорієнтує громадян. Як підкреслює вищеозначений науковець, ідеологічна криза політичних партій проявляється у декількох аспектах.

По-перше, ідеологічна криза стосується нездатності політичних партій запропонувати соціуму не тільки певний ідеологічно-ціннісний ідеал, а ще характеризується відсутністю у них чіткого розуміння фундаментального

положення демократії − захисту прав громадян [226, с. 201].

По-друге, брак ідей стосується всіх політичних партій без винятку, навіть комуністична ідеологія захисту робітничого класу, незважаючи на свою актуальність у перехідних суспільствах, залишається лише теоретичною конструкцією, яка не може бути реалізована з двох причин − сучасні тенденції глобалізації, що розмивають ідеологічні межі між всіма ідеологіями, та загальна нездатність українських лівих політичних сил (навіть за умов перебування у парламентській більшості з владою) реалізувати хоча б частину своїх ідейних положень [226, с. 201].

По-третє, кількісна представленість кожного ідеологічного спектру аж ніяк не говорить про якість у справах захисту інтересів прихильників лібералів, соціалістів чи націоналістів. Навпаки, значна кількість ідеологічно однакових політичних партій слугує найбільшим виявом їх кризи, оскільки відсутність єдності в побудові ідеологічних цінностей актуалізує питання загроз національній безпеці [226, с. 201].

По-четверте, ведучи мову про ідеологічну кризу політичних партій в Україні, ми маємо справу відразу з комплексом криз, а саме: сучасні процеси глобалізації вимагають орієнтації політичних сил на універсальну модель ідеологічних принципів (що руйнує саму ідеологію), і тому ця криза стосується самих політичних партій, які не готові відповісти на виклики сучасності.

По-п’яте, український електорат, маючи понад 200 політичних партій, залишається без інструментів впливу на політичні процеси, оскільки, з одного боку, великі політичні сили є виразниками інтересу крупного капіталу та певних груп тиску, а з другого − дрібні політичні сили не спроможні конкурувати на рівних із крупними політичними силами як через обмеження фінансових ресурсів, так і невизначену природу власних ідеологічних принципів [226, с. 201]. Фактично ідеологічна невизначеність політичних партій в Україні робить їх присутніми у багатьох сегментах політико-інформаційного простору одночасно, але не дозволяє зайняти певну ціннісно-світоглядну нішу на яку б орієнтувалися виборці.

Можна констатувати, що ідеологічна нестійкість політичних партій сприяє

викривленню інформаційного простору суспільства, уповільнює темпи державотворення та демократизації, а як наслідок чинить негативний вплив на національну, в тому числі й інформаційну безпеку країни. Низка партій в Україні взагалі не працюють з електоратом та відповідно не представлені у інформаційному просторі держави, частина політичних сил проявляють активність лише під час виборів, деякі здійснюють деструктивну діяльність та ін. Отже, всі вищенаведені фактори не сприяють структуризації політико-інформаційного простору нашої держави.

У контексті нашої наукової розвідки, треба аргументувати, що інформаційна безпека будь-якої держави залежить від того, чиї саме інтереси переслідує та захищає певна партія, та від того, як у її власній інформаційній політиці репрезентовані та зіставляються державні, народні/громадянські та вузько-партійні й корпоративні інтереси. На сьогоднішній день, низка політичних партій в Україні декларують первинність державних та народних інтересів у своїй діяльності, але часто-густо така публічна позиція є камуфляжом для вузькопартійних та корпоративних інтересів.

На нашу думку, одним з критеріїв ефективного захисту державних та народних інтересів політичною партією, наприклад в Україні, є її конструктивна участь у розбудові демократичної, правової, соціальної країни, результати якої мають бути відображені в її послідовній інформаційній політиці не тільки під час виборів, але й у міжвиборчий період. Як зазначає Л. Хорішко, партії – це важливий політичний інститут, ефективне функціонування якого, має забезпечити демократичні перетворення в країні, стати своєрідним медіатором, що в ідеалі має забезпечувати взаємодію громадянського суспільства з державою [274, с. 85]. Український досвід показав низький рівень впливу громадян на прийняття політичних рішень, що зумовлено неготовністю влади до стійкого діалогу, браком ефективної двосторонньої взаємодії [274, с. 85]. Можна констатувати, що інформаційна політика партії повинна мати багатоканальний характер, щоб стати механізмом ретрансляції політичних цінностей від громадянського суспільства до державних органів та навпаки. В такий спосіб інформаційна політика політичної

партії буде відображати як державні, так і народні інтереси.

В той же час, інформаційна політика партії є потужним інструментом впливу на суспільну свідомість, що може мати як негативні, так і позитивні наслідки у відстоюванні державних та народних інтересів. Підґрунтям для ефективної інформаційної політики партії є її здатність виконувати низку функцій. Серед функцій, які покликані реалізовувати політичні партії можна виокремити такі: вироблення заходів щодо впливу на суспільні інституції та соціальне середовище; здійснення політичної соціалізації; забезпечення безперервності політичних зв'язків і взаємовпливу між парламентом і всією країною; вплив на формування, з іншими політичними інституціями, механізму державного й громадського управління та ін. [132, с. 403].

Більш розгорнуту характеристику сутності, природи та функцій політичних партій як репрезентантів державних і народних інтересів та активних суб'єктів інформаційної безпеки надають вчені Є. Мануйлов й М. Толочко. Зокрема вони зазначають, що політичні партії виникають як продукт громадської ініціативи, а отже, є породженням і частиною громадянського суспільства, котре виступає підґрунтям формування і функціонування правової держави – організації і діяльності політичної влади на засадах визнання та забезпечення прав і свобод людини, верховенства закону і взаємної відповідальності особистості й держави. Політичні партії виконують роль посередника у суспільстві; борються із виявами політичної апатії громадян; прагнуть перебороти політичне неуцтво значного загалу населення, формують політичну культуру громадян; визначають і формують систему цінностей, що відбиває волю безлічі соціальних структур, з яких складається населення країни [183, с. 18].

При цьому, зазначають Є. Мануйлов й М. Толочко, уточнити «загальне призначення політичних партій можна шляхом визначення їх функцій, тобто тих завдань, які вони виконують у політичній системі» [183, с. 18]. Отож, основними функціями політичної партії в сучасному суспільстві є: 1) ідейно-теоретична, або функція артикуляції інтересів електорату. Сприяння формуванню і вираженню політичної волі громадян, інтереси яких партія відстоюватиме і на політичну

підтримку яких вона розраховуватиме в боротьбі за владу. Шляхи реалізації: складання партійних програм, передвиборчих платформ партій, політичних заяв партійних з'їздів, пропагування цих документів серед населення; 2) політичне представництво соціальних інтересів через канали політичної системи; 3) ідеологічна: розроблення ідеології, політичних доктрин і програм, політичного курсу, пошук управлінських моделей його здійснення, стратегії і тактики передвиборчої боротьби, поширення їх з-поміж виборців, що сприяє соціалізації індивідів і соціальних груп та передбачає їхню інтеграцію довкола певних норм і цінностей; ідеологічний вплив на членів партії, її прибічників, пропаганда своїх цінностей і світогляду; 4) електоральна: партії – як найактивніші суб'єкти конкуренції за владу – координують перебіг передвиборної боротьби, беруть участь у фінансуванні виборчих кампаній, боротьба за владу, її використання або контроль над нею; 5) політичне рекрутування: формування кадрового резерву професійних політиків, відбір найгідніших кандидатів на різні політичні посади; 6) наукова: розроблення різних соціальних проектів, технологій виборчої кампанії, проектів законів, програм розвитку, процедур діяльності центрів, аналітичних груп, лабораторій тощо; 7) функція сполучної ланки між суспільством і державою, між народом і владою; 8) встановлення та підтримка ефективного зворотного зв'язку між партіями і суспільством в цілому в інтересах контролю за розвитком політичної ситуації та своєчасним реагуванням на її зміни [183, с. 18-19].

Варто додати, що важливими функціями політичних партій під час здійснення ними інформаційної політики є просвітницька, виховна та інтегральна. Саме партії у своїй інформаційній політиці повинні сприяти об'єднанню України: популяризувати і утверджувати патріотизм, національні цінності й ідеали, демонструвати приклади конструктивного вирішення актуальних для держави проблем.

Одним з інтегральних показників здатності партії захищати державні та народні, а не вузькопартійні інтереси є рівень її суспільної довіри, який проявляється, перш за все, під час виборчих кампаній, а також шляхом проведення соціологічних опитувань. Рівень довіри до політичної партії,

забезпечується в тому числі й за рахунок вдалої інформаційної політики: агітація та пропаганда у ЗМІ, непротирічливість між проголошеними гаслами та реальними справами, пріоритетність народних інтересів над партійними у парламентській діяльності результати захисту яких відображені у ЗМІ тощо.

Разом з тим, політична сила, здійснюючи боротьбу за владу, у інформаційному просторі зокрема, може захопитися цією боротьбою й знехтувати держаними та народними інтересами. В цьому контексті можна погодитись з думкою дослідника Ю. Карпця, який підкреслює, що найважливішою політичною метою політичних партій є збереження високого рівня суспільної довіри [128, с. 257]. Вочевидь, інформаційна політика партії передбачає постійну конкуренцію з іншими політичними силами за більш вдале артикулювання та здійснення державних й народних інтересів.

Нажаль, досить часто політичні партії, здійснюючи інформаційну політику, послуговуються маніпулятивними технологіями, репрезентують неконструктивні, популістські засоби захисту державних й народних інтересів, що показує вузькопартійне і корпоративне мислення їх лідерів. Сьогодні більшість політичних партій, зауважує О. Кіндратець, дуже часто демонструють непримиримість, відсутність толерантності і елементарної політичної культури. Часто особисті цілі стають на заваді виробленню єдиної національної ідеї, довкола якої змогли б об’єднатися громадськість та політичні сили [136, с. 51].

Солідаризуючись з попереднім фахівцем, зазначимо, що національна ідея має бути світоглядно-ціннісним підґрунтям інформаційної політики партій як виразників державних та народних інтересів. До формування та розвитку національної ідеї повинні долучитися всі партії, які декларують своєю метою захист державних й народних інтересів. У інформаційній політиці партій, як зазначають В. Крисаченко, М. Степико і О. Власюк, О. Ляшенко, для подолання вузькопартійних інтересів, мають бути відображені наступні ціннісні орієнтири, які є елементами національної ідеї: 1) По-перше, треба «змістити акценти з боротьби «проти» і «за» на творення «в ім’я» – держави, нації, людини на основі злагоди, толерантності, захисту національних інтересів» [266, с. 254; 436, с. 211].

2) По-друге, в основі націотворення «повинна лежати ідея поліетнічної, соціальної, політичної злагоди на основі загальноприйнятної мети» [266, с. 254; 436, с. 211] – піднесення і добробуту людини в економічно й соціально багатій і правовій державі. 3) По-третє, держава у даній системі цінностей тепер мислиться не як самоціль, а як інструмент, що забезпечує досягнення мети, як засіб самоутвердження нації [436, с. 211]. 4) По-четверте, «Україна повинна бути найвищою цінністю для всіх її громадян як їхня спільна Батьківщина в існуючих кордонах» [266, с. 254; 436, с. 211]. 5) По-п'яте, повинна забезпечуватись «правова рівність громадян України, їхня духовна та культурна цілісність і самобутність, що є важливим чинником консолідації нації» [266, с. 255; 436, с. 211]. 6) По-шосте, повинна культивуватись як національна самоповага, патріотично орієнтована діяльність як спосіб самовираження особи, так і культурна й психологічна сприйнятливість до прогресивних надбань інших націй [436, с. 211]. 7) По-сьоме, громадяни України повинні усвідомлювати свій майбутній розвиток як результат співпраці у громадянському демократичному суспільстві [266, с. 255; 436, с. 211]. 8) По-восьме, національну ідею слід позбавити ідеологічної забарвленості [436, с. 212]. 9) По-дев'яте, громадянські і соціальні цінності повинні бути піднесені до рівня загальнонаціональних [266, с. 254; 436, с. 211].

В наш час, будь-яка політична сила, яка претендує на захист державних та народних інтересів, повинна не тільки бути представленою у медіа-просторі, а й має підготувати професіоналів, які б у ефективний спосіб доносили до аудиторії ключові меседжі політичної партії, могли б популярно розтлумачувати їх сенс.

У світовій практиці партії завжди намагалися забезпечити можливості для своїх членів навчитися, як використовувати нові засоби масової інформації і стати у цьому професіоналами. Навчання суб'єктів політичної діяльності роботі зі ЗМІ не нове, хоча на сьогодні більш важливим є питання щодо його концептуального змісту, тобто його змістових складових. Так, спостерігаються зміни в меті навчання – не просто з'являтися в ЗМІ «у найбільш вигідному вигляді», а управляти ЗМІ. Численні організації пропонують спеціальні тренінгові програми для політиків та посадовців, які розглядають засоби, технології та приклади

ефективної роботи зі ЗМІ. Мета таких організацій, як правило, полягає у тому, щоб їх клієнти під час інтерв'ю почували себе впевненими, володіли навичками контролю не лише за тим, що вони говорять, але і за тим, що говорять про них ЗМІ. Потреба в професійній взаємодії з засобами комунікації викликана багатьма причинами: а) коли суб'єкт політичної діяльності запрошений презентувати свою установу (орган) у телевізійному інтерв'ю, відреагувати на актуальні події дня, обговорити проблемні питання державної політики; б) коли допитливі репортери намагаються отримати інформацію про діяльність органу (установи); в) коли зацікавлені групи, Інтернет-сайти, тощо використовують інформаційну арену для дискредитації органу (установи); г) коли необхідно зробити офіційну заяву, яка матиме важливий вплив на репутацію органу (установи) [142, с. 108].

Таким чином, інформаційна політика партії має бути послідовною, професійною, науково обґрунтованою та ідеологічно виваженою. Партійні діячі повинні підтримувати постійну комунікацію з народом, пропагувати державницькі цінності, вміти мобілізувати електорат щодо захисту інтересів нації та держави.

У науковій літературі широко розповсюдженими поняттями є «національні інтереси» або «національний інтерес», які з нашої точки зору, об'єднують в собі й державні, й народні інтереси. Вочевидь, політичні партії у своїй інформаційній політиці мають орієнтуватися на захист національних інтересів та не оголошувати вузькопартійні інтереси загальнонаціональними. Національний інтерес − це інтегральне вираження інтересів усіх суб'єктів суспільних відносин, що реалізуються через політико-правову структуру та синтезує інтереси кожної людини і/чи групи з інтересами держави. В цьому контексті доречним є розуміння сутності національних інтересів сформульоване американськими дослідниками Ч. Лерчем і А. Саїдом. Вони підкреслюють, що ціннісне наповнення національних інтересів ґрунтується на п'яти «видах «добра»: 1) добро окремих громадян; 2) добро суспільства в цілому; 3) добро держави; 4) добро соціально зацікавлених груп у державі; 5) добро уряду і його членів» [303, с. 11].

Політичні партії, здійснюючи конкурентну боротьбу повинні чітко розуміти ту межу, за якою їх діяльність у інформаційному просторі негативно впливає на національну безпеку держави (інформаційну зокрема). Партійним лідерам варто усвідомити, що політична боротьба не самоціль, а засіб захисту національних та групових інтересів.

Як справедливо зазначають дослідники В. Шахов й В. Мадіссон, часто в політичній боротьбі конкуруючі політичні сили намагаються видавати власні партійні інтереси за «національні». Тому, наголошують вчені, сучасне політичне «життя України підтверджує політологічну теорію про те, що в суб'єктивному плані поняття «національні інтереси» часто стає об'єктом політичних спекуляцій з боку різноманітних політичних сил, які конкурують у національному політичному просторі, часто лобіюючи замість національних інтереси іноземних держав, транснаціональних структур тощо» [282, с. 46]. При цьому вчені продовжують, що «радикалізація поведінки національних сил у боротьбі навколо визначення «національного інтересу», непримиренність, безкомпромісність в узгодженні позицій між політичними супротивниками, неспроможність на національному рівні дійти злагоди в цьому питанні − одна із ознак відкритого й таємного втручання у внутрішні справи України зовнішніх сил в особі головних конкуруючих між собою авторів сучасних геостратегічних проектів формування нового світового порядку» [282, с. 46].

Однією з суттєвих причин, що пояснює неефективний захист політичними партіями в Україні державних й народних інтересів є їх відірваність від суспільства, підпорядкованість деяких з них фінансово-промисловим групам, олігархічним структурам. Саме тому інформаційна політика певних партій є лише ширмою за якою приховані вузькопартійні, бізнесові інтереси лише певних груп населення, а не інтереси народу та держави.

З цього приводу, у науковій літературі підкреслюється, що в Україні, з одного боку, наявний формальний партійний плюралізм, а з другого – партійна система є дуже умовною, бо більшість населення у партійних політичних організаціях не представлена (зокрема, завдяки чинному законодавству). Існуючі

політичні партії в Україні, як єдина організована політична сила, не забезпечують політичну підтримку реформам у перехідний період подібно до відповідних процесів у Польщі, Угорщині, Чехії [229, с. 42]. Крайню точку зору з цього приводу формулює дослідник В. Колісник, який зауважує, що «в умовах імітації дискусій і виборності, та з огляду на домінування формалізму й демагогії, можна без перебільшення стверджувати, що справжніх політичних партій в Україні немає» [141].

Після «Революції гідності» вищеозначена негативна тенденція може бути подолана, оскільки у суспільстві сформувався потужний запит на реформи та на появу тих партій, які будуть спроможні захищати державні та народні інтереси. Інформаційна політика постмайданівських партій має кардинально змінитися: необхідно відмовитись від популізму та демагогії, не використовувати маніпулятивні технології, пропагувати загальнолюдські та національно-державницькі цінності, відверто та з повагою спілкуватися з громадянами.

Разом з тим, необхідно зазначити, що політичні партії у своїй інформаційній політиці можуть відображати державні, народні, суто партійні інтереси й навіть інтереси певних бізнес-груп. Такий стан справ є об'єктивним явищем. Але проблема полягає у пріоритетності, ранжуванні цих інтересів, а також у засобах їх відстоювання. До однієї з технологій захисту різноманітних інтересів, в тому числі й певних соціальних груп, суб'єктами якої є політичні партії можна віднести так званий лобізм.

Лобізм як поняття, найчастіше використовується для означення всієї сукупності способів захисту і просування інтересів, що здійснюється різними каналами і засобами. Істотною особливістю української практики лобіювання є його закрита, непрозора форма, використання нелегальних методів. Більше того, нерегульований лобізм у всіх його іпостасях і тлумаченнях у другій половині 1990-х років утвердився як домінуюча стратегія діяльності груп інтересів і всієї представницької системи українського бізнесу та некомерційних організацій [42, с. 23]. Стосовно ж політичних партій, то вони, як зазначає О. Віннічук, «на відміну від лобістських організацій, ставлять за мету здобуття влади, а не вплив на неї».

Тому, продовжує вчений, хоч і лобізм є складовою діяльності партій, оскільки їх первинна мета полягає в захисті інтересів різних груп, те, як це відбувається, зокрема одержанням влади чи її лобіюванням, не так вже й важливо [42, с. 25].

На нашу думку, у науковій літературі недостатньо уваги приділяється інформаційній складовій сучасного лобізму, яка знаходить відображення у інформаційній політиці партій. Хоча лобізм явище не публічне, але для партій у демократичному суспільстві важливо обґрунтувати свою позицію перед електоратом щодо підтримки того або іншого законопроекту, політичного рішення, представити його життєво необхідним для країни. Проблема в цьому контексті полягає в тому, що у сучасній Україні лобізм так і не став інституціоналізованим явищем, а самі рішення прийняті таким шляхом можуть протирічити народним і навіть державним інтересам.

Для того, щоб лобізм став повноцінним інститутом, необхідні дві умови. По-перше, різноманіття інтересів в суспільстві, що виникає внаслідок його соціальної диференціації, розшарування. По-друге, розширений доступ до влади на основі політичного плюралізму, характерний передусім для демократичних режимів. В Україні ці умови не були реалізовані за часів панування адміністративно-командної системи управління [36, с. 24].

Отже, політичні партії в Україні повинні демонструвати більшу відкритість щодо прийняття важливих для країни рішень, відмовлятися від суто кулуарних процедур обговорення законопроектів, залучати до цього процесу громадськість. Основними принципами інформаційної політики партій у сучасній Україні повинні стати об’єктивність, професіоналізм, інтерактивність та діалогічність, послідовність обраного стратегічного курсу.

Відстоювати державні та народні інтереси від політичних партій повинні вимагати, перш за все, виборці, які своїм ставленням до діяльності політичних сил можуть впливати на їх рішення та позицію. Мова йде не лише про виборчі кампанії, але й про міжвиборчій період, коли найбільш активні й політично свідомі громадяни продовжують активно комунікувати з партійними структурами, контролюючи виконання ними передвиборчої програми. Тому для України вкрай

важливий подальший розвиток громадянського суспільства, підняття рівня політичної й правової культури населення і на цьому тлі організований мирний тиск на владу щодо здійснення демократичних перетворень у державі.

На нашу думку, політичні партії більш послідовно та принципово будуть захищати державні/національні та групові інтереси, коли рівень політичної культури населення не дозволить йому голосувати за ті політичні сили, які не відображають їх інтересів. Високий рівень політичної культури дозволить громадянам розуміти сутність діяльності політичних партій та критично ставитись до їх меседжів у інформаційному полі країни. Партійні лідери будуть змушені у своїй інформаційній політиці та практичні діяльності орієнтуватися на державні та народні, а не на вузькопартійні інтереси. Усвідомлення народом власних та державних інтересів є важливим чинником розвитку політичної культури нації, яка відображається зокрема у різноманітних цінностях, які на нашу думку, мають бути репрезентовані у інформаційній політиці партій.

Відомий фахівець з політичної культури Д. Белл, окреслюючи її світоглядні, ціннісні та інституційні компоненти, наголошував, «що вчинки людей залежать від того, що вони думають, як відчувають, у що вірять». Адже, як вважає вчений, «політична культура складається з ідей, припущень, цінностей, переконань, які зумовлюють політичну дію», а тому й «слугує фільтром або лінзою, через яку політичні актори бачать світ». Відповідно, продовжує він, «політична культура є мовою політичного дискурсу, словником і граматикою політичної дискусії та взаєморозуміння» [цит. з: 192, с. 11]. Фактично демократичний процес, розвиток активістської політичної культури громадян України змушує партійних лідерів переглядати інформаційну політику, очолюваних ними політичних сил, робити її адекватною щодо інтересів народу та держави.

В той же час, як відзначають А. Соловей і В. Штерн, «політична культура сучасного українського суспільства дуже часто набуває демагогічного забарвлення, політичного критиканства та популізму» [251, с. 30]. Річ у тому, продовжує вчений, що «демагогічні тенденції у політичній культурі, як правило, виявляють себе: у популістських гаслах; у відході від конструктивної співпраці

між політичними силами; у продукуванні обіцянок, які неможливо реалізувати; у появі політиків-демагогів, що особливо акцентують увагу на національні почуття громадян, які ідейно й іміджево протистоять політикам-прагматикам; у поширенні неконструктивного способу мислення серед різних груп населення» [251, с. 30]. Причому, констатує науковець, «вищезазначені проблеми та негативні характеристики сучасної української політичної культури значною мірою обумовлені нерозвиненістю демократичних політичних інститутів, низькими темпами реформ та, зрештою, браком часу, що прожило суспільство в умовах демократичних норм, правил та цінностей» [251, с. 30].

У сучасних умовах інформаційних війн та маніпулятивних технологій значно зростає відповідальність партійних лідерів за інформаційну політику керованих ними політичних сил, оскільки наслідки непродуманої, демагогічної, провокативної інформаційної діяльності негативно впливають не тільки на політичну культуру й суспільну свідомість громадян, а й на інформаційну безпеку країни, на якісний рівень захисту народних та державних інтересів.

Як слушно зауважує з цього приводу О. Царенко, «політичні лідери є джерелом «достовірної інформації» через промови та заяви, очікуючи на підтримку громадян», а громадяни же, своєю чергою, «сподіваючись на реалізацію їхніх інтересів, що відповідають цілісній складовій їхньої політичної культури, віддають свій голос за того чи іншого кандидата або проявляють апатію до виборчого процесу, що також є показником діяльності політичної системи загалом та політичної свідомості громадянина особисто» [276, с. 179]. Відповідно, продовжує дослідники, «від того, наскільки якісно політичний лідер буде реалізовувати обіцянки виборців та відповідатиме політико-культурним настановам буде залежати його легітимізована політична активність» [276, с. 179].

Необхідно зазначити, що становлення демократичної політичної культури в Україні є підґрунтям для сутнісних змін у інформаційній політиці партій, оскільки носії вищеозначеного типу культури не будуть сприймати популізм та неконструктивний стиль поведінки політиків, будуть вимагати від них захисту, перш за все, національних інтересів.

Якісний розвиток політичної культури не тільки населення, але й партійних діячів буде сприяти покращенню законотворчого процесу, який є формою захисту народних та державних інтересів. Високий рівень розвитку політичної культури, зумовлює появу ознак демократичного врядування, серед яких суттєвими є такі: а) представництво інтересів населення в належний спосіб через склад та функціонування парламенту; б) перевага консенсусного методу при вирішенні гострих політичних питань; в) можливість локалізації складних соціально-політичних проблеми, що потребують парламентського врегулювання; г) учасники законотворчого процесу зважають на думку усіх зацікавлених сторін; д) внаслідок підвищення ефективності парламентської роботи зменшуються часові витрати на роботу над законопроектом [209, с. 32-33].

Таким чином, становлення демократичного врядування в Україні повинно сприяти професіоналізації діяльності політичних партій, підштовхувати їх до внутрішнього самоочищення і як наслідок до більш ефективного відстоювання державних та народних інтересів. Ці процеси відповідно мають впливати і на інформаційну політику партій: висвітлення чіткої позиції партії з актуальних проблем життєдіяльності суспільства, визначення шляхів їх подолання, визнання зроблених помилок тощо.

Одним з основних завдань партії у здійсненні інформаційної політики є встановлення політичного партнерства між громадянами та владою, заради захисту народних та державних інтересів. Інформаційна політика партії не повинна бути інструментом відстоювання вузькопартійних інтересів, а має бути засобом ретрансляції демократичних норм та цінностей. Політичні сили та їхні політичні лідери мають бути взірцями реалізації та забезпечення стандартів інформаційної і політичної культури у соціумі. Відстоювання інтересів клану, регіону чи окремої партії, ігноруючи інтереси держави й народу є не припустимим явищем у демократичному суспільстві.

Отже, в цьому контексті доречним буде проаналізувати особливості діяльності державницьких та опозиційних партій та рухів в інформаційному розрізі, а також їхній вплив на безпеку особистості й суспільства загалом.

Як відомо для науки, у розвинутих демократичних суспільствах і державницькі, і опозиційні партії у змагальній боротьбі діють за цілком базовим принципом – «не нашкодити державі». Саме тому їх боротьба у суспільному, політичному й інформаційному розрізі регламентована не лише нормативно, а й існуючими стандартами політичної культури. Водночас інша ситуація у країнах (в Україні зокрема), для яких властиві нестабільні демократичні звичаї та традиції, внаслідок чого різна інформаційна діяльність партій і рухів може бути небезпечною для індивідів, груп і загалом суспільства. Визначаючись термінологічно, зазначимо, що у нашому дослідженні ми будемо використовувати поняття «державницькі партії» та «провладні партії» як синонімічні.

Для визначення сутності інформаційної діяльності провладних й опозиційних політичних партій та їх вплив на безпеку особистості та суспільства необхідно з'ясувати, яка модель політичної опозиції склалася в тій або іншій країні. З цього приводу ґрунтуючись на ідеях Г. Гаврилова, «можна виокремити низку типових моделей опозиції, що формуються в рамках відповідних типів політичних систем: політична опозиція в гомогенних біполярних системах; в багатоскладних біполярних системах; в багатоскладних багатополярних системах; в гомогенних багатополярних системах» [45, с. 8]. Вочевидь, що тип системи та модель існуючої опозиції у тій чи іншій країні детермінують здійснення інформаційної політики суб'єктами конкуренції, які в свою чергу впливають на інформаційну безпеку особистості та суспільства.

Узагальнюючи науковий доробок Г. Гаврилова, О. Масловської та Т. Ткаченко, ми дамо розгорнуту характеристику моделей політичної опозиції як підґрунтя інформаційної діяльності провладних і опозиційних партій [45; 186].

Дослідники констатують, що «модель політичної опозиції в консенсусних біполярних системах (Великобританія, США) характеризується абсолютною перевагою системної опозиції, що обумовлено наявністю консенсусу відносно основних принципів державного устрою» [186]. Тому тут, кажуть вчені, «опозиція формується на однопартійній основі», а через те, що «виконавчу владу в цих системах формують переможці виборів, то основні методи опозиційної боротьби

перебувають в електоральній сфері» [186]. З нашої точки, у вищерозглянутій системі інформаційна політика партій обумовлена глибокими історичними традиціями втілення демократії і її реалізація має мінімальні ризики для безпеки суспільства та особистості. В таких політичних системах вже визначені принципові, стратегічні напрямки розвитку країни, що позитивно впливає на стан національної та інформаційної безпеки.

Натомість, зазначає О. Масловська, «модель політичної опозиції в конфліктогенних біполярних системах характеризується наявністю в суспільстві двох потужних сегментів, передбачає формування опозиції за сегментарним принципом, що не передбачає врахування інтересів малих груп» [186]. Тому тут, продовжує вчена, «постійне прагнення однієї з політичних сил до одноособового завоювання влади є чинником формування несистемної опозиції, чия діяльність здатна призвести до розколу системи» [186] (як різного часу в Туреччині, Єгипті, Пакистані, Йорданії, а також деяких інших азійських країнах). На нашу думку, така модель політичної опозиції є підґрунтям до жорсткого протистояння між політичними силами, яке відображається зокрема й у інформаційній боротьбі між ними та може переходити у збройні конфлікти і повстання, що несе загрозу безпеці особистості та суспільства. У таких системах доступ опозиційних партій до ЗМІ є обмеженим, що спонукає їх використовувати різноманітні канали для агітації та пропаганди. Варто згадати так звану «арабську весну», коли саме за допомогою соціальних мереж відбувалося згуртування опозиційних сил для подальших радикальних дій.

Наступна «модель опозиції в консенсусних багатополярних системах» (як в Австрії, Бельгії, умовно Нідерландах і в часті інших континентально-європейських країн), помічає О. Масловська, «характеризується тим, що опозиція має переважно системний характер; при цьому наявність несистемної опозиції не виключається, проте вона представлена у вигляді політичних маргіналів» [186]. Тому тут, каже вчена, «сегментарний принцип формування опозиції значно знижує перспективи опозиційних сил отримати владу електоральними засобами, опозиція може формуватись на коаліційній основі», оскільки «опозиція має

консенсусний характер, що пояснюється прагненням всіх потужних сегментів суспільства до збереження стабільності системи» [186]. Ця система має плюралістичний характер і етнонаціональну, релігійну та політичну строкатість, але в ній сформувалися механізми реалізації суспільного й політичного консенсусу на основі принципів демократії. У інформаційній політиці партій в такій системі, як правило відображені інтереси певного електорального сегменту, який представляє та або інша політична сила. Боротьба політичних партій у інформаційній сфері є вираженням суспільної дискусії з злободенних питань: легалізація наркотиків та одностатевих шлюбів, міграційна політика держави, місце країни у європейських процесах тощо. Такі інформаційні баталії провладних та опозиційних політичних сил як правило не становлять загрозу національній безпеці у всіх її вимірах.

О. Масловська продовжує свій аналіз тим, що ще одна «модель політичної опозиції представлена у конфліктогенних багатополярних системах і характеризується формуванням опозиції за принципом клієнтелізму, що є результатом елітизованого політичного процесу» [186]. У цій моделі, продовжує вчена, «протиставлення гравців є досить жорстким, що істотно звужує поле пошуку консенсусу», а наслідком, своєю чергою, «великої кількості політичних сил, жодна з яких не здатна отримати владу самостійно, є формування нестабільних правлячих коаліцій, мінімальне врахування думки опозиції з боку коаліції знижує цінність парламентського представництва, внаслідок чого опозиційні сили максимально направляють свої зусилля на отримання влади» [186]. Врешті-решт, зазначає вчена, «таким системам притаманна практика блокування роботи парламенту, а відповідно й дій виконавчої влади, що призводить до іммобілізації всієї системи» [186] (як, приміром, в Грузії, Молдові, Україні тощо).

Інформаційна політика урядових та опозиційних партій у такій моделі чи системі є агресивною та безкомпромісною, що негативно впливає на інформаційну культуру і захист людини й суспільства. Часто-густо політичні партії в таких системах не шукають консенсусу, а прагнуть повної перемоги. В

своїй інформаційній політиці як провладні, так і опозиційні партії можуть використовувати технології та політичні штампи, що шкодять безпеці особистості й суспільства. Так, в Україні Партія регіонів заробляла політичні дивіденди протиставляючи Захід й Схід країни, спекулюючи на питанні російської мови, вступу України до НАТО тощо. В свою чергу Комуністична партія активно експлуатувала ідею відновлення Радянського Союзу у іншій формі, ідею підняття добробуту бідних прошарків населення за рахунок більш заможних. Інформаційна політика таких партій мала популістській, недержавницький, антиукраїнський характер, що наносило значну шкоду безпеці особистості та суспільства.

Врешті-решт, зазначає О. Масловська, «модель політичної опозиції в однополярних системах характеризується концентрацією влади в руках одного суб'єкта (глави держави, партії чи державного інституту)» [186], а тому тут «опозиція може мати системний характер, що проявляється у внутрішньопартійній міжелітній боротьбі, та несистемний характер, що передбачає потенційну можливість насильницької зміни режиму» [186] (як в Індії, Росії, Білорусі, Таджикистані, Казахстані тощо). Вище проаналізована модель політичної опозиції частіше за все існує у авторитарних політичних системах. Опозиційні партії в такій системі мають обмежені можливості щодо проведення відкритої, конкурентної інформаційної політики, оскільки існує цензура та основні медіа-ресурси зосереджені у держави й провладних політичних партій. Здійснення провладними політичними силами інформаційної політики може мати маніпулятивний, викривлений характер. Суспільство й громадяни значно обмежені у праві на отримання достовірної інформації, що становить небезпеку для їх життєдіяльності. Відтак маніпулятивна інформаційна політика урядових партій становить небезпеку для свідомості й адекватності сприйняття оточуючого світу людьми (як у сучасній Росії).

Продовжуючи аналіз інформаційної діяльності державницьких й опозиційних партій та політичних рухів, зазначимо їй притаманні так звані фейкові процеси. Як зазначає Н. Астряб, особливо це стосується сфери політичних інтересів як провладних, так і опозиційних партій, а також певних

елементів структури громадянського суспільства та суспільної свідомості [15]. Слово «фейк» англомовне, де має сленгове підґрунтя і розуміється як фальшивка, підробка тощо. Використовується для визначення чогось фальшивого, знеціненого через його не ідентичність. Спираючись на науковий доробок М. Кармазіної вищеозначена дослідниця наводить приклад фейк-утворень на прикладі виборів до Верховної Ради України у 2012 році [15]. Так, на середину 2012 року в Україні функціонувало 202 партії, а у парламентських виборах брала участь лише 21 партія. Отже, більшість партій були фейк-учасницями виборчого процесу. Деякі партії виступали як «технічні», що обслуговували «партію влади», тому вони розглядаються як продовження адміністративного ресурсу. Наступний момент − непрозорість ситуації з партіями для суспільства: недоступність інформації про програмні документи та аспекти діяльності; непрозорість партійного фінансування; закритість механізмів зміни лідера. Отже, партійне середовище як зазначає М. Кармазіна, виступає як середовище фейків, партій-привидів, що є викривленими каналами зв'язку між владою і суспільством [15, с. 491-492]. Фейкові партійні структури або не здійснюють інформаційної діяльності взагалі, або здійснюють пряме й опосередковане інформаційне обслуговування потужних політичних партій. В будь-якому випадку їх діяльність сприяє викривленню інформаційного та політичного просторів держави й чинить негативний вплив на інформаційну безпеку особистості та суспільства.

Особлива активізація інформаційної діяльності партій та політичних рухів спостерігається під час виборчих кампаній. Нажаль, українські політичні партії (як провладні, так і опозиційні) за останні роки застосовували різноманітні інформаційно-пропагандистські технології, які негативно впливають на інформаційну безпеку людини та суспільства. У рекламно-агітаційній кампанії партії використовують такі технології, як «наклеювання ярликів», НЛП-технології, антиреклама та ін. [15].

«Наклеювання ярликів» є простим прийомом, що побудований на навіюванні і може бути деструктивним. Воно у контексті політичних діячів застосовується, щоби зганьбити їх через образи, погані епітети та/чи метафор

негативного змісту. Сприяє цьому використання НЛП-технологій у впливі на підсвідомість людини, серед яких прийоми 25-го кадру, лінії часу, субмодальності. З цього приводу Т. Ященко зазначає, що «за допомогою НЛП політики змушують виборців діяти на свою користь, і в результаті, замість можливості самостійно й свідомо визначатися зі своїм вибором, громадяни отримують порцію жорстких наказів через підсвідомість» [291, с. 110-111].

Цікаво й те, що деструктивний характер інформаційної діяльності провладних та опозиційний політичних партій та рухів репрезентований так званою антирекламою. За формою та суттю антиреклама різниться від традиційних опцій реклами, адже завжди направлена проти політичного опонента або всіх опонентів [291, с. 110-111]. Серед її прикладів –політичні анекдоти та чутки, які сумарно генерують негативний образ політика, політичної партії, діяча, а відтак ведуть до втрати їхнього авторитету поступово втрачають авторитет і повагу. Відповідно такі технології дезінформують громадян, негативно впливаючи на їхній вибір тої або іншої політсили, а тому в кінцевому підсумку їх застосування порушує принципи інформаційної безпеки особистості і суспільства.

Особливо небезпечно деструктивною технологією для інформаційної безпеки громадян і суспільства, яку застосовують провладні партії та рухи, є адміністративний ресурс. В інформаційному плані його сутність полягає в тому, що всі державні та урядові медіа-ресурси працюють задля перемоги певної сили або кількох сил. При цьому, для опозиційних партій та рухів створюються неконкурентні умови у фінансовому й організаційному плані, чи їх представників не допускають на державні і урядові медіа. Відповідно, громадянин втрачає можливість зваженого та об’єктивного вибору, може мати викривлену думку про діяльність певної партії, що негативно впливає на національну та інформаційну безпеку держави й загалом суспільства.

На думку фахівців, зокрема як зауважує Н. Ніколаєнко, «можна виокремити три способи використання адміністративного ресурсу: 1) прямий адміністративний тиск на виборців, включаючи підкуп, погрози й підтасування результатів голосування; 2) тиск на конкурентів у всіх можливих формах:

інформаційна блокада, відсторонення від виборів, карне переслідування тощо; 3) використання адміністративного ресурсу для ефективного проведення власної виборчої кампанії кандидата (партії) влади» [203, с. 477].

Взагалі, як каже Т. Ященко, «природа некоректних і деструктивних технологій носить маніпулятивний характер» [291]. Тому, продовжує вчений, «маніпулювання масовою свідомістю є на сьогодні чи не найважливішим інструментарієм в арсеналі засобів здобуття влади та отримання політичних дивідендів» [291]. При цьому, «у виборчій боротьбі сам виборець зусиллями політиків та політтехнологів перетворюється з суб'єкта політичного процесу на об'єкт цілеспрямованого психологічного впливу» [225, с. 249; 291]. Партії ж, котрі використовують ці технології, по-факту різносторонньо руйнують демократичне волевиявлення громадян, а тому й національну та інформаційну безпеку суспільства й держави.

Подолати вищеозначені негативні тенденції у діяльності, перш за все, провладних політичних партій дозволять принципи та норми інформаційної діяльності розроблені у Європейському співтоваристві. Відповідно до Рекомендації Комітету Міністрів Ради Європи № R (99) 15: «ЗМІ при розміщенні політичної реклами мають забезпечити рівне і недискримінаційне ставлення до всіх політичних партій і кандидатів, які прагнуть придбати рекламний простір [239]; приймаючи замовлення на розміщення платної політичної реклами, забезпечити її розпізнавання як такої згідно з вимогами законодавства та нормами саморегулювання. Також норми законодавства повинні сприяти тому, щоб, оприлюднюючи результати соціологічних опитувань і розвідок, ЗМІ давали громадянам потрібну інформацію, для узагальнень про їхню достовірність, зокрема з приводу партій, організацій, осіб, які їх організовують, проводять тощо.

Інформаційна безпека особистості й суспільства пов'язана не тільки з діяльністю різноманітних партій, а й політичних рухів, які є активними учасниками суспільно-політичних процесів, що знаходить своє відображення у інформаційному просторі. З цього приводу В. Зубар зазначає, що «представники теорії нових суспільних рухів – Ю. Габермас А. Мелучі, П. Гунделах, Р.

Інгельхарт – зазначали, що великий вплив на розвиток суспільно-політичних рухів має розвиток демократії» [118]. Однак рухи в сучасних умовах зосереджені на нових проблемах, нових аспектах соціальних конфліктів. Як підкреслює Н. Смелзер, «старі суспільні рухи – рухи за об'єднання робітничого класу та революційні рухи, які розуміються в контексті марксистського світогляду, – були в основному вичерпані, так само як і марксистський аналіз суспільства» [249, с. 62].

У сучасних умовах сутність та характер суспільно-політичних рухів зазнав певних трансформацій. Одним з важливих аспектів їх діяльності стала інформаційна складова для реалізації просвітницької, правозахисної, агітаційної функцій. Аналізуючи параметри розвитку суспільно-політичних рухів, Е. Гідденс пропонує їхню класифікацію на трансформативні та реформаторські рухи, рухи порятунку і альтернативні рухи [49, с. 89; 118].

В останній час в Україні активну інформаційно-просвітницьку діяльність здійснював суспільно-політичний рух «Чесно», який був створений групою активістів із представниками групи/асоціації «Новий Громадянин». Як зазначає В. Зубар, «рух є відкритою платформою для приєднання громадських організацій та індивідуальних учасників, він не підтримує жодного політика чи політичну силу» [118, с. 69]. Вчений продовжує, що цей «рух здійснює постійний моніторинг діяльності представників влади, зокрема, його членами було розроблено шість критеріїв доброчесності політиків: відсутність фактів порушень прав і свобод людини; незмінність політичної позиції відповідно до волевиявлення виборців; непричетність до корупційних дій; прозорість задекларованих доходів та майна та їх відповідність способу життя; особисте голосування в парламенті; участь у засіданнях парламенту та роботі комітетів» [118, с. 69]. Крім того, вчений зазначає, що «спільно з журналістами та громадськими активістами аналітична команда руху «Чесно» перевірила спочатку 450 народних депутатів, а потім – понад 2500 кандидатів на відповідність цим критеріям» [118, с. 69]. Відповідно, інформаційна діяльність руху «Чесно» значно сприяла поінформованості громадян, а також дозволяла їм обирати кращих серед політиків, давала їм об'єктивну інформацію про функціонування партій та їхніх представників у

легіслатурі й інших органах державної влади. Саме тому загалом інформаційна робота цього руху сприяла зміцненню безпеки людей і суспільства, попереджаючи їх про корупціонерів та непрофесіоналів у сфері політики.

В. Зубар зазначає, що «у 2013 р. в Україні сформувався новий громадсько-політичний рух – Євромайдан, головна його ідея – європейський вибір України» [118, с. 69]. Народжений Євромайданом громадсько-політичний Рух базується на політичному плюралізмі, різних структурах управління. Однак вчений помічає, що «наскільки ефективним стане цей рух покаже час», оскільки «багато залежить від волі всіх учасників Євромайдану, а головне – від його лідерів» [118, с. 69]. Сьогодні ж важливо, продовжує науковець, що «структура управління рухом має відповідати настроям у суспільстві, зокрема, тому факту, що громадськості довіряє більше людей, ніж політичним партіям, адже Рух не може бути утворенням партійних структур, він має бути відкритим» [118, с. 69].

Необхідно зазначити, що особливу роль інформаційна діяльність рухів відіграє під час значних суспільних трансформацій, наприклад, перехід від тоталітаризму або авторитаризму до демократії, коли опозиційних партій, ще немає (тоталітаризм) або їх діяльність є значно обмеженою (авторитаризм). Окреслена діяльність рухів є двоїстою: по-перше, сприяє демократизації, по-друге, може становити загрозу безпеці автократичної країни.

Як зазначає В. Бусленко, характеризуючи системні зміни на пострадянському просторі, «на етапі лібералізації спостерігаємо діяльність громадсько-політичних організації і суспільно-політичних рухів, опозиційно налаштованих до комуністичної влади, які вимагають системних змін». Вчений додає, що «в цей час проявляється така риса опозиції як організованість» [35, с. 316]. І це логічно, адже дійсно досить складно уявити собі неорганізовану масу людей, що борються за домінуючий політичний ресурс. Тим паче, каже В. Бусленко, що «малоймовірно, що неорганізована група могла б ефективно цей ресурс використати», адже «не маючи інституційних важелів впливу на владу, опозиція активно використовувала різноманітні форми мобілізації мас: мітинги, страйки, демонстрації, пікетування тощо» [35, с. 316]. Причому форми прямої

демократії були у той час ефективними в контексті їхнього впливу чи тиску на владу.

При цьому, зі слів В. Бусленка, сама демократична опозиція, за визначенням А. Степана, виконує наступні функції: «1) опір інтеграції в рамках режиму; 2) захист зон автономії проти режиму; 3) підрив легітимності режиму; 4) збільшення політичної ціни авторитарного правління; 5) створення сприйнятливої демократичної альтернативи» [35, с. 316; 311, с. 45]. В. Бусленко уточнює, що «ці функції при відсутності опозиційних політичних партій особливо чітко проявлялися в діяльності суспільно-політичних рухів, які мали масовий характер і включали в себе новостворені громадські організації різного спрямування», а «частина з них пізніше трансформувалися в опозиційні політичні партії» [35, с. 316]. Вчений вважає, що ця «тенденція спостерігалася в Польщі (Солідарність), Україні (Народний рух України)», адже «з НРУ вийшли такі партії націонал-демократичного спрямування як ДемПУ, УРП, УСДП» [35, с. 316]. Отже, опозиційні рухи у авторитарних та тоталітарних країнах є вкрай необхідними, оскільки саме їх інформаційна діяльність у різних формах сприяє руйнуванню інформаційної монополії, встановленою державою. З опозиційних політичних рухів у майбутньому можуть виникнути впливові політичні партії, як підкреслювалося вище.

Висновки до Розділу 4

Інформаційна безпека відіграє провідну роль в забезпеченні життєво важливих інтересів будь-якої країни. Метою її забезпечення є створення розгалуженого і захищеного інформаційного простору, захист національних інтересів держави в умовах формування світових інформаційних мереж, захист економічного потенціалу країни від неправого застосування інформаційних і комунікаційно-технологічних ресурсів, втілення на практиці прав людини й громадян, інститутів та держави на продукування та використання відповідної інформації. Держава – це той визначальний колективний суб’єкт інформаційної

безпеки, що здійснює функції у цій сфері через органи влади.

Комплексна інформаційно-безпекова діяльність держави мусить передбачити правові, організаційно-економічні, технологічні, політичні, а також ціннісно-культурні методи роботи, що доповнюють та увиразнюють зміст один одного. Відтак держава через низку політичних інституцій здійснює заходи щодо забезпечення інформаційної безпеки та є головним агентом збереження стабільної рівноваги і впровадження прогресивних змін у перехідному суспільстві. Вона цілком може як наближати, так і віддаляти перспективу інформаційного суспільства (перешкоджати громадській ініціативі, обмежувати творчий та інтелектуальний порив у цьому напрямку). Державні інститути визначають правові рамки інформаційного простору, але як і будь-які інші можуть й (не)свідомо порушувати відповідні норми в обличчі окремих державних службовців чи й цілих організацій. Держава виявляє та знешкоджує зовнішні інформаційні атаки, але нерідко й у її структурах окремі іноземні агенти реалізують пріоритети і стратегії інших держав. Тож поряд з тим, що існуюча інфраструктура державних інститутів інформаційної безпеки України мусить вибудовуватися за принципом стримувань і противаг, важливо також, щоб державні органи постійно перебували під громадським контролем, відкриті до комунікації зі ЗМІ, прозорі у своїх рішеннях та звітності, зрозумілі для міжнародних партнерів.

Інформаційна діяльність партій і рухів в умовах демократії створює підґрунтя для її розвитку та є запобіжником від руху назад до автократії. Вищеозначені політичні сили є своєрідними форпостами громадянського суспільства, одним з призначень яких є безпека особи й суспільства у різних її проявах, і в інформаційному. Тому партії і рухи беруть доволі активну участь у виробленні стратегії інформаційної безпеки держави. У демократіях до цього долучаються як урядові, так і опозиційні сили. Відповідно, при автократії стратегія інформаційної безпеки є прерогативою лише урядових сил. Інформаційна політика самих партій є чинником інформаційної безпеки людей і суспільства. У країнах з нестійкими демократіями інформаційна політика може негативно впливати на безпеку людини, суспільства й держави.

РОЗДІЛ 5

ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО ТА ЗАСОБИ МАСОВОЇ ІНФОРМАЦІЇ У СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Консолідуючий потенціал громадянського суспільства у системі інформаційної безпеки та чинники його дестабілізації

Важливу роль у формуванні поля національної інформаційної безпеки відіграють волонтерські об'єднання, громадські організації, окремі громадські ініціативи та рухи тощо. Розглянемо це питання детальніше, адже йдеться про важливий пласт інститутів, які постали з інтенсифікацією зв'язків у інформаційному суспільстві, у загальній атмосфері спрощення сучасних інтеракцій і взаємодій, зі зміною способів та цінностей життя сучасників, з утвердженням ролі громадянського суспільства загалом. Взаємозалежність соціально-політичних рішень і процесів активізувала глобалізацію світової економіки, політики, культури, хоча одночасно цифровий світ має і зворотні наслідки для прояву громадської ініціативності, що проявляються в радикальній агресії або слактивізмі. Часто у сучасному світі громадська ініціатива дискредитується, використовується для дестабілізації ситуації, хоча майже завжди вона покликана саме до консолідації зусиль. Загалом йдеться про неоднозначне соціокультурне середовище, у якому розвиваються не лише державні чи суто політичні структури, але громадські формування, потенціал яких у системі інформаційної безпеки ще до кінця не вивчений.

Загалом мають рацію вчені, що в технологічних досягненнях вбачають нові широкі можливості для формування нової соціально-політичної культури, для постійної участі громадян в оцінці проблем, поставлених перед суспільством, визначені необхідних суспільних змін [77, с. 62]. Коло суб'єктів політики розширюються, і в Україні ми також спостерігаємо цю тенденцію, що своїм корінням сягає й інформаційних основ.

У Законі України «Про основи національної безпеки України» відповідні механізми громадської участь та можливостей достатньо демократичні, адже регламентовано, що: «Громадяни України через участь у виборах, референдумах та через інші форми безпосередньої демократії, а також через органи державної влади та органи місцевого самоврядування…реалізують національні інтереси… здійснюють заходи, визначені законодавством України щодо забезпечення її національної безпеки; як безпосередньо, так і через об’єднання громадян привертають увагу суспільних і державних інститутів до небезпечних явищ і процесів у різних сферах життєдіяльності країни…» [114]. Таким чином, громадяни через різноманітні форми участі в політичному житті суспільства, в тому числі і через громадські об’єднання формують поле національної безпеки.

Загальна характеристика участі громадських організацій та рухів в інформаційному просторі суспільства зумовлена, перш за все, становленням нового типу суспільства, в якому саме інформаційний простір постає головною соціальною конструкцією, полем, де відбуваються основні події. У цьому питанні ми послуговуємося авторитетною позицією В. Горбуліна про те, що сучасний світ характеризується постійним зростанням інформаційної індустрії, ця специфічна галузь діяльності людства приносить високі прибутки, тож інформація (її збір, опрацювання, аналіз, поширення, спростування) потребує відповідних коштів, стає найважливішим стратегічним ресурсом, без якого практично усі сучасні сфери життя зазнають відчутних, а іноді й незворотних втрат [52, с. 7].

З цього приводу Л. Абрамов й Т. Азарова зазначають, що «інформаційний простір – це безліч інформації, об'єкти якої зв'язані між собою таким просторовим відношенням, як територія», внаслідок чого «можна говорити про міжнародний, національний, регіональний, місцевий інформаційний простір» [2, с. 14], в тому числі через технології Internet. Вчені продовжують, що «розвиток сучасної технології сприяє створенню єдиного інформаційного простору, не обмеженого локальним рівнем, і такого, що не має регіональних, державних, національних меж», а тому в його рамках «здійснюється інформаційний обмін»

[2, с. 14]. Останній же, зазначають вчені – «це передавання й отримання інформаційних продуктів, а також надання інформаційних послуг», в ході якого «здійснюється процес руху й споживання інформації, що створюється суспільством» [2, с. 14]. Однак таке суспільство може мати різну функціональну якість, змістовну наповненість, психологічну готовність до відповідних обмінів.

У латинській етимології слово «інформувати» позначає здатність «зображати, складати уявлення про що-небудь», тому й «інформаційний простір», «поле інформаційної діяльності» трактується як середовище, де продукуються такі уявлення, тобто виробляється, зберігається, циркулює інформація. Вітчизняні науковці стверджують, що поняття ще й має виражений соціально-політичний контексті, охоплює територіальний, космічний, технічний, економічний фактори, але зокрема і людиновимірний. Адже інформація передусім адресована людині, без якої втрачає свій первинний сенс [126].

Вчені окреслюють множинні функції сучасного інформаційного простору. Серед різних класифікацій нам імпонує підхід, що об’єднує різні функції три визначальні групи. Передусім, акцентують на інтегруючій функції, тобто здатності інформаційного простору об'єднувати в єдину просторово-комунікативну та соціокультурну сферу людей, спільноти, держави, народи, корпорації тощо. Другу групу умовно називають комунікативною, відтак йдеться про значущість транскордонної мобільності, інтерактивності, численних інформаційних обмінів, властивих сучасному світу. Третя – геополітична функція – адже інформаційний простір трансформує традиційні уявлення про міждержавні відносини, владні зв’язки і конкурентні чи навіть військові стратегії. Окремо можна було б також згадати ціннісний потенціал інформаційного простору, який змінює характер, культуру і зміст соціально-політичних відносин, зокрема посилює широку громадську складову у них [182, с. 94].

Було б несправедливо навіть саме поняття інформаційного простору України обмежувати тільки територіально чи за сферами впливу державних інституцій. Тут важливо враховувати усіх суб'єктів і об’єктів політики,

матеріально-технічні й інтелектуальні потужності, що пов’язанні з національними інтересами.

Ми солідарні з вченими, які у структурі інформаційного простору вирізняють громадські та недержавні суб’єкти, зокрема: недержавні інформаційні агентства; недержавні організації – через створені ними у встановленому порядку інформаційні служби; «недержавні установи, служби і центри збирання, зберігання, дослідження та по ширення статистичної, соціологічної, економічної, іншої суспільно значущої інформації»; «спеціальні галузеві та міжгалузеві (проблемні, банково-інформаційні, довідкові тощо) установи і центри … наукової та науково-технічної інформації» [437, с. 141]; аудіовізуальні і друковані ЗМІ та структури, які їх об'єднують; «професіональні творчі об'єднання громадян у галузях науки, літератури і мистецтва, винахідницької та раціоналізаторської діяльності, збереження й охорони історико-культурної спадщини, інформаційного обслуговування (творчі спілки, товариства, асоціації тощо)»; «виставкові організації та центри» [437, с. 141]; «бібліотечні, музейні, клубні та інші культурно-просвітницькі установи, які використовуються в інформаційній діяльності»; зарубіжні і міжнародні громадянські організації, представництва; філії суб'єктів національного інформаційного простору країни за кордоном тощо [127, с. 183; 437, с. 142].

Як зазначає В. Карпенко, національний «інформаційний простір – надзвичайно важливе політичне поняття, яке у вартісній шкалі соціальних цінностей можна поставити на друге місце після державної незалежності» [126]. Держава покликана відігравати провідну роль в інформаційному просторі, від неї залежить спроможність об’єднувати зусилля з протистояння інформаційним атакам. Водночас важливою ланкою формування інформаційного простору вважаються громадяни, оскільки формування державної, партійної, регіональної політики, процеси прийняття політичних рішень, законотворчість загалом не повинні обмежуватися лише вищими владними інститутами, а потребують широкої участі громадян у цих процесах. При чому саме громадські організації науковці вважають тим універсальним посередником між суспільством і

державою, які презентують ширший спектр соціальних інтересів, краще розуміють природу окремих суспільних проблем та шляхи їх подолання [43, с. 3].

Невід'ємною частиною існування суспільства є громадські організації і рухи, які виступають не лише як інструмент інформування громадян і громад та з'ясування їхніх проблем, але і як засіб розв'язання проблем й організації громадянами та громадами своїх запитів. Згідно з Законом України, регламентовано, що «громадське об'єднання – це добровільне об'єднання фізичних осіб та/або юридичних осіб приватного права для здійснення та захисту прав і свобод, задоволення суспільних, зокрема економічних, соціальних, культурних, екологічних, та інших інтересів» [109]. Сьогодні громадянські організації й об'єднання є також знаряддям контролю громадянським суспільством функцій держави та її органів влади.

У сучасних правових документах, в тому числі й міжнародних, у науковій літературі, у публічному дискурсі питання широко висвітлюється та здобула численні трактування навіть на рівні визначень: «третій сектор», «громадська організація», «неурядова організація», «недержавна організація», «non-governmental organizations/NGOS» тощо. У тематичному дослідженні А. Матвійчук наголошує, що категорії «неурядова організація» і «недержавна організація» не зовсім коректно ототожнювати, адже уряд не уособлює повністю всю державну владу. Громадська організація – «це формалізоване самодіяльне (неурядове) неприбуткове об'єднання громадян, спрямоване на реалізацію різноманітних колективних інтересів і захист колективних прав [438, с. 54]. Відповідно, «у такому значенні це досить різні за суттю інституції – політичні партії, власне громадські організації, органи місцевого самоврядування, благодійні фонди тощо» [438, с. 54]. Неурядова організація – громадське об'єднання індивідів або груп, яке бере участь також у політичній діяльності. Неурядова організація – «локальне, національне чи міжнародне об'єднання людей, діяльність яких здійснюється з ініціативи громадян, а не із санкції чи вказівки уряду», й не має на меті отримання прибутку (центральні напрямки їх

діяльності – «захист прав людини, надання допомоги біженцям, боротьба за роззброєння, здійснення дослідницьких та освітніх заходів)» [187, с. 5].

В сучасному українському суспільстві, особливо на загальному тлі трансформації статусу політичних партій, як політичного інституту – втрати ними статусу громадських організацій (статусу суспільних організацій, що представляють інтереси народу у владних структурах), перманентного утворення «партії влади», посилення залежності партій від адміністративно-економічних кланів та фінансово-політичних груп (перетворення партій на політичні представництва, лобістські центри реалізації бізнес-інтересів в органах державної влади), політичні партії сучасної України стали монопольним джерелом формування політико-управлінської еліти та органів державної влади [151, с. 44]. За таких умов участь громадянського суспільства у вигляді громадських ініціатив та рухів є необхідною запорукою демократичності та відкритості інформаційного простору.

Участь громадян і громадських об’єднань у політичному житті означає демократизацію політичного життя в цілому, адже йдеться відтак і про підтримку легітимності державної влади, і про громадський вплив на владу, боротьбу з корупцією, нігілізмом, соціально-політичною апатією та іншими внутрішніми деструктивними впливами. Водночас нерідко йдеться про ефективний громадський контроль зовнішніх інформаційних загроз, відтак впливовість третього сектору посилюється і в глобальній перспективі.

Системно досліджує цю проблематику О. Корнівєвський, який вважає, що саме повсякденна діяльність громадських формувань України часто актуалізує нагальні проблеми, посилює захищеність життєво-важливих інтересів різних соціально-економічних, вікових груп населення, сприяє і результативності відповідної політики (підвищенню рівня, якості, безпеки життя тощо). Така робота, на думку вченого, є одночасно й загальним індикатором функціонування громадських організацій як реальних суб’єктів недержавної системи забезпечення національної безпеки [150, с. 14]. Водночас можемо припустити, що будь-яка, навіть короткочасна статичність, а тим більше тривала

законсервованість у роботі громадського сектору вказує не лише на його бездіяльність, але й загалом демократичний реверс, а також застій у розвитку цифрового суспільства, яке взагалі не мислиме без активних, діяльнісних суб'єктів.

Багато дослідників зазначають, що ефективність вирішення владою будь-яких проблем безумовно підвищується завдяки участі у їх вирішенні громадських представників, які проявляють ініціативу та активність. Найбільш активні члени суспільства створюють та очолюють громадянські ініціативи, рухи, але ефективність їх діяльності напряму залежить від масовості, від обізнаності їх діяльністю тих верств та груп населення, чиї інтереси вони відстоюють. Як зазначають Л. Абрамов і Т. Азарова, «інформаційне забезпечення громадських ініціатив, а також організація інформаційного обміну є необхідною умовою вирішення соціальних проблем, оскільки: 1) якісна інформація відбиває всю розмаїтість життя громади: її інтереси, проблеми, шляхи розвитку місцевого співтовариства; 2) завдяки інформації кожен громадянин має можливість відчути свою власну приналежність до громади й відповідальність за її благополуччя; 3) шляхом вивчення відповідної інформації освоюється соціальний досвід; 4) саме інформація спонукає людей до активної участі в соціальних перетвореннях» [2, с. 5].

В інформаційному просторі громадські об'єднання, організації та рухи виконують функції забезпечення плюралізму та незалежності засобів масової інформації, виступають інструментом соціального і культурного прогресу, сприяють побудові нової архітектури відносин в українському суспільстві та багатогранному функціонуванню всієї системи держави. Для існування та розвитку громадської організації, як і будь-якої іншої організації, важливим фактором є інформація, її продукування та застосування потенціалу інформації для забезпечення організації чи руху.

Громадські організації та стан їх розвитку є індикатором не лише демократизаційних процесів, але й політичної модернізації. Кожен політичний процес сьогодні позиціонується в тому числі і як сукупність емоційних та

раціональних уявлень, що побутують у країні загалом, на рівні широких мас суспільства, (не)формальних комунікацій, тобто загалом він залежить від активного залучення різних спільнот, а також використання інформаційних технологій. Науковці авторитетно стверджують, що існує деякий алгоритм: «надходження повідомлень – формування розуміння, задуму – вироблення установки на діяльність» [213, с. 5], тому у такому світі як сучасний (глобалізований та інформаційний), інакше як поза інформаційними потоками та їх громадським сприйняттям не можливо сформулювати ефективну політичну дію, а отже й запровадити будь-яку політичну реформу.

Зрештою і спроби імплементувати зарубіжний досвід політичної трансформації залежить в тому числі й від потужностей громадського сектору. Сьогодні у безпековій тематиці утверджується поняття «міжнародний інформаційний простір», що вчені пов’язують з інтенсивним розвитком науково-технологічного, кібернетичного напрямків, глобальною інформаційною мережею Інтернет. У міжнародному інформаційному просторі (як сукупності інформації й інформаційних технологій, що забезпечують діяльність міждержавних служб та інститутів, транслюються державами одна на одну і забезпечують основну частину міжнародних політичних відносин) досить важливим є питання «іміджування держави», при чому воно залежить не лише від зусиль державних органів, але й громадянського суспільства, ступеня розвинутості його організацій, їх співпраці зі світовою громадськістю [213, с. 5]. Активні громадяни та їх спільноти часто більше оповідають про спроможність суспільства змінюватися у демократичному напрямку, аніж інституційні заходи відповідальних державних органів.

Розвинута мережа неурядових організацій об'єднує установи, метою діяльності яких є участь у становленні інформаційного суспільства, захист прав і свобод людини у сфері інформації й комунікації, безперешкодне здійснення професійної діяльності, просвітництво та підтримка культурного розмаїття ЗМК. Важливим етапом діяльності громадських та неурядових організацій України стало створення Громадської ради з питань свободи слова та інформації як

незалежного суспільного суб'єкта прийняття рішень з питань інформаційної політики, як складової процесів формування громадянського суспільства в Україні. Громадська рада координує співпрацю недержавних організацій та експертів з органами влади України, міжнародними організаціями та їхніми представниками в Україні, взаємодіє з комітетом Верховної Ради України з питань свободи слова та інформації, Кабінетом Міністрів України, Нарадою України з питань телебачення і радіомовлення, Держтелерадіо, іншими міністерствами та відомствами, органами місцевого самоврядування. Основні цілі Громадської ради − забезпечення права на свободу слова та транскордонну комунікацію, реформування національного інформаційного законодавства. Головні напрями діяльності − громадська експертиза проектів законодавчих актів у сфері інформаційних відносин; аналіз діяльності владних інститутів, пов'язаних з реалізацією інформаційної політики, подання пропозицій з актуальних питань міжнародної співпраці у сфері ЗМІ, проведення досліджень змін інформаційного законодавства, популяризація перспективних ідей інформаційного розвитку [60, с. 341].

Це доповнюють Л. Абрамов і Т. Азарова, які вважають, що значна роль інформаційного потенціалу громадських організацій «у стратегічному плануванні, що спирається на аналітичну інформацію, яка відображає реальні умови та ресурсні можливості організації» [2, с. 7]. Ефективна система управління орієнтує організації на задоволення потреб громадян та передбачає умови для її розвитку і стабілізації. Крім того, продовжують вчені, «прогнозування можливої ефективності організації включає збір і аналіз інформації, яка дозволяє розробити ряд конкретних заходів, щодо досягнення очікуваної ефективності», а на практиці ж прогноз «дозволяє знизити ризики, вплив зовнішніх факторів на діяльність організації, мінімізувати витрати часу на розробку та реалізацію програми (проекту), спрямованих на вирішення соціальних проблем» [2, с. 7]. При цьому, вважають вчені, «облік прогнозної інформації та перспективних факторів у діяльності дозволяє одержати системне рішення проблеми, включаючи етапи збору, обробки, аналізу інформації,

підготовки та усунення проблеми при реалізації управлінського рішення» [2, с. 7]. Нарешті, зазначають вони, «формування прогнозної інформації припускає виявлення загальних тенденцій зміни кількісно-якісних характеристик організації на етапах ресурсного забезпечення, реалізації та просування соціальних послуг», адже «інформаційне забезпечення в розробці та впровадженні управлінської ідеї дозволяє досягти конкурентоспроможності, усунення залежності організації від змінних умов, середовища» [2, с. 7]. Тому задля прийняття незалежного управлінського рішення потрібні належні та чіткі інформаційні та комунікаційні вектори й орієнтири.

Як зазначають дослідники, зокрема О. Литвиненко, «основним суб'єктом недержавної системи забезпечення національної інформаційної безпеки є громадяни», оскільки «без їх активної участі у розбудові незалежної держави, без їх відданості Україні, свідомому та патріотичному служінню ідеалам української нації функціонування надійної системи забезпечення національної безпеки є неможливим» [167, с. 412]. Безпека нації починається з безпеки конкретної особи, але, продовжує вчений, «левова частка уваги має бути зосереджена на усвідомленні кожного громадянина необхідності активної і безпосередньої участі у забезпеченні безпеки» [167, с. 412]. Лише такий підхід робить з пасивних громадян активних учасників і дає можливості реалізації їхнього права на життя та здоров'я.

Отже, громадські організації мають прямий і опосередкований вплив на політичні відносини, інститути і процеси, зокрема й систему прийняття політичних рішень. Опосередкований вплив найчастіше виражається через належність індивіда до громадської організації, непрямі наслідки громадських ініціатив та активностей. Безпосередній вплив потребує конкретних визначень науковців, які вважають, що це влада реалізована через: а) вплив на прийняття рішень органами влади; б) організацію передвиборчих кампаній; в) відстоювання інтересів громадян; г) організацію громадських слухань і публічних консультацій; д) участь у експертних комісіях; е) організацію виконання управлінських рішень; ж) здійснення контролю за діяльністю влади [199, с. 558].

Вітчизняні дослідники особливу увагу приділяють діяльності недержавних аналітичних структур, яка у західних країнах (нерідко в рамках діяльності органів державного управління) передбачає: реальний вплив на політику національних урядів; розробку і реалізацію/співучасть в реалізації національних стратегічних планів; надання консультативних послуг органам влади; дослідження і попередження кризових явищ; моніторинг дій органів влади; захист національних цінностей від руйнівних зовнішніх впливів [150, с. 15]. Доповнює цю думку й міркування Г. Алтинбекової про широку участь громадян у політичному процесі, яка забезпечує: ефективний контроль за посадовими особами, попереджує зловживання владою, відсторонення політиків від народу, бюрократизацію чиновницького апарату, контроль над органами державної влади і місцевого самоврядування, подолання тоталітарних тенденцій у політичній системі [10]. Комплекс завдань і функцій, які стоять перед сучасною активною громадськістю, можна продовжувати, але виразніше їх допоможе пояснити ситуаційний аналіз.

Інформаційний простір як багатокомпонентне та системне утворення використовується для забезпечення власних інтересів всіма учасниками суспільної діяльності. Провладні та опозиційні рухи у боротьбі за національний інформаційний простір постійно перебувають у конкурентній боротьбі, яка ускладнюється самою сутністю інформаційного простору в сучасну епоху. У сучасному інформаційному просторі важлива не лише сама інформація, але способи її конфігурації, тобто незмінних відомостей більше немає, адже увесь сучасний простір інформаційного обміну залежить від суб'єктно представлених її форм, а також загалом способів мислення, рефлексії, інтуїції, досвіду тощо. У цих умовах учасником комунікації (наприклад, політичної) в інформаційному просторі з реальними можливостями надавати найбільш істотний (а іноді і визначальний) вплив на інших суб'єктів та процеси стає той, хто виробляє знання-рішення в конкретних ситуаціях на основі пошуку та аналізу інформації. Відтак творець знання в сучасному інформаційному просторі стає конструктором знань. Конструюються знання завжди доцільно, і тому в

інформаційному просторі (не тільки в Internet, але і у всіх сучасних ЗМІ) учасники комунікації по-своєму і насамперед у залежності від своїх інтересів і цілей інтерпретують і направляють інформаційний потік, використовуючи його в якості свого постійного ресурсу (сировини), а також в якості ресурсу впливу [182, с. 77]. Це небезпечно тим, що поширюючи знання по каналах комунікації, суб'єкт, який створив (згенерував) це знання, може чинити керуючий вплив на інших суб'єктів діяльності, які в силу ряду причин не змогли вчасно згенерувати свій варіант знання для поточної ситуації. Відповідно відбувається маніпулятивний вплив на аудиторію – споживачів інформації.

Учасники інформаційного простору і відображають навколишню реальність, і виступають її творцями, часто несвідомо змінюють конфігурацію владних й опозиційних сил, громадські орієнтації та індивідуальні політичні вподобання. Дослідники розглядають цю властивість інформаційного дискурсу не лише як загрозу політиці, але і як можливістю «творити уявлення про місця, суспільства, часи, представляти різноманітні дії та погляди», зрештою формувати власний національний інформаційний простір, забезпечувати відтак інформаційну незалежність та безпеку держави [24, с. 189]. Сучасні уявлення про політичне життя залежать від простору інформаційного, тому ця гіперреальність настільки значима для збереження досвідів різних громадських ініціатив, політичних протистоянь та інших найрізноманітніших практик у політиці, що позбавить відчуття відчуженості громадян, сприятиме їх зближенню та порозумінню навіть за протилежних переконань.

Ще одним важливим аспектом є необхідність відкритості, незаангажованості (особливо політичної) вітчизняного інформаційного простору (як будь-якої соціальної системи), на чому наголошує В. Ільганаєва [119, с. 97]. Тим не менше, за всієї національної специфіки, кожний інформаційний простір є частиною світового інформаційного поля, адже відкритість сьогодні означає, передусім, обмін інформацією.

Провідними громадськими організаціями України у сфері інформації є Асоціація мережевих телерадіомовників, Комітет «Рівність можливостей»,

Асоціація «Спільний простір», Інститут масової інформації, Український незалежний центр політичних досліджень, Фонд «Інформаційне суспільство України», Фонд «Європа XXI століття», Міжнародна «Інтер-ньюз−Україна», Незалежна асоціація мовників, громадська організація «Інформаційний майдан», Академія української преси, Центр медіа-реформ, Незалежна медіа-профспілка тощо [60, с. 344].

Асоціація мережевих телерадіомовників прагне сформувати нову інформаційну мапу держави, створити умови для адаптації суспільства до широкого використання нових продуктів і послуг інформаційного суспільства, налагодити механізм участі громадськості в реалізації рішень і прийнятті законодавчих актів, протидіяти недобросовісній конкуренції. Метою Асоціації є захист законних інтересів та прав і свобод членів Асоціації у сфері телебачення і радіомовлення та сприяння діяльності телерадіоорганізацій в Україні. Але сьогодні дуже важливим є зберігати баланс об’єктивності та неупередженості в інформаційному просторі. Як зазначає експерт К. Мяснікова: «Дуже легко під час протидії ворогу ввести тоталітарні та авторитарні режими. Суспільство менш чутливе до таких речей і не сприймає їх як утиски своїх прав і свобод. Тонка межа між захистом та утиском може бути легко перейдена. Чим далі ми будемо від неї триматися, тим краще» [191].

Комітет «Рівність можливостей» здійснює моніторинг національних та регіональних ЗМІ в Україні, зокрема досліджує питання прозорості засобів масової інформації під час політичних та виборчих процесів, розглядає факти порушень прав ЗМІ та журналістів на доступ до джерел інформації та її вільне поширення в інформаційному просторі України. Інститут масової інформації є українською недержавною організацією, основна мета якої − дослідження феномена масової інформації в сучасному суспільстві. Сфера діяльності Інституту охоплює захист свободи слова, сприяння розвиткові української журналістики, дослідження громадської думки та інших явиш, пов'язаних із формуванням масової свідомості. Інститут масової інформації здійснює низку проектів із захисту свободи слова в Україні. На його веб-сторінці регулярно

подаються новини про розвиток журналістики в Україні, зокрема відстежується хроніка протистояння ЗМІ та владних структур України. Фонд «Інформаційне суспільство України» є неурядовою неприбутковою організацією, основна мета якої − побудова самодостатньої структури для сприяння у формуванні інформаційного суспільства в Україні. Шляхи реалізації мети Фонду − робота з громадськістю, активна співпраця з усіма секторами суспільства: державними, неурядовими організаціями та юридичними особами для створення сприятливих умов у сфері інформаційної освіти, ІТ-бізнесу та суспільної комунікації [60, с. 346].

Однак ставлення до громадських організацій в Україні суперечливе, їх вважають: індикатором демократії, зразковими моделями самоорганізації, або іноземними агентами, безвідповідальними акторами політичного простору тощо. Оціночні судження часто підкріплюються загалом малою обізнаністю щодо діяльності громадянського суспільства в Україні. Міфологізація, стереотипи, що склалися довкола громадських формувань, також склали виразну частину сучасного інформаційного простору України. Відтак проблема потребує уважного вивчення та аналітичних висновків.

В Україні громадські організації пройшли складний шлях виникнення і розвитку, який можна поділити на чотири основних періоди: перший з них, період зародження, започаткувався в процесі формування громадських об’єднань, насамперед, так званих, церковних братств, які найбільш активно проявили себе ще в XVI-XVШ ст. З кінця XIX ст. розпочинається другий період розвитку громадських організацій в Україні – період їхнього становлення, що продовжувався до середини 20-х років XX ст. у Радянській Україні, та до кінця 30-х років XX ст. – у Західній Україні. Третій період розвитку громадських організацій позначився певною консервацією громадянської активності, які втрачають самостійність, перейшовши під ручне керівництво держави, яка намагається повністю підпорядкувати собі всі громадські організації. Четвертий період розвитку громадських організацій пов’язаний з процесами розпаду СРСР, здобуттям та утвердженням української державності. З середини 80-х років XX

ст. громадський рух в Україні характеризувався появою багатьох нових різноманітних громадських структур, що називалися тоді «неформальними об’єднаннями». Вони масово займалися проблемами підвищення рівня політичної культури, пробудження національної самосвідомості, підвищення інтересу до історії України, національних традицій українського народу тощо [187, с. 16].

Трансформаційні процеси, що протікають в Україні в останні роки, призвели до значної активізації громадської ініціативи і створення кількох десятків тисяч самостійних громадських об'єднань, покликаних акумулювати і виражати суспільні інтереси, представляти їх в публічному просторі та організовувати захист та реалізацію цих інтересів. Громадські організації, як провладні так і опозиційні, завжди консолідуються навколо найважливішого для них питання – прав і свобод людини та виконують певну контролюючу функцію по відношенню до державних інституцій щодо дотримання цих прав за допомогою засобів, які знаходяться в їх розпорядженні, а саме громадської думки та вільних засобів масової інформації. Завдяки притаманним їм функціям структурування, комунікації, стабілізування суспільно-політичного життя, вони виступають своєрідними індикаторами суспільних потреб, компонентами груп тиску, інституціоналізованими каналами залучення людей до політичних процесів [69]. Правозахисний аспект у функціонуванні громадянського суспільства складає і важливі безпекові орієнтири, зокрема у частині забезпечення прав громадян на свободу слова, доступ до інформації тощо

Створені громадські об'єднання розрізняються як за своїми масштабами, так і за спрямованістю. У своїй діяльності вони активно взаємодіють з різними політичними інститутами, що дозволяє їм підвищувати статусність і збільшувати число своїх прихильників. Слід визнати, що більшість з них прагне до активної взаємодії з органами влади всіх рівнів з метою прийняття необхідних управлінських рішень, витрачання частини бюджетних коштів на реалізацію інтересів, які вони захищають. Таким чином, громадські об'єднання, виступаючи самостійним учасником політичних відносин, здатним формулювати цілі для

органів влади, роблять значний вплив на характер і спрямованість політичного процесу на різних рівнях [88, с. 6]. В Україні у світлі реформи децентралізації, особливої актуальності набувають такі громадські формування, що здатні відстоювати регіональні інтереси, підтримувати місцеві громади, розвивати вільну культуру локальної демократії. Відтак гостро постає і проблема забезпеченості інформаційного простору громад відповідною якістю політичних змістів, форм, артикуляції інтересів.

Таким чином, призначення організацій третього сектору полягає в тому, що вони стримують сучасні демократичні держави від надмірної централізації і відіграють вирішальну роль у створенні державою умов для оптимального функціонування життєдіяльності суспільства. Саме тому громадські організації щодо держави виконують як опозиційну, так і творчу функції. Опозиційна функція спрямована на конструктивну критику, а часом і блокування державних програм, що негативно впливають на демократичні перетворення. Виконуючи цю функцію, НДО може об'єднувати зусилля з політичною опозицією або профспілками, використовувати ЗМІ для формування громадської думки та ін. Щодо творчої функції, то громадські організації можуть виконувати контрактні роботи для розвитку урядових соціальних програм, пропонувати державі шляхи розв'язання тих або інших проблем [3, с. 6]. Діалектика критичної та співтворчої участі громадських інститутів у діяльності держави добре відображає сучасну сутність і значущість цих суб’єктів політики. Жодна із цих функцій не має бути втрачена для ефективного розвитку демократичної системи, особливо в умовах інформаційного суспільства, де взаємодоповнюваність цих важливих візій (замість однобокої лояльності або навпаки – критицизму) допомагає державі ефективніше безпекову стратегію, а суспільству – проявляти максимальний потенціал розвитку.

Не випадково окремі опозиційні громадські об’єднання та рухи в ході розвитку власної діяльності, а також у процесі суспільно-політичних змін можуть переходити від статусу опозиції до провладних. Зокрема таким був шлях українського руху «Євромайдан», який у грудні 2013 року став громадсько-

політичним. Із часів «Народного руху України за перебудову» це − чи не перший такий же широкий Рух із переважаючим позитивним орієнтиром на основі національного консенсусу, метою якого є творення, а не руйнування [217], а згодом визначальною політичною рушійною силою розвитку держави.

Втім деякі громадські ініціативи мають суперечливий інформаційних та політичний резонанс, відтак у цьому середовищі варто вирізняти різні проекти за низкою й інших ознак. За ознакою узгодженості дій організацій з чинним законодавством дослідники вважають за доречне виокремити такі форми громадсько-політичної участі: 1) конвенційні /легальні, тобто голосування, партійне членство, участь у політичних організаціях чи компаніях, зборах громад, публічних слуханнях, волонтерство тощо; 2) не конвенційні, тобто участь у вуличних демонстраціях, мітингах та інших формах протесту з порушенням законів тощо [57, с. 239].

Окрім нелегальних форм активностей, існує ще чимало відкритих і прихованих ризиків для національної безпеки, пов’язаних з розгортанням громадських ініціатив. Серед таких можемо назвати проблему політичної заангажованості громадських об’єднань. Вчені вважають, що такі організації серед інших відрізняють: виражена політико-ідеологічна складова діяльності; підлаштування під порядок денний великих політичних гравців, кланових і фінансово-промислових груп; «підміна інтересів» (замість соціальних та національних – на інтереси окремої групи людей, псевдо-еліт, згаданих вище впливових політичних сил тощо); безальтернативне нав’язування конкретних політичних, оціночних, світоглядних візій тощо [150, с. 19]. Механізми прихованого злиття зацікавлених політичних суб’єктів та псевдогромадських об’єднань не завжди можна вчасно відстежити. Проте сучасне інформаційне суспільство все більше потребує дієвих можливостей відрізнити вдавані від реальних громадських ініціатив. Адже у системі національної безпеки будь-яка імітація незалежної діяльності, що водночас є цілком конкретним політико-владним ресурсом, лише додає їй вразливостей, зокрема розвиває корупційну складову, соціальну і політичну байдужість, а іноді й екстремістські прояви.

Близька до цього загроза вбачається також в можливостях та вже реальних прикладах використання інформаційної діяльності громадських організацій владними суб'єктами на свою користь, при чому таке використання не завжди узгоджене, відпрацьоване у спільних проектах чи попередніх домовленостях (як у прикладі з квазігромадськими активістами). Мова йде про зрілість окремих громадських об'єднань загалом, їх готовність до незалежного, демократичного функціонування, усвідомлення реальних ризиків політико-владного світу, а також їх вразливість до деструктивних, в тому числі й інформаційних впливів. У цьому зв'язку, як слушно зауважують дослідники, владні суб'єкти добре усвідомлюють потенціал організованої громадськості (об'єднана в мережеві структури, вона спроможна мобілізувати значну кількість людей на масові протестні акції, у просвітницькі та інші кампанії, активно використовувати інтернет-технології на виборах, вплинути на прийняття політико-управлінських рішень тощо) та намагаються максимально використати цей своєрідний комунікаційний майданчик для просування власних інтересів під виглядом суспільних [150, с. 23]. Відтак для збереження національної безпеки та загалом збалансування інтересів в політиці дуже важливою є саме усвідомлена, недискредитована, відповідальна та недеморалізована громадська ініціатива, яка існуючі конфлікти перетворить у конкуренцію ідей, владний тиск трансформує у інформаційний привід для гласності, а реальні можливості відрізнить від прихованих загроз у інформаційному полі.

Окрему нішу тут займають організації громадянського суспільства, що детально аналізують проблеми національної безпеки в Україні, системно моніторять виклики і загрози обороні, розвивають сучасну безпекову культуру в суспільстві загалом, а також проводять комплексні програми з інформаційної грамотності. Серед таких є аналітичні та просвітницькі об'єднання, за форматом – аналітичні центри, форуми, регіональні осередки, що проводять також регулярні або разові практичні конференції, круглі столи, займаються активною видавничою діяльністю, беруть участь у міжнародних тематичних заходах. До таких авторитетних осередків, за якими вже закріпилася певна статусність у

суспільстві, вчені відносять Центр Разумкова, Центр міжнародної безпеки та стратегічних студій (ЦМБСС), Центр миру, конверсії та зовнішньої політики України; всеукраїнські громадські організації: «Демократична дія», «Громадська Ліга Україна–НАТО», «Рада Громадської Безпеки України», «Екологічна безпека» та багато інших [151, с. 49].

Особливе значення в умовах інформаційної війни тут відіграє спроможність таких організацій співпрацювати та буквально допомагати органам державної влади у питаннях інформаційної безпеки, зокрема розвивати сучасні методики мережевого аналізу, виявляти інформаційні небезпеки у громадському секторі, налагоджувати неформальні зв'язки з міжнародними громадськими інституціями-партнерами у питаннях спільного безпечного простору життєдіяльності тощо. Варто зауважити, що в Україні потенціал та значимість таких центрів помітно зріс після 2014 р., як зросло і число відповідних громадсько-аналітичних та волонтерських ініціатив. Як приклад можемо навести діяльність Центру дослідження безпекового середовища «Прометей», заснованого у 2015 р., який системно розвиває аналітичну традицію осмислення сучасних гібридних викликів. Напрацювання аналітиків (політологів, істориків, військових експертів, ІТ-спеціалістів) цього центру відобразилися у публікації серії доступних, фахових, ілюстративних довідників про сірі зони безпекового середовища, зокрема анексований Кримський півострів та окремі території Донбасу [417; 418]. Об'єднуючи зусилля фахівців та волонтерів з усього світу, комплексні видання перекладені багатьма мовами та адресовані передусім небайдужій світовій громадськості: зарубіжним політикам, дипломатам, журналістам, інтелектуалам. Відтак незалежні аналітичні матеріали передані у численні державні структури України, які використовують їх на авторитетних міжнародних форумах, під час зарубіжних візитів, загалом у спільній боротьбі за безпечний та справедливий інформаційний простір свободи. Подібні приклади продукування аргументованої, перевіреної фактажем аналітичної думки, продуктивних обмінів цінною інформацією між відповідальними інституціями державного та громадського секторів найкраще

зміцнюють взаємну довіру в суспільстві.

Сучасні аналітичні центри можуть стати та вже стають могутньою силою популяризації об’єктивних джерел інформації, протистояння масованій дезінформації. Важливість інформаційних загроз, розширення їх географії все ще часто недооцінюють, тому адекватна реакція з боку світової спільноти видається неможливою без спільної протидії аналітиків, експертів, громадських активістів, волонтерів.

Національна держава, яка знаходиться сьогодні в кризовому стані, все менше здатна бути ефективним та єдиним суб'єктом політичного управління. Вона позбавлена тієї довіри і навіть пієтету, яким володіла протягом перших двох третин XX ст. Її, на думку М. Кастельса, має замінити держава мережевого типу – «нова держава інформаційної епохи являє собою новий тип мережевої держави, заснованої на мережі політичних інститутів та органів прийняття рішень національного, регіонального, місцевого та локального рівнів, неминуче взаємодія яких трансформує прийняття рішень в нескінченні переговори між ними» [131, с. 29]. За таких умов важливою площиною активності громад і громадських організацій у суспільно-політичному житті є вибори.

Специфіка інформаційної політики громадських організацій в період виборчих компаній зумовлена посиленням їх впливу на перебіг виборів, в тому числі в Україні на всіх його стадіях, адже через виборчі процедури вдається чи не найкраще «збалансовувати та узгоджувати інтереси політичних еліт, соціальних класів, груп усього суспільства, наблизити владу до потреб народу, громадський сектор при цьому відіграє позитивну роль у процесах стабілізації та гармонізації взаємин у суспільстві та виборчого процесу зокрема» [247, с. 874].

Громадські організації як невід'ємна складова суспільно-політичного життя країни у визначеній їм формі впливають на характер виборчого процесу, презентують і захищають інтереси соціальних груп, здійснюють контроль за прозорістю виборів, діяльністю влади та політичних партій, стимулюють до виконання виборчих програм. Рівень інформаційного впливу громадських організацій на суспільні, у тому числі на виборчі процеси, перебуває у прямо

пропорційній залежності від правової свідомості суспільства. Таким чином, задача організацій третього сектору – розширити інформаційну, організаційну базу прийняття рішень і привернути увагу до тих проблем, які могли б залишитись поза полем зору державних органів. Передвиборча кампанія може використовуватися як реальна можливість для того, щоб привернути увагу громадян, офіційних кіл, а також кандидатів у депутати до будь-якої актуальної суспільної проблеми [69].

Інформаційна політика громадських організацій та рухів у ході виборчого процесу детермінується низкою факторів. Серед таких факторів вчені передусім відмічають кількісне і якісне зростання інституцій громадянського суспільства загалом, їх значущості у процесах трансформації України. Йдеться зокрема про недержавні організації, які залучені до політичної діяльності, мають доступ до медіа, а відтак і громадської думки. Важливим фактором є і відносна сформованість необхідного правового поля, яке, за окремими винятками, загалом розкриває достатньо широкі можливості для третього сектору за сучасними демократичними стандартам. Не забувають аналітики і про достатньо багату історію громадянського суспільства в Україні за роки незалежності, численні парламентські та президентські виборчі кампанії, які поповнили досвід роботи організацій у відповідному полі. Важливим фактором послугувало і постійне прагнення українських громадських організацій до співробітництва із зарубіжними та міжнародними, успішні спільні проекти і програми обміну [208, с. 226]. Загалом в українському суспільстві все ще не сформований стабільний попит на інформаційний продукт незалежних громадських формувань, однак його роль у стабілізації виборчого процесу є беззаперечною, тож вочевидь буде поступово усвідомлюватися і у широких суспільних колах.

Ми погоджуємося з тезою про те, що формування сталого позитивного ставлення до влади у значної частини електорату і забезпечення участі населення в управлінні справами держави і суспільства є ефективнішим, якщо органи державної влади вступають у діалогічні відносини не з дифузним електоратом, а зі структурами громадянського суспільства [44, с. 10-11]. Використовуючи

інформаційні ресурси громадських організацій та їх можливості впливу на громадян суспільство може вдосконалити виборчій процес, забезпечити його прозорість та адекватність, залучити широкі верстви населення до виконання громадянських обов’язків, інформувати та роз’яснювати. Крім того, громадські організації під час виборів здійснюють моніторинг виборчого процесу, проводять широку роз’яснювальну, інформаційно-просвітницьку роботу серед виборців, вивчають діяльність виборчих комісій, здійснюють аналіз їх кадрового потенціалу, надають інформаційно-методичну допомогу членам виборчих комісій, сприяють оскарженню допущених правопорушень під час виборів в судовому порядку, інформують вітчизняну та світову громадськість про дотримання виборчого законодавства, проводять екзит-поли на регіональному та національному рівні з метою збору даних про явку виборців та оцінку тенденцій голосування. Проводять інформаційні кампанії серед виборців із закликом перевірити себе у списках виборців. Здійснюють моніторинги, зокрема моніторинги повідомлень про порушення прав громадян обирати та бути обраними, моніторинг висвітлення виборчої кампанії у ЗМІ. Також здійснюють збір інформації з метою здійснення післявиборчого моніторингу виконання передвиборчих обіцянок. Крім основних напрямів діяльності українських ГО, що здійснюють виборчі проекти, як то здійснення контролю над чесністю й прозорістю виборів, інформування громадськості, прагнення гарантувати проведення чесних і рівних виборів, створення умов для політичної конкуренції, важливе значення має напрям діяльності, що спрямований на формування й артикуляцію соціального порядку денного. До виборів ГО активно впливають на зміст передвиборних програм партій, після виборів ГО спостерігають за виконанням партіями своїх обіцянок [69].

З іншого боку, мережі громадських об'єднань, відстоюючи суспільно-значущі інтереси, все частіше використовують політичні механізми тиску на владу і фактично роблять значний вплив на процес прийняття політичних рішень. Вони знаходять властивості суб'єктів політичного процесу, поряд з державними структурами та іншими політичними акторами. Останнім часом на

місцевих та регіональних виборах мережеві структури використовуються в діяльності виборчих штабів. Через мережі запускається як позитивна інформація про кандидата (виборчому об'єднанні), так і негативна – про опонентів [88, с. 91].

Специфіка інформаційної політики громадських організацій під час виборчого процесу залежить, перш за все від типу участі зазначених організацій у виборах. Дійсно, з одного боку, такі організації можуть бути лише інструментом політики, використовуватися політичними партіями та лідерами виборчих перегонів для досягнення власних цілей у боротьбі. Відтак НДО у інформаційному полі лише обслуговують відповідні політичні інтереси: проводять цільову агітаційно-пропагандистську роботу, формують враження про масову підтримку партії/лідера тощо. Деякі організації первинно засновуються як громадські, але з перспективою перерости у власне політичні та здобути владу – тут їх суб'єктність більш окреслена, аніж у першому прикладі. Особливо цінна для розвитку і захищеності сучасного інформаційного простору є діяльність тих громадських організацій, що здійснюють незалежні дослідницькі проекти, детально аналізують політико-правові, організаційні, ідеологічні та інші аспекти виборчого процесу, й відтак напрацьовують відповідні аналітичні звіти, рекомендацій органам влади, інформаційні матеріали. Ще одну умовну групу складають неурядові організації зі забезпечення чесних та прозорих виборів, які є важливим суб'єктом процесів демократизації та політичної модернізації. Серед них традиційно називають Комітет виборців України (КВУ), Коаліція громадських організацій «Свобода вибору», Комітет «Рівність можливостей» та інші [208, с. 227-228].

Необхідною умовою участі громадських організацій у виборах в якості офіційного спостерігача було закріплення такої можливості безпосередньо у виборчому законодавстві України. Законом України «Про вибори народних депутатів України» передбачено, що громадські організації, до статутної діяльності яких відносяться питання виборчого процесу і спостереження за ним, зареєстровані в законодавчо-встановленому порядку не менше ніж за два роки до дня виборів, мають право з дозволу Центральної виборчої комісії мати офіційних

спостерігачів, які ведуть спостереження за ходом виборчого процесу, зокрема за голосуванням, підрахунком голосів і встановленням підсумків голосування на виборчій дільниці чи територіальному виборчому округзі. Мають право бути присутніми на засіданнях виборчих комісій, перебувати на виборчих дільницях під час цих процедур. Важливість даного кроку полягає в тому, що позапартійні спостерігачі не зацікавлені у результатах виборів, а лише дбають про законність їх проведення. Вони зацікавлені в забезпеченні справедливості процесу голосування та захисту прав виборців [69].

Однак все частіше інформаційна діяльність громадських організацій та рухів, особливо останнім часом стосується створення так званого «чорного» піару проти конкурентів певних політичних сил, дезінформації, пропаганди, свідомого обману виборців, «застосування маніпулятивних технологій, проведення акцій, які мають відверто протиправне і антиконституційне спрямування, розпалювання соціальної, міжнаціональної, міжконфесійної ворожнечі» [208, с. 228]. Такі дії, як вважає Ю. Опалько, «становлять безпосередню загрозу національній безпеці України, шкодять її національним інтересам» [208, с. 228]. Однак часто виявити змовницький характер діяльності НДО, відрізнити їх від реальних адвокаційних кампаній досить складно, тонкою є відповідна межа між сучасними форматами само презентації в інформаційному просторі.

«Квазігромадські формування» ще одна небезпечна тенденція сучасного інформаційного суспільства, вона деформує саму сутність демократичної конкуренції, розуміння колективної громадської дії та цивілізованої боротьби за владу. Фахівці Інституту стратегічних досліджень ведуть постійний моніторинг подібних деформацій перехідного суспільства та відмічають, що саме у процесі виборчих кампаній окремі політичні сили та лідери формують так звані низові структури громадської підтримки у вигляді неурядових організацій і навіть їх коаліцій; це своєрідні імітатори допомоги третього сектору тій чи іншій політичній силі [150, с. 23].

Крім того, сучасний світ багатьма сучасниками мислиться як «культура

реальної віртуальності», тобто, за М. Кастельсом, як «система, в якій сама реальність (тобто матеріальне / символічне існування людей) повністю схоплена і занурена у віртуальні образи, у вигаданий світ, де зовнішні відображення не просто знаходяться на екрані, але самі стають досвідом» [4, с. 134]. Це сприяє можливості використовувати інформаційні технології для маніпулювання виборчим процесом з боку громадських організацій різного спрямування. Логіка та технологія Інтернету дозволяє вести тривалі відкриті дискусії з відносно низьким рівнем небезпеки для її учасників. Тут можна актуалізувати численні інформаційні приводи, але зберігати відносну анонімність. Практично будь-який значущий політичний проект, перш ніж реалізовуватися, сьогодні тестується у віртуальному інформаційному середовищі, отримуючи там суспільну підтримку або осуд. У цих умовах новий зміст знаходить поняття «свобода», яка трактується, насамперед, як простір, «не стільки фізичне, в сенсі свободи пересування, скільки простір багатовимірного континууму, в якому завжди одночасно існує кілька систем координат і потрібно визначити в них свої параметри» [193]. Сучасник стоїть перед самостійним вибором, у яких мережах брати політичну участь, які повідомлення продукувати, які спільноти навпаки – ігнорувати. У мережевому суспільстві індивід стає вузловим елементом складної конфігурації мереж, водночас сама ця самостійність все більше видається дискусійною сутністю.

Істотні зміни відбуваються і в механізмах політичної мобілізації. В умовах мережевого суспільства з'явилося і набуло широкого поширення таке нове соціальне і політичне явище, як «мережевий протест», або «Твіттер-революція». Суть даного феномена полягає в активному і масовому використанні Інтернет-технологій (соціальних мереж і сервісів (Facebook, YouTube, Twitter), різного роду блогів, чатів тощо) для мобілізації протестної активності громадян. Мережеві медіа, або, як їх ще визначають медіа, «від багатьох до багатьох» (many-to-many media), виступають в якості майданчиків акумуляції протестної активності та інструментів координації дій протестного електорату. Прикладами таких «мережевих протестів» в сучасній політичній історії є масові заворушення

у Франції 2005 року, загальнонаціональні протести в Греції в кінці 2008 року, молодіжні бунти в Будапешті 2006 року, виступи опозиції в Ірані в 2007 році, політичні перевороти в Тунісі та Єгипті на початку 2011 року, в Україні в 2014 році [160, с. 115].

Вітчизняні дослідники спробували вирізнити найпоширеніші форми участі громадських організацій у виборчих процесах в Україні. Відтак це 1) переформатування громадських організацій або їх коаліцій у політичні партії та блоки; 2) взаємодія громадських організацій з певною політичною партією чи лідером; 3) участь у ролі офіційних спостерігачів від громадських організацій; 4) громадський контроль за прозорістю та законністю виборчого процесу; 5) правозахисна та модернізуюча діяльність у відповідній сфері; 6) просвітницька діяльність в електоральному полі; 7) аналітична робота (з програмними документами партій, практиками реалізації передвиборних обіцянок, тощо); 8) невтручання у виборчий процес [43, с. 7]. Окремо можна було б назвати також політичне коментаторство лідерів думок, тематичне блогерство, поширене в наш час. У цій класифікації на одному рівні розглядаються ангажовані, аполітичні та незалежні громадські ініціативи.

За іншою класифікацією, до відповідних активностей громадських формувань дослідники також відносять: проведення екзит-полів, паралельні опитування і підрахунок голосів, організацію під час виборів громадських приймалень, співпрацю з територіальними громадами, участь у процесах виборчої інженерії, роботу у молодіжному середовищі, комунікації з міжнародними спостерігачами, спостереження за виборами в інших країнах тощо [69]. Головний акцент тут вирізняє розуміння глобального чинника, коли національні чи локальні вибори осмислюються як частина світового процесу, а громадські об’єднання як мобільні та динамічні канали зв’язку українського виборця з кращими міжнародними практиками та повчальним досвідом політичної участі.

Як зазначає О. Корнієвський у своєму дисертаційному дослідженні, присвяченому саме визначенні ролі громадських об’єднань у системі

національної безпеки, на тлі світової фінансово-економічної кризи та її наслідків, за неефективної економічної та соціальної державної політики, об'єднання громадян своєю повсякденною діяльністю, спрямованою на надання соціальних послуг населенню та створення робочих місць, задоволення потреб громадян у різних сферах життєдіяльності, сприяють забезпеченню соціальної, гуманітарної та інших складових національної безпеки, ініціюють політичні, правові та інші зміни [150, с. 2]. В цьому полягає конструктивно творча та маніпулятивна діяльність громадських організацій та рухів. Тому необхідно також враховувати основні суперечності їх інформаційної діяльності в контексті безпеки.

Громадські об'єднання та рухи нерідко допомагають владним структурам у виконанні ними управлінських завдань, звертають увагу громадськості до проблем розвитку і пропонують способи їх розв'язання. Недержавні організації для розвинених країн позначають можливість громадян впливати на політику, економіку, культуру, науку, освіту, щонайменше засвідчити свою присутність і контроль у всіх галузях життя суспільства. Молодіжні і професійні, жіночі та ветеранські, релігійні та аналітичні – не залежно від численних спрямувань, такі організації утверджують розуміння влади громади поряд з державою. Через громадські ініціативи частина соціальних, економічних, екологічних, освітніх та деяких інших проблем можуть бути вирішенні людьми самостійно, порушує питання морального оздоровлення нації, захисту духовної екології людини. Участь громадян країн з усталеними традиціями демократії настільки значна, що американський вчений Дж. Коумен визнав за можливе назвати потенціал взаємної довіри і взаємодопомоги «соціальним капіталом» [151, с. 48]. Всякий капітал є цінним політичним ресурсом, пов'язаним з новими можливостями інформаційного суспільства.

Відтак, коли йдеться про динаміку сучасних інформаційних обмінів, актуалізується питання важливих зворотних громадсько-політичних зв'язків, мережевих структур суспільства, принципово нових співтовариств людей, об'єднаних програмами дій, загальною ціллю та завданнями. Сучасні дослідники переконують, що за допомогою інформаційно-комунікаційних технологій

можна: підвищувати ефективність роботи органів влади (відстоювати свої права та інтереси, брати участь у прийнятті рішень, отримувати інформацію про органи влади та місцевого самоврядування, отримувати адміністративні послуги) або навіть стати політичною силою (збирати мережі прибічників спільних ідей, самоорганізовуватися в рамках окремих акцій чи структур, боротися за владу, впливати на певні рішення органів публічної влади) [21, с. 164].

Зважаючи на нові можливості громадянського суспільства цілком можливо й переглянути державницькі позиції щодо нього. Наприклад, доречним міг би бути єдиний координуючий орган як методичний та організаційний центр недержавної системи забезпечення національної безпеки. Дехто з вітчизняних фахівців пропонує створити при РНБО України Центр недержавного забезпечення національної безпеки України (незалежну громадську консультативну раду з представників українського і міжнародного експертних співтовариств). Він міг би об'єднати зацікавлених фахівців громадських організацій, аналітичних центрів, правозахисного руху тощо. Інші вчені обережніші з відповідними пропозиціями, адже запровадження постійно діючих механізмів співпраці державних та громадських органів потребує ґрунтовного аналізу схожих зарубіжних практик (особливо у сфері безпеки), а також розуміння широкого кола громадських формувань, які вже працюють у цьому напрямку в Україні [151, с. 49]. Серед можливих негативних наслідків такого рішення – заснування чергової інституції, що у складній системі інформаційної безпеки нашої країни не знайде самостійної ніші для ефективної та суспільно корисної діяльності.

Основними формами співпраці громадських організацій та органів місцевого самоврядування, дослідники і практики найчастіше називають, участь у проведенні громадських слухань, діяльність громадських, консультативних рад, звернення громадян, проведення семінарів, круглих столів, конференцій, громадську експертизу і її споріднений механізм – громадський моніторинг, тощо [43, с. 14]. Усі ці напрями в Україні мають на даний час уже серйозні здобутки, але все ще потребують подальшого юридично врегулювання,

кадрового забезпечення, культури локальної демократії загалом.

Основним же предметним акцентом нашого дослідження є інформаційна підтримка відповідних напрямків, тож які б проблеми не обрала чи яких форматів би не набула та чи інша громадська ініціатива, важливо, щоб у сучасному цифровому просторі вона мала адекватну інформаційну підтримку. Серед ознак сучасного високотехнологічного суспільства вже традиційно вирізняють такі: заміна інформаційно-технологічними потоками матеріально-грошових; робота з обслуговування інформації як один з основних видів зайнятості; визначальність для всебічного розвитку інформаційної оснащеності, доступності інформації та знань; визначальність комунікаційного виміру політики; соціальні девіації як наслідок інформаційних маніпуляцій. Відтак погоджуємося з дослідниками, які вважають, що численні різновиди сучасної діяльності громадських організацій мають неоднозначний (амбівалентний) характер, адже формуються і проявляються в інформаційній сфері життя суспільства [213, с. 16]. Продуктивні, деструктивні або провокативні наслідки діяльності політиків і громадських активістів можуть при цьому реалізовуватися у паралельних площинах сучасного інформаційного суспільства, тобто фактор інформатизації для конкретної громадської акції може відіграти, наприклад, цілком позитивну роль у внутрішнього споживача, але нейтрально відобразитися у структурі загальнонаціональних інтересів і потреб, або ж мати негативний відгук у міжнародній спільноті.

В. Дзюндзюк та інші дослідники визначають також появу нової загрози національній інформаційній безпеці, пов’язану із поширенням інформаційних мереж. Подібні загрози можуть виходити із існування та діяльності так званих мережевих співтовариств, які маючи значно більші інформаційні можливості аніж громадянські об’єднання попереднього етапу розвитку поступово зрощується з діяльністю громадянських ініціатив. Самі по собі мережеві співтовариства не є негативною практикою, адже забезпечують соціальну взаємодію і навіть деяку ідентичність. Особливої уваги потребують самоорганізуючі простори комп'ютерних інформаційно-символічних світів

(віртуальні простори), які впливають на окрему людину, співтовариства, суспільства і людство в цілому. Погоджуємо з дослідниками, що це неоднозначна ситуація, оскільки сучасний етап інформаційного суспільства відкриває широкі перспективи розвитку людини та об’єднання людей до рухів та організацій. Відтак людина допускає множинність реальностей, використовує інформаційно-культурні ресурси за допомогою різних технічних і технологічних форм, але при цьому усвідомлює свою «відносну» включеність у ці реальності та визнає первинність реального буття у фізичному і соціокультурному просторі. Водночас існує загроза, що комп'ютерні інформаційно-комунікативні середовища з часом все більше підмінятимуть собою звичайну реальність, зменшуючи усвідомлення «відносності» включеності у них, все більше впливатимуть на формування особи і її ідентичність[75].

Нові інформаційно-комунікативні технології для появи та утвердження сучасної ролі віртуальних співтовариств зробили значний внесок, забезпечивши їх такими важливими механізмами як інтерактивність, низька витратність, мультимедійність, асинхронність, глобальність, анонімність. Важливо, що у багатьох державних та міжнародних, загалом політичних комунікаціях відповідні суб’єкти досі не використовують усього цього арсеналу сучасних механізмів, які би могли посприяти і пошукам взаємних інтересів, і узгодженню назрілих протистоянь, загалом порозумінню, готовності прийняти спільні орієнтири подальшого розвиту.

Соціально-мобілізаційна активність деструктивного характеру, а також акції протесту, що, як зазначає Р. Гумінський, «організовуються із застосуванням інструментарію соціальних мереж (рухи, демонстрації, флешмоби, перекриття трас тощо)» [61, с. 21], стають повсякденними у житті сучасного суспільства. Перевагами цього різновиду спільнот, продовжує вчений, «є небачена раніше оперативність, лабільність, доступність, ємність, а найголовніше – інтерактивність і мережна архітектура, що уможливлює і навіть стимулює необмежене зростання їхньої аудиторії» [61, с. 21]. Сценарій інформаційного впливу в Інтернет середовищі не відрізняється від класичних методів

інформаційного впливу і починається з атаки на масову свідомість використовуючи класичні явні та неявні методи інформаційних війн (пропаганди та контрпропаганди). Для цього використовуються форуми, блоги, на базі яких створюються співтовариства – журнали, які ведуться колективно. Уже зараз, як показує практика сьогодення і демонструє дослідник, потенціал ВС «є достатнім, аби з їх допомогою влаштувати повномасштабний соціальний катаклізм, загальнонаціональну акцію, організувати громадський або політичний рух тощо» [61, с. 21].

Проте, за висновком науковців, може бути і навпаки, коли віртуальні спільноти можуть діяти як колективний стимулятор протестного руху. Це своєрідна ілюзія опозиційної політичної активності, слактивізм, що поглинає протестну енергію, яка інакше могла б вилитися у «фізичні» протести на вулицях. При обидві ситуації можуть бути небезпечними. Отже, і держава, і особливо за сучасних умов громадянське суспільство потребує чіткого усвідомлення відповідних загроз, розвиненої системи медіа-просвітництва, а також інформаційної грамотності, що дозволили б ідентифікувати об’єктивні реалії, критично оцінювати свої можливості та актуальні виклики, зрештою адекватно сприймати простір дії та ризики віртуальної реальності.

Дослідники вважають, що віртуальні співтовариства полегшують можливість об'єднання осіб, що ставлять перед собою завдання захоплення влади, у тому числі і незаконного [75]. Також віртуальні співтовариства можуть і непомітно/несвідомо підривати деякі державні основи. При цьому методики громадської активності суттєво урізноманітнилися, серед них багато привабливих та вражаючих в очах громадськості, але одночасно й таких, що містять елементи прихованих небезпек. Флешмобінг у деяких ситуація можна віднести саме до таких технологій, у ньому немає прямих загроз для людей чи соціуму, але апробація такої технології може у подальшому призвести до організації потужніших безладів та цілком реальних загроз.

Широкі можливості інформаційних та комунікаційних процесів в глобалізованому світі привносять і такі ж широкі загрози, в тому числі й для

громадянського суспільства, і для держави. Наприклад, Дж. Арквілл, застерігає людство від негативного впливу соціальних рухів на основі нових інформаційних технологій – мережевих війн – як «війн ідей» [13, с. 87]. Подібні війни передбачають розвинуті навички роботи з інформаційними ресурсами, широкі комунікаційні мережі, використання географічно розподіленої сили, змагання інтелектів, але все менше потребують фізичного насильства. У такі війни можуть залучатися численні громадські об'єднання.

Друга загроза – це проблема захисту внутрішньої інформації, тобто власне питання загроз інформаційні безпеці особи, суспільства і держави. У питаннях організації технологій створення, розповсюдження, зберігання та використання інформації важливу роль відіграють встановлені державою правовідносини [158], а втім і громадський сектор мусить усвідомлювати власну відповідальність, постійно моніторити відповідні загрози, належним чином здійснювати громадський контроль за цією площиною віртуальної реальності. Від тісної співпраці між ними залежать безпечні умови життєдіяльності.

Третя загроза пов'язана з поняттям цифрової нерівності, що полягає у відмінностях життя громадян і навіть цілих суспільств через різні можливості доступу до інформаційних комп'ютерних технологій. Доступ до інформаційних послуг часто відрізняється між поколінням, представниками різних статей, спеціалістами різних професій, людьми з різною освітою, між організаціями в залежності від їх фінансового стану, статутних завдань тощо, між регіонами і т.д. [21]. З посиленням карантинних заходів в усьому світі ця загроза для багатьох стала реальністю, коли цифрова нерівність негативно позначається на можливостях багатьох людей отримувати якісну освіту, вступати у правові відносини, брати участь в актуальних політичних подіях тощо. При цьому все більше очевидно, що ані держава, ані громадські об'єднання, ані приватний сектор не можуть вирішити назрілі проблеми самотужки. Тут вкотре затребуваною є здатність громадянського суспільства оперативно налагоджувати комунікації, платформи для діалогів та спільних дій.

Водночас перед державною владою з розвитком соціальних мереж

постають такі завдання: структуризація віртуальних спільнот у вітчизняних соціальних мережах, усвідомлення їх впливовості та можливостей; пошук та вироблення адекватних реакцій на реальні і потенційні загрози, приховані у віртуальному громадському просторі; розвиток доступних механізмів державного регулювання такого соціального феномену, слідування демократичним традиціям у цій справі. Значення таких завдань та відповідних механізмів не варто переоцінювати, адже з багатьма віртуальними викликами державі не впоратися виключно бюрократичними чи адміністративними методиками. Серед насправді дієвих механізмів державного регулювання часто називають моніторинг віртуальних спільнот і соціальних мереж загалом [61, с. 24]. Це складна аналітична та прогностична діяльність, що потребує науково-методичного апарату, інфраструктури, якісного кадрового забезпечення (нерідко з середовища того ж громадянського суспільства). Підкреслимо, що затрачений ресурс на організацію такої діяльності цілком виправданий у контексті можливих наслідків від реалізованих ворожих намірів.

Однак перебільшувати загрози громадянського суспільства і при цьому недооцінювати його можливостей для системи інформаційної безпеки все ж не варто, особливо в умовах демократизації. Ці суперечливі тенденції пов’язанні між собою. Часто саме зі стихійних рухів, не до кінця усвідомлених громадських активностей, не формалізованих об’єднань громадян зростають дієві та ефективні соціально значущі проекти інформаційного простору. Ми погоджуємося з дослідниками, які вважають, що обсяг і якість змістовного наповнення національного інформаційного простору України свідчить про все більше відчуження між публічною інформацією, раціональним знанням і державною політико-правовою стратегією [77, с. 66]. При цьому громадський сектор може як посилювати цей дисбаланс (через окремі зацікавлені у дестабілізації групи), так і виступити у ролі зв’язкового каналу, що поєднуватиме розірвані інформаційні простори. Поки якісний рівень поінформованості населення все ще потребує особливої уваги усіх зацікавлених у захисті національних інтересів суб’єктів політики.

В Україні люди переважно цікавляться соціально-політичними новинами, однак якість цих інформаційних повідомлень не сприяє ані загальній політичній культурі, ані дієздатності суспільства, що його споживає. Громадські ініціативи зі своєчасного, достовірного, об'єктивного інформування могли би поступово долати загальну атмосферу нігілізму, корумпованості, примітивності, а нерідко й безпорадності чи дезорієнтованості. Однак у загальному масиві інформації сучасного суспільства такі якісно нові, модернізовані формати донесення суспільно важливих сенсів громадськими організаціями все ще поодинокі.

Інформаційне споживання в Україні все ще мало пов'язане з інформаційною продукцією, виробленою громадським сектором, незалежними аналітичним центрами, просвітницькими, культурними організаціями та професійними об'єднаннями громадян. Водночас спроможність суспільства впливати на владу, змінювати у позитивному значенні політичне життя країни залежить від якісної та вчасно отриманої інформації. Таким чином, інформаційні засоби комунікації створюють особливі форми прямого міжперсонального спілкування поза посередництвом соціальних і політичних утворень, а це сприяє роздрібненню суспільства і є загрозою його безпеки. Колишні форми соціально-класової та етнонаціональної солідарності розпадаються. До того ж зростає значимість не так реальних подій, фактів, вчинків у політиці, скільки їх медіа-представлення, через яке формуються й загальні оцінки окремих громадсько-політичних діячів, організацій, держав. Ці контексти поглиблюють стихійну плюралізацію позицій, інтересів і поглядів людей, хаотизують політику на локальному, національному та міжнародному рівнях. Громадська ініціатива у цьому сенсі є винятковим прикладом солідаризованої дії, що може мати і реальний, і віртуальний вимір, об'єднувати людей зі спільними цінностями й інтересами заради сучасних загальнонаціональних та навіть загальнолюдських міжнародних орієнтирів безпеки та розвитку.

5.2. Засоби масової інформації як інститути інформаційної безпеки: проблеми (не)залежності та (без)відповідальності

Засоби масової інформації є головними носіями і розповсюджувачами інформації у суспільстві. Їх роль і значення – неоціненні. Вони можуть сприяти зміцненню інформаційної безпеки, але й можуть дестабілізувати її. Зупинимось на розгляді цього питання більш детально.

Традиційно засоби масової інформації (ЗМІ) або Мас медіа (Mass Media) визначають через перерахування технічних засобів поширення інформації – преса, масові довідники, радіо, телебачення, кіно- і звукозапис, відеозапис тощо. Окрім того, у навчальній літературі можна зустріти визначення ЗМІ, які акцентують увагу на їх інституціональному характері та функціональному призначенні. Зокрема, автори популярного посібника з політології В. Пугачов та А. Соловйов визначають ЗМІ як «установи, створені для відкритої, публічної передачі за допомогою спеціального технічного інструментарію різних відомостей будь-яким особам» [231, с. 296]. У підручниках із соціології масових комунікацій ЗМІ розуміють як «організаційно-технічні комплекси, що зайняті збором, обробкою і розповсюдженням для масової аудиторії словесної, образної, музичної інформації» [129, с. 35]. Так чи інакше, у більшості джерелах ЗМІ трактуються як організації, що забезпечують масові комунікації з різними аудиторіями.

Поняття ЗМІ не можливо розглядати окремо від категорії масова інформація або масова комунікація. Не випадково саме на цьому феномені традиційно зосереджується дослідницька увага. Масову комунікацію визначають як процес повідомлення інформації за допомогою технічних засобів – засобів масової комунікації – чисельно великим, розосередженим аудиторіям з метою впливу на оцінки, думки і поведінку людей [129, с. 29] або суспільство в цілому та його окремі елементи. При цьому акцентується увага на тому, що масова комунікація відрізняється від інших видів спілкування або обміну інформацією певними специфічними рисами: опосередкованість спілкування спеціальними

технічними засобами, (наявність спеціальних приладів, апаратури) та соціальна спрямованість, соціальна орієнтованість спілкування (спілкуються не окремі люди між собою, а великі соціальні групи). Вказані ознаки є одночасно ключовими рисами ЗМІ. До переліку таких рис варто також додати наступні характеристики ЗМІ, як зазначають В. Пугачов і А. Соловйов: «публічність, тобто необмежене і надперсональне коло споживачів»; «непряма, розділена в просторі і в часі взаємодія комунікаційних партнерів»; «односпрямованість взаємодії від комунікатора до реципієнта, неможливість зміни їх ролей»; «непостійний, дисперсійний характер їхньої аудиторії, яка утворюється від випадку до випадку в результаті загальної уваги, проявленої до тієї чи іншої передачі чи статті» [231, с. 296].

З точки зору класичної схеми комунікації, запропонованої на початку минулого століття американським дослідником Г. Лассуелом (SCMR, де S (sender) – відправник, комунікатор, C (chanal) – канал, засіб передання інформації, M (message) – власне повідомлення, R (reciever) – отримувач, якому призначена інформація і який її інтерпретує), засоби масової інформації є каналом за допомогою якого відбувається передання повідомлення, спілкування між комунікатором та реципієнтом.

З позиції теорії інформаційних революцій, яка виходить із постулату про те, що реформування суспільних відносин залежить від появи нових технологій обробки інформації, ЗМІ є продуктом індустріального суспільства. Мануфактурізація виробництва, коли відбувалося об'єднання людей, що спеціалізуються на окремій операції, на створенні окремої деталі товару, поглиблення розподілу праці (передусім, визначення соціальної ролі власника готового продукту) й нарешті зростання потреби у реалізації готової продукції зумовили соціальну потребу у створенні нових інформаційних каналів між виробництвом і населенням, виробниками та споживачами продукції. Зокрема, Л. Федотова потребу появи нових інформаційних каналів між виробництвом і населенням пояснює необхідністю зняття можливих напружень в суспільстві, спілкування власників засобів виробництва зі своїми працівниками, мета якого

не в останню чергу була пов'язана з обґрунтуванням перед ними заробітної плати, тривалості трудового дня тощо, а з часом й усвідомленням важливості створення сприятливої громадської думки для збільшення попиту на свої робочі місця. Разом з тим працівники ставали споживачами готової продукції, потребуючи не меншою мірою, ніж виробники, інформаційного забезпечення тобто реклами [271].

Однак не лише економічні фактори формували соціальне замовлення на формування та зміцнення ЗМІ. Політичні зміни індустріальної епохи – поява масових політичних партій, актуалізація політичної участі громадян також зробили свою справу. У зв’язку з цим варто згадати аргументацію В. Соловйова щодо появи політичної реклами. Зокрема, він зазначає, що остання є результатом виникнення та співіснування трьох типів ринків у просторі політики: продавців (партій), носіїв рекламної продукції (ЗМІ) та покупців (політично активної частини населення) [252]. Тобто ЗМІ стали одночасно фактором та наслідком розвитку політичної активності населення.

Підкріплені досягненнями науково-технічного прогресу усі ці економічні, політичні та соціальні процеси сприяли розвитку ЗМІ.

Однак, як вже було зазначено у наших попередніх дослідженнях, у постіндустріальному, інформаційному суспільстві, коли інформація та знання стають основними його ресурсами, роль ЗМІ суттєво зростає [440, с. 29]. Питання про роль ЗМІ в інформаційному суспільстві підіймалось практично усіма теоретиками інформаційного суспільства та його сучасними дослідниками. Зокрема, один із засновників теорії інформаційного суспільства австрійсько-американський економіст Фріц Махлуп у свій праці «Виробництво та розповсюдження знань у США» [188], яка побачила світ ще у 1962 році, ЗМІ характеризує як один з п'яти секторів «індустрії знань», тобто інформаційної діяльності у суспільстві, наряду із освітою, науковими дослідженнями і розробками, інформаційними технологіями та інформаційними послугами [188; 440, с. 29].

Ми зазначаємо, що інші теоретики інформаційного суспільства М.

Маклюен, О. Тоффлер, М. Кастельс, Дж. Нейсбіт, Й. Масуда, Т. Фрідман та ін., які у своїх працях вказують на такі важливіші риси інформаційного суспільства як доступність необхідної інформації для всіх його членів, здатність суспільства виробляти всю необхідну для його життєдіяльності інформацію, а також забезпечити всіх громадян засобами доступу до цієї інформації, також підкреслюють зростаючу роль ЗМІ у цих процесах [440, с. 29].

Відповідно нами зазначено, що в цьому контексті на особливу увагу заслуговує концепція відомого канадського дослідника Маршалла Маклюена, яка знайшла втілення у працях «Розуміння Медіа: зовнішнє розширення людини» (1964), «ЗМІ і є саме повідомлення. Перелік наслідків» (1967), «Закони медіа» (1988). Досліджуючи три історичні епохи розвитку комунікації (усної комунікації або дописемної культури, писемної комунікації або друкованої культури та електричну або аудіовізуальну епоху), М. Маклюен вказує, що ЗМІ (передусім електронні) є визначною рисою сучасної аудіовізуальної епохи [440, с. 29]. Саме вони замінили друковану мову інформації на новій електронно-індустріальній основі, де першочерговим став розвиток природного візуально-слухового сприйняття світу [68, с. 12; цит.: 440, с. 29]. Зупинимося більш детально на деяких положеннях концепції М. Маклюена, що висвітлені у праці «Розуміння Медіа: зовнішнє розширення людини» [176] та наочно демонструють роль ЗМІ в інформаційному суспільстві [440, с. 29].

По-перше, М. Маклюен вказує на підвищення ролі самого каналу комунікації, який задає повідомлення. Він зазначає: «Засобом комунікації є повідомлення, оскільки саме засіб комунікації визначає і контролює форму людської асоціації та людської дії» [176, с. 11; цит.: 440, с. 29]. Силу впливу засобу комунікації на свідомість та поведінку людини М. Маклюен пояснює тим, що «йому [засобу комунікації] надається у якості «змісту» якийсь інший засіб комунікації» [176, с. 22]. В результаті засоби комунікації стають розширенням людських органів чуття й жодна людина не в змозі захистити себе від їх впливу [440, с. 29].

По-друге, він розглядає світ як одне глобальне село, єдність якого

досягається за рахунок ЗМІ [440, с. 29]. «Після трьох тисяч сторіч наростання спеціалізму та відчуження в технологічних розширеннях наших тіл, зазначає дослідник, наш світ дякуючи драматичному процесу звернення почав стискуватися. Ущільнений силою електрики наш земний шар тепер – не більш ніж село» [176, с. 5; 440, с. 30].

По-третє, нами раніше встановлено, що М. Маклюен запропонував цікавий розподіл на «гарячі» і «холодні» ЗМІ. Гарячі засоби завантажують один орган чуття повністю до міри «високої визначеності» (стану наповненості даними), холодні – через «низку визначеність» (надаючи неповну інформацію) змушують підключати інші органи чуття [440, с. 30]. Гарячі засоби, залишаючи аудиторії не багато простору для заводнення та завершення, згідно М. Маклюену, характеризуються низкою мірою участі аудиторії, а холодні – навпаки високою мірою участі аудиторії або добудовування нею відсутнього [176, с. 28; 440, с. 30]. Чисельними прикладами дослідник демонструє як гарячі засоби комунікації виштовхують холодні, залишаючи людині все менше простору для самостійних висновків та суджень. Саме тому М. Маклюен стверджує, що «епоха тривоги та електричних засобів є також епохою несвідомого та апатії, а також усвідомлення несвідомого» [176, с. 57; 440, с. 30]. Цю тезу дослідник пояснює зростаючою силою суспільної думки, яка транслюється засобами комунікації. Як наслідок «замість буржуазного духу індивідуальної роз'єднаності та індивідуальних точок зору… в електричну епоху ми носимо на собі як свою шкіру усе людство» [176, с. 57; 440, с. 30]. Однак, в епоху електричних засобів, згідно М. Маклюєну, все ж таки є простір для «істини та одкровення». Момент зустрічі засобів комунікації – це момент свободи та визволення з буденного трансу і зацепеніння, які були нав’язані цими засобами нашим органам чуття» [176, с. 67; 440, с. 30].

Таким чином, не дивлячись на чисельні докази демонізації ЗМІ в аудіовізуальну епоху, висновки М. Маклюена цілком оптимістичні. Приводом для оптимізму слугує висновок автора про те, що «нова еклектична технологія, виносить назовні миттєву обробку інформації через взаємне зв’язування, яка тривалий час відбувалась всередині нашої нервової системи» [176, с. 401; 440, с.

30]. ЗМІ відповідно стають насправді масовими не через розмір їхньої аудиторії, а в силу того факту, що в один час кожний стає до них долученим. «Автоматизація, зазначає М. Маклюен, чинить вплив не лише на виробництво, але й на усі фази споживання і маркетингу, адже у ланцюгу автоматизації споживач стає виробником подібно тому як читач мозаїчної телеграфної преси створює власні новини і навіть сам стає новиною» [176, с. 402; 440, с. 30]. Відповідно, дякуючи тому, що інформація стає ресурсом, який потенційно стає доступним усім, перспективи людства залежать від нього самого. Децентралізація та багатоманітність, які привносить аудіовізуальна епоха, таким чином здатна зробити людину творцем свого майбутнього. Свою епохальну працю М. Маклюен завершує тезою: «Паніка навколо автоматизації як загрози одноманітності у світовому масштабі – це проекція у майбутнє механічної стандартизації та спеціалізму, час яких уже минув» [176, с. 413; 440, с. 30].

Ми вважаємо, що розуміння ролі медіа у інформаційному суспільстві дещо трансформується у працях відомого американського футуролога Елвіна Тоффлера «Шок майбутнього» (1970), «Третя хвиля» (1980) та «Метаморфози влади» (1990). У цих працях він розмірковує про роль ЗМІ в інформаційному суспільстві через пояснення різниці між медіа «трьох хвиль» [440, с. 30]. За логікою Е. Тоффлера, в аграрних суспільствах Першої хвилі, коли переважна більшість комунікацій здійснюється всередині маленьких груп людей, що спілкуються особисто, передаючи повідомлення один одному, єдиним способом передачі повідомлення великій аудиторії було зібрати разом велику кількість людей. Тобто, натовп людей, за Тоффлером, являв собою перший засіб масової інформації. Система виробництва Другої хвилі, заснована на фабричному масовому виробництві, потребувала посиленні комунікації на великих відстанях й зумовила появу традиційних у нашому розумінні ЗМІ [440, с. 30]. Відповідно газети, журнали, кінофільми, радіо і телебачення, що здатні одночасно передати одне і те ж повідомлення мільйонам людей, стали основними знаряддями масовізації в індустріальних суспільствах. Система Третьої хвилі відображає, за Е. Тоффлером, потреби в економіці постмасового виробництва. Подібно самим

пізнім підприємствам з «гнучким виробництвом», вона виготовляє свою образну продукцію за спеціальними замовленнями і розсилає різні образи, ідеї і символи групам населення, підібраним за певною спільною ознакою [440, с. 30]. Ця нова вельми висока ступінь різноманітності повідомлень та ЗМІ необхідна, тому що нова система створення матеріальних благ вимагає набагато більш гетерогенної робочої сили та населення. Демасифікація, поява якої було передбачена в книзі Е. Тоффлера «Шок майбутнього» і детально розглянута в «Третьої хвилі», стала, таким чином, ключовою характеристикою нової системи ЗМІ [261, с. 422-423; 440, с. 30-31].

Ми у своїх працях фіксуємо, що основний напрямок змін у мас-медіа, за Е. Тоффлером, принаймні з 1970 р, коли в книзі «Шок майбутнього» була передбачена майбутня демасифікація ефіру, полягає в поділі масової аудиторії на сегменти і підгрупи, кожна з яких отримує свою конфігурацію програм і повідомлень [440, с. 31]. Поряд з цим відбувається величезна експансія образів, що передаються телебаченням у формі новин і різних розважальних програм [261, с. 401; 440, с. 31]. Саме тому Е. Тоффлер пророкував, що на зміну широкомовним телевізійним і радіомережам прийдуть нові станції мережевого мовлення, що колосально збільшать можливість вибору. Свої прогнози Е. Тоффлер супроводжував ілюстраціями прикладів подібних тенденцій у США та Європі [440, с. 31].

Також ми констатуємо, що окреслені зміни за переконанням Е. Тоффлера суттєвим чином порушать владу ЗМІ, що утвердилась у індустріальному суспільстві [440, с. 31]. «Найсильніший вплив ЗМІ надавали тоді, коли було всього лише кілька каналів, коли було мало різних широкомовних компаній, і тому у глядачів і слухачів було мало можливостей вибору. Але в майбутньому нас очікує прямо протилежна ситуація. У той час як зміст кожної окремої програми може бути добрим чи поганим, найважливіше в новому «змісті» – це величезна різноманітність» [261, с. 413; 440, с. 31], зазначає Е. Тоффлер. Окрім того, перехід від мас медіа з малим вибором до мас медіа з величезним вибором має не тільки культурне, але й політичне значення. Уряди високорозвинених

країн стоять обличчям до майбутнього, в якому їх народи зовсім не будуть задовольнятися поодинокими відомостями, повторюваними в унісон декількома станціями, які належать магнатам мас медіа; навпаки, вони з усіх боків потраплять під обстріл різноманітної, часто суперечливої інформації, що виготовлена за спеціальним замовленням. У цих нових умовах стара «політика мобілізації мас» і «інженерія консенсусу» стають важко здійсненими [440, с. 31].

Разом з тим, як зазначено в наших працях, Е. Тоффлер вказує ще на одну тенденцію – злиття засобів масової інформації. «На відміну від ЗМІ періоду Другої хвилі, коли кожне з них діяло більш-менш незалежно один від одного, нові ЗМІ найтіснішим чином пов'язані і злиті один з одним, поставляючи дані, образи і символи туди і сюди, від одного до іншого [440, с. 31]. Саме ця висока ступінь проникнення один в одного і перетворює індивідуальні ЗМІ в якусь систему. Разом з процесом глобалізації це зменшує значення кожного окремого засобу інформації, каналу, публікації або технології. У той же час це наділяє ЗМІ як ціле неймовірно великою владою, яка пронизує всю нашу планету. Тому те, що насправді «працює», – це не «Відеократія», а злиття воєдино всіх ЗМІ «media-fusion» [261, с. 424-425; цит.: 440, с. 31].

Додамо, що до феномену «злиття» («fusion») Е. Тоффлер додає феномен «поширення» («diffusion»), бо ніяка частина світу не може сьогодні бути відрізана від решти. Інформація проникає через самі щільно закриті кордони. Отже, ЗМІ доходить висновку Е. Тоффлер за теперішніх часів стають ключовою складовою революційних стратегій, підтверджуючи дану тезу чисельними прикладами мобілізації через ЗМІ [440, с. 31].

Ми також аргументуємо, що один з найбільш пізніх теоретиків інформаційного суспільства іспанський соціолог пост-марксист М. Кастельс, наслідуючи окремі ідеї Е. Тоффлера у праці «Інформаційна епоха: економіка, культура, суспільства» (1996), характеризуючи роль ЗМІ у інформаційному суспільстві апелює категоріями «культура ЗМІ» та «культура реальної віртуальності» [440, с. 31]. Спостерігаючи реальні зміни інформаційної епохи, М. Кастельс зазначає: «Система ЗМІ втілила більшість рис, про які писав Маклюен

на початку 1960-х років, – вона стала «галактикою Маклюена». Однак той факт, що аудиторія – не пасивний об'єкт, але інтерактивний суб'єкт, відкрив шлях до диференціації аудиторії і з того моменту як технологія, корпорації й інститути дозволили такі кроки, – до наступної трансформації ЗМІ в сторону сегментації, «роботи на замовлення», індивідуалізації» [131, с. 40; цит.: 440, с. 31].

Услід за Е. Тоффлером М. Кастельс, стверджує, що протягом 1980-х рр. нові технології перетворили світ ЗМІ. При цьому «самою вирішальною подією стало збільшення числа телевізійних каналів, що веде до їх зростаючої диверсифікацій [440, с. 31]. Розвиток кабельного телебачення, що підштовхувалося в 1990-х роках волоконною оптикою і цифровою технологією, поряд з розвитком прямого супутникового мовлення надзвичайно розширили спектр передач і обмежили структури влади по частині державного контролю комунікацій взагалі і телебачення зокрема» [131, с. 41; цит.: 440, с. 31-32]. Однак через контроль з боку корпорацій та інститутів диверсифікація ЗМІ не перетворила односпрямовану логіку їх мовлення і не дозволила встановити справжній зворотний зв'язок. Хоча аудиторія отримувала все більше і більше різноманітного інформаційної сировини, з якої кожна людина могла конструювати власний образ всесвіту, «галактика Маклюена» була світом односпрямованої комунікації, а не взаємодії. Лише з появою комп’ютерів, а потім Інтернету, зазначає М. Кастельс, «аудиторія змогла сказати своє слово» [131, с. 45; цит.: 440, с. 32]. Незважаючи на спроби регулювати, приватизувати і комерціалізувати Інтернет, мережі комп'ютерних комунікацій характеризуються найширшим розповсюдженням, багатосторонньою децентралізацією. На відміну від ЗМІ в «галактиці Маклюена», в них технологічно і культурно вбудовані властивості інтерактивності та індивідуалізації [131, с. 70; цит.: 440, с. 32].

Ми продовжуємо, що чимало сучасних дослідників розвивають цю тезу М. Кастельса, порівнюючи переваги Інтернету з традиційними ЗМІ [440, с. 32]. Зокрема, основними перевагами, що вирізняють Інтернет, науковці і практики у сфері журналістики визначають такі [129]: а) мультимедійність (Інтернет об’єднує візуальні, звукові, друковані та відеоаспекти традиційних ЗМІ); б)

інтерактивність (Інтернет пропонує діалог, так званий зворотний зв'язок – feedback, а не монолог, який характерний для традиційних медіа; зворотний зв'язок, діалог між великою кількістю користувачів можливий через електронну пошту, форуми, чати, веб-конференції); в) персоналізація (Інтернет забезпечує необхідною інформацією на будь-якому рівні зацікавлених у ній індивідів чи групи людей); г) відсутність посередників (Інтернет надає можливість владі прямого доступу до населення, населенню – до влади без втручання і маніпулювання з боку ЗМІ); д) позагеографічність або позапросторовість Інтернету, яка дає змогу користувачеві уникати маніпуляцій, характерних для традиційних медіа, і формує можливість спротиву індоктринованому дискурсові [129; цит.: 440, с. 32].

Усі ці переваги нових засобів комунікації сприяють розвитку демократичного мислення та участі. Не випадково саме теоретики інформаційного суспільства стали засновниками концепцій комунікативної, теле- і кібердемократії, й нарешті електронної демократії [440, с. 32]. В основі теорії кібердемократії лежить уявлення про формування кіберпростору як світу інтерактивної взаємодії громадян, громадських організацій, органів влади. Відповідно до цієї теорії, утворення кіберпростору неминуче здійснить значний уплив на сучасний політичний процес, створюючи умови для появи принципово нових форм демократії [242, с. 8; цит.: 440, с. 32]. Передбачається, що в «електронній демократії» громадяни повинні грати роль політично активних громадян [440, с. 32].

Також нами вже раніше було помічено, що у теперішній політичний практиці суть електронної демократії зводиться до використання інформаційних технологій з метою посилення демократичних процесів у державі, передусім участі громадськості у прийнятті державних рішень та здійснення впливу на творення державної політики. За великим рахунком термін «електронна демократія» характеризує саме технічні аспекти взаємодії між громадянами, структурами громадянського суспільства та інститутами влади [440, с. 32]. Вона виявляється у застосуванні ІКТ у електоральному процесі, проведенні

електронних референдумів, забезпеченні доступу до інформації та консультуванні населення. Фактично йдеться про певну форму винесення інститутів представницької демократії у кібер-простір [440, с. 32].

Окрім того, зазначає Т. Авксентьева, сучасні інформаційні технології відкривають можливості утвердження деліберативної демократії (тобто демократії обговорення) [6; цит.: 440, с. 32], адже вони: створюють нові форми комунікації у сфері публічної влади та послаблюють інформаційну залежність суспільства від традиційних медіа, які редагують інформацію відповідно до своєї мети, а отже, до розширення діапазону доступних для громадян думок [440, с. 32].

Навіть у разі скептичного сприйняття моделей деліберативної та електронної демократії, можна погодитися із твердженням Г. Вайштейна, що інформаційні технології «розширюють можливості взаємодії громадян і урядових органів, що, революціонізуючи систему зв'язків між суспільством і владою, і роблячи більш чутним голос звичайних людей, змінює саму тканину демократичного процесу» [38, с. 15; цит.: 440, с. 32-33].

Однак, як й будь-які процеси, що відбуваються у світі, впливи нових засобів комунікації на суспільний розвиток мають зворотній бік. Зокрема, той же М. Кастельс один з перших вказує на нього вводячи категорію «культура реальної віртуальності», що виникає як результат перетворення комунікаційної системи [440, с. 33]. Реальну віртуальність М. Кастельс розуміє як «систему, в якій сама реальність (тобто матеріальне / символічне існування людей) повністю занурена у віртуальні образи, у вигаданий світ, світ, в якому зовнішні відображення знаходяться не просто на екрані, через який передається досвід, але самі стають досвідом» [131, с. 114; цит.: 440, с. 33].

Цікаву авторську концепцію про роль ЗМІ, а саме телебачення, висуває автор роману «Генерація П» В. Пелєвін, коли людина перестає бути «Homo Sapiens», перетворюючись в «Homo Zapiens» – людина що переключається (як програми в телевізорі). Автор виділяє так звані «об'єкт номер один», «об'єкт номер два» та «суб’єкт номер один» й «суб’єкт номер два».

Так чи інакше, але культура віртуальності знаходить відображення у політичному процесі. Вчені доволі часто стверджують, що політика «медіатизується», а політичний простір «віртуалізується». Тому вчені вказують, що медіатизація політики має такі негативні наслідки як: зміна системи представництва громадянських інтересів відповідно до медійного формату; перетворення політики у медіа процес та створення політичної та медійної «гіперреальності», що, у свою чергу, породжує феномен медіакратії [289, с. 104; цит.: 440, с. 33].

Ми також наполягаємо, що віртуалізація політичного простору виявляється у переплетінні реальності з вигаданими подіями, що підриває основи раціональної політичної орієнтації, породжує у людини елементи скепсису та іронії [440, с. 33]. У політичній культурі інформаційного суспільства, на думку А. Дернера, складається «культура політичної розваги», яка через утворений нею утопічний світ дає користувачам ЗМІ та ІКТ спрощене розуміння, інтерпретацію та осмислення політичної реальності [71, с. 29-30; цит.: 440, с. 33]. Безумовно, спрощення є фактором, який полегшує управління політичною активністю людей: штучно конструюються реакції на політичні події, люди, не усвідомлюючи своїх справжніх інтересів залучаються у кимось сконструйовані політичні акції [440, с. 33].

Тому наші попередні розвідки виявляються, що прогнози та ідеї цитованих вище провідних теоретиків інформаційного суспільства, а також наукові розвідки їх чисельних послідовників в усіх кінцях світу дозволяють виокремити деякі спільні характеристики реальності масових комунікацій, що властиві сучасній епосі: 1) глобалізація та взаємозалежність інформаційного простору; 2) зростання доступності двостороннього та багатостороннього обміну інформацією, що зумовлює перехід від моноцентричної моделі традиційних ЗМІ до поліцентричної; 3) швидке зростання кількості та спектру нових ЗМІ, а також їх можливостей; 4) посилення персоналізації інформації, збільшення швидкості, адресності та масштабу її поширення; 5) віртуалізація соціальної реальності через ЗМІ; 6) зростання маніпулятивних та мобілізаційних можливостей ЗМІ

[440, с. 33].

Таким чином, загалом ми констатували, що ЗМІ є важливим компонентом життя людини інформаційному суспільстві, який чинить вплив на усі сфери нашого життя. Однак, як зазначено у рекомендаціях Парламентської асамблеї Ради Європи, «було б неправильно, виходячи з важливості цієї ролі, зробити висновок про те, що ЗМІ дійсно репрезентують громадську думку, або про те, що вони мають взяти на себе конкретні функції органів державної влади чи її установ освітнього або культурного характеру [440, с. 33]. Це призвело б до перетворення ЗМІ на владу або антивладу (медіократію)… Робота, яку виконують ЗМІ, це одна з форм посередництва й надання інформаційних послуг, а права, які мають ЗМІ в зв'язку зі свободою інформації, залежать від одержувачів (цих послуг), тобто громадян» [233; цит.: 440, с. 33]. Самі ці обставини зумовлюють потребу у контролі за діяльністю ЗМІ з боку суспільства та держави й запровадження більшості країнами світу державної інформаційної політики. Розглянемо особливості законодавчого врегулювання діяльності ЗМІ в Україні.

Як зазначає Ю. Нестеряк, «основою правової регламентації діяльності засобів масової комунікації та законодавчого регулювання інформаційного простору в Україні є положення ст. 34 Конституції України, які утверджують право кожного громадянина вільно шукати, одержувати, передавати, виробляти та поширювати інформацію будь-яким законним способом» [145].

Українське законодавство про ЗМІ та інформаційний простір, яке формується починаючи з 1992 року, на сьогодні включає в себе значну кількість нормативних документів. Серед них закони України «Про інформацію» (1992), «Про друковані засоби масової інформації (пресу) в Україні» (1993), «Про телебачення і радіомовлення» (1994), «Про авторське право і суміжні права» (1994), «Про інформаційні агентства» (1995), «Про рекламу» (1996), «Про державну таємницю» (1994), «Про внесення змін і доповнень до положення законодавчих актів України, що стосуються захисту честі, гідності та ділової репутації громадян і організацій» (1993), «Про зв’язок» (1995), «Про

Національну раду України з питань телебачення і радіомовлення» (1997), «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (1997), «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» (1997), «Про видавничу справу» (1997), «Про захист суспільної моралі» (2003), «Про Суспільне телебачення і радіомовлення України» (2014) та ін. Крім законів, функціонування українських ЗМІ детермінують акти Президента України, постанови ВРУ, КМУ та інші нормативні документи владних структур і відомств.

Передусім зупинимося на тому, яким чином трактуються ЗМІ в українському законодавстві та які форми контролю з боку держави за ними передбачені.

Закон України «Про інформацію» від 02.10.1992 трактує ЗМІ як «засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації» [101], а масову інформацію як «інформацію, що поширюється з метою її доведення до необмеженого кола осіб» [101]. Цей закон закріпив право громадян України на отримання інформації, права власності на інформацію, встановив основні принципи інформаційних відносин і визначив державну інформаційну політику. Ним гарантовано доступність, цілісність та конфіденційність інформації, заборону цензури і втручання в діяльність журналістів і засобів масової інформації.

Закони України про окремі ЗМІ гарантують свободу їх діяльності й неприпустимість зловживання цією свободою, деталізують правові, економічні, соціальні, організаційні умови їх функціонування, порядок реєстрації та ліцензування (у разі аудіовізуальних ЗМІ), регламентують права та обов'язки журналіста, редакції, видавця, розповсюджувача (у разі друкованих ЗМІ та інформаційних агентств), телерадіоорганізацій, їх працівників, телеглядачів та радіослухачів (у разі електронних ЗМІ), а також передбачують відповідальність за порушення свободи діяльності ЗМІ та законодавства про ЗМІ. Окрім того, усі

ці закони повторюють положення Закону про інформацію щодо заборони цензури.

Зокрема, друкованими ЗМІ або пресою в Україні, згідно з відповідним Законом України № 2782-XII від 16.11.1992 є «періодичні і такі, що продовжуються, видання, які виходять під постійною назвою, з періодичністю один і більше номерів (випусків) протягом року на підставі свідоцтва про державну реєстрацію» [111].

Аудіовізуальним (електронним) ЗМІ в Україні, згідно з Законом України про телебачення і радіомовлення № 3759-XII від 21.12.1993, є «організація, яка надає для масового приймання споживачами аудіовізуальну інформацію, передану у вигляді електричних сигналів і прийняту за допомогою побутових електронних пристроїв» [92].

Інформаційними агентствами, згідно з відповідним законом № 74/95-В від 28.02.1995, є «зареєстровані як юридичні особи суб'єкти інформаційної діяльності, що діють з метою надання інформаційних послуг» [112].

Основні принципи державної політики у сфері друкованих та аудіовізуальних ЗМІ можна звести до кількох положень [111; 92]: 1) політика протекціонізму; 2) створення умови для забезпечення культурних та інформаційних потреб громадян; 3) підтримка самоврядності суб'єктів інформаційної діяльності; 4) можливість прямого прийому програм з інших країн, які транслюються мовою меншини або регіональною чи міноритарною мовою; 5) обмеження щодо монополізації ЗМІ промислово-фінансовими, політичними та іншими групами чи окремими особами, їх захист від фінансового і політичного тиску; 6) гарантія реалізації прав на інформацію, вільного і відкритого обговорення суспільно важливих проблем; 7) забезпечення ідеологічного і політичного плюралізму; 8) реєстраційні та регулюючі функції.

Окрім того, закони про ЗМІ встановлюють певні обмеження щодо їхнього використання. Зокрема, стаття 3 Закону України Про пресу констатує, що друковані ЗМІ не можуть бути використані для: «закликів до захоплення влади, насильницької зміни конституційного ладу або територіальної цілісності

України»; «пропаганди війни, насильства та жорстокості»; «розпалювання расової, національної, релігійної ворожнечі»; «розповсюдження порнографії, а також з метою вчинення терористичних актів та інших кримінально караних діянь» [111].

Ще більший перелік обмежень передбачено у сфері телебачення і радіомовлення. Окрім обмежень, перерахованих вище, стаття 6 відповідного закону «Про телебачення і радіомовлення» [92] забороняє: поширення відомостей, що становлять державну таємницю; необґрунтований показ насильства; «пропаганду винятковості, зверхності або неповноцінності осіб за ознаками їх релігійних переконань, ідеології, належності до тієї чи іншої нації або раси, фізичного або майнового стану, соціального походження»; «трансляцію програм та передач, у яких надаються послуги з ворожіння та гадання, а також платні послуги у сфері народної та/або нетрадиційної медицини (за певними виключеннями)»; «трансляція програм або їх відеосюжетів, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей і підлітків, якщо вони мають змогу їх дивитися»; «пропаганду наркотичних засобів, психотропних речовин з будь-якою метою їх застосування»; «використання у програмах та передачах прихованих вставок, які впливають на підсвідомість людини та/або чинять шкідливий вплив на стан їх здоров'я»; «поширення інформації, яка порушує законні права та інтереси фізичних і юридичних осіб, посягає на честь і гідність особи»; «здійснення інших вчинків, за якими наступає кримінальна відповідальність» [92].

Закон «Про інформаційні агентства» також встановлює певні обмеження на кшталт тих, що згадуються в законі про пресу. Інновацією цього закону стало положення про заборону «розповсюджувати інформацію, яка підриває суспільну мораль або підбурює до правопорушень, принижує честь і гідність людини, а також інформацію, яка ущемляє законні права й інтереси громадян, давати оцінку щодо винуватості осіб у вчиненні кримінального правопорушення, вказувати на особу, яка ніби вчинила кримінальне правопорушення до рішення

суду, публікувати матеріали, які розкривають тактику і методику досудового розслідування» [112].

Пізніше усі ці та інші обмеження у розгорнутому вигляді знайшли втілення у Законі України № 1296-IV від 20.11.2003 «Про захист суспільної моралі», який «встановлює правові основи захисту суспільства від розповсюдження продукції, що негативно впливає на суспільну мораль» [99].

Варто згадати таке важливе питання як фінансування ЗМІ, адже економічний контроль за ЗМІ, є суттєвим важелем впливу на їх редакційну політику й традиційно розглядається як авторитарний засіб контролю. Стаття 19 Закону України «Про телебачення і радіомовлення» констатує, що джерелами фінансування телерадіоорганізацій є бюджетні асигнування на виконання державного замовлення, абонентна плата, кошти, отримані від виробництва і трансляції реклами, створення телерадіопрограм на замовлення, іншої передбаченої законодавством і статутними документами комерційної діяльності, кредити, інвестиції, внески засновників, спонсорів, благодійних організацій. При цьому Законом забороняється будь-яке пряме бюджетне утримання телерадіоорганізацій органами державної влади, політичними партіями, професійними спілками, релігійними організаціями. А іноземні інвестиції допускаються в порядку, встановленому законодавством України [92].

Характеризуючи питання фінансування ЗМІ, не можна залишити поза увагою також Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» № 540/97-ВР від 23.09.1997. Державна підтримка ЗМІ даним законом трактується як «сукупність правових, економічних, соціальних, організаційних та інших заходів державного сприяння зміцненню і розвитку інформаційної галузі, її інфраструктури» [110]. Визначені цим Законом норми державної підтримки застосовуються до всіх ЗМІ, які діють відповідно до Конституції України, окрім ЗМІ рекламного та еротичного характеру, а також ЗМІ, заснованих за участю юридичних або фізичних осіб, до сфери діяльності яких входять виробництво та постачання паперу, поліграфічного обладнання, технічних засобів мовлення; заснованих в Україні

міжнародними організаціями або за участю юридичних чи фізичних осіб інших держав, осіб без громадянства; у яких понад 50% загального обсягу випуску становлять матеріали зарубіжних ЗМІ.

В цьому законі зазначено, що «державна підтримка ЗМІ здійснюється шляхом протекціоністської політики зниження споживчої вартості інформаційної продукції, включаючи податкове, тарифне, митне, валютне та господарське регулювання, відшкодування збитків, подання фінансової допомоги» [110]. Основними одержувачами державної адресної підтримки виступають ЗМІ для дітей та юнацтва, для інвалідів, спеціалізованим, «наукові видання, що видаються науковими установами та навчальними закладами не нижче третього рівня акредитації, ЗМІ, які цілеспрямовано сприяють розвитку мов та культур національних меншин України, а також періодичні видання літературно-художнього напряму» [110].

Також особливої уваги заслуговує Закон України № 539/97-ВР «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» від 23.09.1997 [113]. Він гарантує, що ЗМІ мають право висвітлювати всі аспекти діяльності органів державної влади та органів місцевого самоврядування, а останні у свою чергу зобов'язані надавати ЗМІ повну інформацію про свою діяльність через відповідні інформаційні служби органів державної влади та органів місцевого самоврядування, забезпечувати журналістам вільний доступ до неї, крім випадків, передбачених Законом України «Про державну таємницю», не чинити на них будь-якого тиску і не втручатися в їх виробничий процес [113]. Окрім того, згідно з цим законом, ЗМІ можуть проводити власне дослідження і аналіз діяльності органів державної влади та органів місцевого самоврядування, їх посадових осіб, давати їй оцінку, коментувати [113].

Усі закони, що регламентують інформаційну сферу було прийнято у перше десятиріччя української державності (безумовно вони регулярно оновлюються відповідно до потреб та викликів, що виникають). Порівняно новим в інформаційному правому полі є Закон України № 1227-VII «Про Суспільне

телебачення і радіомовлення України» від 17.04.2014 [115], хоча це не перший закон про суспільне телебачення. Ще 18 липня 1997 р. Верховна Рада України ухвалила закон «Про систему Суспільного телебачення і радіомовлення України», однак до кінця 2004 р. жодних конкретних кроків зі створення суспільного або громадського телерадіомовлення органами державної влади зроблено не було. Новий закон має на меті відповідно до вимог Ради Європи ліквідувати державне мовлення, яке ми успадкували від авторитарної системи, та окреслити перші кроки до створення в Україні ефективної, прозорої системи суспільного мовлення, яка б відповідала загальноєвропейським стандартам і виконувала б роль об'єктивного, неупередженого інформатора суспільства, гаранта підконтрольності влади громадянам, прозорості прийняття найважливіших для країни рішень, вільного обміну ідеями й поглядами. На практиці трансформувати державне мовлення в суспільне виявилось дуже складним завданням й заходи із реалізації даного закону втілюються в життя дуже повільно (більш детально відповідне питання буде розглянуто пізніше).

Іншим завданням, яке потребує вирішення є питання правового регулювання діяльності «Інтернет – ЗМІ». Справа у тому, що чинне в нашій державі законодавство фактично не містить визначення поняття, яке відповідає засобам масової інформації в мережі Інтернет, а також спеціального нормативно-правового акту, який би визначав їх статус, порядок створення та засади діяльності. При цьому Національний реєстр електронних інформаційних ресурсів ще у 2008 році налічував 164 найменування електронних варіантів друкованих видань, 17 назв сайтів, які стосуються телебачення, 23 – радіо і 66 назв виключно мережевих видань [280]. Щоправда станом на січень 2015 року національний реєстр електронних інформаційних ресурсів налічує всього 108 записів [196], що підтверджує очевидно той факт, що дані реєстру не відображають реального стану.

Певним чином відповідна сфера регулюється Законом України № 1280-IV «Про телекомунікації» від 18.11.2003 [91], який є правовою основою у сфері телекомунікаційних послуг. Хоча Закон «визначає засади захисту прав

споживачів та контролю за ринком телекомунікацій з боку держави» [91], він жодним чином не згадує Інтернет-ЗМІ.

При цьому сьогодні все частіше виникають ситуації, коли в Інтернет-ресурси, які себе позиціонують як Інтернет-ЗМІ, розміщують неперевірену інформацію, яка не відповідає дійсності. Таку інформацію передруковують газети та транслюють телерадіокомпанії з посиланням на відповідне джерело в мережі Інтернет. У зв’язку з цим, авторів таких матеріалів неможливо притягати до відповідальності, а честь, гідність та ділову репутацію осіб немає можливості захистити правовими засобами [155].

Загальний порядок спростування інформації, передбачений ст. 277 Цивільного кодексу України [277]. Відповідно до п.1 цієї статті «фізична особа, особисті немайнові права якої порушено внаслідок поширення про неї та (або) членів її сім'ї недостовірної інформації, має право на відповідь, а також на спростування цієї інформації» [277]. Саме ж спростування здійснюється особою, яка поширила інформацію. Якщо її пошук у друкованих ЗМІ, радіо та телебаченні не завдає особливого клопоту, то у мережі Інтернет знайти автора повідомлення у вигляді публікації чи то коментаря стає вкрай важко. Адже більшість інтернет-користувачів залишають свої тексти у різних форумах чи сайтах анонімно. У такому випадку, коли не вдається встановити поширювача неправдивої інформації, п. 4 ст. 277 ЦКУ наділяє фізичну особу, право якої порушено, можливістю звернутися до суду із заявою про встановлення факту недостовірності цієї інформації та її спростування [277]. Проте, такий шлях розв’язання проблеми не влаштовує потенційних позивачів, оскільки більшість з них прагне домогтися через суд не лише спростування неправдивої інформації, а й стягнення грошової компенсації за нанесення моральної та матеріальної шкоди [259].

У своїх раніших працях ми вже констатували, що через надмірне зростання обсягу неправдивої інформації, яка розповсюджується Інтернет-виданнями й передруковуються або переказується традиційними ЗМІ, та надзвичайну складність знайти автора неправдивого повідомлення питання про роль ЗМІ у

поширенні правдивої, неправдивої й суперечливої інформації як чинник інформаційної безпеки суспільства заслуговує на особливу увагу [383, с. 4]. У цьому контексті інформаційну безпеку ми розуміємо як стан захищеності особистості, різноманітних соціальних груп та суспільства в цілому від впливів, здатних проти їхньої волі і бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку, обмежувати свободу вибору [246; цит.: 383, с. 4].

В наш час стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Інформація стала чинником, здатним призвести до великомасштабних аварій, військових конфліктів, дезорганізації суспільства [383, с. 4]. А ЗМІ відповідно є провідним каналом, здатним цю інформацію донести великим аудиторіям. Отже, ЗМІ, поширюючи інформацію різної спрямованості, можуть як консолідувати суспільство, так й відігравати деструктивну роль, підриваючи соціально-психологічну стійкість суспільства шляхом створення і просування у масову свідомість негативних ціннісних образів, ідеалів і цінностей [383, с. 4].

Відповідь на питання про роль ЗМІ у поширенні правдивої, неправдивої й суперечливої інформації, на нашу думку [383, с. 4], являє собою окремий випадок відповіді на більш широке питання про роль ЗМІ у суспільстві та державі.

У наших працях показано, що сучасна суспільна теорія пропонує два протилежних підходи до розуміння цієї ролі ЗМІ, які відповідають демократичній та авторитарній традиції [383, с. 4]. Прихильники першого ліберального підходу вважають, що все, цікаве і важливе для аудиторії має бути відображено в новинах. Інший підхід уособлює соціально-відповідальна журналістика, з точки зору якої ЗМІ слугує для підтримки моральних засад суспільства та виховання людей з метою вдосконалення їх як соціальних суб'єктів. Такого роду підхід характерний для суспільств, де ЗМІ монополізовано державою, а сама держава одержима опікою своїх громадян [279; цит.: 383, с. 5]. У межах першого підходу поширення правдивої, неправдивої й суперечливої

інформації – є виключно сферою відповідальності самих ЗМІ, які діють у умовах конкуренції. Відповідно розповсюджувачі неправдивої інформації можуть бути покарані законами ринку. У межах другого підходу поширення правдивої, неправдивої й суперечливої інформації – монополія держави. Держава дозує інформацію, визначаючи яка є корисною або некорисною для громадян. Неправдива інформація відповідно може бути виявлена лише через утікання інформації, що може мати наслідком суттєві суспільні зміни [383, с. 5].

Ці два загальних підходи більшою мірою розкривають шість нормативних моделей взаємодії ЗМІ та держави: модель незалежної преси, модель соціальної відповідальності, модель демократичного представництва, радянська модель, авторитарна і модель розвитку [129, с. 41-43; цит.: 383, с. 5]. Ці моделі демонструють, що між повною свободою та залежністю ЗМІ існує великий простір інших стосунків. Перші три моделі можна вважати такими, що властиві демократичній традиції, адже у кожній з них ЗМІ постає як агент суспільства, три останні – такими, що властиві авторитарній традиції (ЗМІ постає як агент держави) [383, с. 5].

Отже, як помічено нами раніше, перша модель «незалежної преси» абсолютизує ліберальний підхід, виходячи з того, що розповсюдження інформації має бути доступне для індивідів без попереднього дозволу чи ліцензії. Вона орієнтована на обізнаного споживача інформації, який не потребує захисту з боку державних чи інших структур [383, с. 5]. Втім за теперішніх умов принципи цієї моделі стає все важке реалізовувати на практиці. Навіть у США, де право особи на доступ до інформації тривалий час забезпечується Першою поправкою до Конституції країни, сьогодні діє чимало законодавчих актів, що регулюють конкретні способи поширення інформації [383, с. 5].

Друга модель соціальної відповідальності виходить з того, що ЗМІ повинні виконувати певні зобов'язання перед суспільством, висловлюючи різні точки зору і надаючи можливість відповіді на критику [383, с. 5]. Це передбачає публікацію матеріалів, відповідних високим професійним стандартам інформативності, точності, об'єктивності та збалансованості. За таких умов

втручання в діяльність ЗМІ може бути виправдане необхідністю забезпечення громадської безпеки. Очевидно саме ця модель є взірцем для більшості демократичних країн, що опікуються інформаційною безпекою своїх громадян, піклуючись про те, щоб діяльність ЗМІ прямо або побічно не сприяла прояву насильства, суспільних безладів, образі меншин. Очевидно принципи цієї моделі стали основою при розробці інформаційного законодавства України [383, с. 5].

Третя модель демократичного представництва виходить з того, що ЗМІ служать насамперед своїй аудиторії, отже окремі громадяни, соціальні групи та організації повинні мати право на використання ЗМІ в своїх власних інтересах [383, с. 5]. Така модель здебільшого відповідає згадуваним вище уявленням Е. Тоффлера та Е. Кастельса про роль ЗМІ у інформаційному суспільстві. Представляючи комунікацію як децентралізовану систему, така модель орієнтована на забезпечення інформаційної безпеки суспільства через саморегуляцію [383, с. 5].

Усі три демократичні моделі орієнтовані передусім на моральний, меншою мірою на нормативний контроль за діяльністю ЗМІ. Водночас усі вони не виключають економічного контролю за ЗМІ, коли фінансово-економічні групи або окремі особи через фінансування окремих ЗМІ та медіа-холдингів можуть суттєво впливати на їх редакційну політику, розповсюджуючи правдиву, неправдиву та суперечливу інформацію у своїх інтересах [383, с. 5]. Зокрема, в Україні з кінця 1990-х великі бізнес-групи почали виявляти активність у придбанні медіа-ресурсів. Причому в Україні інтерес до медіа з боку політико-економічних груп, на думку експертів Українського незалежного центру політичних досліджень, визначається не тільки тим, що ЗМІ є різновидом бізнесу, а й пошуком дієвих механізмів і важелів політичного впливу, прагненням забезпечити собі гарантії у відносинах із владою [383, с. 5]. Саме тому влада в Україні досить легко використовувала ЗМІ, підконтрольні бізнес-групам, у своїх політичних цілях. Як показали виборчі кампанії 2000-х р., вплив власників на ЗМІ надто сильний, що забезпечує їм можливість здійснювати практично повний контроль над змістом інформації. ЗМІ віддають перевагу

позиції влади і власників, оскільки ці джерела фінансування все ще залишаються для них основними. Споживачі ЗМІ поки що не мають значного впливу на зміст матеріалів, оскільки інформаційна сфера, передусім теле- і радіомовлення, ще не перетворилася на прибутковий вид бізнесу [60; цит.: 383, с. 5].

Ми підсумовуємо, що для інших трьох недемократичних моделей взаємодії ЗМІ та держави властиві нормативні, структурні та економічні засоби контролю за ЗМІ, які використовуються у різних комбінаціях, передбачаючи різноманітні види цензурування й дозування інформації [383, с. 5].

Четверта радянська модель виходить з того, що ЗМІ – головне знаряддя панівної ідеології, що знаходиться під керівництвом партійно-державних органів. Вона за великим рахунком абсолютизує уявлення про соціально-відповідальну журналістику та втілює в життя явно виражену систему дозування інформації, цензури і санкцій по відношенню до інакомислячих [383, с. 5]. Вона сама задає критерії для того яку інформацію вважати правдивою, яку ні, й відповідно виступає знаряддям інформаційної безпеки не суспільства, а держави. Особливості реалізації на практиці даної моделі Україна відчула у радянські часи [383, с. 6].

П‘ята авторитарна модель виходить з того, що діяльність ЗМІ не повинна призводити до підриву існуючої влади, отже як й попередня модель є знаряддям інформаційної безпеки держави. Вплив фінансово-промислових груп, які зрощені з владою, на зміст інформації, що транслюється ЗМІ, у цьому випадку доволі потужний [383, с. 6]. Саме за допомогою цієї моделі можна охарактеризувати відносини ЗМІ і держави в Україні у часи становлення вітчизняного медіа-бізнесу зразку кінця 1990-х – початку 2000-х, який, між іншим, зумовив появу специфічної форми цензури. Учасники фахової дискусії «Політична цензура в Україні: наслідки запровадження та засоби протидії», що відбулась 28 січня 2003 р., визначили наступні її особливості: цензура мала політичний характер і була спрямована передусім проти політичної опозиції; її головним організатором виступала президентська адміністрація; український варіант цензурування не був формалізований у формі законів чи постанов уряду,

були відсутні спеціальні структури для її організації й здійснення: право підмінялося самочинними «темниками», які готувалися на замовлення АПУ [60; цит. 383, с. 6].

Й нарешті, як вказано в наших дослідженнях, остання модель розвитку, яка була запропонована для пояснення ситуації в інформаційній сфері у країнах «третього світу», виходить з того, що своєю діяльністю ЗМІ повинні сприяти досягненню цілей національно-державного будівництва [383, с. 6]. Відповідно свобода ЗМІ може бути обмежена у зв'язку з пріоритетами в економіці та потребами розвитку суспільства в цілому, а держава інтересами національного розвитку може обґрунтовувати право на введення обмежень і цензури щодо діяльності ЗМІ. Сьогодні, коли в інформаційному просторі України спостерігається низка негативних явищ, у тому числі психологічний тиск з боку іноземних та вітчизняних ЗМІ, що ведуть так звану «інформаційну війну» проти України, з метою поширення неправдивих відомостей про події, що дійсно відбуваються в державі, подібна стратегія державної інформаційної політики стає властивою для України [383, с. 6].

Прибічники обмеження свободи ЗМІ пояснюють свою позицію передусім потребами формування спільної національної ідеї та цілісної національної ідентичності [383, с. 6]. Причому аргументація, яка ними висловлюються доволі переконлива: «Інформаційно-культурний простір нашої держави формується під впливом могутніх інформаційних потоків зарубіжних країн, заповнений культурними зразками не найкращої якості, чужими ідеалами й цінностями і, по суті, не є національним за своїм змістом. За цих умов засоби масової інформації не сприяють формуванню і зміцненню національної свідомості, а виступають потужним і постійно діючим фактором обездуховлення та денаціоналізації українців, деморалізації та ідейно-політичної дезорієнтації суспільства» [125; цит. 383, с. 6].

Тому ми констатуємо, що загалом цілком виправдано, що в умовах посилення негативних інформаційних впливів через ЗМІ та збільшення випадків несанкціонованого поширення, використання, порушення цілісності,

конфіденційності та доступності інформації, питання забезпечення інформаційної безпеки України набуло першочергового значення. У політичних і наукових колах дискутується питання з одного боку про роль ЗМІ у формуванні української національної свідомості, з іншого боку про міру втручання держави у діяльність ЗМІ з метою забезпечення інформаційної безпеки суспільства [383, с. 6].

Україна наразі по суті балансує між двома окресленими вище моделями взаємодії ЗМІ і держави – моделлю соціальної відповідальності та моделлю розвитку [383, с. 6]. Обидві моделі передбачають втручання держави у діяльність ЗМІ, однак перша необхідність державного втручання обґрунтовує через риторику «громадської безпеки» і є за своєю суттю демократичною, друга – через риторику «цілей національно-державного будівництва» і є недемократичною. Драматичність української ситуації полягає у тому, що безпека громадян та забезпечення громадянського миру в країни безпосередньо пов’язані з цілісним національним інформаційно-культурним простором, без якого неможлива ні політична єдність нації, ні формування самої національної ідентичності [383, с. 6].

Отже, перед Україною постає доволі складне завдання формування та реалізації виваженої державної інформаційної політики, основними напрямами якої були б законодавчий і адміністративний захист національних ресурсів і національного інформаційного простору, організаційне поліпшення управління інформаційними ресурсами держави [383, с. 6]. При цьому жодні завдання та пріоритети національно-державного будівництва не можуть бути виправданими, якщо вони допускають одну з принципових загроз національної безпеці держави – «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [114; цит.: 383, с. 6], що була визначена в Законі України «Про основи національної безпеки» від 19.06.2003.

Першочерговими завданнями державної інформаційної політики є вдосконалення законодавчої та нормативно-правової бази, що регулює відносини

в інформаційній сфері, а також запровадження дієвої системи суспільного мовлення, що має стати однією з надійних гарантій остаточного припинення практики закритого прийняття суспільно значущих рішень державною владою та нав'язування народу викривленої чи дозованої інформації [383, с. 6]. Ухвалений 17 квітня 2014 року Закону України «Про Суспільне телебачення і радіомовлення України» є лише початком процесу становлення незалежного суспільного мовлення, яке має слугувати інтересам усього суспільства, а не тих чи інших політичних груп впливу, широко представляти інтереси усіх соціальних, релігійних та культурних верств громади. Протягом останніх років фахівцями та дослідниками ЗМІ послідовно проводиться думка, що суспільне телебачення та радіомовлення покликане започаткувати створення в Україні справді незалежних ЗМІК європейського рівня, які зможуть забезпечувати громадян України правдивою та повною інформацією, слугуватимуть запорукою формування відкритого громадянського суспільства у країні [60; цит.: 383, с. 7].

Згідно зі Законом України «Про Суспільне телебачення і радіомовлення України» [115]КМУ на базі кількох телерадіоорганізацій для забезпечення поступового та послідовного становлення Суспільного телебачення і радіомовлення України утворює юридичну особу публічного права «Національна суспільна телерадіокомпанія України» [383, с. 7]. Основними її завданнями проголошується: «1) об’єктивне, повне, своєчасне і неупереджене інформування про суспільно значущі події в Україні та за кордоном; 2) сприяння консолідації українського суспільства; 3) розвиток і зміцнення статусу української мови та культури, сприяння розвитку мов і культур національних меншин; 4) сприяння якнайповнішому задоволенню інформаційних, культурних та освітніх потреб населення України, у тому числі шляхом створення та поширення економічних, історично-документальних, культурно-мистецьких, навчально-пізнавальних, розважальних, спортивних програм, програм для дітей та молоді, людей з обмеженими фізичними можливостями, національних меншин, інших соціальних груп; 5) оперативне інформування населення про надзвичайні ситуації, що становлять загрозу життю чи здоров’ю людей; 6)

надання громадянам України затребуваних інформаційних продуктів, відсутніх на комерційному ринку; 7) сприяння зміцненню міжнародного авторитету України» [115; цит.: 383, с. 7].

Поставлені завдання є дійсно тими, які завжди потребувало українське суспільство й потребує сьогодні. Наскільки вдасться їх вирішити новоутвореній структурі, покаже час. Втім, головною проблемою, яку досі намагаються вирішити законодавці, полягає в тому як державне мовлення перетворити на суспільне. Адже суспільне мовлення має будуватися на принципово інших засадах, аніж державні чи комерційні телерадіоорганізації [383, с. 7]. Розробники закону очевидно керувались принципом, що «Суспільне (громадське) мовлення має бути громадським за змістом, але державним за формою» [60; цит.: 383, с. 7], вважаючи оптимальним фінансування із держбюджету, однак не виключи інші джерела фінансування. Згідно прийнятому закону, перші чотири роки фінансування НСТУ здійснюється за рахунок коштів Державного бюджету [383, с. 7]. Після завершення цього періоду «НСТУ може фінансуватися за рахунок: продажу власної теле- і радіопродукції, плати за користування авторськими та суміжними правами; державного і місцевих бюджетів; добровільних і благодійних внесків, пожертвувань фізичних і юридичних осіб, крім анонімних; інших надходжень [115; цит.: 383, с. 7]. Саме питання фінансування новоствореної структури виявилось найбільш дискусійним й вже сьогодні підіймається питання про внесення змін у прийнятий закон, передусім які стосуються фінансування суспільного мовлення [383, с. 7].

Ми вважаємо, що справа у тому, що у більшості країн світу, що запровадили громадське або суспільне мовлення, воно фінансується суспільством, а не державою. Так, у Німеччині основне фінансування суспільного мовника за рахунок спеціального збору з глядачів за схемою – 86% абонентська плата (телеподаток) + реклама, спонсорство та продаж програм [383, с. 7]. Це означає, що кожна родина сплачує телеподаток, незалежно від наявності чи відсутності телевізору [5; цит.: 383, с. 7].

В Україні питання про подібне фінансування суспільного мовлення розглядається як можлива, хоча й довгострокова перспектива. Учасники дискусії про «суспільне мовлення» тривалий час ігнорували той факт, що проект може здійснитися лише за умови, якщо український громадянин захоче платити за таке мовлення, усвідомивши, що йдеться не про зміну вивісок, а про об'єктивну суспільну потребу [383, с. 7]. Втім вже сьогодні приходить розуміння, лише за умов фінансування суспільством, громадське мовлення буде асоціюватись у громадян з правдою, чесністю, простотою, нейтральністю. «Довіра – головна особливість відносин громадянина і громадського мовлення, зазначає один з авторів роботи конкурсу журналістських матеріалів про суспільне мовлення, що організований громадською організацію «Телекритика» і проектом MEMEDIA. Суспільство повинно зрозуміти, що саме воно керує цим мовленням, контролюючи потік «чистої» інформації, а не ковтаючи вже готову, зредактовану в кабінетах «наживку». Це розуміння приходить, поступово, так само як і формування українського громадського мовлення» [172; цит.: 383, с. 7].

Безумовно державна політика, що встановлює законодавче регулювання діяльності ЗМІ, впроваджує на тих чи інших засадах суспільне мовлення є дієвим чинником забезпечення інформаційної безпеки суспільства. Однак, не лише держава, але й самі ЗМІ здатні нести відповідальність в цій сфері [383, с. 7].

Висвітлюючи питання про відповідальність ЗМІ за інформаційну безпеку суспільства, варто зазначити, що сьогодні практично в усіх демократичних державах діють системи добровільного саморегулювання ЗМІ. Це, Як стверджує Ю. Нестеряк, «ради в справах преси, наділені повноваженнями заслуховувати і ухвалювати рішення за індивідуальними скаргами на ЗМІ», більшість з яких «розробила кодекси професійної етики журналістів, якими керуються під час ухвалення рішень» [201].

Окрім того, є низка міжнародних документів, у яких закладені певні етичні критерії для практичної діяльності журналістів. Зокрема, Декларація принципів поведінки журналістів, що була прийнята на Другому Всесвітньому Конгресі Міжнародної Федерації журналістів (Бордо, 25-28 квітня 1954 р.) зі змінами на

XVIII Всесвітньому Конгресі МФЖ (Хельсингьор, 2-6 червня 1986), містить дев’ять принципів, що задають стандарт професійної поведінки журналістів в області придбання, передачі, розповсюдження та коментування інформації та опису подій. Майже усі вони тією чи іншою мірою стосуються вимоги оперування правдивою інформацією, у деяких безпосередньо робиться акцент на відповідальності журналіста за інформаційну безпеку суспільства. Зокрема, пункт 5 проголошує: «Журналіст повинен зробити все можливе для виправлення або спростування інформації, яка може завдати серйозної шкоди»; пункт 7 «Журналіст повинен усвідомлювати ту небезпеку, яку таїть у собі заклик до дискримінації, поширений через ЗМІ, і повинен зробити все можливе для того, щоб уникнути навіть мимовільного стимулювання дискримінації на основі раси, статі, сексуальної орієнтації, мови, релігії, політичних або інших переконань, національного та соціального походження» [66].

Парламентська асамблея Ради Європи (ПАРЕ) у своїх чисельних рекомендація неодноразово акцентувала увагу на питанні відповідальності ЗМІ перед суспільством. Уперше чітко така позиція ПАРЕ була виражена у Резолюції 1003 «Про етичні принципи журналістики» (1993), де йдеться, що «ЗМІ мають моральну відповідальність перед громадянами й суспільством, що слід підкреслити саме зараз, коли інформація та комунікація відіграють дуже важливу роль у формуванні особистих позицій громадян і в розвитку суспільства та демократичного життя» [233].

Окрім дотримання етичних принципів та вимоги «несприяння будь-якому насильству, ненависті, нетерпимості або дискримінації, що ґрунтуються, зокрема, на підставі раси, статі, сексуальної орієнтації, мови, релігії, політики чи інших поглядів, національного, релігійного або соціального походження» [236], ПАРЕ акцентує увагу на неприпустимості маніпуляцій через ЗМІ.

Зокрема, у вже згадуваній Резолюції «Про етичні принципи журналістики» акцентується увага на тому, що «журналістика не повинна змінювати правдиву й неупереджену інформацію або чесні думки, використовувати їх на користь ЗМІ, намагаючись створити чи сформувати громадську думку, оскільки законність

журналістики ґрунтується на ефективній повазі основоположного права громадян на інформацію як складовій поваги демократичних цінностей. Тому журналістика, пов'язана із законними розслідуваннями, обмежується достовірністю й чесністю інформації та думок і є несумісною з журналістськими кампаніями, що проводяться на підставі заздалегідь випрацюваних позицій і спеціальних інтересів» [233].

Інша Резолюція 1276 «Про силу візуальних образів» [235] (1995), яка визнає зростаючий «ризик маніпулювання образами» наголошує: «Свободу вираження поглядів – основоположне право, закріплене в статті 10 Європейської конвенції з прав людини, – слід забезпечувати разом із відповідальністю, з якою воно пов'язане. У певних випадках обмеження свободи вираження поглядів може бути виправдане з метою його узгодження з потребою захисту інших прав і свобод, зокрема прав дітей» [235]. Висловлена вище ідея про обмеження свободи вираження поглядів отримала розвиток у Рекомендації ПАРЕ № R (97) 19 «Про показ насильства електронними ЗМІ»: «Деякі форми необґрунтованого показу насильства можуть законним чином бути обмежені, враховуючи обов'язки й відповідальність, що їх несе із собою здійснення права на свободу вираження поглядів... Конкретніше – засоби, вжиті на противагу необґрунтованому показу насильства електронними ЗМІ, можна законним чином розглядати як такі, що гарантують повагу людської гідності й захищають вразливі групи, наприклад, дітей і підлітків, фізичному, розумовому й моральному розвитку яких може зашкодити показ такого насильства» [232].

Окрему увагу ПАРЕ приділяє впливу нових комунікативних та інформаційних технологій на демократію. У відповідній резолюції 1120 (1997) Асамблея вважає за доцільне «шукати способів уникнення таких ризиків, як зменшення політичного вибору, маніпуляції зі свідомістю, комерціалізація й фрагментація політичних повідомлень, надмірна кількість громадських опитувань, маргіналізація парламентських процедур, соціальна дискримінація, контроль за громадянами й тенденція до негайної, проте девальвованої форми демократії» [234], рекомендуючи вживання законодавчих заходів для

забезпечення найефективнішого використання нових комунікативних та інформаційних технологій на користь суспільства.

Окреслені вище рекомендації ПАРЕ та інших міжнародних організацій тією чи іншою мірою знайшли втілення в українському законодавстві, зокрема у згадуваних вище законах про окремі види ЗМІ, а також у національному професійному кодексі журналістів (точніше у кількох версіях таких кодексів – Кодексі професійної етики українського журналіста, що прийнято на X з'їзді Національної спілки журналістів України 14 квітня 2002 року, Етичному кодексі українського журналіста, що не був офіційно затверджений, але був відкритим для підписання серед вітчизняних журналістів, та об'єднаному Кодексі етики Українського журналіста, що був ухвалений Національною спілкою журналістів України 12 грудня 2013 року).

Перший «Кодекс професійної етики українського журналістика», що було прийнято на X з'їзді Національної спілки журналістів України 14 квітня 2002 року, містить 11 принципів. В умовах існування альтернативного професійного кодексу, ці принципи часто розглядались як такі, що носять суто декларативний характер. Серед них є положення про «відповідальність журналіста перед читачем, слухачем та глядачем» [140], де йдеться про вимогу уникання «неповноти або неточностей чи викривлень інформації, які могли б завдати моральної шкоди честі та гідності людини», «образ з приводу національних, расових, етичних та релігійних поглядів і почуттів людей…, натяків або коментарів, що стосуються фізичних недоліків чи хвороб людини,… вживання образливих висловів, ненормативної лексики» [140], а також про «моральну відповідальність перед суспільством за правильність повідомлень і справедливість суджень, поширених за власним підписом, під псевдонімом чи анонімно, але з його відома та згоди» [140].

Другий альтернативний етичний кодекс українського журналіста, добровільно прийнятий і відкритий на підпис, традиційно привертав більшу увагу громадськості, адже при його розробці були враховані західні аналоги, а за його дотриманням стежила спеціальна комісія з журналістської етики. 12 грудня

2013 року Національна спілка журналістів України на своєму пленумі офіційно ухвалила рішення про участь у Комісії з журналістської етики, затвердила об'єднаний Кодекс етики українського журналіста і звернулися до журналістів та ЗМІ з пропозицією підтримати єдиний Кодекс (відтепер на офіційному сайті Комісії з журналістської етики розміщено обидві кодекси).

Об’єднаний Кодекс етики Українського журналіста від 12.12.2013, який включає 19 принципів, не містить положень по відповідальність журналіста перед читачем, слухачем глядачем та суспільством в цілому на кшталт тих, що були включені у перший кодекс. Проте він констатує: «Служіння інтересам влади чи засновників, а не суспільства, є порушенням етики журналіста» [139]. У ньому ключова увага приділяється нормам, які орієнтовані на транслювання правдивої та об‘єктивної інформації, запобіганню фальсифікацій та викривленню змісту, включаючи випадки «вибіркового цитування соціологічних досліджень». Окрім того, він містить норми міжнародного права про запобігання дискримінації через стать, мову, расу, релігію, національне, регіональне чи соціальне походження, політичні уподобання, фізичні недоліки чи хвороби людини, а також містить положення про розгляд конфліктних ситуацій Комісією з журналістської етики.

Жодний з міжнародних та вітчизняних документів у сфері професійної етики журналістів не згадує категорію «інформаційна безпека суспільства», проте їхні норми тією чи іншою мірою орієнтовані на захист особи, різноманітних соціальних груп та суспільства в цілому від впливів, здатних проти їхньої волі змінювати психічні параметри й характеристики людини і її поведінку, обмежувати свободу вибору. Дуже важливо, щоб задекларовані у відповідних документах норми були насправді керівними принципами у діяльності журналістів та ЗМІ.

Висновки до Розділу 5

Інформаційне споживання в Україні все ще мало пов’язане з інформаційною продукцією, виробленою громадським сектором, незалежними аналітичним центрами, просвітницькими, культурними організаціями та професійними об’єднаннями громадян. Водночас потенціал громадянського суспільства, як доведено подіями помаранчевої та Революції гідності, є високий і має тенденцію до подальшого зростання. Внаслідок цього інститути громадянського суспільства володіють відчутним рівнем консолідуючого потенціалу у системі інформаційної безпеки. Громадські ініціативи виступають винятковим прикладом солідаризованої дії, що може мати і реальний, і віртуальний вимір, об’єднувати людей зі спільними цінностями й інтересами заради сучасних загальнонаціональних та навіть загальнолюдських міжнародних орієнтирів безпеки та розвитку.

Підсумовуючи результати здійсненого дослідження ролі ЗМІ у забезпеченні інформаційного безпеки суспільства, варто зазначити наступне. Основи правового регулювання ЗМІ в Україні були закладені у перші роки української державності. У відповідності з нормами міжнародного права з 1992 до 1997 років були прийняті основні нормативно-правові акти, що регулюють основні види ЗМІ, видавничу справу та рекламу, захищають авторське право та суспільну мораль та встановлюють порядок висвітлення ЗМІ діяльності органів влади та самоврядування в Україні. Порівняно недавно законодавчо унормовано систему суспільного телебачення та радіомовлення, хоча процес становлення суспільного мовлення в Україні тільки розпочався, а також потребує законодавчого регулювання діяльність Інтернет-ЗМІ, які за розміщення неперевіреної або недостовірної інформації сьогодні фактично не неможливо притягати до відповідальності.

Відповідь на питання про роль ЗМІ у поширенні правдивої, неправдивої й суперечливої інформації як фактор інформаційної безпеки суспільства являє собою окремий випадок відповіді на більш широке питання про роль ЗМІ у

суспільстві та державі, яку наочно демонструють шість нормативних моделей взаємодії ЗМІ та держави: модель незалежної преси, модель соціальної відповідальності, модель демократичного представництва, радянська модель, авторитарна і модель розвитку. Очевидно, що Україна має орієнтуватись на демократичну модель соціальної відповідальності, яка виходить з того, що ЗМІ повинні виконувати певні зобов'язання перед суспільством, висловлюючи різні точки зору і надаючи можливість відповіді на критику [383, с. 5]. Повноцінне втілення в життя такої моделі можливе у разі успішного запровадження в Україні системи суспільного мовлення, що буде фінансуватись суспільством та асоціюватись у громадян з правдою, чесністю, простотою, нейтральністю.

Не лише держава, але й самі ЗМІ здатні нести відповідальність ЗМІ за інформаційну безпеку суспільства. Відповідні положення закладені у міжнародних та національних етичних кодексах журналістів. В Україні через існування тривалий час кількох таких кодексів, уявлення про відповідальність журналіста перед суспільством не були конкретизовані. Нещодавно прийнятий об’єднаний Етичний кодекс українського журналіста вимагає від нього служити інтересам суспільства, розповсюджуючи правдиву та об‘єктивну інформації, запобігаючи фальсифікаціям та усім виявам дискримінації. Сумлінне слідування вітчизняних журналістів цим принцам та належний громадський контроль за їх дотриманням є важливою запорукою забезпечення інформаційної безпеки українського суспільства.

Загалом проблематика інформаційної безпеки індивіда, суспільства, держави і навіть світового співтовариства часто залежить від того, який шлях пройшли та якої якості набули у цьому процесі засоби масової інформації. Визначальними на цьому шляху є як глобальні тенденції, так і національна специфіка, однак універсальними критеріями для оцінки функціонування ЗМІ як інститутів інформаційної політики та інформаційної безпеки є їхня незалежність та відповідальність.

РОЗДІЛ 6

СТРАТЕГІЧНІ ОРІЄНТИРИ ПРОТИДІЇ ЗОВНІШНІМ І ВНУТРІШНІМ ІНФОРМАЦІЙНО-ДЕСТАБІЛІЗАЦІЙНИМ ВПЛИВАМ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Інформаційна безпека осмислюється нами у контексті викликів сучасної демократизації і політичної модернізації, тобто як вид безпеки національної, орієнтованої на демократичні права і свободи людини мати вільний доступ до інформації, на створення і впровадження безпечних інформаційних технологій, на вільну журналістську діяльність, на захищені права інтелектуальної власності, на орієнтування у глобальному просторі можливостей інформаційного суспільства тощо. Однак сучасні українські реалії передбачають також розгляд можливих диверсій у цю сферу. Українське суспільство за багатьма вимірами – інституційними, політико-правовими, ціннісно-культурними – виявилось непідготовленим до протидії внутрішнім і зовнішнім інформаційно-деструктивним впливам. Водночас інформаційна війна, яку розгорнув агресор проти України, зобов'язує до активної, цілеспрямованої, стратегічної протидії атакам і війнам в інформаційному полі.

Ця проблематика багатоаспектна, її неможливо розглянути в рамках однієї дисертації. Тому зупинимось на окремих її аспектах: 1) диверсифікація джерел інформації; 2) відкритість інформаційного простору та контроль за доступністю інформації; 3) протидія маніпулятивним впливам (засоби, технології, можливості); 4) підривна діяльність російських ЗМІ та завдання протидії їм.

Диверсифікація джерел інформації є дуже важливою проблемою, до якої ми неодноразово зверталися у своїх публікаціях [367]. Інформаційний вплив не новий загалом для сучасного суспільства, від давніх часів перші інформаційні атаки супроводжувалися поширенням численних міфів (потужні ворожі війська нерідко заходили на чужу територію лише після поширення на іншій стороні низки чуток про їхню надприродну силу, жорстокість, що деморалізувало

супротивників). Власне й орієнтири на боротьбу, захист батьківщини, перемогу мають відповідний інформаційний супровід у (псевдо)історичних оповідях, легендах, а пізніше й цілісних ідеологіях, системах освіти та виховання.

Принципово нові умови для формування світогляду та психологічних реакцій людей створили сучасні засоби комунікації та обробки інформації. У наш час інформаційна сфера на рівні з економічною, виробничою, побутовою, політичною, військовою та ін. є самостійною, прибутковою, але вирізняється не до кінця усвідомленими та вивченими потужностями, потенціалом, що неоднозначно оцінюється. При чому йдеться не лише про об'єднання національних інформаційних і телекомунікаційних систем, але і їх інтеграцію у глобальну інформаційну інфраструктуру. Нові інформаційні технології змінюють свідомість і підсвідомість, побут і поведінку людини, а у масштабах великих груп людей та сучасних суспільств вони провокують до нових конфліктів, але також і продукують нові можливості взаємодій.

У цьому зв’язку нам імпонують застереження О. Волянюк, яка розглядає соціально-політичний потенціал сучасних технологій AR, VR чи IoT, що, на її думку, «цілком можуть змінювати наші уявлення про минуле (переписувати історію), розставляти акценти сьогодення (формувати порядок денний політики), моделювати політичне майбутнє (конструювати стратегії розвитку)», але зрештою реальні можливості яких залежать від загальної демократичної зрілості [415, с. 91]. Тобто готовність суспільства як сприймати консолідуючий потенціал, так і боротися з соціально деструктивними ефектами сучасних інформаційних потужностей передбачає, що: 1) таке суспільство саме по собі відкрите до комунікацій та позитивних трансформацій, поважає та розвиває наукові та освітні інститути, продуктивно співпрацює з державою тощо 2) відповідна держава подбала про встановлення прозорих та зрозумілих правил гри у політиці, інформаційну інфраструктуру, зміцненням безпекових інститутів, поглиблення міжнародної співпраці тощо. Не варто недооцінювати у цих питаннях і роль міжнародної політичної кон’юнктури, яка може суттєво впливати і на суспільні настрої, і на державні спроможності.

Безумовно, йдеться також про нову соціальну та особистісну залежність – залежність від інформації – що як і всяка інша посилює вразливість та задає нові параметри системи національної безпеки. У цьому зв'язку згадана вище «відкритість» сучасних суспільств, до певної міри навіть ускладнює безпекову ситуацію. Особливо відкритість, що не підкріплена загальною захисною готовністю, освіченістю, культурою споживання інформації тощо, часто переростає у примітивність та/чи радикалізм під впливом взаємопересікання обсягів різноманітних потоків інформації. Втім така вразливість сучасної цивілізації сформувалася не стільки у напрямку до інформації як такої, скільки до інформаційної зброї, яка все більше урізноманітнюється за допомогою теперішніх технологій та набуває все нових форм і змістів. Швидкість інформаційних потоків настільки висока, що непідготовлений споживач складно відрізняє звичайні повідомлення від провокативних, деструктивних, ворожих, чим по суті сприяє подальшому множенню небезпечних інформаційних мереж.

Традиційно прийнято вважати, що інформаційно-правове поле, суспільне мовлення, державницька доктрина складають інтегральну основу для суспільства, солідаризують його. Однак в Україні все ще спостерігається фрагментарне бачення стратегії розвитку держави, суперечливе наповнення спільного інформаційного простору, незавершеність формування законодавчої бази інформаційного суспільства.

Найперше все більше дослідників, аналітиків експертів пов'язують цю ситуацію з неефективною та недобросовісною роботою ЗМІ та ЗМК, роль яких не лише посилилась, але й набула цілком вирішальних значень у політиці. Сьогодні це і самостійний суб'єкт і інструмент політичного впливу. Через суспільну важливість, масовість та доступність інформації ці гравці політичного поля виробляють продукт, у якому відчуває потребу фактично кожна сучасна людина. Згадана раніше інформаційна залежність сучасника проявляється також як влада ЗМІ формувати громадську думку. Домінуючі ідеї, комерційні пріоритети, порядок денний національної політики чи глобальні рухи – усі проблеми з відповідних сфер потрапляють у медіапростір, трансформуються в ньому або

навіть з нього й починаються. Такою владою зловживають, а у перехідних суспільствах подібні зловживання набувають системного характеру.

Сучасні журналісти мають регламентоване, навіть конституційно, право на свободу висловлювань, думки й переконань (ст.34 Конституції України), втім таке право часто розцінюють у дещо спотворених формах. Інформація у медіа з'являється фрагментарно, однобоко, неповно, ангажовано. При цьому матеріальні стимули роботи для окремих журналістів та медіа часто пріоритетніші за професійні стандарти й етичні норми. Позаяк безпекові фактори у подібній системі пріоритетів навіть не другорядні, відтак у такий спосіб підготовлена інформація у ЗМІ може мати незворотно деструктивний виплив на суспільство, державу та її громадян.

Загалом бачимо, як змінюється змістовне розуміння більшості базових політологічних категорій. Поняття «громадська думка», що й без того рядом дослідників тлумачилось як вигаданий конструкт, під впливом інформаційних атак сьогодні все більше втрачає свою діалогічну сутність та зводиться до штучних конструктів довкола заданого в медіа набору варіантів. Поняття «офіційної цензури» практично не використовується у демократичних режимах, але практики добровільного самоцензурування журналістів, структура власності на медіа-ринку, загалом більш витончені методики маніпулювання інформацією фактично відроджують цю категорію у світлі нових інформаційних викликів. Феномен та цінність «свободи слова» взагалі набув медійних деформацій, а в Україні частково дискредитований розважальним контентом мовленням. Навіть поняття «суверенітету» та його різновиду – «інформаційного суверенітету» – не набуло ціннісного змісту, особливо у перехідній системі, де основні владні ресурси, зосереджені в корпоративно-державних структурах, а інформаційний простір позбавлений характерної комунікаційної сутності, що підміняється інформаційними маніпулюваннями і пропагандистськими повідомленнями.

Науковці все частіше пишуть про нову політичну реальність на межі тисячоліть, за якої стрімка інформатизація у всіх сферах життя людей, розвиток мережі Інтернет сприяли винайденню інноваційних способів подання, зберігання і

пошуку інформації, формуванню унікального соціокультурного, політико-правового, економічного і навіть лінгвістичного середовища. У цьому ж ключі Ю. Половинчак вказує, що характерна для сучасності «оперативність, полілогічність, персоналізованість і відсутність обмежень дає соціальним медіа істотні переваги та робить їх, водночас полем застосування маніпулятивних технологій» [342].

Отже, попри здобутки та напрацювання сучасних ЗМІ у політичному житті суспільстві, варто виокремити й деструктивні наслідки медіа-охоплення людства: формування «масової» людини, розривання соціальних контактів, дезінтеграція суспільства, витіснення традицій, заміщення прямих контактів кібер-комунікаціями, байдужість, некритичність, де зорієнтованість, надмірна емоційність і навіть агресивність сучасника. Наявність одночасно багатьох джерел інформації, попри усі переваги цього інструменту у XXI ст., на практиці часто є всього лише доступом до суперечливих та взаємовиключних суджень. Відтак не аргументований аналіз залишає умовний слід у пам’яті людини, а вражаючий, оперативніший, часто спрощений інформаційний продукт.

Американський політолог та відомий дослідник комунікацій в політиці Г. Лассуел виділив чотири основні функції ЗМІ: споглядання за світом (у форматі збору та розповсюдження інформації); «редагування» (у форматі відбору інформації та її коментування); творення громадської думки; розповсюдження культури. Сукупність комунікативних засобів, спрямованих на підвищення ефекту мовного впливу, означена ним як «переконуюча комунікація». При чому така переконуюча комунікація (як і маніпулювання інформацією) в ЗМІ, каже дослідник, реалізовується передусім через виявлення та показ різних фактів і подій та ігнорування іншими цінними об'єктами уваги спостерігачів й аудиторії [355]. У нашому дослідженні інститутів інформаційної безпеки це зауваження дуже важливе, адже знову ж таки повертає нас до ціннісно-культурної складової проблематики. Механізми і норми, якими б точними вони не були, не зможуть ані заповнити політико-культурного «вакууму», ані окремо, без медіа-підтримки, трансформувати існуючий стан речей у суспільстві. Функція «поширення

культури» (за Г. Лассуелом) не може монопольно належати державі, у сучасному цифровому суспільстві її часто виконують ЗМІ, а також інші суб’єкти інформаційної політики.

Сьогодні в Україні все ще зростає кількість ЗМІ та ЗМК, які періодично публікують дезінформацію, переважно негативні новини, замовні статті, вигадані факти, спотворені, однобокі оповіді про актуальні події, суспільно-політичних акторів, важливі інституції тощо. Інформаційний простір країни деформований до такої міри, що об’єктивні матеріали, аргументована аналітика, глибокі дослідження не знаходять у ньому своєї ніші.

Така ситуація найбільше пов’язана зі встановленими на інформаційному ринку правилами взаємодій та активностей, зокрема закріпленою мережею співпраці зі суб'єктами впливу (переважно державною владою і приватним сектором). Зауважимо, що згадані раніше громадські організації як суб’єкти інформаційної політики фактично не реалізують свого потенціалу на інформаційному полі, адже у вказаній системі взаємодій лише незначна частка медіа-проектів враховуватиме впливовість цих інститутів.

Часто таке викривлене сприйняття суспільно-політичної реальності та її специфічне відображення медіа пов’язане не тільки з фінансово-матеріальними стимулами діяльності журналістів. Загальну тональність політичних відносинам і процесам, а відтак і їх висвітленню у ЗМІ задає структура власності на них, а також певний тиск на журналістську діяльність, що все ще зберігається у нашому суспільстві.

Слід зауважити, що ця ситуація не може бути охарактеризована однозначно. Тактика влади щодо захисту журналістів, забезпечення свободи слова та розвитку інформаційного простору в Україні неодноразово змінювалася, була часто залежною від виборчих циклів, зовнішньополітичних декларацій, культури владної діяльності тієї чи іншої елітарної групи. Прозорих механізмів та єдиних для усіх підходів у цій сфері бракувало завжди.

Для розуміння проблеми варто навести результати незалежних зовнішніх спостерігачів за медіа-сферою в Україні. Таким може бути, наприклад, «Індекс

свободи преси» від авторитетної організації «Репортери без кордонів». У 2020 р. Україна у ньому зайняла 96-у позицію серед 180 країн. Згідно дослідженням, загальносвітова ситуація зі свободою слова погіршується і Україна також погіршує свої показники у цьому напрямку, хоча порівняно з деякими іншими країнами ще не настільки стрімко. Деякий час (2016-2018 рр.) незалежні аналітики відмічали прогрес нашої держави на цьому шляху, однак зараз відзначають такі проблеми: недофінансування нового незалежного державного мовника; влада олігархів у ЗМІ; інформаційна війна з Росією; напади на журналістів; обмежений доступ до інформації; маніпулювання новинами; порушення конфіденційності джерел; кібератаки; надмірності у боротьбі з фейковими новинами (запропонований закон про дезінформацію); закриті для журналістів та іноземних спостерігачів зони конфлікту [422].

За час незалежності в Україні поряд зі загальними деклараціями про державні гарантії свободи слова розвивалися й можливості для її обмеження. Відомі приклади застосування насильства та жорстокості до журналістів, їх убивств. Крім того, ставали різними й адаптивними і інші методи владного, силового та корпоративно-комерційного впливу та тиску політико-правових й економічних реалій на ЗМІ.

Можливість доступу до інформації за таких умов також досить умовна, адже навіть за умови подолання усіх обмежень, немає жодних гарантій, що відповідна зацікавлена сторона отримає саме об’єктивну, правдиву, повну і достовірну інформацію. Серед обмежень доступу до джерел варто все вказати відомчу чи корпоративну належність зацікавленої особи/організації; її посадове становище; соціальний статус; фінансові можливості. Навіть у цифрову еру вільний доступ до віддалених інформаційних ресурсів в Україні все ще сприймається як виключення, аніж правило. Більшість громадян здобуває інформацію через друковані видання, радіо, телебачення, зростає значимість соціальних мереж, однак всеохопного доступу до комп'ютерних інформаційних мереж все ще не досягнуто, як і відповідного рівня критичного сприйняття інформації, медіа-грамотності і загальної культури споживання інформаційних

продуктів

Відчутний є фактор урбанізації у питаннях доступності джерел. Жителі великих міст, а особливо столиці мають доступ до значно більшого числа газет, каналів телебачення і радіомовлення, а також ширшої інфраструктури та простору інформаційно-культурного життя як джерела інформації (бібліотеки, наукові та освітні осередки, музеї, виставкові зали, театри, арт-галереї, дискусійні майданчики, конференційні зали, книжкові крамниці тощо). Для жителя периферії обсяги доступних носіїв інформації суттєво менші. У багатьох частинах країни зберігають позиції регіональні видавці-монополісти інформаційного простору. Цей нерівномірний розподіл інформаційних ресурсів, обмеження вибору джерел інформації, мізерні можливості для розвитку платформ неупередженого інформування ставить населення різних регіонів у заздалегідь нерівні умови для реалізації своїх прав та свобод. З розвитком інтернет-видань є сподівання, що цей прояв нерівності все ж буде подоланий, водночас не виключенні й нові способи локального обмеження права людей на свободу слова.

Доступність інформації часто обумовлена політичними преференціями й відтак створює окремі загрози. Протистояння різних політичних сил в Україні також прямо відображається в її інформаційному просторі. Дискредитація політичних супротивників, репутаційні зазіхання, іміджеві стратегії, партійний брендинг, негласні внутрішньопартійні заборони – усе це складає підґрунтя для продукування обмежених, спотворених, ангажованих інформаційних продуктів. Часто альтернативна їм інформація залишається поза увагою, на маргінесі масової аудиторії.

Власне ці обмеження бувають пов’язаними не лише з політичними маніпуляціями, але й зі специфікою масової свідомості як такої. Вибір тематики у ЗМІ загалом нерідко орієнтований на залучення уваги масової аудиторії, а не на критичне осмислення фактів та подій. Погоджуємося з В. Комаровським, який «відзначає, що таким чином мас-медіа формує певну картину світу» [327], а тому налаштовує соціальні групи на підтримку конкретних цілей, визначену поведінку і комунікацію в суспільстві. При чому у деяких країнах цілі мережі ЗМІ вже

історично виконують свої функції в режимі пропаганди, коли навіть сучасні інтернет-видання працюють у ідеологічному, а не інформаційну ключі [331]. Загалом можливості для скорочення доступу до правдивих відомостей однаково зумовлені і політичною кон'юнктурою, і специфікою масової свідомості, й історичними традиціями кожного конкретного суспільства.

Умовна «чистота», доступність інформаційного довкілля є важливою метою політичної модернізації та усіх суб'єктів демократизаційних процесів. Показовим у цьому зв'язку видається європейський досвід, а також загалом практики інформаційного суспільства у сучасних демократичних країнах. Зокрема у 1980-х рр. у звіті під назвою «Багато поглядів – один світ» (Many Voices, One World), за результатами роботи Комісії щодо формування засад міжнародної політики, ключовим критерієм свободи інформації трактують розмаїття її джерел у поєднанні з прозорим і вільним доступом до них; стверджувалася цінність широкого спектру інформації і думок з різних питань; підкреслено демократичну роль ЗМІ і гостру необхідність їхнього захисту від тиску як з боку уряду і економічних структур. Суспільно-політична думка відтак розвинулась ще більше: самої лише диверсифікації власності замало, потрібні диверсифікація джерел інформації та поглядів, а відтак і регулювання монополізму і концентрації власності на ЗМІ, виправдання високих стартових витрат для випуску інформаційної продукції, підтримка неприбуткових і громадських комунікаційних структур [353]. Усі вказані напрямки сьогодні вчені та медіа-фахівці пов'язують і з додержанням демократичних принципів функціонування держави, і з ухваленням ефективних політичних рішень, і зі зростанням свідомої політичної участі громадян. Поза такою структурою доступності інформації неможливо й досягти глобального миру та продуктивної міжнародної співпраці.

Сучасні аналітики з провідних західних країн також переконують, що у зв'язку зі зростанням значення інформаційних зв'язків диверсифікація джерел отримання даних й інформації, а також способів їхнього операціоналізації й обробки і представлення громадськості (як споживачам) повинна передбачати: системний моніторинг на політико-владному, воєнному, промисловому рівнях для

максимально ефективних рішень; створення національних інформаційних агентств з незалежною мережею кореспондентів, готових виявляти дезінформацію; продумані стратегії антикризового менеджменту; укладання баз достовірних і оперативних даних за участі наукових установ, аналітичних центрів, комерційних структур, приватних осіб тощо.

Власне термін «диверсифікація має латинське походження та дослівно означає різноманіття, різнобічність. Це важливий орієнтир щодо інформаційного простору, адже може розумітися і як збільшення кількості суб'єктів, що діють у відповідній сфері, і як поява нових способів поширення інформації та засобів і платформ комунікації, і як сучасна методика сегментації інформаційного простору, окреслення у ньому таргетованих адресних груп. Треба зауважити, що у цьому комплексі проблем вітчизняні політологи роблять наголос ще й на геополітичному вимірі, який особливо увиразнився зі загальними установками на політичну трансформацію та пошук нових форм порозуміння у світі [423]. Водночас складність, безпечність інформаційного простору та сучасної діяльності ЗМІ зобов'язують розуміти диверсифікацію джерел інформації також і на загальнонаціональному, і на регіональному рівнях. Розмаїття інформаційних джерел та способів їх споживання в сучасних українських реаліях бачиться як реальний вектор демасифікації сучасної політичної культури, відмови від спрощених трактувань та популістських посилів у політиці.

Це положення потребує певного пояснення, адже йдеться про відносно суперечливі тенденції. Диверсифікація джерел інформації привносить у суспільство цінність вільного поширення смислів, повідомлень, різнопланових матеріалів, з іншого ж боку, розвиває деяку самобутність у цій сфері, індивідуальні інформаційні преференції споживачів відповідної інформації.

Про два протилежних наслідки (спеціалізацію та взаємозалежність), що супроводжують процеси ускладнення інформаційної-комунікативної сфери, пишуть у наш час численні дослідники. Інтенсивні комунікативні процеси одночасно додають стабільності й динамізму інформаційному життю суспільства, відтак основна функція мас-медіа у рефлексії за соціальною системою [331, с. 9-

15]. Це складна функція ЗМІ, пов’язана також з їхньою соціальною та політичною відповідальністю. Її розуміння та усвідомлення значимості відобразилося також у основних міжнародних документах з інформаційно-безпекового спрямування, у національних положеннях про професійну етику журналістів. Соціальна відповідальність передбачає, що у роботі медіа цілком вільні у виборі жанрів і висвітленні різних тематик суспільного життя, часом вузькій їх спрямованості (спеціалізація), однак у будь-якому випадку повинні об’єктивно висвітлювати існуючі проблеми, відносини, інтереси, що характерні для суспільства, гарантувати якість, достовірність інформаційних повідомлень, послідовно і цілісно розкривати контекст інформації (взаємозалежність) тощо.

Загалом у контексті протидії дестабілізуючим інформаційним впливам описаний вище підхід передбачає: право суспільства отримувати точну інформацію про факти і події; чітке розмежування між інформаційним повідомленням та приватним/професійним коментарем; уникнення невиправданих посягань на приватне життя; виправлення будь-якої оприлюдненої інформації, яка є неточною; дотримання таємниці з приводу конфіденційності джерел будь-якої інформації; заперечення насильства, нетерпимості, ненависті чи дискримінації на расі, статі, мові, релігії, політиці чи будь-яких інших думках і походженні; громадський контроль за діяльністю ЗМІ тощо. Суспільство має право знати за допомогою медіа про усі актуальні події і проблеми політичного життя, про діяльність (не)системної опозиції. Власне й самі ЗМІ нерідко повинні займати дещо опозиційну до влади позицію, яка дозволить максимально повно представляти громадськості здобутки та недоліки існуючої системи.

Може видатися, що у такому ключі ЗМІ стануть загрозою національній безпеці, однак, як слушно застерігав Ю. Габермас на практиці диверсифікація джерел має зворотній, демократичний ефект і навпаки: якщо мас-медіа не справляються з місією організації безперервного суспільного діалогу, то сфера публічності неодмінно починає згортатися і втрачає свої важливі атрибути медіатора між державою і громадянським суспільством [356]. У цьому випадку загроз національній безпеці значно більше.

Утаємниченість, бюрократизм, системні обмеження, тотальний контроль в інформаційній сфері перехідного суспільства лише ускладнює загальнополітичну ситуацію та посилює суспільну напругу. Дзеркально доповнює несприятливу для демократичного розвитку картину також зростаюча зовнішня інформаційно-психологічна експансія, яку дізнає сучасне українське суспільство. Відтак першочергові заходи з протидії таким загрозам є в асиметричних рішеннях, зокрема й диверсифікації джерел інформації, відкритість інформаційного простору загалом.

Відкритість інформаційного простору та контроль за доступністю інформації теж є важливим чинником протидії інформаційним загрозам. Відкритість стала можливою через глобальне подолання відстаней від інформатора до споживача інформаційного продукту, через оновлення комунікаційних можливостей (комп'ютеризації, телефонізації, Інтернету), а також через демократизаційні процеси у сучасному світі. Відкритість змінює поведінку і світогляд людини, економіку підприємства та інформаційну культуру, соціальну структуру суспільства та інституції держави, публічну політику і державне управління.

Однак така відкритість потребує і певного контролю, чітко визначених правил політико-правових механізмів і норм. В Україні у політичних відносинах, зокрема й міжнародних, політичній свідомості народу і правлячої еліти, в політичних повноваженнях державних структур та партій, навіть в інститутах громадянського суспільства вони поки що значною мірою втаємничені. Хоча всі ці структури, займаючись політикою й відіграючи активну роль у державному управлінні, особливо в розробці різних цільових програм і концепцій, контролі діяльності державних органів, захисті прав і свобод людини, часто залишають громадянина за межами своєї діяльності. Як наслідок політичні, економічні й виховні засоби влади самі по собі не забезпечують потрібного результату, зокрема під час реалізації так званих непопулярних рішень у боротьбі зі злочинністю, корупцією, бюрократизмом, проявами зловживання владою, захистом свободи слова.

Отже, в основі розв’язання проблеми забезпечення сталого розвитку інформаційного суспільства лежить низка питань, які потребують визначення чіткої методології правової підтримки порядку інформаційних відносин усіх учасників суспільства. Уявляється, що такий підхід повинен передбачати й відповідь на запитання про те, як зв’язати інституції (структури) громадянського суспільства, з одного боку, і забезпечити кожного громадянина суспільства визначеними повною мірою (конституційно), правами й обов’язками в інформаційній сфері, зокрема правом громадян на отримання потрібної їм інформації. За таких умов розширення застосування в суспільстві інформаційно-комунікаційних технологій стає одним із ключових чинників у процесі трансформації суспільства у відкрите, а сама проблематика інформаційно-комунікаційних технологій має значний політичний і економічний резонанс [347].

Свобода у відкритому суспільстві передбачає наявність можливості вільного масового поширення інформації, яке є ефективним засобом захисту прав і свобод людини, формування громадської думки, реального впливу на суспільство й державну владу. Для відомого теоретика й класика свободи преси Дж. Мілля в середині XIX ст. було фактом те, що «свобода друку є однією із необхідних гарантій проти урядових репресій та утисків» [334].

Забезпечення громадян суспільства широким і вільним доступом до отримання інформації, її використання та обміну нею є найважливішою соціальною передумовою успішного розвитку сучасного інформаційного суспільства. Так, М. Моісеєв зазначає, що «вільний доступ до інформації, без якого немає сенсу вести мову про інформаційне суспільство, – найскладніша соціально-політична проблема» [335, с. 469]. Однак наявність знань та інформації задля успішної еволюції й функціонування інформаційного суспільства ще недостатньо. Необхідне, як вказує О. Антіпова, «створення умов для того, щоб члени суспільства мали вільний доступ до якісної інформації й можливість її використання у своїй практичній діяльності» [315, с. 208].

Вільний доступ усіх членів суспільства до інформації – провідна, характерна риса інформаційного суспільства. У зв'язку із цим, дослідники

справедливо вважають головною ознакою інформаційного суспільства ту обставину, що будь-який індивід або група чи організація в будь-якому місці та просторі й у будь-який час можуть одержати за винагороду чи безкоштовно й автоматизовано будь-яку інформацію й знання, потрібні для їхньої життєдіяльності й розв'язання особистих і соціально чи навіть політично значимих завдань. Така думка передбачає вироблення певної стратегії діяльності держави в цьому напрямі та докорінну зміну умов життєдіяльності людини та суспільства загалом.

Якщо у західних суспільствах за участі незалежних, професійних, позапартійних ЗМІ формується та розвивається відкритість політичної системи, прозорість органів державної влади, то у суспільствах, що лише прагнуть демократії, ці інститути часто втрачають свою суб'єктність, а нерідко саме за їх сприяння утверджується імітаційна демократія, закритий простір прийняття владних рішень, недосяжний клуб політичних еліт. Водночас ЗМІ та ЗМК перехідних суспільств можуть періодично/ситуативно продукувати і цілком об'єктивні матеріали, відкривати окремі аспекти політичної дійсності, що залежить від політичної кон'юнктури та відрізняє їх від медіа авторитарних режимів.

Становлення українських засобів масової інформації як потужного інституту сучасного суспільства відбувалося одночасно і разом зі становленням незалежності України. Дослідники переконані, що демократичному, правовому суспільстві, побудова якого декларується в Конституції України, засоби масової інформації, їх незалежність, свобода відіграють одну з провідних ролей у функціонуванні громадянського суспільства та владних інститутів. Подекуди вплив незалежних засобів інформації є потужнішим, аніж діяльність політичних партій та громадських об'єднань [320, с. 23].

Серед центральних проблем розвитку інформаційної сфери в Україні варто окремо вирізнити забезпечення права на вільне отримання та вільний обмін інформацією. Воно потребує не так політичних декларацій, як системної роботи, відповідних законодавчих механізмів, комплексних заходів зі запобігання

кланового і державного тиску на ЗМК з боку владних структур та фінансових кланів, технологічних і змістовних трансформацій національного медіа-ринку, зрештою демократичного світогляду еліт та суспільства. Така комплексна візія орієнтує сучасне українське суспільство також на розбудову системи інформаційного менеджменту, тобто принципове оновлення підходів, концептів та структур.

Завдання може видатися складним, але ґрунтовно відпрацьованим зарубіжними практиками управління в інформаційній сфері. Навіть на основі складного міжнародного співробітництва сучасні дослідники приходять до висновку, що незважаючи на різні визначення, національні візії та виміри безпеки, все ж існує деяка їхня спільна риса, що особливо важлива для налагодження ефективної системи менеджменту у відповідній сфері. На прикладі управління безпекою та управління інформаційними ресурсами вчені вважають, що йдеться про універсальну схему: «суб'єкт хоче захистити об'єкт від джерела небезпек за допомогою певних методів» [429]. Розуміння цих чотирьох складових (предмету / сфери безпеки, об'єкту захисту, джерела загроз та методів безпеки) дозволяє найкращим чином організувати управління системою інформаційної безпеки, в тому числі й захистити право людей на інформацію в Україні.

Стосовно українського законодавства в інформаційно-комунікативній галузі, ми присвятили цій проблемі окремий розділ, але у контексті забезпечення прав маємо відмітити його високу наближеність до міжнародних правових стандартів і європейських норм. Наприклад, гарантії доступу до інформації та її поширення аналогічно сформульовані у Міжнародному пакті про громадські та політичні права [341]. Уточнимо, що йдеться про комплекс документів, адже законодавство України, що регулює відносини у інформаційному просторі низку законі України (раніше загадані «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про авторське право і суміжні права», «Про інформаційні агентства», «Про рекламу», «Про державну таємницю», «Про внесення змін і доповнень до положення законодавчих актів України, що стосуються захисту честі, гідності та ділової

репутації громадян і організацій», «Про зв’язок», «Про Національну раду України з питань телебачення і радіомовлення», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про видавничу справу», «Про систему Суспільного телебачення і радіомовлення України» та ін.); відповідні акти Президента України, постанови Верховної Ради, Кабінету Міністрів та інші нормативні документи владних структур і галузевих відомств.

Відносно успішно враховано не лише міжнародні норми, але й застереження окремих науковців, в тому числі й західних. Наприклад, зауваги щодо розуміння кібербезпеки, яку часто плутають з інформаційною. І хоча, як стверджують дослідники, між проблемами є спільні виміри, ці два концепти не є повністю аналогічними. В інформаційній безпеці посилання на людський фактор, як правило, стосується ролі людини в системі безпеки. Кібербезпека виходить за межі інформаційної, включаючи не тільки захист інформаційних ресурсів, але й захист інших активів, зокрема саму особу. Люди у цій системі відносин осмислюються у різних ролях (і як потенційні об'єкти кібератак, і як несвідомі її учасники тощо), що має відповідні етичні наслідки та посилює питання соціальної відповідальності [424].

Водночас декларативні норми все ще не гарантують реального та дієвого захисту інтересів суспільства, в тому числі й у питаннях отримання об’єктивної інформації. Не врегульованим залишається питання щодо концентрації медіа в країні у вузькому колі власників, стосовно діяльності зарубіжних ЗМІ на території України. Державної підтримки, в тому числі й унормування потребує вітчизняне книговидання, україномовна книга як важливий чинник соціо-гуманітарного розвитку. Виникає ряд труднощів і через недостатню увагу законотворця до теле- та радіомовлення, періодичних друкованих видань українською мовою.

Крім того задекларованe право щодо незалежності засобів масової інформації від владних структур носить суто популістський характер. Повною мірою це стосується місцевої преси. Як справедливо зазначає М. Яковенко, «з

одного боку, щодо цих мас-медіа імпонує ідея закону про повне відмежування преси від органів державної влади та органів місцевого самоврядування» [352, с. 24]. З іншого, продовжує вчений, «у демократично і економічно нерозвинутих країнах така преса миттєво перетворюється на залежну від грошових мішків або ж перетворюється на рекламно-еротичні видання з набором сумнівних сенсацій» [352, с. 24]. А саме тоді неможливим постає виконання через ЗМІ таких функцій, як інформаційна, просвітницька, культурологічна.

У своїх інших дослідженням ми з цього приводу констатуємо, що незалежними від місцевих бюджетів засоби масової інформації можуть стати лише за умов, коли зможуть самоокуповуватися й існувати за рахунок надходжень від реклами та передплати. На даному ж етапі необхідно забезпечити невтручання владних структур у творчі процеси, пільгове кредитування, інші економічні важелі щодо налагодження вітчизняного газетного виробництва [381, с. 33].

Ми також вважаємо, що нагальним питанням постає оптимізація структури власності суб'єктів інформаційної діяльності, якнайшвидший розвиток суспільного сектора, особливо в галузі електронних мас-медіа [381, с. 33]. Створення організаційно-правової бази цих змін, згідно з нашими поглядами, – це ще одне нагальне завдання всіх гілок української влади. Крім цього, забезпечення інформаційної безпеки України і захист національного медіа-ринку вимагає перегляду основних принципів регулятивної політики на засадах інформаційної відкритості й підтримки власних медіа-виробників. Головним об'єктом такої підтримки має стати український зміст інформаційної продукції [381, с. 33].

Доповнюємо такі ідеї зауваженням, що державна політика забезпечення інформаційної безпеки повинна бути відкритою і передбачати інформування суспільства про діяльність державних органів і суспільних інститутів у сфері інформаційної безпеки з урахуванням обмежень, встановлених чинним законодавством України [381, с. 33]. Тому стверджуємо, що вона має виходити з принципу безумовної правової рівності всіх суб'єктів інформаційних відносин незалежно від їхнього політичного, соціального та економічного статусу, ґрунтуватися на обов'язковому забезпеченні прав громадян і організацій на вільне

створення, пошук, отримання, накопичення, зберігання, перетворення і поширення інформації у будь-який законний спосіб [381, с. 33].

Також у наших працях зазначено, що «державна політика у сфері суспільно-інформаційних відносин повинна спрямовуватися на забезпечення права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційної діяльності в національному інформаційному просторі України» [381, с. 33]. Річ у тому, що, на думку Н. Войцих «Для становлення демократичного суспільства важливим є недопущення втручання будь-кого у зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законом відповідно до Конституції України» [318, с. 8; 381, с. 33].

Увиразнюємо ми це тим фактом, що сьогодні найбільш гострою проблемою в Україні є відсутність у переважної більшості громадян довіри до державної влади, впевненості в тому, що всі гілки і структури влади, всі її посадові особи працюють в інтересах суспільства, а не в інтересах самої влади або своїх особистих. Тому вістря державної інформаційної політики має бути, перш за все, спрямоване на усунення «дефіциту довіри до влади», який перешкоджає просуванню по шляху реформ [381, с. 33].

У цьому сенсі, вважаємо ми, ключовим завданням є створення відкритого інформаційного середовища, включаючи забезпечення інформаційної прозорості державної влади, необхідної для формування громадянського суспільства і досягнення взаємодії між суспільством і владою на принципах довіри, взаєморозуміння та ділового партнерства [381, с. 33].

Річ у тому, що збалансоване функціонування системи інформаційної безпеки забезпечується за рахунок постійного обміну інформаційними потоками як усередині держави, так і між державами [381, с. 33]. С. Мошковська з цього приводу зазначає: «Будь-яка держава є відкритою системою, яка задіяна в кругообігу інформації. І якщо не буде відбуватися природний обмін в інформаційному просторі, то система руйнується» [336, с. 119]. Тому завдання політики на інформаційному рівні керування процесом обміну. Останній не є хаотичним і підпорядковується цілком визначеним законам, один з яких можна

сформулювати таким чином: інформація не викидається в інформаційний простір довільним способом, а посилається передусім туди, де вона необхідна і її здатні сприйняти [338; 381, с. 33-34].

Ми також зазначаємо, що для створення відкритого інформаційного простору в Україні, перш за все, необхідно запустити механізм практичної реалізації конституційного права на свободу одержання інформації. Правовою основою такого механізму повинні стати законодавчо закріплені чіткі правила, умови і порядок отримання громадянами та інституційними структурами суспільства інформації в органах державної влади і місцевого самоврядування, від інших державних і недержавних юридичних осіб, а також прямого доступу до державних і недержавних інформаційних ресурсів [381, с. 34]. Як зазначає з цього приводу М. Гуцалюк, органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки. На теперішній час окремі елементи системи інформаційної безпеки створені та функціонують (органи зовнішньої розвідки, інформаційні служби різноманітних міністерств, система технічного та криптографічного захисту інформації держави і т. н.). Проте для їхнього функціонування ще недостатня правова база. Зміст діяльності органів інформаційної безпеки також ще не в повній мірі відповідає покладеним на них завданням. Це пояснюється в першу чергу недостатнім опрацюванням питань, що стосуються форм і способів забезпечення інформаційної безпеки [323, с. 3; цит.: 381, с. 34].

Тому нами вмотивовано у наших попередніх працях, що для ефективної реалізації державної політики, щодо побудови відкритого правового інформаційного простору України потрібно виконати ряд головних вимог [381, с. 34]. Більшість дослідників одностайні щодо переліку таких вимог. Так, наприклад А. Ф. Грицик зазначає: 1) в системі органів державної влади має бути сформована єдина структура, функцією якої є проведення державної інформаційної політики.

Ця структура повинна охоплювати всі гілки і рівні державної влади і включати як спеціалізовані органи влади, що забезпечують регулювання інформаційної сфери, так і підрозділу в інших органах влади, відповідальні за інформаційні аспекти діяльності в сфері їх компетенції [322, с. 211; цит.: 381, с. 34]; 2) державне управління інформаційною сферою має бути планомірно забезпечене фінансовими і матеріальними ресурсами за рахунок бюджетного фінансування – природно, виходячи з реальних можливостей держави за статтею витрат на державне управління [322, с. 211; цит.: 381, с. 34]; 3) проведення державної інформаційної політики має координуватися з єдиного центру на рівні вищого керівництва країни при персональній відповідальності одного з вищих посадових осіб держави за вирішення цього завдання [322, с. 211; цит.: 381, с. 34]. Адже право самостійно виражати свої власні думки та накопичувати, отримувати і розповсюджувати інформацію, як і кожне інше право, має свої власні обмеження.

Загалом нам вдалось аргументувати, що співіснування влади і суспільства в контексті соціальної історії визначається взаємозв'язком, в результаті якого суспільство формує відповідну часу владу, а вона, посилаючись на реалізацію національних інтересів, мусить контролювати суспільство [381, с. 34]. Одним з найважливіших елементів управління суспільством є державний контроль над інформацією. Система контролю і дозування інформації існує в кожній державі [348; 381, с. 34]. Але головне питання, яке так чи інакше постає в цьому контексті: в чиїх інтересах здійснюється такий контроль [381, с. 34].

Наш висновок полягає у тому, що, на жаль, в даний час не тільки жодна з перелічених вище вимог у повному обсязі не виконується, але і на рівні вищого українського керівництва проведення цілеспрямованої інформаційної політики не розглядається в ряду першочергових завдань державного управління. Подібне неадекватне ставлення до створення відкритого і контрольованого інформаційного простору призводить до негативних наслідків, істотно відображаючись на розвитку України. Варто зауважити, що таке ставлення державної влади до інформаційної політики не тільки призвело до інформаційної війни, в стані якої перебуває Україна, а й створило можливості для успішної

реалізації Росією інших елементів гібридної війни [381, с. 34].

Протидія маніпулятивним впливам (засоби, технології, можливості) є надзвичайно актуальною, що теж засвідчено у наших інших працях [377]. В них встановлено, що сучасний глобалізований світ з кожним днем стає все більш інформаційно насиченим, а тому часто незрозумілим для людей. Людина не здатна самостійно отримати й перевірити всю необхідну для неї інформацію, тому, вимушена багато що сприймати як правду [377, с. 181]. Наповнюючи потрібним змістом повідомлення, що передаються різноманітними комунікаційними потоками, можливо подавати суспільству не лише знання про навколишню дійсність, але й цілеспрямовано формувати емоційні та поведінкові стереотипи, внутрішню картину світу людей, своєрідні когнітивно-поведінкової матриці, на основі яких і відбувається орієнтація в світі. І в цьому значенні людина інформаційного суспільства не є вільною, оскільки не має змоги самостійно одержувати повні й, головне, достовірні знання про події, що відбуваються [324; 377, с. 181].

Ми вважаємо, що у неконтрольованому інформаційному просторі формується своєрідна ілюзія демократії, спотворюються трактування політико-правової реальності, ціннісні орієнтири, морально-етичні норми. Адекватність реальним викликам підмінюється симулякрами, всілякими формами мімікрії, при чому як на рівні державних службовців, політичних діячів, так і у широких суспільних верствах. Впевнені позиції посередника у цьому процесі зберігають ЗМІ як інструменти маніпулятивних стратегій політичних сил. А відсутність ефективної системи соціально-психологічного захисту в масштабах цілого суспільства лише посилює згадані тенденції [377, с. 181].

На сьогоднішній день проблема маніпулювання громадською думкою, а відтак і суспільною свідомістю залишається невирішеною, хоча й широко вивчається. Інтерес до неї пов’язаний з наявністю чималого досвіду застосування маніпулятивних технологій як в Україні, так і в цілій низці країн світу, що стали на шлях демократизації з розпадом Радянського блоку.

У практиці політичного маніпулювання враховують і використовують

соціально-психологічні ефекти, що виникають у групах людей (ефекти «присутності інших», гомогенності, впливу меншості, наслідування, конформізму, зараження тощо). На думку О.Д. Бойко застосування як важелів впливу цих ефектів має свою специфіку на рівнях «людина – група – маса», суть якої полягає в тому, що зі збільшенням кількості людей, на яких націлена маніпулятивна дія, розмивається її адресність, звужується, примітивізується маніпулятивний арсенал, зростають масштаби емоційного зараження тощо [317; цит.: 377, с. 182].

Ми вважаємо, що більшість дослідників погоджуються з тим, що способи маніпуляції можуть бути різноманітними, єдине, що їх пов'язує між собою, − це переінакшення думок споживачів інформації на користь певної особи або групи для отримання прибутків або іншої вигоди [377, с. 182]. Наприклад І. Кочнев до них відносить: явну брехню, повторення, роздратування, гнів, спокушання, підкуп, шантаж, погрози, залякування, сором і відчуття провини, сарказм, турботу, гордість, лестощі тощо [328; цит.: 377, с. 182].

Однак, попри всі особливості, констатуємо ми й інші дослідники, «формула успіху психологічного маніпулювання залишається незмінною і ґрунтується на «трьох китах»: привертанні уваги об’єкта маніпуляції; жонглюванні аргументами (фактами, доказами) з метою відволікання або зміщення уваги та подальшої її жорсткої концентрації на другорядних деталях (впродовж процесу відбувається підміна чогось суттєвого на несуттєве); стимулюванні, підштовхуванні об’єкта маніпуляції до дії, яка цілком «логічно» випливає зі штучно створеної ситуації» [337; 377, с. 182].

Цікаво, що наслідки маніпулювання досить мають негативні результати. Про це стверджують майже всі дослідники цього феномену. Так, визначають, що деструктивні маніпуляції людиною, суспільною думкою та масовою свідомістю, поряд з національними конфліктами, екологічними катастрофами і демографічними проблемами перетворяться в глобальну світову проблему початку третього тисячоліття [325, с. 16; цит.: 377, с. 182].

Вчені справедливо попереджають, що визначальною інформаційною загрозою національній безпеці слугує саме маніпуляція суспільною свідомістю,

адже це дестабілізуючий вплив і на інформаційну структуру країни, і на її інформаційні ресурси, і на суспільство загалом та окрему особистість як його члена. Маніпуляції відкривають доступ до найскладніших елементів культури, цінностей, інтересів, переконань, тому на рівні поведінки, діяльності та можуть легко модифікувати державну політику, електоральну динаміку чи навіть військові операції. Отже, захист інформаційного простору, на думку Г. Почепцова, мав би значною мірою бути пов'язаним із захистом національної системи символів – «соціальних конструктів, які сприяють солідарності, орієнтації значної кількості співвітчизників на сприйняття цінностей як спільних, що мотивують різні соціальні групи задля підтримки безпеки окремої людини, суспільства та держави» [223].

Сучасна інформаційна політика у комплексі з гуманітарною покликана не лише розвивати суспільство за демократичними орієнтирами (що є також складним і відповідальним завданням). Її модернізація, яким парадоксальним це б не видавалося, полягає у здатності зберігати і примножувати традиції, зокрема прищепити патріотичні почуття, сприяти національній культурі, звичаям, державній мові, розумінню історії свого народу. Системне недоопрацювання у цьому другому напрямку, таке ж згубне, як і стихійність або непослідовність демократичних реформ. Свого часу відсутність цілісної та широко представленої системи загальнонаціональних цінностей, а також відповідного медійного супроводу в Україні до певної міри уможливили зайняття відповідного місця у свідомості людей ворожою системою ціннісних координат. Для жителів окремих територій Донбасу, АР Крим, м. Севастополь це зрештою означало тимчасову втрату Батьківщини, а нерідко й фізичне знищення, втрату майна тощо. Чужа та недержавна інформаційна картина світу посприяла таким втратам.

Необхідно констатувати, що доречно зроблено в наших інших дослідженнях, що інформація і її специфічне маніпулятивне використання стає сьогодні основним засобом маніпулювання у суспільній сфері [377, с. 182]. Водночас слід розуміти й те, що протидія громадянського суспільства маніпулюванню значною мірою залежать від таких чинників, як відкритість і

доступність інформації та від рівня політичної поінформованості та компетентності громадян, рівня усвідомлення їх політичних інтересів. Приходить розуміння, що забезпечити інформаційну безпеку неможливо через тотальну утаємниченість чи певні обмеження, тож варто застосовувати інші методи для вирішення цієї проблеми [377, с. 182].

Особливо важливою в такому контексті є відсутність дієвої системи соціально-психологічного захисту в масштабах цілого суспільства, так як традиційні механізми захисту зруйновані або не відповідають розвитку сучасних маніпулятивних технологій, а нові механізми захисту під впливом нових умов ще тільки формуються. В процесі формування системи захисту від маніпулювання як окремої особистості, так і суспільства загалом відіграє особливе значення специфіка самих маніпулятивних технологій, адже сьогодні поширюються та охоплюють різні сфери суспільства, в тому числі і політичну, новітні маніпулятивні технології, такі як НЛП – нейролінгвістичне програмування, тощо [377, с. 182].

Велике значення, стверджуємо ми, має й те, що окремі громадяни не знають основних механізмів індивідуального психологічного захисту від маніпулятивного впливу. В розвинутих країнах процес застосування маніпулятивних впливів та відповідно набуття захисних механізмів від них тривав достатньо довгий час. Наша ж держава з отриманням незалежності та відкритості поринула у безмежний світ впливів та взаємовпливів, в тому числі і негативних, і виявилась разом з своїм населенням не готовою до адекватного сприйняття реальності та існування у нових, швидкозмінюваних умовах [377, с. 182].

З цього приводу нами відзначено, що в науковій літературі поняття захисту від політичного та інформаційного маніпулювання трактується по-різному, але у найзагальнішому розмінні можемо стверджувати, що таким захистом передбачається своєчасна, продумана та обґрунтована діагностика стану спільноти/індивіда, а також узгоджені, комплексні дії, які покликані послабити та зрештою нейтралізувати негативні переживання, тривожність, дезорієнтованість й інші деструктивні наслідки інформаційного впливу [377, с. 182]. Вчені також

ведуть мову про два визначальні способи індивідуального захисту від маніпуляцій: 1) дотримання наперед визначеної точки зору з певного питання, намагання зберегти незалежність, впевненість, послідовність; 2) спростування як лінія захисту (ретельне і детальне вивчення маніпулятивного повідомлення, підготовка та висунення протилежних доказів і аргументів) [316; 377, с. 182].

Ці самі науковці пропонують, з чим ми погоджуємось, три стратегії зменшення уразливості до маніпулювання. Перша з них передбачає регулювання та обмеження у законодавчому порядку методів маніпулювання, а також надання їм якостей «чистоти», «ясності» та «чесності» [377, с. 182]. Подібно до того, як певні свідчення у суді визнаються неприйнятними, а юридичні маневри – недозволеними, так і певні тактики у політичній сфері – «нечесні» та «брудні», мають бути заборонені. Однак таке законодавче регулювання тактик маніпулювання може загрожувати засадам свободи слова. Окрім того, українська законодавча база у цій сфері ще не відрізняється довершеністю та системністю, а також характеризується внутрішньою суперечливістю, що дає змогу громадянинові забезпечити лише мінімальний та частковий його захист [332; 377, с. 183].

Суть другої стратегії полягає у тому, що самого лише знання громадянина про наміри інших маніпулювати ним, недостатньо для запобігання маніпулюванню. Значення має й те, що він робитиме у подальшому з цим попередженням, як воно допомагатиме йому у підготовці до отримання маніпулятивного повідомлення та оцінки його змісту [332; 377, с. 183].

Нарешті, ми вважаємо, що третя стратегія передбачає вироблення методів спротиву маніпулятивному переконанню з конкретної проблеми (теми). Щоб зміцнити вже сформовані уявлення особистості у певній темі, слід спершу усвідомити їх вразливість, а далі – для успішного захисту свідомості необхідні «мінімальні тренувальні атаки» на особисті відчуття. Саме такі «атаки» й формують здатність особи до спротиву подальшим маніпуляціям, творячи мотивацію для захисту власних вірувань, а також набуття своєрідної практики організації інформаційно-психологічного захисту особистості, а отже, кращого її

«озброєння» для спротиву впливу серйозніших технологій такого типу [332; 377, с. 183].

Згадані автори виділяють два підходи до протидії «пропаганді», яка, у цьому випадку, може трактуватись як синонім «маніпулюванню». У наших працях констатовано, що протидія маніпулятивним впливам передбачає активність та усвідомлення людиною факту маніпулювання. Тобто протидія – це форма активного захисту. Проте існує і пасивна форма, вироблена еволюцією та суспільством – захисні механізми психіки (витіснення, перенос, раціоналізація, іронія, проекція, ідентифікація, реактивний опір та інші) [377, с. 183]. Їм притаманні дві важливі характерні риси: по-перше, вони діють непомітно на рівні підсвідомості й людина не усвідомлює ні причин і мотивів, ні цілей, ні самого факту своєї захисної поведінки щодо певного явища або об'єкту; по-друге, захисні механізми завжди спотворюють, фальсифікують або підміняють реальність. Тому захисні механізми психіки не сприяють раціональному вибору, але тим не менше, дозволяють людині уникати психологічного дискомфорту [377, с. 183].

Ми також зазначаємо, що застосування контр-маніпулятивних технологій теж не є вирішенням проблеми. Це пояснюється тим, що на відміну від ситуацій міжособистісної взаємодії, коли одна людина маніпулює іншою, інша може вдатися до контрманіпулювання, адже безпосередній вплив робить можливим аналогічний зворотній зв’язок [377, с. 183]. В ситуації, коли вплив здійснюється через мас-медіа, а це основний спосіб здійснення маніпулятивного впливу в сучасному інформаційному світі, ні контрманіпулювання, ані повна ізоляція від впливу на практиці не видається можливою [351; цит.: 377, с. 183].

Щоб виробити адекватні способи протидії маніпулятивним впливам, важливо знати, на що вони спрямовані. Мішенями маніпулювання виступають такі особистісні структури, як мислення, емоції та поведінка. У більшості людей ці елементи тісно пов’язані між собою. Тому маніпулятивна технологія, спрямована, наприклад на емоційну сферу («Голосуй серцем») призводить до зміни як мислення так і поведінки людини. Слід сказати, що почуття та емоції – улюблена мішень для маніпуляторів. Проте емоційна, поведінкова та когнітивна

сфери людської особистості та життєдіяльності є не лише мішенями, але й зброєю проти маніпулювання [377, с. 183].

Так, емоційна сфера, дозволяє ідентифікувати наявність маніпулятивного втручання, і вивести його на рівень усвідомлення. Наша когнітивна сфера, є більш вразливою до маніпулювання, ніж здається багатьом, адже людям властива схильність переоцінювати силу інтелекту, насамперед власного. Численні соціально-психологічні експерименти довели, що людина прагне причинності, і готова йти на поступки, якщо їх необхідність обґрунтована [377, с. 183]. Це саме ж стосується і вибору. Політтехнологи В. Януковича добре знали про таку особливість людської психіки, і намагалися задовольнити цю потребу гаслом «Тому що...». Якщо Ви сумніваєтесь в дієвості цієї технології, ось приклад з «Соціальної психології» Дж. Маєрса. Було проведено наступний експеримент. Дівчина просила людей в черзі до ксерокопіювальної машини поступитися їй, тому що «їй треба зробити копії». 80% погодились. Кількість тих, хто готовий був поступитися чергою «без причини» було обернено пропорційним [317; цит.: 377, с. 183].

З іншого боку, саме завдяки когнітивній сфері, люди здатні до критичного мислення, яке, є найпотужнішою зброєю проти маніпулювання. Під час електоральних кампаній, в ситуації інформаційної війни, до будь яких статей та інформаційних повідомлень варто ставитись критично [377, с. 183]. Навіть нейтральні за тональністю повідомлення можуть ставати знаряддям маніпуляції залежно від їх місця в інформаційному потоці («солодкий сендвіч», «отруйний сендвіч»). Також не приймати лише одне пояснення певної ситуації, мисліть альтернативно, і не поспішайте з висновками [329; цит.: 377, с. 183].

Поведінка є по суті рухом волі, спрямованої інтелектом та емоціями. Тому вплив на неї, на щастя, опосередкований. Адже часи, коли влада застосовувала репресивні методи, як засіб переконання, сподіваємось, відійшли для України в минуле. Проте, щоб не піддатися на маніпулятивний вплив, необхідно, перед тим, як висловити підтримку певній політичній силі, задати собі два питання, і спробувати чесно відповісти на них. Перше – що я зараз роблю? Друге ж – навіщо

це мені? [377, с. 183].

На думку дослідниці Л. Кучми, «здатність індивіда протидіяти маніпуляції визначається поєднанням як зовнішніх, так і внутрішніх чинників. Найкращим їх поєднанням є таке, за якого особистість має необхідні знання про ознаки та прийоми маніпулятивного впливу на неї, навиками захисту від них, і має можливість перебувати у соціальному оточенні, яке підтримує такий її спротив» [330, с. 72; цит.: 377, с. 183-184].

Ми вважаємо, що колективний захист вимагає консолідованих зусиль як окремих особистостей, так і інститутів громадянського суспільства (громадських організацій, освітніх закладів, ЗМІ). Основними формами та умовами колективної протидії маніпулятивним впливам є: просвітницька діяльність, проведення заходів, завдяки яким громадяни могли б навчитися протистояти маніпулюванню; моніторинг діяльності ЗМІ; розвиток у суспільстві конкуруючих мереж розповсюдження інформації (диверсифікація); вироблення й популяризація критеріїв оцінки суспільної та політичної відповідальності представників влади (наприклад, одним з таких критеріїв може бути показник «декларативності», що даватиме можливість оперативно виявляти політичні обіцянки й позиції, які не можуть бути реалізовані в принципі (з політичних, економічних і соціальних причин) і є лише інструментами маніпулювання свідомістю громадян) [377, с. 184].

Таким чином, інформаційно-психологічна безпека пов’язана з відчуттями захищеності окремих осіб, соціальних груп осіб, зокрема стосовно деструктивних інформаційних впливів [377, с. 184]. Зі сучасними глобальними перетворення, інформаційними загрозами та демократизійними викликами, що стоять перед Україною, важливо на усіх цих рівнях (держави, суспільства, індивідів) усвідомлювати присутність і впливовість інформаційно-психологічної експансії, що позначається на психіці та поведінці, на рішеннях і програмах дій. При цьому нагальні заходи з протидії відповідним загрозам починаються все ж з конкретного індивіда, а саме з його: здатності усвідомити значимість інформації для життя та розвитку; спроможності адекватно сприймати дійсність, перевіряти факти, діяти

та мислити реальними категоріями; вміння формувати власні установки, орієнтири, переконання; проявляти лояльність до власної держави, надавати підтримку національним програмам; відстоювати власні та національні інтереси, приймати адекватні рішення тощо.

Підривна діяльність російських ЗМІ є великою загрозою для України. Тому паралельно із заходами, спрямованими на протидію воєнній загрозі з боку Росії, чільну увагу слід приділяти загрозам національній безпеці України в гуманітарній сфері. Вони здаються матеріально невідчутними, але за своєю природою становлять стратегічну загрозу № 1, яка є міною уповільненої дії під спорудою української державності. Україна має шанс вистояти у протиборстві з РФ лише як українська Україна [377, с. 184]. Як справедливо зазначає В. Василенко «Тотально зросійщена (лінгвістично і змістовно) Україна становитиме лише периферійну частину «Русского міра», а не повноцінну національну суверенну державу. Не випадково сучасні російські пропагандисти висунули гасло «Нам нужна не пророссийская, а русская Украина» [319; цит.: 377, с. 184].

У наших раніших працях продемонстровано, що головним знаряддям реалізації цього гасла є гуманітарна агресія, яку Росія здійснює одночасно в кількох напрямах, ведучи проти України інформаційно-пропагандистську, історіософську та конфесійну війни. Наступ на українську ментальність, традиційні цінності, мову, культуру, систему освіти, історичну пам’ять народу, національні церкви має стратегічну мету: знищення ідентичності української нації, яка є системоутворюючим складником громадянської нації та Української національної держави [377, с. 184].

Ми вважаємо, що неефективність прояву належної гуманітарної та інформаційної політики, усвідомлення керівництвом країни значення й ролі масово-комунікаційної та соціально-комунікаційної складової державної політики у XXI ст. стали одними з ключових чинників, що призвели до складної зовнішньо- і внутрішньополітичної ситуації, у якій опинилася Україна у 2014 році [377, с. 184]. Російські сценарії анексії Криму та збройного протистояння на Донбасі не могли б бути реалізовані без масштабної масово- та соціально-комунікаційної

роботи, яку системно проводила Російська Федерація. Без аналізу відповідної складової російської зовнішньої політики неможливими є упередження її негативних впливів на суспільство та на позиції України на світовій арені, повноцінне забезпечення державної безпеки, ефективна реалізація національних інтересів [377, с. 184].

При цьому, уже в 1990-х роках Росія домінувала в українському інформаційному просторі, включаючи телевізійну продукцію, радіоефір, шоу-бізнес, друковані засоби масової інформації, книжковий ринок. Цього Російській Федерації вдалося досягнути як за допомогою державного фінансування випуску відповідної російської продукції, так і через дії потужного лобі серед українських політиків і чиновників, які саботували підтримку випуску української продукції, а також «крізь пальці» дивилися на масове завезення контрабандою до України дешевих російських книжок, що робило нерентабельною роботу українських видавців [377, с. 184].

У 2000-х роках же, із стрімким зростанням світових цін на нафту й газ, Російська Федерація отримала фінансові можливості істотно розширити арсенал засобів інформаційного впливу на українське суспільство, як і на суспільства інших країн [377, с. 184]. За державним замовленням і фінансуванням розпочалося масове виробництво російських художніх і мультиплікаційних фільмів, телесеріалів, телешоу, які заполонили телеефір України та інших пострадянських держав [377, с. 184]. Більшість із них мають явний або прихований ідеологічний підтекст, поширюючи вигідні для Росії смислові конструкції, сприяючи формуванню міфів про «русский мир», протиставляючи їх Заходу, апелюючи до ностальгії за «славним» радянським та імперським минулим, формуючи образ ворога з «бандерівців» і «западенців». На замовлення російського капіталу аналогічна медіа-продукція вироблялася і в самій Україні [377, с. 184].

Особливу увагу Росія приділяє новітнім медіа – інтернет-виданням, соціальним мережам, форумам. У всіх соцмережах, які мають значну кількість користувачів у Росії та в Україні (перш за все «ВКонтакте» та Facebook), було створено та популяризовано ряд груп, явні та приховані модератори яких

нав’язують учасникам основні кліше російської пропаганди, закликають до антиукраїнських дій [377, с. 184]. Кремль утримує «армію» високооплачуваних так званих інтернет-тролів, до завдань яких входить написання вигідних Москві коментарів у соціальних мережах та інтернет-форумах, впливаючи, такими чином, на громадську думку не лише в Росії та Україні, а й у Європі та США [357; цит.: 377, с. 184-185].

Нами помічено, що українська медійна сфера виявилася неготовою протистояти таким технологіям, і вітчизняні засоби масової інформації, свідомо чи несвідомо, стали провідниками російської пропаганди, метою якої була підміна понять «окупанти» чи «російські військові» на «ввічливі люди зі зброєю» [377, с. 185]. Відомий вітчизняний дослідник Г. Почепцов справедливо зазначає, що аналогічним чином росіяни запровадили в медіа-простір поняття «народний мер», «народний губернатор», прибравши таким чином прикмети незаконності самопроголошених лідерів сепаратистів. Натомість легальну українську владу російські засоби масової інформації подають не інакше як «хунта» і «самопроголошена київська влада» [343; цит.: 377, с. 185].

На відміну від України, Росія роками ґрунтовно готувалася до інформаційного та ідеологічного протистояння, вивчаючи світовий досвід застосування масово- й соціально-комунікаційних технологій і пристосовуючи його до своїх цілей. У Росії було написано десятки дисертацій і монографій, присвячених інформаційним війнам і використанню інформації в цілях геополітики [377, с. 185]. Поруч із глибокими дослідженнями масово-комунікаційних впливів, як, наприклад, праця Д. Ольшанського «Психологія мас» [339], у Росії значною популярністю користуються також праці С. Кара-Мурзи [326], І. Панаріна [340] та ряду інших авторів, які досить вільно інтерпретують історичні факти та західні комунікаційні теорії, пристосовуючи їх до потреб офіційної кремлівської пропаганди [377, с. 185].

Російська комунікаційна школа за останні півтора десятиліття освоїла основні західні концепції масово- та соціально-комунікаційних впливів, сприймаючи їх через призму радянської, імперської ідеології та розглядаючи їх як

інструментарій агресивної реалізації державних інтересів Російської Федерації на світовій арені в тому вигляді, у якому уявляє ці інтереси сучасна російська правляча верхівка [377, с. 185]. При цьому російські дослідники витворили своєрідний симбіоз, поєднавши радянські авторитарні технології пропаганди з новітніми західними досягненнями в галузі масових і соціальних комунікацій. Застосування комунікаційних технологій у реалізації зовнішньої політики Російської Федерації передбачено в нормативних документах останньої, зокрема в оновленій Концепції зовнішньої політики Російської Федерації (2013 р.) і у Федеральному законі «Про державну політику Російської Федерації по відношенню до співвітчизників за кордоном» (у редакції 2010 р.) [377, с. 185]. Масово- та соціально-комунікаційні технології впливу Російської Федерації на зовнішню та внутрішню політику сусідніх держав, у тому числі на Україну, спрямовані на недопущення формування власної національної ідентичності, просуваючи, натомість, залучення громадян цих держав до так званого «русского мира» як спільного ідеологічного, мовно-культурного, релігійного, освітньо-наукового, мас-медійного середовища на базі російської євразійської ідентичності [377, с. 185].

Сукупність заходів із застосування технологій масово- та соціально-комунікаційних впливів на свідомість і підсвідомість громадян України стали на заваді переходу від радянської до української ідентичності людей старшого покоління, а також формували в значної кількості молодих людей, особливо на Сході та Півдні України, радянсько-російський менталітет та українофобію [377, с. 185].

Населення Кримського півострову та Донбасу від часу здобуття Україною незалежності знаходилося під постійним російським впливом, інформаційні можливості якого у різні роки мали різні масштаби. Однак цілеспрямоване російське мовлення у цих регіонах було посилено напередодні реалізації планів з окупації, а також підсилене слабким загальноукраїнським мовленням. Інформаційне, культурне, загалом гуманітарне середовище, позбавлене об’єднуючих сенсів, легко вразливе. У ньому простіше культивувалися

сепаратистські настрої, ключові тези кремлівської пропаганди, а відтак і цілком природними презентувалися наступні злочинні моделі поведінки (зрада в лавах силових і правоохоронних органів України під час збройної агресії Росії, збройні напади, насильство, грабежі тощо).

Інформаційний фронт війни Росії проти України, на думку В. Горбуліна, розгортається одразу на кількох напрямах. Передусім: (1) серед населення в зоні конфлікту; (2) серед населення країни, проти якої здійснюється агресія, однак територія якої не охоплена конфліктом; (3) серед громадян країни агресора; і (4) серед міжнародного співтовариства [321; цит.: 377, с. 185].

У наших дослідженнях ми вже зупинялись на основних формах і методах інформаційної війни, якими користується Росія. Сфабриковані повідомлення російських засобів масової інформації, що особливо активно поширюються на сході України, мають на меті формування негативного образу української влади та військовослужбовців, звинувачуючи її у фашизмі та утисках жителів Донецької і Луганської області [377, с. 185]. Для російських інформаційних «атак» характерні наступні тренди:

Телевізійні канали Російської Федерації систематично транслюють репортажі про «звірства карателів фашистської хунти» [377, с. 185]. Так на каналі ОРТ вийшов сюжет, автор якого повідомляє, що українські бійці отримали наказ вбивати мирне населення, а воюють вони за обіцянку отримати винагороду – «клаптик землі и два раба» [349; цит.: 377, с. 185]. Телеканал РЕН-ТВ масово поширював сфабриковану інформацію про так звану «нову Хотинь», коли в селищах Саурівка і Степанівка Донецької області бійці української Нацгвардії нібито влаштовували безчинства, вбивали всіх чоловіків, а жінок ґвалтували [377, с. 185].

Російські медіа відтворюють відеосюжети про українську владу у відредагованому вигляді, з відривом від контексту. «Перший канал» у випуску новин (14.11.2014 р.) повідомив про те, що Президент України Петро Порошенко нібито збирається задавити Донбас економічним пресингом, а донбаських дітей примусити сидіти в підвалах. Однак насправді у повній версії відеовиступу

президент України говорить про те, що через те, що Донбас «відрізаний» від України озброєними бойовиками, страждають місцеві жителі, які змушені сидіти без пенсій та у підвалах [377, с. 185].

Окрім того, у соціальних мережах поширюються підроблені фотографії, які демонструють наслідки «звірств», що відбуваються в Україні. Так на одній з фотографій в соцмережі «Одноклассники» зображено собак, які обгризають схожі на людські кістки, та представляється як актуальне фото зі східної України: «Собаки доїдають труп українського бійця. ВСУ наплювати на своїх загиблих, а місцеві жителі відмовляються ховати тих, хто прийшов на їх землю поневолювати і вбивати» [377, с. 185]. Однак фактично це фото було скопійоване з сайту демотиваторів. Російськими спецслужбами також була здійснена спроба дискредитувати мобілізацію українських військовослужбовців шляхом поширення чуток в соціальних мережах про нібито затримання юнаків на вулицях та примусове відправлення їх до зони АТО [344; цит.: 377, с. 185-186].

Таким маніпулятивним технологіям з боку Російської Федерації сприяло і саме інформаційне середовище Сходу України, в якому відбувалось зомбування населення: російські телеканали були джерелом політичних новин для 78 % жителів Сходу та Півдня України (відповідно до опитування з 8 по 18 лютого 2014 року) [377, с. 186]. Крім того, незважаючи на тимчасове призупинення 25 березня 2014 року судом (за позовом Національної ради з питань телебачення і радіомовлення) ретрансляції на території України російських каналів «Первый канал. Всемирная сеть», «РТР-Планета», «Россия-24», «НТВ-Мир», багато місцевих провайдерських компаній не припиняли трансляцію через постійні погрози [377, с. 186]. Також у Донецьку і Донецькій області в радіусі до 70 км, що складає більше 37 % населення області, мовлення ведуть виключно російські телеканали. При цьому з Волновахи ряд українських каналів досягає західної частини і центру Донецька, але якість сигналу при цьому багато в чому залежить від рельєфу місцевості. У Луганській області російські та сепаратистські телеканали транслюються з об’єктів в Луганську та Ровеньках, які контролює так звана ЛНР (охоплюють близько 56 % населення області) [377, с. 186]. Що

стосується радіомовлення, то в Донецькій області російські радіостанції транслюються тільки з радіорелейних станцій (РРС) Донецька з територією покриття міста і населених пунктів в радіусі до 50 км (охоплено близько 35 % населення області) [377, с. 186].

Така технічна ситуація стала визначником передбачуваних результатів соціологічних досліджень [цит.: 377, с. 186]: – підтримка 17 % населення Луганської та Донецької області ідеї відокремлення регіону від України і створення незалежної держави (опитування станом на квітень 2014 р.); – зміна свідомості переважної більшості населення Сходу. Зокрема, виникнення у донеччан відчуття страху перед радикально налаштованими жителями Західної України – «бандерівцями» (загрозу від них вбачають 60 % опитаних), страху перед центральною владою в Києві (47 %), страху утручання європейських та американських політиків (38 %). Менша частина основні загрози відчуває від громадян Росії, які беруть участь в організації проросійських мітингів (23 %), і від російських політиків та військових (21 %). В Луганській області проросійські настрої в деяких населених пунктах переважають у – 95 % населення, а найменше їх (30 %) в українізованій частині області, де історично більше українців [377, с. 186].

Водночас безпосередній тиск на аудиторію та дія відповідного кумулятивного ефекту не вичерпують усього негативного впливу пропаганди. Зазвичай поза увагою залишається т.зв. зворотній вплив – ефект, що справляє пропаганда на суб'єкта її реалізації. Маємо підтвердження цього факту і в умовах російської агресії (зокрема, в публікації колишнього співробітника Російського інституту стратегічних досліджень О. Ситіна «Анатомия провала: О механизме принятия внешнеполитических решений Кремля») [377, с. 186].

Підсумовуючи, в наших дослідженнях і в цій праці доведено, що в процесі російської інформаційної агресії використовувались маніпулятивні механізми, що зокрема включали: систематичні фейкові репортажі про «карателів київської фашистської хунти», відредаговані відеосюжети про українську владу з відривом від контексту, поширення підроблених фотографій у соціальних мережах, які

нібито демонструють наслідки «звірств», що відбуваються в Україні [377, с. 186]. Ефективності інформаційного впливу сприяло переважання російських джерел інформації в східних регіонах України – російські телеканали були джерелом політичних новин для 78 % мешканців [377, с. 186].

Такі маніпулятивні технології Російської Федерації порушували, зокрема, Європейську конвенцію про транскордонне телебачення, зокрема ст. 7, у якій говориться: «програми в цілому, їх представлення та зміст повинні забезпечувати повагу до гідності людської особи та основних прав інших людей… Зокрема, вони не повинні: надмірно виділяти насильство і сприяти расової ненависті. Телемовник повинен забезпечувати, щоб в новинах факти і події подавались справедливо та сприяли вільному формування думок») та Кримінальний кодекс України ст.161., яка передбачає «…умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності…» [цит.: 377, с. 186].

Пропагандистська кампанія, що ведеться проти України в інтересах зовнішнього агресора потребує цілісної та системної відповіді з боку держави, що передбачає вироблення більш чіткого та зрозумілого механізму науково обґрунтованого визначення пропаганди, маніпуляції та їх впливу на розгортання конфлікту [377, с. 186]. Так на думку дослідників: «Національні інтереси та безпека України потребують негайного розроблення і втілення комплексу державної інформаційної політики (внутрішньої та зовнішньої), розбудови вітчизняного гуманітарного простору з ефективним застосуванням сучасних масово- та соціально-комунікаційних технологій. Необхідним є залучення до розробки відповідного комплексу заходів вітчизняних науковців і фахівців-практиків у відповідних галузях» [333, с. 86; цит.: 377, с. 186].

Загалом утвердження незалежної аналітики, ґрунтовних дослідницьких напрямків, системних шкіл вивчення агресора та суміжних питань (інформаційної політики, гібридних воєн, політико-безпекових орієнтирів сучасного світу та окремих регіонів, локальних спільнот у ньому тощо) є одним із найважливіших напрямків протистояння. Українські мозкові центри та науково-дослідні установи

мають усі шанси стати конкурентоспроможними у світі, адже предметне поле їх дослідження унікальне за своєю сутністю, а розуміння внутрішніх механізмів російської гібридної агресії може скласти важливий міжнародний досвід. Сфера політичної аналітики та науки потребує потужної підтримки держави, комерційних структур, міжнародних фондів, але також і високого рівня усвідомленості проблематики самими вченими та експертами, відповідальної та солідарної позиції у боротьбі за автономію та свободу наукового пошуку.

Зрештою ця проблематика до певної міри характерна і для сучасних західних країн, навіть для США, які залишаються впливовим центром аналітичної думки, виробництва політологічних знань та освіти політологів. Зокрема серед останніх нашу увагу привертає дослідження про упередженість політології в США, яка зокрема впливає на те, що вивчається, які питання задаються, як інтерпретуються відповідні докази, зокрема й у безпековій тематиці (на прикладі висвітлення проблем ядерної зброї та глобальної безпеки). Авторка аргументовано доводить, що американські вчені, які аналізують розповсюдженні ядерної зброї, часто перебувають під впливом національних упереджень (що має низку негативних наслідків), й відтак закликає до систематичнішого підходу, здорових дискусій, міждисциплінарних обмінів та інших заходів заради об’єктивності сучасних досліджень [428]. Цілковито викорінити упередженість у такій діяльності досить складно, особливо в умовах війни. Проте саме прагнення протистояти агресору, розвивати сили своєї країни потужним та беззаперечним науковим потенціалом може слугувати важливим ціннісним орієнтиром, при чому не тільки для професійної спільноти політологів, соціологів, істориків, правознавців, але й для усього українського суспільства.

Ми вже раніше стверджували [377], що найважливішим напрямом протидії інформаційній експансії геополітичних супротивників України є створення інформаційно-психологічних підрозділів для забезпечення психологічної безпеки особистості, суспільства, держави. Їх основне завдання − розробка і здійснення стратегічних та оперативних заходів із попередження і нейтралізації негативного інформаційно-психологічного впливу на державному, регіональному і місцевому

рівнях [377, с. 186]. Суттєво зростає також обсяг інформаційно-аналітичної роботи. Виникає необхідність формування єдиної системи соціальної інформації України і державної системи інформаційного моніторингу. Такі системи мають аналізувати інформацію на різних рівнях (державному, регіональному, місцевому), а результати слід постійно враховувати при розробленні та проведенні заходів із забезпечення національної безпеки держави [345; цит.: 377, с. 186].

У протистоянні російській інформаційній агресії державним структурам України особливо варто пам’ятати про спільне минуле, історичну та інституційну пам'ять, яка зберігається в обох країнах та може також становити окремий спектр загроз. Серед сучасних досліджень нашу увагу в цьому контексті привертає стаття «Інформація, безпека та авторитарна стабільність: розповсюдження та координація політики Інтернету в пострадянському регіоні», де акцентується на подібній проблематиці. Зокрема йдеться про пострадянські режими, які застосовують подібні підходи до контролю вмісту та використання Інтернету на своїх територіях. При чому конкретні правові рамки, технічні системи та інші практики контролю Інтернету тут зазнали глибокого впливу і складних регіональних взаємозалежностей [427]. Автор великою мірою має рацію, адже тривалий час навіть окремі формулювання та положення вітчизняного законодавства в інформаційній сфері нагадували норми РФ. Знання про функціонування інформаційних мереж ворога є також потужним інструментом протистояння йому. Не менш важливо усвідомлювати, що і російські інформаційні системи контролю та координації глибоко інкорпоровані в українські, що безумовно потребує нагальних заходів.

Ми вважаємо, що стратегія формування позитивної для України суспільної думки в умовах збройного конфлікту є довгостроковою програмою дій в інформаційному середовищі світового співтовариства, узгодженою за метою, завданнями, умовами, засобами і ресурсами. Реалізовувати цю стратегію мають спеціальні інформаційно-психологічні структури при різних органах державного, регіонального і місцевого управління України [377, с. 186]. Інформаційно-психологічним структурам варто тісно взаємодіяти із засобами масової

інформаціями, оскільки саме мас-медіа формують суспільну думку шляхом доведення інформаційного повідомлення і свого коментаря до аудиторії. Основними напрямами роботи із засобами масової інформації є: 1. Оперативне розповсюдження достовірної, повної та об'єктивної інформації про діяльність українських військовослужбовців у районі збройного конфлікту. 2. Підготовка і розповсюдження у засобах масової комунікації готових інформаційних, довідкових і роз'яснювальних матеріалів з метою цілеспрямованого просування інформації, в якій зацікавлені державна влада і силові структури. 3. Оцінка реакції суспільства на діяльність державної влади і силових відомств України в районі збройного конфлікту на основі публікацій і вироблення пропозицій за темами, характером і змістом інформації, яку доцільно розмістити в мас-медіа. 4. Організація стратегічної та оперативної взаємодії із засобами масової інформації на основі постійних ділових і доброзичливих відносин з їх представниками [377, с. 187].

Також ми зауважуємо, що основними формами взаємодії із засобами масової інформації є: 1. Організація прес-конференцій, брифінгів, інтерв'ю та інформаційних зустрічей державного керівництва і представників силових відомств із представниками мас-медіа. 2. Поширення в засобах масової комунікації офіційних повідомлень у формі прес-релізів. 3. Підготовка і поширення в засобах масової інформації друкованих, інформаційних, аудіо-, відео- і фотоматеріалів про діяльність українських військових і органів державного управління в районі збройного конфлікту. 4. Підтримка постійних робочих контактів із головними редакторами, журналістами газет і журналів, керівниками телерадіокомпаній та інформаційних агентств. 5. Аналіз, узагальнення й оцінка публікацій, що зачіпають інтереси державних і силових структур у районі збройного конфлікту. 6. Надання вітчизняним і зарубіжним засобам масової комунікації, що лояльно ставляться до української державної політики, ексклюзивної інформації за темами, що ще не висвітлювалися в пресі. 7. Забезпечення захисту прав і законних інтересів представників державних структур у районах збройних конфліктів у випадках оприлюднення наклепницьких

матеріалів [377, с. 187].

Сучасні інформаційні війни є формою соціальної взаємодії різних суб'єктів, що у своїх діях керуються стандартами відповідних моделей світу [377, с. 187]. На думку М. Сенченко, щоб вчасно і, головне, адекватно оцінити з інформаційної точки зору ситуацію, що склалася, потрібно вивчити форми та класифікувати інформаційний вплив з урахуванням його характеру, напряму й адресності. Означену проблему в збройних силах вирішують інформаційні війська, які сьогодні активно формуються в різних країнах світу, зокрема в США, Китаї, Російській Федерації, Польщі, Німеччині тощо. Основні завдання діяльності інформаційних військ Війни в Іраку, Лівії, Сирії й інших країнах показали, що склад спеціальних військ має поповнюватись інформаційними структурами, здатними відбивати інформаційні атаки, а також виконувати відповідний комплекс бойових завдань оборонного й наступального характеру [346; цит.: 377, с. 187].

Потужні країни використовують інформаційний потенціал для досягнення військових, політичних, культурних, економічних та багатьох інших цілей. Інформація та технологія стають інструментами та ресурсами впливу та протистоянь, і це чітко прочитується у Національній стратегії кіберзахисту США. Ця країна «створила Інтернет і поділилася ним зі світом», часто раніше за інші стикалися з негативними наслідками інформаційних загроз, має широкий досвід захисту інформаційної безпеки, але також досі навіть на рівні офіційних документів визнає, що її «приватні та державні організації все ще борються за захист своїх систем, а супротивники збільшили частоту та вдосконалення своєї зловмисної кібер-діяльності» [425]. Відтак інформаційних захист та його системи не можуть сприйматися як щось раз і назавжди встановлене, це динамічна система, яка постійно потребує модернізації, в тому числі й політичними засобами.

Як зазначає М. Сенченко, «ураховуючи підсумки війн і конфліктів XXI ст. до складу Української армії потрібно ввести інформаційні війська, що матимуть спеціальні організаційно-управлінські й аналітичні структури для протидії

інформаційним агресіям» [345, с. 3]. Він наполягає, що «до складу таких інформаційних підрозділів мають входити представники державних і військових засобів масової інформації, міжнародні та внутрішньополітичні експерти, редактори, журналісти, сценаристи, оператори, хакери, перекладачі, працівники зв'язку, веб-дизайнери, які працюватимуть як на зовнішню, так і на внутрішню аудиторію, щоб просто і зрозуміло пояснювати світовому товариству принципи української ідеології» [345, с. 3].

Вчений продовжує, що «основні завдання діяльності інформаційних підрозділів такі: перше − стратегічний аналіз; друге − інформаційний вплив; третє − інформаційна протидія» [345, с. 3]. Науковець зазначає, що «вони включають і координують питання, що перебувають у віданні різних органів» [345, с. 3].

Важливо, помічає вчений, що «для вирішення першого завдання слід створити центр стратегічного аналізу мереж управління. Його функції − це входження в мережі з подальшим блокуванням, контррозвідка, заходи з оперативного маскування, забезпечення безпеки власних сил і засобів, безпеки інформації» [345, с. 3]. Він продовжує, що «для вирішення другого завдання варто створити антикризовий центр, державний медіа-холдинг зі зв'язків із телеканалами й інформаційними агентствами для забезпечення їх потрібною інформацією. У ньому можуть бути задіяні державні засоби масової інформації, агентства зі зв'язків із суспільством, структури, пов'язані з підготовкою журналістів із міжнародної і військової тематики, телерадіомовлення» [345, с. 3]. І врешті-решт, він констатує, що «для вирішення третього завдання потрібно створити центр визначення критично важливих структур супротивника, їх фізичного знищення, радіоелектронної боротьби, психологічних і мережевих (підготовка хакерів) операцій» [345, с. 3-4]. Загалом М. Сенченко аргументує, що «сьогоднішня підготовка спеціалістів у сфері інформаційних війн не дозволяє забезпечити Україну кадрами, що володіють необхідними практичними навичками для підтримання відповідної ідейної і морально-психологічної стійкості суспільства. Потрібна система підготовки кадрів для інформаційно-психологічного протиборства. Варто визначити, в яких навчальних закладах має

здійснюватися їх багаторівнева підготовка, де будуть одночасно готувати спеціалістів зі стратегічного аналізу, інформаційного впливу й інформаційної протидії» [345, с. 4].

Треба відзначити, що до інформаційних викликів та загроз повинні бути готові і відповідні професійні осередки, які передусім надаються інформаційним атакам або самі можуть (не)свідомо сприяти їх просуванню у суспільстві. Такими є сучасні журналісти, при чому не лише в Україні. Як відмічають зарубіжні дослідники, протягом останніх кількох років численні журналісти та інформаційні служби повідомляли про випадки, коли їхні мережі були зламані, перехоплені або викрадені. Особливо небезпечними є ситуації, за яких акаунти журналістів уразливі до хакерів або прихованого стеження, адже відтак і здатність інформаційних агентств якісно виконувати свої завдання суттєво знижується. У 2014 р. експерти з безпеки «Google» виявили, що 21 із 25 найпопулярніших у світі ЗМІ був об’єктом випробовування хакерських операцій. Чимало журналістів безпорадно спостерігали, як хакери брали під контроль їхні акаунти в соціальних мережах. Однак досі є й такі співробітники ЗМІ, що не вживають заходів інформаційної безпеки, не вважають ці загрози реальними [426]. Отже, особливої уваги на шляху розвитку дієвої системи інформаційної безпеки заслуговує журналістська спільнота, і не лише у забезпеченні її конституційних прав, свободи слова, але й у розширенні її можливостей, навиків, компетентностей, інформаційної грамотності, професійності, які у своїй сукупності зможуть ефективно протиставлятися російській пропаганді.

Інформаційна війна у сучасному світі є цілком реальним фактором геополітики, який тривалий час недооцінювався політичною елітою України [345], а іноді й досі не осмислюється у всій його глибині та небезпеках. При цьому є розбіжності у розумінні ключових, нав’язаних з РФ, інформаційних загроз та відповідних концептів як в українському середовищі, так і загалом у західному середовищі. Це вносить деструктив у партнерські відносини та лише посилює позиції агресора.

На таку особливість звертає увагу вже ряд зарубіжних вчених. Зокрема

аргументовано доведено, що існують помітні відмінності в концепціях кібервійни в російській та американській політичній та військовій думці. Кібервійна мислиться як частина сучасної гібридної. В американських джерелах останній концепт використовується для опису окремих нових форм війни, передусім на Близькому Сході. Натомість у російській думці «гібридна війна» позначає політичні та інформаційні операції (у зв'язку з кольоровими революціями, арабською весною, уявленням про те, що РФ постійно атакується США та їх союзниками тощо) [430]. Різні концепції ускладнюють пошук ефективних методів протистояння інформаційній агресії, та знову ж актуалізують необхідність подальших ґрунтовних досліджень в Україні, в тому числі і затребуваність системної аналітики російських внутрішньополітичних контекстів.

У цьому розрізі апелюємо до комплексу ідей, котрі висловлює П. Шевчук і котрі зводяться до того, що «з метою суттєвого покращення стану вітчизняної інформаційної політики та національної безпеки загалом, зменшення інформаційно-психологічних впливів Російської Федерації та захисту інформаційного поля держави насамперед необхідно: створити плацдарм для якісної зміни внутрішньої та зовнішньої інформаційної політики, розробивши коротко- та середньострокову стратегію на основі доповненої законодавчої та нормативно-правової бази, гармонізованої з нормами міжнародного права; припинити руйнацію моральної єдності українського суспільства та почати діяти в інтересах усієї єдиної української політичної нації, працювати на зближення політичних проектів двох Україн; взяти під контроль захист національної інформаційної сфери, водночас знаходити шляхи просування українського інформаційного продукту на територію Росії, шляхом використання сучасних високих технологій та розширення кола наших симпатиків; працювати на зростання іміджу України та її конкурентоспроможності на міжнародній арені шляхом підвищення та покращення її бренду; розвивати та поширювати іномовлення, а також вітчизняні Інтернет-ресурси іноземними мовами; – усіма засобами проривати інформаційну блокаду РФ та обмежити російський інформаційний вплив на Півдні та Сході України; посилити контроль над ЗМІ

інших країн, які функціонують та акредитовані в Україні; провести люстраційну політику серед власників українських медіа-ресурсів, зменшити вплив олігархів на ЗМІ; сприяти розвитку громадського медіа-сектора як незалежного, неупередженого, об'єктивного інституту, основна мета якого – донесення правомірної інформації до споживача; контролювати частотний ресурс біля власних кордонів, не допускати інформаційної контрабанди; суттєво покращити якість та збільшити кількість українського видавничого продукту, сприяти створенню гідних та цікавих телепрограм, розвитку вітчизняного кінематографу; замість заклику «не купуй російське» (саме інформаційний продукт) краще використовувати гасло «купуй українське, тому що воно якісне, рідне, модне та перевірене»; налагодити дієву роботу з проукраїнськими Інтернет-спільнотами, на основі яких створювати відповідні «троль»-угруповання на певним чином акцентувати їхню діяльність, створити блокаду Інтернет-ресурсів, які несуть загрозу інформаційній безпеці держави; сприяти діяльності громадських організацій, здатних виконувати інформаційно-психологічні операції та оперативне інформування; удосконалити рівень підготовки фахівців із інформаційної безпеки та протидії засобам психологічного впливу» [350,с. 17]. Відтак вчений зазначає, що «виконання цих заходів дасть змогу зменшити конфронтацію між традиційними і новими центрами протистояння, унеможливить подальше маніпулювання суспільною свідомістю для досягнення широкомасштабної інформаційної експансії, сприятиме захисту інформаційного поля та інформаційній безпеці Української держави» [350,с. 17].

Прогресивна журналістська спільнота у цьому питанні солідарна з науковцями та вважає, що поряд із відродженням безпекового сектору, підвищенням обороноздатності ЗСУ серед державних пріоритетів має бути «системна україноцентрична гуманітарна політика», тобто дієвий інструментарій зміцнення солідарності українського суспільства, утвердження незалежної державності України, противаги російській гуманітарній агресії та слугувати [319].

Висновки до Розділу 6

Таким чином, в основі боротьби проти зовнішніх і внутрішніх інформаційно впливів та дестабілізаторів у розрізі зміцнення безпеки в інформаційній сфері в Україні в першу чергу лежить узгодження вітчизняного законодавства в інформаційній сфері з європейськими стандартами, а також здійснення контролю за безумовним його дотриманням. Не в останню чергу держава повинна активно розвивати інформаційні технології та забезпечувати умови для розвитку інформаційної інфраструктури. Активізація формування громадянського суспільства, яка відбулась нещодавно, повинна сприяти втіленню принципу безумовної правової рівності всіх учасників процесу інформаційної взаємодії незалежно від їх політичного, соціального та економічного статусу. В свою чергу саме це сприятиме тому, що обмеження доступу до інформації стане винятком із загального принципу відкритості інформації і здійснюватиметься тільки на основі законодавства. Лише законними засобами держава здатна забезпечити захист суспільства від неправдивої, перекрученої і недостовірної інформації, захистити національні інтереси. Запозичення досвіду провідних країн світу в інформаційній сфері, раціоналізована кадрова політика, активна співпраця з міжнародними структурами щодо протидії інформаційному тероризму, хакерству можуть суттєво змінити баланс сил в інформаційній війні, яку нині розгорнув агресор проти України.

ВИСНОВКИ

Відтак після визначення основних джерел, витоків і детермінант актуальності питань інформаційної безпеки були розглянуті й порівняні різні дискурсивні традиції і методи означення категорій «інформаційної безпеки», що розповсюджені в українському і зарубіжних філософсько-політичних дискурсах. Цілісно проаналізувавши інформаційну безпеку в інформаційній політиці України та впливових країн світу, ми можемо зробити деякі взаємопов'язані висновки з приводу основних принципів наших досліджень з цього питання та теоретичних та методологічних принципів

По-перше, розглянувши та систематизувавши основні джерела та детермінанти питань інформаційної безпеки, у дослідженні було якісно відображено актуальність і багатовимірність концептуальних та теоретичних розвідок й аналізу цього питання у сучасній філософії, політології та дискурсі національної безпеки. При цьому, головним фактором, який визначає актуальність питань інформаційної безпеки, є значне збільшення інформаційного потоку та комунікацій у глобальному масштабі. Таке зростання призвело до багатьох проблем і викликів у галузі національної безпеки, що вимагає постійних досліджень та пошуків. Інформаційне втручання на регіональному геополітичному рівні додає інших важливих небезпек. У той же час з інформаційними викликами стикаються всі – громадяни, суспільні групи, держави, людство тощо. Це спричиняє надзвичайну важкість концептуальних і теоретичних досліджень з питань інформаційної безпеки. У нашій роботі одним із базових методів, котрі були застосовані, є комплексний системний підхід, на підставі якого ми провели загальне і структурне дослідження питань інформаційної безпеки, з якими стикаються людство, суспільство і країна, в тому числі на прикладі України. Багатосуб'єктність у галузі інформації та безпеки визначає складність, важливість та актуальність дослідження проблеми з точки зору політичної науки та аналізу політичної безпеки.

По-друге, встановлено, що у сучасній політичній науці та політичному дискурсі, розглядаючи основні принципи та стандарти, які визначають поняття

«інформаційна безпека» у суспільстві, підкреслено надзвичайну розмаїтість і багатогранність цих категорій. Українські та зарубіжні науковці із цього питання визначили зміст категорії інформаційної безпеки, обговорили такі аспекти, як роль глобальної цивілізації, національна безпека та національна оборона, інформаційні та технічні параметри в рамках визначення безпеки, а також важливість інформаційної безпеки для кожної людини чи конкретної соціальної групи людей. Зважаючи на різноманітність методів, ключовою теорією і методологічним принципом нашого дослідження став принцип системності, що базується на всебічному, структурному і функціональному аналізі категорії «інформаційна безпека» та розглядає її окремішній, соціальний, національний і глобальні виміри. З огляду на це, особливої важливості набув комплексний фактор чи фактори, які поєднують інформаційну безпеку країни та суспільства із інформаційною, психологічною і світоглядно-феноменологічною безпекою людини й соціальних груп. На підставі теоретичних і методологічних засад вивчення питань інформаційної безпеки, ми дефініювали це поняття як різновид національної безпеки, що має на меті забезпечити вільний доступ до інформації, створення та впровадження захищених і цілком безпечних інформаційних технологій та захист прав інтелектуальної власності й інформаційної свободи для всіх учасників.

По-третє, внутрішня і міжнародна експертиза українського інформаційного законодавства свідчить, що воно відповідає європейським стандартам/вимогам. Однак, прийняті норми поки що мало відображаються у суспільно-політичних реаліях: відчутні недоліки загальної культури дотримання встановлених норм як політичними суб’єктами, інститутами державної влади різних рівнів так і широкими масами громадян. Окрім того ознаками правового унормування інформаційного простору України виступають: фактична відсутність правового регулювання функціонування в країні міжнародних інформаційних систем, серед яких Інтернет, відтак й труднощі діяльності для Інтернет- ЗМІ та загрози від окремих з них; суперечливі трактування у нормативно-правовому забезпеченні діяльності ЗМІ загалом; відсутність дієвих норм сприяння економічно незалежним медіа; не врегульований статус конфіденційної інформації. Одночасно говорячи

про формування правових основ і гарантій міжнародної інформаційної безпеки, слід визнати, що наразі можна засвідчити різні позиції провідних держав сучасності щодо розуміння новітніх потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства.

По-четверте, уніфіковані норми правового регулювання міжнародної інформаційної безпеки стають необхідністю нашого часу, що характеризується всеохоплюючою глобалізацією та потужними антиглобалізаційними рухами, зростанням гострих протистоянь між ними, в тому числі й у інформаційному просторі; порушенням територіальної цілісності і інформаційного суверенітету держав, поєднанням конвенційних і не конвенційних засобів сучасної війни; зрештою дрібними кіберзлочинами та масштабними хакерськими атаками, масованим інтелектуальним піратством. Особливий вплив на необхідність продовження напрацювання спільних стандартів регулювання міжнародної інформаційної безпеки мали інформаційна агресія Російської Федерації під час анексії Криму і фактичної війни в окремих частинах Донецької і Луганської областей, яка була спрямована не лише на громадян України, але і по відношенню до громадян Росії і цілого світу.

По-п’яте, провівши порівняльний аналіз питань інформаційної безпеки в контексті інформаційної політики України і впливових країн світу, було доведено потребу конструювання систематичної стратегії формування інформаційної та безпекової політики України. Сьогодні в нашій країні не існує системи інформаційної безпеки, що відповідає сучасним цивілізаційним і геополітичним викликам. Тому насправді управління безпекою інформації потрібно посилити у всіх сферах: в нагляді, організації та управлінні й інформаційних технологіях. Але спочатку існує дуже гостра необхідність у формулюванні чіткої стратегії трансформації сектору інформаційної безпеки країни та національного й громадянського суспільства. Ця стратегія повинна ґрунтуватися на міцній концепції, теорії, науці і практиці та формуватися у рамках національної політичної науки та дискурсу. А тому вивчення багатьох аспектів національної, соціальної та людської інформаційної безпеки є надзвичайно актуальним і важливим

завданням, яке сьогодні стоїть перед науковою спільнотою в нашій державі. Окрім новітніх викликів та реалій, що не врегульовані або не передбачені існуючим законодавством, не одне десятиріччя існують проблеми інформаційного простору, що потенційно становлять ризики і для інформаційної безпеки нашої держави. Серед них ми можемо виділити: 1) проблеми створення суспільного мовлення та приналежності засобів масової інформації фінансово-промисловим олігархічним групам; 2) проблеми законодавчого регулювання інформаційної діяльності в мережі Інтернет і поширення інформації у соціальних Інтернет-мережах; 3) проблеми авторського права за умов поширення Інтернет-технологій та ідентифікації джерел.

По-шосте, провівши деталізований концептуально-теоретичний аналіз суб'єкт-об'єктних характеристик інформаційної безпеки держави і соціуму, виділено декілька ключових активних груп, що визначають таку суб'єктність. До них насамперед відносяться держані органи, відповідальні за забезпечення інформаційної безпеки, політичних акторів національного поля (партії, лідери, активні лобістські групи тощо), громадські організації, асоціації, інституції, засоби масової інформації. При цьому, на нашу думку, суб'єкт-об'єктні відносини у системі інформаційної безпеки великою мірою залежать від діяльності державних структур загалом, а у контексті пропонованої проблематики – від інститутів інформаційної безпеки, які функціонують в системі державного управління й адміністрування**.** Держава задає загальну динаміку та правила роботи на інформаційному ринку країни, встановлює норми та обмеження для розвитку інформаційної демократії, захищає інформаційний простір не лише від загалом атак, але й конкретних суб'єктів інформаційного маніпулювання. У державній системі координат інформаційної безпеки кожен суб'єкт політики має знайти своє місце, якщо дбає про збереження цілісності країни, суверенітет держави, соціально-політичний розвиток суспільства, до якого належить.

По-сьоме, доведено, що власне на державу покладається головна відповідальність по забезпеченню інформаційної безпеки та координації зусиль всіх суб'єктів, причетних до імплементації функцій захисту інформаційного простору. Визначено, що існуюча інфраструктура державних інститутів інформаційної безпеки України мусить вибудовуватися за принципом стримувань і противаг,

важливо також, щоб державні органи постійно перебували під громадським контролем, були відкриті до комунікації зі ЗМІ, прозорі у своїх рішеннях та звітності, зрозумілі для міжнародних партнерів. В процесі аналізу партійної діяльності в контексті проблематики інформаційної безпеки, слід зазначити, що інформаційна безпека країни залежить від того, чиї інтереси представляє і захищає та чи інша політична партія, бо в її інформаційній політиці відображаються і пов'язуються інтереси країни, народу та партії. В цьому аспекті детально проаналізовано особливості діяльності державницьких та опозиційних політичних партій і рухів в інформаційному та технологічному вимірі, а також їхній вплив на безпеку особистості, держави та суспільства. Констатовано, що в Україні не існує спільного політичного розуміння відповідальності за інформаційну безпеку нації, держави, соціуму, а політичні сили готові жертвувати загальноукраїнськими інтересами заради досягнення тимчасових вузькопартійних цілей в процесі боротьби за владні, посадові повноваження. Перелік важливих та життєво необхідних для суспільства і політичної системи функцій, які покладаються на державу як суб'єкта інформаційної політики, є досить великим. Це і збереження інформаційного суверенітету держави, і попередження безконтрольного впливу на інформаційний простір, і захист та гарантії усім суб'єктам інформаційних відносин, і забезпечення прав людини та громадянина. Дії окремих державних органів чи посадовців можуть мати негативний інформаційний вплив на суспільство; шкоди завдає і неповна, невчасна, недостовірна комунікація державних діячів зі суспільством; поширеним є явище нераціонального застосування інформаційних технологій, порушення конфіденційності в держструктурах тощо. Раціональне та адекватне позиціонування держави на інформаційному ринку також може бути ускладнене відсутністю стратегічних пріоритетів і визначень у цій сфері, зрощуванням приватних інтересів окремих зацікавлених сторін із державними, надмірною електоральною залежністю (популізмом) високопосадовців, або ж навпаки – ігноруванням зв'язків з громадськістю, залежністю від іноземних суб'єктів тощо. Тобто йдеться на загал про комплекс проблем, пов'язаних з виробленням політики і її виконанням, що впливає на стан захищеності суспільства.

По-восьме, здійснивши загальний аналітичний огляд особливостей законодавчого врегулювання діяльності ЗМІ в Україні, а також визначивши ключову роль засобів масової інформації у розповсюдженні правдивої чи неправдивої інформації як чинник інформаційної безпеки суспільства й держави, доведено, що на особливу увагу заслуговує проблема фундаментальної відповідальності ЗМІ за інформаційну безпеку суспільства. В цьому контексті, ілюструється, що ЗМІ, будучи продуктом індустріального суспільства, в епоху інформаційного суспільства набувають нових якостей та характеристик. Мультимедійність, інтерактивність, можливість зворотного зв'язку та навіть діалог між великою кількістю користувачів, персоналізація, відсутність посередників, позагеографічність або позапросторовість інформаційно-комунікативних технологій перетворюють ЗМІ на доволі значущий чинник формування особистих позицій громадян і розвитку суспільства та демократичного життя. Водночас зростають маніпулятивні можливості ЗМІ та збільшуються ризики деструктивного впливу ЗМІ на перебіг суспільних процесів. Об'єктивна потреба у посиленні демократичного представництва і контролю через ЗМІ з одного боку, та запобіганні утвердження медіакратії (влади ЗМІ) з іншого боку, зумовлюють необхідність здійснення цілеспрямованої державної політики в інформаційній сфері, однією з важливіших складових якої є забезпечення інформаційної безпеки суспільства. Одночасно варто виокремити і проблемні результати діяльності ЗМІ: формування «масової» людини, розрив соціальних контактів, дезінтеграція суспільства, витіснення традицій, заміщення прямих контактів кібер-комунікаціями, байдужість, некритичність, де зорієнтованість, надмірна емоційність та навіть агресивність. Наявність одночасно багатьох джерел інформації, попри усі переваги на практиці досить часто виявляє лише доступ до суперечливих та взаємовиключних суджень.

По-дев'яте, визначивши протидію різноманітним інформаційно-дестабілізаційним впливам в зміцненні інформаційної безпеки держави чи суспільства ключовим завданням всіх відповідальних суб'єктів в цій сфері, сформульовані головні пріоритети, що постають перед всіма сторонами, що впливають на рівень інформаційної безпеки української держави і соціуму. Такими завданнями, зокрема,

ми окреслили: 1) диверсифікацію джерел інформації; 2) відкритість інформаційного простору та контроль за доступністю інформації; 3) протидію маніпулятивним впливам (засоби, технології, можливості); 4) адекватний захист та відповідь на підривну діяльність російських засобів масової інформації і завдання боротьби з ними інформаційних інститутів в Україні. Необхідно, щоб ініціативи держави та наддержавних інституцій щодо кібер- та інформаційної безпеки були достатньо розвинутими. Вони можуть носити різний характер – від антитерористичних дій спеціальних служб із правом застосування насильства до захисту вітчизняного мовного та культурного простору. Проте, для України важливо взяти на озброєння принаймні ті з них, які дозволять адекватніше відповідати на виклики інформаційної безпеки в умовах недомінантних умов у власному інформаційного простору. Крім того, важливо встановити чітку ієрархію інформаційно-безпекових принципів та цінностей (наприклад унормувати поняття, класифікувати та конкретизувати інформаційні загрози, вирішити дилему свободи розповсюдження інформації та запобіганні деструктивним інформаційним впливам), виробити чіткі норми та інструкції для органів безпеки, систематизувати правовий корпус в галузі інформаційних відносин та ієрархію державних інституцій, що їх забезпечують, а не створювати нові установи з повноваженнями, що дублюють одне одного. Тільки за умов чіткого визначення ключових пріоритетів інформаційної безпеки на держаному рівні, а також при нагальній розробці дієвих механізмів її забезпечення, у України з’явиться шанс на ефективну протидію зовнішнім та внутрішнім небезпекам інформаційної дестабілізації. Цим і зумовлена значна актуальність та важливість дослідницьких результатів, представлених в даному дисертаційному дослідженні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакумов В. Правове регулювання протидії інформаційним війнам в Україні: автореф. дис. ... канд. юрид. н. (спеціальність: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право). Запоріжжя, 2011. 22 с.
2. Абрамов Л. Інформаційний компонент діяльності НДО. Кіровоград: ІСКМ, 2009. 80 с.
3. Абрамов Л. Стратегія неполітичної громадської організації під час передвиборчої кампанії. Кіровоград: ЦПТІ, 2001. 120 с.
4. Абрамов Р. Сетевые структуры и формирование информационного общества // Социологические исследования. 2002. № 3. С. 133–140.
5. Авдієнко К. Німецьке суспільне мовлення як приклад для України // Суспільне. URL: https://stv.detector.media/dosvid/movnyky_svitu/nimetske_suspilne_movlennya_yak_dosvid_dlya_ukraini/
6. Авксентьєва Т. Політика і влада в інформаційну епоху: український контекст: монографія. Харків: ХНУ імені В.Н. Каразіна, 2013. 324 с.
7. Актуальні проблеми національної безпеки суспільства: монографія / за заг. ред. В.О. Ананьїна. Київ: НВФ «Славутич–Дельфін», 2008. 251 с.
8. Алешина И. Паблик рилейшнз для менеджеров и маркетеров. М.: Гном-Пресс, 1997. 255 с.
9. Алиева М. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. Вып. № 4 (108). С. 47–52.
10. Алтынбекова Г. Гендерное измерение политического участия: нове концепции и подходы // GWAnet. URL: http://www.gender.cawater-info.net/publications/articles.htm
11. Алямкін Р. Правове забезпечення національної інформаційної безпеки // Наукові записки Інституту законодавства Верховної Ради України. 2013. № 4. С. 91–96.

12. Ананьїн В., Пучков О. Інформаційна безпека як складова національної безпеки України // Гілея: науковий вісник: зб. наук. пр. 2014. Випуск 85 (6). С. 194−197.
13. Арквілл Дж. Мережі і мережеві війни: майбутнє терору, злочинності та бойових дій / пер. з англ. А. Іщенко; ред. Д. Арквілл, Д. Ронфельдт. Київ: вид-й дім «Києво-Могилянська академія», 2005. 352 с.
14. Архипова Є. Соціально-філософське осмислення поняття «інформаційна безпека» // Вісн. НТУУ «КПІ». Філософія. Психологія. Педагогіка. 2011. № 3. С. 7–11.
15. Астряб Н. Особливості фейкових процесів в українському суспільно-політичному просторі // Гілея: науковий вісник: зб. наук. пр. 2013. № 75. С. 491−493.
16. Бабіна В. Реклама як комунікативна технологія у політичному просторі // Політологічні записки. 2012. № 6. URL: http://nbuv.gov.ua/j-pdf/Polzap_2012_6_42.pdf
17. Балинський І. Політичні комунікації в УАНЕТі // Теле та радіожурналістика. 2011. № 10. С. 137–141.
18. Баранов А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. 2001. № 1 (13). С. 70−76.
19. Бень О. Політичний дискурс в уявленнях мешканців м. Львова про сучасні громадські організації // Український соціум. 2013. № 2 (45). С. 177−188.
20. Березовська І. Питання реформування законодавства в сфері забезпечення інформаційної безпеки України // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 1 (29). С. 307−312.
21. Бєльська Т. Комунікаційна взаємодія влади та громадськості в інформаційному суспільстві // Публічне управління: теорія та практика. 2012. № 3. С. 163–169.
22. Биктимирова З. Безопасность в концепции развития человека // Общественные науки и современность. 2002. № 6. С. 135−142.
23. Біла книга Держспецзв’язку // Державна служба спеціального зв'язку та захисту інформації України. URL: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941

24. Біловус Л. Український інформаційний простір: сьогодення та перспективи // Український інформаційний простір. 2013. Т. 1. Ч. 1. С. 188–191.
25. Богуш В. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.
26. Боднар І. Інформаційна безпека як основа національної безпеки // Механізм регулювання економіки. 2014. № 1. С. 68–75.
27. Бодрунова С. Современные стратегии британской политической коммуникации. М.: КМК, 2010. 424 с.
28. Бойченко О. Міжнародна інформаційна безпека: проблеми і перспективи // Форум права. 2009. № 3. С. 74–79.
29. Бойченко О. Міжнародне співробітництво правоохоронних органів держав в галузі забезпечення інформаційної безпеки // Форум права. 2009. № 2. С. 56–62.
30. Бойченко О. Політика інформаційної безпеки в системі інформаційного забезпечення органів внутрішніх справ // Форум права. 2009. № 1. С. 50−55.
31. Бондар Ю. Національний інформаційний простір новітньої України: становлення та функціонування у процесі політичної трансформації суспільства. Київ: МАУП, 2007. 271 с.
32. Борисова Л. Інформаційна безпека як визначальний компонент національної безпеки України // Право і безпека. 2013. № 1 (48). С. 39−42.
33. Брижко В. До питання сучасної інформаційної політики // Вісник Академії управління МВС. 2009. № 2. С. 27−47.
34. Бурило Ю. Участь недержавних суб’єктів у здійсненні державного управління інформаційною сферою // Правова інформатика. 2007. № 4. С. 31−41.
35. Бусленко В. Політична опозиція в перехідних демократіях: категоріальний аналіз феномену // Studia politologica Ucraino-Polona. 2013. № 3. S. 311−317.
36. Бутенко В. Лобізм: різновиди та перспективи легалізації в Україні // Політологічний вісник. 2003. № 3. С. 17−26.
37. Вайнштейн Г. Интернет как фактор общественных трансформаций // Мировая экономика и международные отношения. 2002. № 7. С. 16–27.

38. Вайнштейн Г. Мир в начале тысячелетия. Информационная революция и демократия: ожидания, реальность, перспективы // Мировая экономика и международные отношения. 2003. № 7. С. 13–21.
39. Вакулич В. Державна інформаційна політика як механізм реалізації інформаційної функції сучасної держави // Публічне управління: теорія та практика. 2014. Вип. 1. С. 97−107.
40. Варивода Я. Інформаційні стратегії у зовнішній політиці США та Росії за кризових умов: автореф. дис. ... канд. політ. н. (спеціальність: 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку). Київ. 2004. 21 с.
41. Вахрамєєва Н. Інтернет-комунікації у діяльності політичних партій // Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер.: Політологія. 2011. Т. 155. Вип. 143. С. 32−36.
42. Віннічук О. Особливості прояву політичного лобізму в Україні // Політологічні студії. 2013. Вип. 3. С. 21−29.
43. 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.
44. Воробьев Ю. Коммуникативное взаимодействие гражданского общества и структур публичной власти как управленческий процесс: автореф. дис…д-ра социол. н. (специальность: 22.00.08 – социология управления). М. 2008. 37 с.
45. Гаврилов Г. Модели политической оппозиции: теоретико-методологический анализ: автореф. дис. ...канд. полит. н. (специальность: 23.00.01 – теория политики, история и методология политической науки»). Екатеринбург. 2003. 24 с.
46. Галлін Деніел С. Сучасні медіасистеми: три моделі відносин ЗМІ та політики / Пер. з англ. О. Насика. Київ: Наука, 2008. 320 с.
47. Гіда О. Фактори, що впливають на формування викликів національним інтересам України в інформаційному просторі // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 2. С. 228−236.

48. Гіда О. Щодо основних засад формування державної інформаційної політики // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 1. С. 333−341.
49. Гідденс Э. Соціологія Київ: Основи, 1999. 726 с.
50. Глебова Н. Формування свободи й відкритості в глобальному інформаційному просторі // Соціологічні студії. 2013. № 2 (3). С. 22−27.
51. Горбань Ю. Сучасні виклики інформаційного простору для демократичної держави // Актуальні проблеми державного управління, педагогіки та психології: збірник наукових праць. 2013. Випуск 2. С. 36−41.
52. Горбулін В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ: Інтертехнологія, 2009. 164 с.
53. Горєлов Д. Аналітична записка відділу стратегій розвитку громадянського суспільства та протидії корупції // Уніан: інформаційне агенство. URL: http://human-rights.unian.net/ukr/detail/187585
54. Горєлов М. Цивілізаційна історія України. Київ: «ЕксОб», 2005. 632 с.
55. Грачев М. Демократия: методология исследования, анализ перспектив. М.: Изд-во «Алкигамма», 2004. 128 с.
56. Грачев М. Политическая коммуникация: теоретические концепции, модели, векторы развития М.: «Прометей», 2004. 328 с.
57. Грачев М. Политическое участие // Зарубежная политология: Словарь-справочник / Под ред. А. В. Миронова, Г. А. Цыганкова. М.: Социально-политический журнал, Независимый открытый университет, 1998. С. 239–241.
58. Григор'єв В. Інформаційна безпека у державному управлінні // Бібліотекознавство. Документознавство. Інформологія. 2013. № 4. С. 53−55.
59. Громико І. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам // Право України. 2008. № 8. С. 130–134.
60. Губерський Л. Інформаційна політика України: європейський контекст. Київ: Либідь, 2007. 360 с.
61. Гумінський Р. Віртуальні спільноти як суб'єкт інформаційної безпеки держави // Захист інформації. 2012. № 3 (56). С. 18–25.

62. Гурковський В. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання // Вісник УАДУ при Президенті України. 2002. № 3. С. 27−32.
63. Гурковський В. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дисертація на здобуття наукового ступеня кандидата юридичних наук (спеціальність: 25.00.02 – механізми державного управління). Київ. 2004. 225 с.
64. Гусаров В. Матриця інформаційної безпеки України // Інформаційно-аналітичний центр РНБО. 25 листопада 2014. URL: http://mediarnbo.org/2014/11/25/matritsya-informatsiynoyi-bezpeki-ukrayi/
65. Даниленко С. Громадянський вимір інформаційно-комунікаційної революції: концептуально-теоретичні та політико-прикладні аспекти: автореф. дис. ... докт. політ. н. (спеціальність: 23.00.03 – політична культура та ідеологія). Київ. 2011. 27 с.
66. Декларація принципів поведінки журналістів // Комісія з журналістської етики: офіційний сайт. URL: http://www.cje.org.ua/international/39/
67. Дем'янчук В. Культура безпеки людини – безпека суспільства в XXI столітті // Наукові записки Рівненського державного гуманітарного університету. Вип. 8 (51). Рівне: РДГУ. 2014. С. 42−46.
68. Денисюк С. Технологічні виміри політичної комунікації: монографія. Вінниця: ВНТУ, 2010. 276 с.
69. Держалюк О. Роль громадських організацій у реалізації виборчих прав громадян України // Національний інститут стратегічних досліджень. URL: www.old.niss.gov.ua›MONITOR/Juli08/14.htm
70. Держкомтелерадіо передав на розгляд уряду проект Указу Президента України «Про Доктрину інформаційної безпеки України» // Інформаційний портал Телекритика. URL: www.telekritika.ua›pravo/2014-11-20/100609
71. Дернер А. Политика как развлекательный жанр // Государственная информационная политика: Реферативный бюллетень. М. 2001. № 3(39). С.29–35.
72. Дзьобань О. Національна безпека України: концептуальні засади та світоглядний сенс: монографія. Х.: Майдан, 2007. 284 с.

73. Дзьобань О., Пилипчук В. Інформаційне насильство та безпека: світоглядно-правові аспекти: монографія / За заг. ред. проф. В. Г. Пилипчика. Харків: Майдан, 2011. 244 с.
74. Дзьобань О. Інформаційне насильство та безпека: світоглядно-правові аспекти: монографія. Харків: Майдан, 2011. 244 с.
75. Дзюндзюк В. Віртуальні співтовариства: потенційна загроза для національної безпеки // Державне будівництво. 2011. № 1.
76. Дмитренко М. Політична система України: розвиток в умовах глобалізації та інформаційної революції: монографія. Видання 2-ге з доп. та змінами. Київ:Університет «Україна», 2011. 820 с.
77. Добровольська А. Інформаційний простір: проблеми становлення нової якості національного росту // Наука України у світовому інформаційному просторі. 2010. Вип. 3. С. 61–70.
78. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201). Нью-Йорк: Организация Объединенных Наций. 2012. URL: https://namib.online/wp-content/uploads/2020/04/Report-of-the-UN-Group-of-Governmental-Experts-on-Developments-in-the-Field-of-Information-of-30-July-2010.pdf
79. Доктрина Інформаційної безпеки України: Затверджено Указом Президента України від 8 липня 2009 року № 514/2009 // Офіційна вебсторінка Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/514/2009#Text
80. Дорош Л. Інформаційно-психологічна безпека особи, суспільства та держави: новітні виклики міжнародній безпеці // Українська національна ідея: реалії та перспективи розвитку. 2013. Вип. 25. С. 107–112.
81. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция A/RES/54/49 ГА ООН // Нью-Йорк. Организация Объединенных Наций. URL: https://ifap.ru/ofdocs/un/5449.pdf
82. Дотримання інформаційних прав і свобод українських громадян: нормативно-правове забезпечення і регулятивні важелі: аналітична записка / С. Гнатюк //

Національний інститут стратегічних досліджень. 19 травня 2010 р. URL: http://www.niss.gov.ua/articles/231/

83. Дубас О. Інформаційний розвиток сучасної України у світовому контексті: політологічний аналіз: автореф. дис. ... канд. політ. н. (спеціальність: 23.00.02 – політичні інститути та процеси). Київ. 2004. 23 с.
84. Євдоченко Л. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: автореф. дис. ...канд. держ. управління (спеціальність: 25.00.01 − теорія та історія державного управління). Львів. 2011. 24 с.
85. Жовтенко Т. Інформаційне забезпечення політики держави у боротьбі з міжнародним тероризмом: на прикладі США: автореф. дис. ...канд. політ. н. (спеціальність: 21.01.01 – основи національної безпеки держави). Київ. 2010. 22 с.
86. Забара І. Міжнародна інформаційна безпека в міжнародному праві: до питання визначення // Український часопис міжнародного права. 2012. № 4. С. 63–69.
87. Забара І. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві // Теорія і практика правознавства. 2013. Вип. 2.
88. Заббаров А. Сетевые структуры общественных объединений в современном политическом процессе: дис. ...канд. полит. наук (23.00.02 – политические институты и процесы, технологии). Саратов: Поволжская акад. гос. службы им. П.А. Столыпина. 2011. 195 с.
89. Задорожня Л. Питання вдосконалення законодавства України у сфері інформації та інформатизації // Додаток до наук. журналу «Правова інформатика». Київ: Академія правових наук. 2005. 31 с.
90. Зайцев М. Суб’єкти забезпечення інформаційної безпеки України // Форум права. 2013. № 3. С. 231–238.
91. Закон України «Про телекомунікації» // Відомості Верховної Ради України. 2004. № 12. С. 155.
92. Закон України «Про телебачення і радіомовлення» // Відомості Верховної Ради України. 1994. № 10. С. 43

93. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (Із змінами, внесеними згідно із Законом № 1313-VII від 05.06.2014) // Відомості Верховної Ради України. 2014. № 29. С. 946.
94. Закон України «Про державну таємницю» // Відомості Верховної Ради України. 1994. № 16. С. 93.
95. Закон України «Про доступ до публічної інформації» // Відомості Верховної Ради України. 2011. № 32. С. 314.
96. Закон України «Про друковані засоби масової інформації (пресу) в Україні» // Відомості Верховної Ради України. 1993. № 1. С. 1.
97. Закон України «Про засади запобігання і протидії корупції» // Відомості Верховної Ради України. 2011. № 40. С. 404.
98. Закон України «Про захист персональних даних» // Відомості Верховної Ради України. 2010. № 34. С. 481
99. Закон України «Про захист суспільної моралі» // Відомості Верховної Ради України. 2004. № 14. С. 192.
100. Закон України «Про звернення громадян» // Відомості Верховної Ради України. 1996. № 47. С. 256.
101. Закон України «Про інформацію» // Відомості Верховної Ради України. 1992. № 48. С. 650.
102. Закон України «Про Концепцію Національної програми інформатизації» // Відомості Верховної Ради. 1998. № 27−28. С. 182.
103. Закон України «Про Національну раду України з питань телебачення і радіомовлення» (із змінами, внесеними згідно Закону N 1222-VII (1222-18) від 17.04.2014 // Відомості Верховної Ради. 2014. № 26. С. 895.
104. Закон України «Про оборону України» (із змінами, внесеними згідно Закону № 1194-VII від 09.04.2014) // Відомості Верховної Ради. 2014. № 25. С. 890.
105. Закон України «Про основи національної безпеки» // Відомості Верховної Ради України. 2003. № 39. С. 351.
106. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» // Відомості Верховної Ради. 2007. № 12. С. 102.

107. Закон України «Про Службу зовнішньої розвідки України» // Відомості Верховної Ради України. 2006. № 8. Ст. 94.
108. Закон України «Про телебачення і радіомовлення» // Відомості Верховної Ради України. 1994. № 10. С. 43.
109. Закон України «Про громадянські об'єднання» // Відомості Верховної Ради України. 2013. № 1. С. 1.
110. Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» // Відомості Верховної Ради України. 1997. № 50. С. 302.
111. Закон України «Про друковані засоби масової інформації (пресу) в Україні» // Відомості Верховної Ради України. 1993. № 1. С. 1.
112. Закон України «Про інформаційні агентства» // Відомості Верховної Ради України. 1995. № 13. С. 83.
113. Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в України засобами масової інформації» // Відомості Верховної Ради України. 1997. № 49. С. 299.
114. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. 2003. № 39. С. 351.
115. Закон України «Про Суспільне телебачення і радіомовлення України» // Відомості Верховної Ради. 2014. № 27. С. 904.
116. Зернецька О. Засоби масової комунікації в сучасній світовій політичній ситуації // Соціальна психологія. 2009. № 2. С. 24−28.
117. Золотар О. Класифікація загроз інформаційної безпеки // Інформація і право. 2013. № 3 (9). С. 105−112.
118. Зубар В. Роль сучасних суспільно-політичних рухів у розвитку української державності // Українська національна ідея: реалії та перспективи розвитку. 2014. Вип. 26. С. 65−70.
119. Ільганаєва В. Теоретико-методологічний синтез соціально-комунікаційного знання // Філософія спілкування: філософія, психологія, соціальна комунікація. 2009. № 2. С. 96–101.

120. Інтерв'ю керівника Міністерства інформації Ю. Стеця від 3.12.2014 телеканалу Еспресо TV «У новоствореному Міністерстві інформації України буде створено кілька департаментів, які займуться розробкою концепції інформаційної політики країни» // Еспресо TV. URL: https://espreso.tv/news/2014/12/03/stec_rozpoviv__chym_bude_zaymatysya_ministerstvo_informaciyi
121. Інформаційна безпека (соціально-правові аспекти): підручник. Київ: КНТ, 2010. 776 с.
122. Інформаційне законодавство: збірник законодавчих актів у 6 т. / За заг. ред. Ю. Шемшученка, І. Чижа. Т. 5. Міжнародно-правові акти в інформаційній сфері. Київ: ТОВ «Видавництво «Юридична думка», 2005. 328 с.
123. Історія інформаційно-психологічного протиборства: підручник / За заг. ред. Є. Скулиша. Київ: Науково-видавничий відділ НА СБ України, 2012. 212 с.
124. Калюжний Р. Інформаційне право України: концептуальні основи формування // Науковий вісник Дніпропетровського юридичного інституту МВС України. № 3 (6). 2001. С. 234–244.
125. Карлова В. Вплив засобів масової інформації на формування української національної свідомості // Національна академія державного управління при Президентові України. URL: http://academy.gov.ua/ej/ej6/txts/07kvvunc.htm
126. Карпенко В. Інформаційна політика та безпека: підручник. К.: Норапрінт, 2002. 348 с.
127. Карпенко В. Інформаційний простір як чинник національної безпеки України // Українознавство: Науковий громадсько-політичний культурно-мистецький релігійно-філософський педагогічний журнал. 2005. № 3. С. 182–192.
128. Карпець Ю. Вплив як форма та результат взаємодії суб'єктів політики // Актуальні проблеми політики. 2013. Вип. 50. С. 252−261.
129. Карпова М. Социология массовой коммуникации: учебно-методическое пособие. Пенза: Изд-во ПГУ, 2011. 128 с.
130. Карчевський М. До питання визначення інформаційної безпеки як об'єкта кримінально-правової охорони // Боротьба з організованою злочинністю і

корупцією (теорія і практика). Науково-практичний журнал. 2012. № 1 (27). С. 267−272.

131. Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под научн. ред. О.И. Шкаратана. М.: ГУ-ВШЭ, 2000. 608 с.
132. Кафарський В. Політичні партії та групи тиску: проблеми взаємодії та правове регулювання // Університетські наукові записки. 2006. № 2 (18). С. 403−410.
133. Каштелян С. Сутність та зміст поняття «безпека» у контексті забезпечення національної безпеки України у прикордонній сфері // Честь і закон. 2013. № 1 (44). С. 17−21.
134. Кирильчук Є. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції // Наукові праці МАУП. 2013. Вип. 1 (36). С. 60–63.
135. Кирильчук Є. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції // Наукові праці МАУП. 2013. Вип. 1 (36). С. 60−63.
136. Кіндратець О. Українська інтелігенція і влада // Політичний менеджмент. 2009. № 2. С. 46−55.
137. Кісілевич-Чорнойван О. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять // Юриспруденція: теорія і практика. 2009. № 8. С. 11–18.
138. Коваль З. Політико-правові механізми державного управління інформаційно-психологічною безпекою України: автореф. дис. ... канд. н. з держ. упр. (спеціальність: 25.00.02 – механізми державного управління). Одеса. 2011. 22 с.
139. Кодекс етики українського журналіста // Комісія з журналістської етики: Офіційний сайт. URL: https://www.cje.org.ua/ua/code
140. Кодекс професійної етики українського журналіста. Прийнятий на X з'їзді Національної спілки журналістів України (квітень 2002 року) // Комісія з журналістської етики: Офіційний сайт. URL: https://www.cje.org.ua/ua/code
141. Колісник В. Демократія в Україні після і до реформи // Українська правда. 19 жовтня 2010. URL: https://www.pravda.com.ua/articles/2010/10/19/5492052/

142. Колісніченко Н. Медіа-навчання суб'єктів політичної діяльності: світовий досвід та уроки для України // Наукові праці [Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»]. Сер.: Державне управління. 2010. Т. 125. Вип. 112. С. 106−111.
143. Конах В. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): автореф. дис. ...канд. політ. н. (спеціальність: 21.01.01 – основи національної безпеки держави). Київ. 2005. 20 с.
144. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
145. Конституція України // Відомості Верховної Ради України. 1996. № 30. С. 141.
146. Концепція (основи державної політики) національної безпеки України: Схвалено постановою Верховної Ради України від 16.01.1997 // Урядовий кур'єр. URL: http://zakon4.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80
147. Концепція реформування законодавства України у сфері суспільних інформаційних відносин // Науково-дослідний інститут інформатики і права Національної академії правових наук України. URL: http://ndcpi.org.ua/jurnal/16_12.htm
148. Кормич Б. Інформаційна безпека: організаційно-правові основи: навч. посібн. Київ: Кондор, 2008. 382 с.
149. Кормич Б. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ...докт. юрид. н. (спеціальність: 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право). Харків. 2004. 42 с.
150. 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.
151. Корнієвський О. Громадські об'єднання як суб'єкт політики національної безпеки: постановка проблеми // Стратегічні пріоритети. 2009. №1 (10). С. 44–51.
152. Корольов М. Проблематика дослідження питань інформаційної безпеки у державному управлінні // Вісник Східноукраїнського національного університету ім. В. Даля. 2013. № 15(1). С. 88–92.

153. Косогов О. Методика визначення пріоритетів показників, що характеризують рівень загроз інформаційній безпеці держави // Збірник наукових праць Харківського університету повітряних сил. 2014. Вип. 2 (39). С. 163−166.
154. Кравець Є. Інформаційна безпека держави // Юридична енциклопедія: У 6 т. / Ред. кол.: Ю. Шемшученко (голова редкол.) та ін. Київ: Укр. Енцикл., 1998–1999. Т. 2. С. 714–715.
155. Красноступ Г. Правове регулювання «Інтернет – засобів масової інформації» // Міністерство юстиції України. URL: http://www.minjust.gov.ua/24640
156. Крилова Н. Підходи до визначення і розуміння поняття «інформаційна безпека» в рамках національного безпекознавства // Гілея: науковий вісник: зб. наук. пр. 2010. Вип. 36. С. 423−428.
157. Крутов В. Щодо правового статусу структур недержавного сектору національної безпеки України // Проблеми боротьби зі злочинністю. 2009. № 2 (57). С. 161−168.
158. Крюков О. Інформаційна безпека держави в умовах глобалізації // Державне будівництво. 2007. № 2.
159. Кудрявцева С. Міжнародна інформація: навч. посібник. Київ: Слово, 2005. 400 с.
160. Курочкин А. Политика в условиях сетевого общества: новая структура и содержание // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: Грамота, 2011: в 3-х ч. Ч. II. С. 113–117.
161. Лазарев Г. Защита информации в информационно-теле-комуникационных системах // Національна безпека і оборона. 2001. № 1. С. 80–83.
162. Лазаревич А. Глобальное коммуникацинное общество. Минск: Белорусская наука, 2008. 350 с.
163. Лантінов Я. Щодо визначення національної безпеки України як об’єкта кримінально-правової охорони // Форум права. 2011. № 1. С. 570–574.
164. Левченко О. Проблеми і шляхи формування системи інформаційної безпеки держави // Збірник наукових праць Харківського університету повітряних сил. 2014. Вип. 2 (39). С. 166−168.

165. Литвиненко О. Інформація і безпека // Нова політика. 1998. № 1. С. 47−49.
166. Литвиненко О. Спеціальні інформаційні операції: монографія. Київ: НІСД, 1999. 148 с.
167. Ліпкан В. Національна безпека України: навч. посібник. Київ: Кондор, 2008. 552 с.
168. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. Київ: КНТ, 2006. 280 с.
169. Ліпкан В. Національна безпека України: навч.посібник. 2-ге вид. Київ: КНТ, 2009. 576 с.
170. Лісовська Ю. Адміністративно-правова діяльність недержавних органів та організацій як структурних елементів системи забезпечення інформаційної безпеки // Наукові праці МАУП. 2014. Вип. 2 (41). С. 108–113.
171. Логінов О. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: автореф. дис. ... канд. юрид. н. (спеціальність: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право). Київ: Національна академія внутрішніх справ України. 2005. 22 с.
172. Ломоносов М. Суспільне мовлення: українське бачення // MyMedia URL: http://www.mymedia.org.ua/articles/psb/susp_lne_movlennya_ukra_nske_bachennya.html
173. Лопатин В. Информационная безопасность России: Человек. Общество. Государство. СПб.: Фонд «Университет», 2000. 428 с.
174. Макаренко Є. Міжнародна інформаційна політика: структура, тенденції, перспективи: автореф. дис. ...докт. політ. н. (спеціальність: 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку). Київ, 2002. 22 с.
175. Макаренко Є. Політичні доктрини глобальної інформаційної безпеки // Вісник Інституту міжнародних відносин Київського національного університу ім. Т. Шевченка. 2007. № 2. С. 45–51.
176. Маклюэн М. Понимание Медиа: Внешнее расширение человека / Пер. с анг. В. Николаева. М. Жуковский. «Какон-пресс-Ц»; «Кучково поле», 2003. 464 с.

177. Максименко Ю. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис. ...канд. юрид. н. (спеціальність: 23.00.01 − теорія та історія держави і права, історія політичних і правових учень). Київ. 2007. 22 с.
178. Малик І. Народження «Доктрини інформаційної безпеки України»: від теорії до практики // Українська національна ідея: реалії та перспективи розвитку: Збірник наукових праць. Львів: Видавництво Львівської політехніки, 2010. Вип. 22. С. 76−81.
179. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду // Ефективність державного управління: збірник наукових праць Львівського регіонального інституту державного управління НАДУ при Президентові України. 2012. Вип. 32. С. 20−27.
180. Мамадьярова Р. Информационная безопасность, ее сущность, структура и обеспечение в конфликтных ситуациях // Гілея: науковий вісник: зб. наук. пр. 2012. Вип. 56 (1). С. 591−594.
181. Мамука С. Особливості формування державної регуляторної політики у сфері телебачення і радіомовлення в Україні // Державне управління: теорія та практика. 2010. № 1. С. 118–128.
182. Манойло А. Государственная информационная политика в особых условиях: монография. М.: МИФИ, 2003. 388 с.
183. Мануйлов Є. Право громадян на свободу об'єднання в політичні партії: філософський аналіз // Вісник Національної юридичної академії України імені Ярослава Мудрого. Сер.: Філософія, філософія права, політологія, соціологія. 2013. № 5. С. 15−23.
184. Марков В. Актуальні проблеми інформаційної безпеки України в системі міжнародної координації // Право і Безпека: Науковий журнал. 2013. № 1 (48). С. 78−80.
185. Марущак А. Інформаційне право: Доступ до інформації: навч. посібник. Київ: КНТ, 2007. 532 с.
186. Масловська О. Політична культура опозиції в умовах становлення демократії // Політологічні записки. 2012. № 6.

187. Матвійчук А. Громадські організації як чинник становлення громадянського суспільства: автореф. дис. …канд.. політ. н. (спеціальність: 23.00.02 – політичні інститути і процеси). Київ: Київський національний університет ім. Т. Шевченка. 2008. 20 с.
188. Махлуп Ф. Производство и распространение знаний в США. М.: Прогресс, 1966. 462 с.
189. Медиакратия: современные теории и практики / под ред. А. Пую, С. Бодруновой. СПб: Издательство Санкт-Петербургского университета, 2013. 352 с.
190. Морозов О. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності // Віче. 2007. Том 1. № 12. С. 23−25.
191. Мяснікова Е. Межа між захистом та утиском дуже мала // Незалежна асоціація телерадіомовників. URL: http://www.nam.org.ua/
192. Нагорна Л. Політична культура українського народу: історична ретроспектива і сучасні реалії Київ: Стилос, 1998. 278 с.
193. Назарчук А. Социальные сети и трансформация политического порядка // Вестник аналитики. 2007. № 30 (4). С. 108−128
194. Наливайко Л. Інформаційна безпека та інформаційна політика в Україні: конституційно правовий аспект // Вісник Запорізького державного університету. Сер.: Юридичні науки. 2003. № 1. С. 60–65.
195. Національна стратегія розвитку сфери інтелектуальної власності в Україні на період до 2020 р. // Ліга-Закон. URL: https://ips.ligazakon.net/document/NT1009
196. Національний реєстр електронних інформаційних ресурсів України. URL: https://e-resources.gov.ua/#/
197. Нашинець-Наумова А. Теоретико-правові основи забезпечення інформаційної безпеки українського суспільства // Вісник Національного технічного університету України «Київський політехнічний інститут». Сер.: Політологія. Соціологія. Право. 2013. № 4. С. 124–127.
198. Несвіт Г. Інформаційна політика держави як фактор реформування суспільства: автореф. дис. ...канд. політ. н. (спеціальність: 23.00.02 − політичні інститути і процеси). Одеса. 2001. 19 с.

199. Нестеренко Г. Політична участь як основна форма реалізації влади громадських організацій // Громадські організації у дискурсі демократизації суспільства: монографія / Нац. пед. ун-т ім. М. П. Драгоманова; за ред. В. Беха. Київ: Вид-во НПУ ім. М. П. Драгоманова. 2011. С. 550–574.
200. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз // Публічне управління: теорія та практика. 2014. Вип. 1. С. 62−67.
201. Нестеряк Ю. Законодавче врегулювання відносин влади і засобів масової комунікації: принципи та механізми на основі узагальнення міжнародного досвіду // НАДУ. URL: http://www.academy.gov.ua/ej/ej14/txts/Nesteryak.pdf
202. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз // Вісник Національної академії державного управління при Президентові України. Науковий журнал. 2013. № 3. С. 40−45.
203. Ніколаєнко Н. Форми застосування адміністративного ресурсу в контексті виборчої кампанії // Гілея: науковий вісник: зб. наук. пр. 2010. Вип. 41 (11). С. 474–482.
204. Окінавська хартія глобального інформаційного суспільства / Міжнародний документ від 22.07.2000 // Офіційний сайт Верховної Ради України. URL: http://zakon2.rada.gov.ua/laws/show/998_163
205. Олійник О. Адміністративно-правові засади інформаційної безпеки // Європейські перспективи. 2012. № 4 (1). С. 65–68.
206. Олійник О. Позитивні та негативні впливи інформаційної революції на забезпечення інформаційної безпеки особи, суспільства, держави // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2011. Вип. 25–26. С. 321–328.
207. Олійник О. Стан забезпечення інформаційної безпеки в Україні // Юридичний вісник. Повітряне і космічне право. 2014. № 2. С. 59–65.
208. 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.

209. Орлов С. Політична культура як основа формування парламентаризму // Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право. 2013. № 3. С. 31−34.
210. Отрешко В. Інформаційна безпека в контексті мовних пріоритетів українського державотворення // Гілея: науковий вісник: зб. наук. пр. 2014. Вип. 89 (10). С. 319−323.
211. Павлюк К. Діяльність неурядових громадських організацій у контексті забезпечення національної безпеки України // Вісник Національної академії державного управління при Президентові України. 2012. № 2. С. 210−218.
212. Пазюк А. Питання міжнародного інформаційного права: предмет, завдання та принципи // Український часопис міжнародного права. 2013. № 1. С. 46−50.
213. 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.
214. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи // Юридичний журнал. 2009. № 5. С. 122–134.
215. Петрицький А. Інформаційне законодавство України: актуальні проблеми та шляхи їх вирішення // Вісник Маріупольського державного університету. Серія: Право. 2013. Вип. 5. С. 64−68.
216. Петров В. Воєнно-інформаційна безпека України за умов посилення загроз інформаційних війн: автореф. дис. ...канд. політ. н. (спеціальність: 21.01.01 − основи національної безпеки держави). Київ. 2010. 24 с.
217. Плахтій Т. Перетворення Євромайдану в громадсько-політичний рух і навпаки // Дзеркало тижня. 20.12.2013. URL: https://zn.ua/ukr/internal/peretvorennya-yevromaydanu-v-gromadsko-politichniy-ruh-i-navpaki-_.html
218. Пода Т. Інформаційно-комунікаційні технології в контексті сучасних міжнародних відносин: соціально-філософський аналіз // Вісник Національного авіаційного університету. Серія: Філософія. Культурологія: Збірник наукових праць. Київ: НАУ. 2013. С. 59−63.

219. Полевий В. Що захищаємо в інформаційній війні та хто за це відповідає? // Рідна країна: світоглядний портал. 15 жовтня 2014 року.
220. Попов С. Проблеми інформаційної безпеки України // Форум права. 2011. № 1. С. 798–801.
221. Поппер К. Открытое общество и его враги. Т. 1: Чары Платона / Пер. с англ. под ред. В. Садовского. М.: Феникс. Международный фонд «Культурная инициатива», 1992. 448 с.
222. Постанова Верховної Ради України «Про Рекомендації парламентських слухань на тему «Законодавче забезпечення розвитку інформаційного суспільства в Україні» від 3 липня 2014 р. № 1565-VII. // Відомості Верховної Ради. 2014. № 33. С. 1163.
223. Почепцов Г., Чукут С. Інформаційна політика: навч. посіб.: 2-ге вид. К., 2008. 663 с.
224. Правосвідомість і правова культура як базові чинники державотворчого процесу в Україні: монографія. Харків: Право, 2009. 352 с.
225. Прасюк О. Маніпуляція свідомістю виборців як комунікативна технологія здобуття політичної влади // Збірник наукових праць ЛНУ ім. І. Франка. Львів. 2009. С. 246–255.
226. Примуш М. Ідеологічна криза українських політичних партій // Вісник Національної юридичної академії України імені Ярослава Мудрого. Сер.: Філософія, філософія права, політологія, соціологія. 2014. № 1. С. 195−202.
227. Присяжнюк М. Інформаційна безпека України в сучасних умовах // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 42−46.
228. Проблеми інформаційного законодавства України в сфері створення, поширення та використання інформації та шляхи їх вирішення: Аналітична записка // НІСД. 07.06.2013. URL: http: http://www.niss.gov.ua/articles/1189
229. Пронюк Н. Національне законодавство і його роль у демократичних перетвореннях в Україні: дис. … канд. юрид. наук (спеціальність: 12.00.01 – теорія та історія держави і права; історія). Київ. 2003. 201 с.

230. Проскуріна О. Інформаційна стратегія України в сучасному геополітичному просторі // Політичний менеджмент. 2009. № 3. С. 137–144.
231. Пугачев В. Введение в политологию: учебник для студентов вузов. 4-е изд., перераб. и доп. М.: Аспект Пресс, 2004. 479 с.
232. Рада Європи. Рекомендація № R (97) 19 «Про показ насильства електронними ЗМІ» (ухвалена Комітетом міністрів 30 жовтня 1997 року на 607'му засіданні заступників міністрів) // Стандарти Ради Європи у сфері медіа: Законодавчий бюлетень. К. 2005. URL: http://www.archives.gov.ua/International/R_E_final.pdf
233. Рада Європи. Парламентська асамблея. Резолюція 1003 (1993) Про етичні принципи журналістики // Стандарти Ради Європи у сфері медіа. К. 2005. URL: https://old.archives.gov.ua/International/R_E_final.pdf
234. Рада Європи. Парламентська асамблея. Резолюція 1120 (1997) «Про вплив нових комунікативних та інформаційних технологій на демократію» // Стандарти Ради Європи у сфері медіа: Законодавчий бюлетень. К. 2005. URL: https://old.archives.gov.ua/International/R_E_final.pdf
235. Рада Європи. Парламентська асамблея. Резолюція 1276 (1995) «Про силу візуальних образів» // Стандарти Ради Європи у сфері медіа. К. 2005. URL: https://old.archives.gov.ua/International/R_E_final.pdf
236. Рада Європи. Резолюція № 2 «Свободи журналістів і права людини» // 4-та Європейська конференція міністрів з питань політики в галузі ЗМІ «ЗМІ в демократичному суспільстві» (Прага, 7−8 грудня 1994 року) // Стандарти Ради Європи у сфері медіа: Законодавчий бюлетень. К. 2005. URL: https://old.archives.gov.ua/International/R_E_final.pdf
237. Радковець Ю. Погляди на створення системи інформаційної безпеки України та її Збройних Сил // Наука і оборона. 2014. № 1. С. 38−42.
238. Резолюція учасників науково-практичної конференції «Професійні стандарти та етика в журналістському середовищі України: проблеми і перспективи» // URL: http://nsju.dp.ua/profesijni-standarti-ta-etika-v-zhurnalistskomu-seredovishhi-ukrayini-problemi-i-perspektivi.html

239. Рекомендація Комітету міністрів Ради Європи № R (99) 15 // Верховна Рада України: офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/994_726#Text
240. Романчук Ю. Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти: автореф. дис. ...канд. політ. н. (спеціальність: 23.00.04 − політичні проблеми міжнародних систем та глобального розвитку). Київ. 2009. 16 с.
241. Рубан Ю. Україна як суб'єкт і об'єкт сучасних міжнародних інформаційних воєн // Стратегічні пріоритети. 2009. № 2 (11).С. 5−9.
242. Руденко В. Новые Афины, или электронная республика. О перспективах развития прямой демократии в современном обществе // Полис. 2006. № 4. С. 7–16.
243. Рудницька Т. «Інтернетизація» і «вестернізація» життєвого світу особистості в Україні // Соціологія: теорія, методи, маркетинг. 2002. № 2. С. 32–45.
244. Руснак О. Медіа-інформаційна безпека України: правові аспекти // Стратегічні пріоритети. 2013. № 3. С. 147–150.
245. Сагайдак О. Інформаційна безпека України в умовах глобалізаційних викликів // Вісник Луганського національного університету ім. Т. Шевченка. Соціологічні науки. 2010. № 12. Т. 2 (2). С. 115–125.
246. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки // Сайт Інституту журналістики КНУ імені Тараса Шевченка. URL: http://www.journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.
247. Сердюк Є. Адміністративні процедури у сфері забезпечення виборчих прав громадян // Форум права. 2012. № 1. С. 874–877.
248. Сіленко А. Медіаполітика: сутність поняття // Актуальні проблеми політики. 2013. Вип. 50. С. 156–164.
249. Смелзер Нейл Дж. Проблеми соціології. Георг-Зімелівські лекції, 1995. Львів: Кальварія, 2003. 128 с.
250. Смола Л. Інформаційно-психологічні детермінанти сучасного політичного процесу (світовий та вітчизняний контексти): автореф. дис. ...докт. політ. н. (спеціальність: 23.00.01 − теорія та історія політичної науки). Львів, 2011. 34 с.

251. Соловей А. Політична культура сучасного українського суспільства (теоретико-методологічні виміри та суспільна практика) // Панорама політологічних студій. 2012. Вип. 9. С. 26–32.
252. Соловьев А. Политическая комуникация: учеб. пособие для студентов вузов. М.: Аспект Пресс, 2004. 332 с.
253. Сопілко І. Роль доктрини інформаційної безпеки України в реалізації державної інформаційної політики України // Журнал східноєвропейського права. 2014. № 2. С. 36–42.
254. Степко О. Інформаційна діяльність ООН: автореф. дис. ...канд. політ. н. (спеціальність: 23.00.04 − політичні проблеми міжнародних систем та глобального розвитку). Київ. 2004. 17 с.
255. Субіна Т. Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України: автореф. дис. ...канд. юрид. н. (спеціальність: 12.00.07 − адміністративне право і процес; фінансове право; інформаційне право). Ірпінь. 2010. 24 с.
256. Терепищий С. Футурология как предмет социальной философии // Studia Warmińskie. 2015. Vol. 52. S. 63–74.
257. Терепищий С. Ідентичність сучасних освітніх ландшафтів в контексті проблем інтернаціоналізації // Гілея: науковий вісник. 2016. Вип. 105. С. 219–223.
258. Терепищий С. Оппозиционные принципы и аргументы антиглобализма: мир перед угрозой кризиса // Studia Warmińskie. 2014. Vol. 51. S. 53–63.
259. Тимощук В. Нові виклики часу. Відповідальність за поширення інформації в Інтернеті // Юрінком Інтер.
URL: https://yurincom.com/legal_practice/analitychna_yurysprudentsiia/novi-vyklyky-chasu-vidpovidalnist-za-poshyrennia-informatsii-v-interneti/
260. Тихомиров О. Класифікації забезпечення інформаційної безпеки // Вісник Запорізького національного університету. Сер.: Юридичні науки. 2011. № 1. С. 164–168.
261. Тоффлер Е. Метаморфозы власти: знание, богатство и сила на пороге XXI в. / Пер. с англ. Белокосков В. и др. М.: АСТ, 2001. 670 с.

262. Триняк В. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз): автореф. дис. ...канд. філос. н. (спеціальність: 09.00.03 − соціальна філософія та філософія історії). Дніпропетровськ. 2009. 24 с.
263. Указ Президента України «Про Доктрину інформаційної безпеки України» від 08 липня 2009 р. // Верховна Рада України: офіційний стайт. URL: http://zakon2.rada.gov.ua/laws/show/514/2009
264. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28.04.2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»» від 1 травня 2014 // Верховна Рада України: офіційний стайт. URL: http://www.president.gov.ua/documents/17588.html
265. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»» від 25 лютого 2017 року // Верховна Рада України: офіційний стайт. URL: http://www.president.gov.ua/documents/472017-21374
266. Українська політична нація: ґенеза, стан, перспективи / За ред. В. Крисаченка. К.: НІСД, 2004. 648 с.
267. Українчук В. Забезпечення національної безпеки в умовах формування в Україні громадянського суспільства. Харків: Ун-т внутр. справ, 1996. 164 с.
268. Укрепление международного мира, безопасности и международного сотрудничества во всех его аспектах в соответствии с Уставом ООН. Резолюция A/RES/44/21 ГА ООН // Official Documents System of the United Nations. URL: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/44/21&Lang=R
269. Фань Ч. Правове забезпечення інформаційної безпеки в системі сучасної міжнародної співпраці // Наукові праці МАУП. 2012. Вип. 4 (35). С. 110–115.
270. Федорук О. Концептуальні засади формування системи забезпечення національної інформаційної безпеки // Вісник соціально-економічних досліджень. 2013. Вип. 2 (1). С. 182–188.
271. Федотова Л. Социология массовых коммуникаций: учебник для вузов. СПб.: Питер, 2003. 400 с.

272. Харченко Л. Інформаційна безпека України: Глосарій. Київ: Текст, 2004. 136 с.
273. Хімей В. Основні сучасні проблеми інформаційної безпеки України // Теле- та радіожурналістика. 2014. Вип. 13. С. 127–132.
274. Хорішко Л. Регіональний аспект формування іміджу політичних партій // Політичний менеджмент. 2009. № 6. С. 85–93.
275. Хуан Ц. Інформаційна політика Китайської Народної Республіки в сучасних міжнародних відносинах: автореф. дис. ...канд. політ. н. (спеціальність: 23.00.03 − політична культура та ідеологія). Киіів. 2007. 14 с.
276. Царенко О. Політична культура як чинник впливу на політичну поведінку громадян // Панорама політологічних студій. 2013. Вип. 10. С. 176−182.
277. Цивільний кодекс України // Відомості Верховної Ради України. 2003. № 40−44. С. 356.
278. Цимбалюк В. Інформаційне право (основи теорії і практики): монографія. Київ: Освіта України, 2010. 388 с.
279. Цуладзе А. СМИ в системе диалога партий и социальных групп в контексте формирования в обществе установок толерантности. URL: http://dzyalosh.ru/01-comm/statii/culadze-02/pol.html
280. Чабаненко М. Що відомо і що невідомо про перші українські сайти // Детектор Медіа. 16 квітня 2008. URL: https://detector.media/rinok/article/37855/2008-04-16-shcho-vidomo-i-shcho-nevidomo-pro-pershi-ukrainski-sayty/
281. Чічановський А. Інформаційні процеси в структурі світових комунікаційних систем: підручник. Київ: Грамота. 2010. 568 с.
282. Шахов В. Національний інтерес і національна безпека в геостратегії України // Вісник Національної академії державного управління при Президентові України. 2013. № 2. С. 44−56.
283. Шовкун І. Політична реклама як комунікативний процеси: автореф. дис. ... канд. політ. н. (спеціальність: 23.00.02 – політичні інститути та процеси). Київ: Київський національний університет імені Тараса Шевченка. 2004. 17 с.
284. Юдін О. Концептуальний аналіз уразливості державних інформаційних ресурсів // Наукоємні технології. 2013. № 3 (19). С. 299−304.

285. Юдін О. Інформаційна безпека держави: навч. посібник. Харків: Консум, 2005. 576 с.
286. Юричко А. Інформаційні маніпуляції у повідомленнях світової періодичної преси в контексті інформаційної безпеки України: стан та шляхи протидії: автореф. дис. ...канд. філолог. н. (спеціальність: 10.01.08 – журналістика). Київ. 2007. 18 с.
287. Ющук О. Інформаційна безпека користувачів мережі Інтернет // Наукові записки. Серія «Культура та соціальні комунікації». 2009. Вип. 1. С. 224−231.
288. 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.
289. Яковлев В. Медіатизація політики в умовах становлення демократичного режиму // Вісник СевДТУ. Вип. 91: Політологія: зб. наук. пр. 2008. С. 103–105.
290. Ярошенко А. Напрями модернізації української освітньо-інформаційної політики // Міжнародний науковий форум: соціологія, психологія, педагогіка, менеджмент. 2010. Вип. 3. С. 122−130.
291. Ященко Т. Загальна характеристика деструктивних технологій у контексті виборчих кампаній // Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер.: Політологія. 2012. Т. 178. Вип. 166. С. 109−112.
292. Allison R. Russian «deniable» intervention in Ukraine: how and why Russia broke the rules // International Affairs. 2014. Vol. 90. No. 6. P. 1255−1297.
293. Balfour M. Propaganda in War, 1939−1945: Organisations, Policies, and Publics, in Britain and Germany. Taylor & Francis, 1979. P. 7−10.
294. Bērziņš J. Russia’s new generation warfare in Ukraine: Implications for Latvian Defense Policy // Policy Paper. 2014. Vol. 2. P. 2002−2014.
295. Bey H. The information war // Virtual Futures. 1994. P. 2.
296. Campen A. D. First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. AFCEA International Press, 1992. P. 10−20.

297. Deibert R., Rohozinski R., Crete-Nishihata M. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war // Security Dialogue. 2012. Vol. 43. No. 1. P. 3–24.
298. Felgenhauer P. After August 7: the escalation of the Russia-Georgia war // The guns of August. 2008. P. 162–180.
299. Haukkala H. From cooperative to contested Europe? The conflict in Ukraine as a culmination of a long-term crisis in EU-Russia relations // Journal of Contemporary European Studies. 2015. Vol. 23. No. 1. P. 25–40.
300. Herring G., Paterson T. Aid to Russia 1941–1946: strategy, diplomacy, the origins of the Cold War. Columbia University Press, 1973. 365 p.
301. Jonsson O., Seely R. Russian full-spectrum conflict: An appraisal after Ukraine // The Journal of Slavic Military Studies. 2015. Vol. 28. No. 1. P. 1–22.
302. Larrabee F. Russia, Ukraine, and Central Europe: the return of geopolitics // Journal of international affairs. 2010. Vol. 63. No. 2. P. 33–52.
303. Lerche C., Said A. Politics Concepts of International in Global Persptctive. Prentice-Hall, 1979. 336 p.
304. Maurer T., Janz S. The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context // The International Relations and Security Network. 2014. Vol. 17. URL: https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf
305. Pain E. The Second Chechen War: The Information Component // Military Review. 2000. Vol. 80. URL: https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/243760
306. Pilkerton C. Traffic Jam: Recommendations for Civil and Criminal Penalties to Curb the Recent Trafficking of Women from Post-Cold War Russia // Michigan Journal of Gender & Law. 1999. Vol. 6. No. 1. P. 221–259.
307. Reed W. Information, power, and war // American Political Science Review. 2003. Vol. 97. No. 4. P. 633–641.
308. Sakwa R. New Cold War'or twenty years' crisis? Russia and international politics // International Affairs. 2008. Vol. 84. No. 2. P. 241–267.

309. Snegovaya M. Putin’s information warfare in Ukraine // Soviet Origins of Russia’s Hybrid Warfare: Russia Report. 2015. Vol. 1. P. 10−13.
310. Snow N. Information war: American propaganda, free speech and opinion control since 9-11. Seven Stories Press, 2011. 176 p.
311. Stepan A. On the Task of a democratic Opposition // Journal of Democracy. 1990. Vol 1. No. 2. P. 44–46.
312. Suny R. The Soviet experiment: Russia, the USSR, and the successor states. New York: Oxford University Press. 1998. 540 p.
313. Tumber H., Webster F. Journalists under fire: Information war and journalistic practices. Sage, 2006. 192 p.
314. Ushakin S. The patriotism of despair: nation, war, and loss in Russia. Ithaca: Cornell University Press, 2009. 299 p.
315. Антіпова О. Філософсько-аксіологічні проблеми свободи слова в українському інформаційному просторі // Гілея: науковий вісник. 2013. № 74. С. 207–209.
316. Аронсон Э. Эпоха пропаганды: механизмы убеждения, повседневное использование и злоупотребление. СПб.: Прайм-ЕВРОЗНАК, 2003. 84 с.
317. Бойко О. Політичне маніпулювання. Київ: Академвидав, 2010. 432 с.
318. Войцих Н. Державна політика в українському інформаційному просторі: стан та проблеми // Міжнародна інформація та міжнародні відносини. 2013. Вип. 2. С. 6–12.
319. Василенко В. Війна 2014 року: спроба системного аналізу // Український тиждень. 17–23.10.2014. № 42 (362).
320. 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.
321. Горбулін В. Гібридна війна» як ключовий інструмент російської геостратегії реваншу // «Дзеркало тижня. Україна». 23 січня 2015. № 2. URL: https://zn.ua/ukr/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html

322. Грицик А. Правова відповідальність за зловживання свободою інформації // 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. 209–215.
323. Гуцалюк М. Інформаційна безпека України: нові загрози // Бизнес и безопасность. 2003. № 5. С. 2–3.
324. Дуцик Д. Політична журналістика. Київ: Вид. дім «Києво-Могилянська академія», 2005. 138 с.
325. Ермаков Ю. Манипуляция личностью: Смысл, приемы, последствия. Екатеринбург: Издательство Уральського университета, 1995. С. 15–20.
326. Кара-Мурза С. Манипуляция сознанием. М.: Эксмо, 2007. 864 с.
327. Комаровский В. Государственная служба и СМИ. Воронеж: Издательство Воронежского Государственного Университета, 2003. 114 с.
328. Кочнев И. 30 способов манипуляции людьми: Ч. 1 (1–15). URL: http://iterant.ru/30-sposobov-manipulyacii-chast-1/
329. Круглашов А. Способи протидії маніпулюванню електоральною поведінкою. URL: http://old.pinchukfund.org/storage/students/works/2009/621.doc
330. Кучма Л. Подолання політичного маніпулювання: суб'єктний вимір // Українська національна ідея: реалії та перспективи розвитку. 2010. Вип. 22. С. 70–75.
331. Куренной В. Кризис публичной сферы // Политический журнал. 2007. № 3–4. С. 9–15.
332. Кучма Л. Політична освіта та її роль у контексті основних стратегій протидії маніпулюванню // Українська національна ідея: реалії та перспективи розвитку. 2011. Вип. 23. С. 102–107.
333. Хилько М. Масово- та соціально-комунікаційні технології в реалізації цілей зовнішньої політики російської федерації у XXI ст. // Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2014. Вип. 39. С. 84–92.
334. Милль Дж. О свободе // О свободе. Антология мировой либеральной мысли (I половины XX века). М.: Прогресс-Традиция, 2000. С. 288–392.

335. Моисеев Н. Расставание с простотой. М.: АГРАФ, 1998. 472 с.
336. 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.
337. Ничта Н. Функціональна модель протидії психологічному маніпулюванню громадською думкою // Публічне управління: теорія і практика. 2012. № 2 (10). С. 68–74.
338. Олійник О., Соснін О., Шиманський Л. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави // Держава і право. 2001. Вип. 13. С. 534–541.
339. Ольшанский Д. Психология масс. СПб.: Питер, 2002. 368 с.
340. Панарин И. Информационная война и геополитика. М.: Поколение, 2006. 560 с.
341. Петрова Н., Якубенко В. Медіа-право для студентів факультетів/відділень журналістики. Київ: ТОВ «Київська типографія», 2007. 280 с.
342. Половинчак Ю. Мобілізаційний та маніпулятивний потенціал дискурсу соціальних медіа в умовах перехідного суспільства // Україна: події, факти, коментарі. Інформаційно-аналітичний журнал. 2014. № 21. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=1083:mobilizatsijnij-ta-manipulyativnij-potentsial-diskursu-sotsialnikh-media-v-umovakh-perekhidnogo-suspilstva&catid=127&Itemid=460
343. Почепцов Г. Первая смысловая война в мире (Украина, Крым, Россия) // ПСИ-ФАКТОР. URL: https://psyfactor.org/psyops/infowar27.htm
344. Российские спецслужбы пытаются дискредитировать мобилизацию в Украине – СНБО // Украина – Сегодня. URL: https://ukraine.segodnya.ua/ukraine/rossiyskie-specsluzhby-pytayutsya-diskreditirovat-mobilizaciyu-v-ukraine-snbo-541015.html
345. Сенченко М. Запорука національної безпеки в умовах інформаційної війни // Вісник Книжкової палати. 2014. № 6. С. 3–9.
346. Сенченко М. Латентна світова інформаційна війна. Київ: Стебеляк, 2014. 384 с.

347. Соснін О. Інформаційна сфера в реалізації інтересів інноваційного розвитку нації // Віче. 2011. № 15/16. С. 17–21.
348. Україна: політична історія. XX – початок XXI століття. Київ: Парламентське видавництво, 2007. 1028 с.
349. Украинцы воюют, чтобы получить двух рабов из Донбасса и кусок земли – репортаж «Первого канала» России: Видеофайл // Цензор.Нет. URL: http://censor.net.ua/video_news/310035/ukraintsy_voyuyut_chtoby_poluchit_dvuh_rabov_iz_donbassa_i_kusok_zemli_reportaj_pervogo_kanala_rossii
350. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти // Демократичне врядування. Науковий вісник. 2014. Вип. 13. С. 15–26.
351. Эндмюллер А. Техники манипуляции: распознавание и противодействие. М.: Омега-Л, 2006. 144 с.
352. Яковенко М. Інформаційний простір: філософські аспекти формування поняття // Вісник Національного університету «Львівська політехніка» (Філософські науки): зб. наук. праць. 2011. № 692. С. 22–27.
353. MacBride A. A living legacy // MacBride A. Many voices, one world. London: Kogan Page; New York: Unipub; Paris: Unesco, 1980.
354. Matterlart A. Mapping World Communication: War, Progress, Culture. University of Minnesota Press, 1994. 294 p.
355. Lasswell H. Propaganda, Communication and Public Order. Princeton, 1946. 120 p.
356. Habermas J. The Structural Transformation of the Public Sphere. Cambridge: The Mit Press, 1991. 301 p.
357. Seddon M. Documents Show How Russia's Troll Army Hit America // BuzzFeed. June 2, 2014. URL: https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america
358. McCombs M., Shaw D. The evolution of agenda-setting research: Twenty-five years in the marketplace of ideas // Journal of Communication. 1993. Vol. 43. No. 2. P. 58–67.
359. Енциклопедія політичної думки / Пер. з англ. К.: Дух і Літера, 2000. 472 с.

360. Політична енциклопедія / редкол.: Ю. Левенець, Ю. Шаповал. К.: Парламентське видавництво, 2011. 808 с.
361. Сучасна політична лексика: навч. енциклопед. словник-довідник / І. Вдовичин, Л. Угрин, Г. Шипунов та ін.; за наук. ред. Хоми Н. Львів: «Новий Світ-2000», 2015. 394 с.
362. Захаренко К. Категорія інформаційної безпеки у вітчизняному політологічному дискурсі // Вісник Львівського університету. Серія філос.-політолог. студії. 2019. Вип. 23. С. 158–165.
363. Захаренко К. Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток. Київ: Вид-во НПУ імені М.П. Драгоманова, 2017. 389 с.
364. Захаренко К. Теоретичні засади дослідження інформаційної безпеки // Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 2 (4). С. 107–116.
365. Захаренко К. Чинники здійснення державної інформаційної політики України // Регіональні студії. 2019. № 17. С. 15–19.
366. Захаренко К. Правовий супровід інформаційної безпеки суспільства // Державо і право. 2019. Вип. 83. С. 128–138.
367. Захаренко К. Диверсифікація джерел інформації в контексті інформаційної безпеки // Политикус. 2019. № 1. С. 5–9.
368. Захаренко К. Міжнародний досвід інформаційної безпеки // Сучасне суспільство: політичні науки, соціологічні, культурологічні науки. 2019. Вип. 1 (17). С. 95–109.
369. Захаренко К. Роль громадських організацій і рухів у формуванні національної інформаційної безпеки // Гілея: науковий вісник: зб. наук. пр. 2016. Вип. 115. С. 426–430.
370. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки // Нова парадигма. 2015. Вип. 127. С. 40–53.
371. Захаренко К. Глобальна природа інформаційної безпеки // Політологічний вісник. 2015. Вип. 79. С. 181–189.
372. Захаренко К. Партії і політичні рухи в інформаційному вимірі сучасної держави // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 116. С. 285–289.

373. Захаренко К. Держава як суб’єкт інформаційної безпеки суспільства // Політологічний вісник. 2015. Вип. 78. С. 86–96.
374. Захаренко К. Інформаційні впливи як джерела загострення інформаційної небезпеки // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 126. С. 331–336.
375. Захаренко К. Стратегія формування ефективної системи державної інформаційної безпеки // Гілея: науковий вісник. 2018. Вип. 131. С. 268–272.
376. Захаренко К. Засоби масової інформації як необхідний елемент розвитку інформаційного суспільства // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 132. С. 250-254.
377. Захаренко К. Засоби масової інформації як чинник розвитку суспільства // Вісник Інституту розвитку дитини. Серія: Філософія, педагогіка, психологія. 2015. Вип. 38. С. 29–36.
378. Захаренко К. Информационная безопасность в системе глобального информационного пространства //Strategiю Bakuю 2017. № 3–4 (21–22). С. 223–234.
379. Захаренко К. Інформаційна безпека суспільства як предмет правового регулювання // Гілея: науковий вісник: зб. наук. пр. 2019. Вип. 148. С. 26–31.
380. Захаренко К. Особливості формування ефективної державної інформаційної політики // Політичне життя. 2019. №3. С. 71–76.
381. Захаренко К. Відкритість інформаційного простору та контроль за доступністю інформації. 2020. Вип. 14. С. 46–55.
382. Захаренко К. Специфіка позиціювання політичної партії в інформаційному просторі держави і суспільства // Державо і право. 2019. Випуск 85. С. 338–348.
383. Захаренко К. Відповідальність засобів масової інформації в системі інформаційної безпеки суспільства // Політикус. 2019. № 5. С. 4–9.
384. Захаренко К. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі // Гуманітарний вісник ЗДІА. 2018. Випуск 72. С. 44–52.
385. Закон України «Про національну безпеку України» // Відомості Верховної Ради. 2018. № 31. С. 241.

386. Доктрина інформаційної безпеки України (затверджена Указом Президента України від 25 лютого 2017 року № 47/2017) // Верховна Рада України. Сайт. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text
387. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» // Верховна Рада України. Сайт. URL: https://zakon.rada.gov.ua/laws/show/995_c57?find=1&text=%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81#w1_2
388. Захаренко К. До питання про розвиток національної системи інформаційної безпеки: досвід сусідів // Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія. 2018. Вип. 50. С. 176–189.
389. Бабкіна О. Між минулим і майбутнім: відповідальність інтелектуалів за соціально-політичні перетворення // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін: [зб. наук. праць]. 2018. Вип. 24. С. 3–10.
390. 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
391. Міністерство інформаційної політики України // Офіційний сайт. URL: https://mip.gov.ua
392. Постанова Кабінету Міністрів України від 2 вересня 2019 року № 829 «Деякі питання оптимізації системи центральних органів виконавчої влади» // Кабінет Міністрів України. Сайт. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-optimizaciyi-sistem-829
393. Деякі питання оптимізації діяльності центральних органів виконавчої влади. Постанова Кабінету Міністрів України від 26.03.2020 // Верховна Рада України. Сайт. URL: https://zakon.rada.gov.ua/laws/show/238-2020-%D0%BF#Text
394. Міністерство культури та інформаційної політики України // Офіційний сайт. URL: https://mkip.gov.ua/content/pro-ministerstvo.html

395. Положення про Державне агентство з питань електронного урядування України (затверджено постановою Кабінету Міністрів України від 1 жовтня 2014 р. № 492) // Верховна Рада України. Офіційний вебсайт. URL: https://zakon.rada.gov.ua/laws/show/492-2014-%D0%BF#Text
396. 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
397. 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
398. Положення «Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації» (затверджено Указом Президента України від 23 листопада 2011 року 1067/2011) // Верховна Рада України. Вебсайт. URL: https://zakon.rada.gov.ua/laws/show/1067/2011#Text
399. Закон України «Про Службу безпеки України» // Відомості Верховної Ради України. 1992. № 27. С. 382.
400. Положення «Про Міністерство культури України» (затверджено постановою Кабінету Міністрів України від 3 вересня 2014 р. № 495) // Міністерстько культури України. URL: http://mincult.kmu.gov.ua/control/uk/publish/article?art_id=244908502&cat_id=244908427
401. 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
402. Комітет ВРУ з питань гуманітарної та інформаційної політики // Офіційний сайт. URL: http://kompkd.rada.gov.ua/
403. Комітет ВРУ з питань свободи слова // Сайт. URL: http://komsvobslova.rada.gov.ua/

404. Комітет ВРУ з питань цифрової трансформації // Офіційний сайт. URL: http://komit.rada.gov.ua/
405. 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
406. Положення «Про Раду з питань інформаційної політики при Президентові України» (затверджено Указом Президента України від 3 квітня 2001 року № 230/2001) // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/230/2001#Text
407. Положення «Про Національну комісію з утвердження свободи слова та розвитку інформаційної галузі» (затверджено Указом Президента України від 6 червня 2006 року № 493/2006) // Верховна Рада України. Сайт. URL: https://zakon.rada.gov.ua/laws/show/493/2006#Text
408. Положення «Про Раду з питань захисту професійної діяльності журналістів та свободи слова» (затверджено Указом Президента України від 23 лютого 2016 року № 61/2016) // Верховна Рада України. Офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/61/2016#Text
409. Положення «Про Раду з питань свободи слова та захисту журналістів» (затверджено Указом Президента України від 6 листопада 2019 року № 808/2019) // Верховна Рада України. Сайт. URL: https://zakon.rada.gov.ua/laws/show/808/2019#Text
410. Державний комітет телебачення і радіомовлення України (Держкомтелерадіо) // Сайт. URL: http://comin.kmu.gov.ua/control/publish/article/main?art_id=70793&cat_id=70792
411. Національна рада України з питань телебачення і радіомовлення // Офіційний сайт. URL: https://www.nrada.gov.ua/about/#history
412. Служба безпеки України // Офіційний сайт. URL: https://ssu.gov.ua/
413. Інформаційно-аналітичний центр Національної безпеки України // Офіційний сайт. URL: http://mediarnbo.org/sample-page/
414. Волянюк О. Політична реальність і доповнена реальність: особливості сумісності // Науковий часопис Національного педагогічного університету

імені М. П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін [Відп. ред. О.В.Бабкіна]. Випуск 26: збірник наукових праць. 2019. С. 86–93.

415. 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.
416. Крим за завісою. Путівник зоною окупації / Під заг. ред. А. Майорової; авт. колектив О. Волянюк, К. Добровольська, М. Майоров. Київ, 2019. 156 с.
417. Донбас в огні. Путівник зоною конфлікту / Під заг. ред. А. Майорової; авт. колектив М. Балабан, О. Волянюк, К. Добровольська, Б. Балабан, М. Майоров. Львів: «Прометей», 2017. 98 с.
418. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради. 2017. № 45. С. 403.
419. Астанинская юбилейная декларация: на пути к сообществу безопасности // OSCE Chairperson-in-Office. URL: https://www.osce.org/ru/cio/74990
420. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности (резолюция принятая Генеральной Ассамблеей ООН. 2 декабря 2014 года) // Организация Объединенных Наций. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/69/28&referer=/english/&Lang=R
421. 2020 World Press Freedom Index // Reporters Without Borders. URL: https://rsf.org/en/world-press-freedom-index
422. Лепська Н. Диверсифікація геополітичного простору в умовах сучасної трансформації світоустрою // Вісник Львівського університету. Серія філософсько-політологічні студії. 2018. Вип. 17. С. 201–208.
423. von Solms R., van Niekerk J. From information security to cyber security // Computers & Security. 2013. Vol. 38. P. 97–102.
424. National Cyber Strategy of the United States of America. Washington: The White House, 2018. 26 p. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

425. Henrichsen J. Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies // Digital Journalism. 2020. Vol. 8. No. 3. P. 328–1346.
426. Kerr J. Authoritarian Practices in the Digital Age| Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region // International Journal of Communication. 2018. Vol. 12. P. 3814–3834.
427. Braut-Hegghammer M. Proliferating Bias? American Political Science, Nuclear Weapons, and Global Security // Journal of Global Security Studies. 2019. Vol. 4. No. 3. P. 384–392.
428. Wu Y., Meng F. Categorizing Security for Security Management and Information Resource Management // Journal of Strategic Security. 2018. Vol. 11. No. 4. P. 72–84.
429. Raychev Y. Cyberwar in Russian and US Military-Political Thought: A Comparative View // Information & Security Journal. 2019. Vol. 43. No. P. 349–361.
430. Зозуля О. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства: автореф. дис. ... канд. наук з державного управління (спеціальність: 25.00.01 – теорія та історія державного управління). Київ: Національна академія державного управління при Президентові України. 2017. 251 с.
431. Красноступ Г. Правове забезпечення державної інформаційної політики // Міністерство юстиції України. URL: https://minjust.gov.ua/m/str_22116
432. 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
433. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856 // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text
434. Малик І. Інформаційна безпека України: стан та перспективи розвитку // Ефективність державного управління: Збірник наукових праць. 2015. Вип. 44. С. 13–20.

435. Карчевська О. Роль політичної комунікації в електоральному процесі: теоретико-методологічний аналіз // Політологічні записки. 2012. № 6.
436. Ляшенко О. Українська політична нація: етнополітичний аспект // Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. 2012. С. 205–216.
437. Логовський І. Проблеми розвитку інформаційного простору України як чинника формування духовно-моральнісних якостей сучасного студентства // Духовно-моральнісні 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.
438. Лойко Л. Типологічне позиціювання національних організацій в інституціональній структурі громадянського суспільства // Політичний менеджмент. 2005. № 5. С. 51–60.
439. Копійка М. Інституціональний концепт інформаційної безпеки України // Деокупація і реінтеграція інформаційного простору Криму: міжнародно-правові та медіакомунікативні інструменти: матеріали міжнародної науково-практичної конференції. м. Київ: 18 квітня 2019 року. Київ. 2019. С. 17–22.
440. Захарченко К. Засоби масової інформації як чинник розвитку суспільства // Вісник Інституту розвитку дитини. Серія: Філософія, педагогіка, психологія. 2015. Вип. 38. С. 29–35.
441. Бауман З. Глобализация. Последствия для человека и общества / Пер. с англ. М.: «Весь мир», 2004. 188 с.
442. Бауман З. Индивидуализированное общество / Пер. с англ. под ред. В. Иноземцева. М.: «Логос», 2005. 390 с.
443. Bell D. The coming of post-industrial society: A venture of social forecasting. N.Y.: Basic Books, 1976. 507 p.
444. Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. Москва: «Прогресс», 1986. С. 330–342.

445. Бжезінський З. Велика шахівниця. Американська першість та її стратегічні імперативи / Пер. з англ. О. Фешовець. Івано-Франківськ: Лілея-НВ, 2000. 236 с.
446. Бжезинский З. Выбор: Мировое господство или глобальное лидерство / Пер. с англ. Е. Нарочницкой, Ю. Кобякова. М.: Международные отношения, 2010. 262 с.
447. Бодрияр Ж. Символический обмен и смерть / Пер. с фр. М.: «Добросвет», 2000. 387 с.
448. Бодрияр Ж. Симулякры и симуляция / Пер. с фр. А. Качалова. М.: Рипол-классик, 2015. 240 с.
449. Isard W. Spatial Dynamics and Optimal Space-Time Development. North-Holland. 1979. 434 p.
450. Дарендорф Р. Современный социальный конфликт. Очерк политики свободы. М.: РОССПЭН, 2002. 284 с.
451. Domenach J.-M. La propagande politique. P.U.F., 1950. 127 p.
452. Kahn H. The Coming Boom: Economic, Political, and Social. New York: Simon and Schuster, 1982. 237 p.
453. Kahn H. The Next 200 Years. Morrow. 1976. 241 p.
454. Katz E. Personal Influence. New York: Free Press, 1955. 400 p.
455. Katz E. Personal influence: The part played by people in the flow of mass communications. Routledge, 2017. 434 p.
456. Парето В. Трансформация демократии / Пер. с итал. М. Юсима. М.: Издательский дом «Территория будущего», 2011. 208 с.
457. Тойнби А. Цивилизация перед судом истории: Сборник / Пер. с англ. М.: Рольф, 2002. 592 с.
458. Тойнби А. Исследование истории: В 3 т. / Пер. с англ., вступ. статья и комментарии К. Кожурина. СПб.: Изд-во С.-Петербургского ун-та: «Издательство Олега Абышко», 2006. 1333 с.
459. Тойнби А. Вызовы и ответы. Как гибнут цивилизации. М.: Алгоритм, 2016. 288с.
460. Хантингтон С. Третья волна. Демократизация в конце XX века М.: РОССПЭН, 2003. 368 с.

461. Хантингтон С. Столкновение цивилизаций М.: АСТ, 2003. 603 с.
462. Хантингтон С. Политический порядок в меняющихся обществах. М.: Прогресс-Традиция, 2004. 480 с.
463. Габермас Ю. Структурні перетворення у сфері відкритости. Львів: Літопис, 2000. 320 с.
464. Габермас Ю. Залучення іншого: Студії з політичної теорії / Пер. з нім. А. Дахнія. Львів: Астролябія, 2006. 416 с.
465. Габермас Ю. До реконструкції історичного матеріалізму / Пер. з нім. В. Купліна. К.: Дух і літера, 2011. 320 с.
466. Шарп Дж. От диктатуры к демократии: Стратегия и тактика освобождения: монография. 2-е изд. М.: Новое издательство, 2012. 84 с.
467. Шарп Дж. 198 Методов Ненасильственного Действия. // Философия науки. № 12. С. 33–40.
468. Grama J. Legal and Privacy Issues in Information Security. Jones & Bartlett Learning. 2020. 552 p.
469. Moore T., Ioannidis C. Economics of Information Security and Privacy. Springer Science & Business Media, 2010. 320 p.
470. Nemati H. Information Security and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications. IGI Global, 2007. 4478 p.
471. Cavelty M. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Taylor & Francis, 2007. 192 p.
472. Kremer J.-F., Müller B. Cyberspace and International Relations: Theory, Prospects and Challenges. Springer Science & Business Media, 2013. 284 p.
473. Eriksson J., Giacomello G. International Relations and Security in the Digital Age. Routledge, 2007. 236 p.
474. Gupta M., Sharman R. Handbook of Research on Social and Organizational Liabilities in Information Security. IGI Global, 2008. 596p.
475. Choucri N. Cyberpolitics in International Relations. MIT Press, 2012. 311 p.
476. Manjikian M. Introduction to Cyber Politics and Policy. CQ Press, 2020. 432 p.

477. Kahl C. International Relations, International Security, and Comparative Politics: A Guide to Reference and Information Sources. Greenwood Publishing Group, 2008. 423 p.
478. Rosenau J., Singh J. Information Technologies and Global Politics: The Changing Scope of Power and Governance. SUNY Press, 2002. 312 p.
479. Smith M. International Security: Politics, Policy, Prospects. Macmillan International Higher Education, 2010. 384 p.
480. Lacy M., Wilkin P. Global Politics in the Information Age. Manchester University Press, 2005. 208 p.
481. Whyte C., Mazanec B. Understanding Cyber Warfare: Politics, Policy and Strategy. Routledge, 296 p.

ДОДАТКИ

Додаток А
Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Монографії:

1. Захаренко К. Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток. Київ: Вид-во НПУ імені М.П. Драгоманова, 2017. 389 с.

Наукові статті:

2. Захаренко К. Відкритість інформаційного простору та контроль за доступністю інформації. 2020. Вип. 14. С. 46–55.
3. Захаренко К. Відповідальність засобів масової інформації в системі інформаційної безпеки суспільства // Політикус. 2019. № 5. С. 4–9.
4. Захаренко К. Глобальна природа інформаційної безпеки // Політологічний вісник. 2015. Вип. 79. С. 181–189.
5. Захаренко К. Держава як суб’єкт інформаційної безпеки суспільства // Політологічний вісник. 2015. Вип. 78. С. 86–96.
6. Захаренко К. Диверсифікація джерел інформації в контексті інфоормаційної безпеки // Политикус. 2019. № 1. С. 5–9.
7. Захаренко К. Ефективність використання потенціалу недержавних суб’єктів інформаційної безпеки // Нова парадигма. 2015. Вип. 127. С. 40–53.
8. Захаренко К. Засоби масової інформації як необхідний елемент розвитку інформаційного суспільства // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 132. С. 250–254.

9. Захаренко К. Информационная безопасность в системе глобального информационного пространства //Strategiю Bakuю 2017. № 3–4 (21–22). С. 223–234.
10. Захаренко К. Інформаційна безпека суспільства як предмет правового регулювання // Гілея: науковий вісник: зб. наук. пр. 2019. Вип. 148. С. 26–31.
11. Захаренко К. Інформаційні впливи як джерела загострення інформаційної небезпеки // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 126. С. 331–336.
12. Захаренко К. Категорія інформаційної безпеки у вітчизняному політологічному дискурсі // Вісник Львівського університету. Серія філос.-політолог. студії. 2019. Вип. 23. С. 158–165.
13. Захаренко К. Міжнародний досвід інформаційної безпеки // Сучасне суспільство: політичні науки, соціологічні, культурологічні науки. 2019. Вип. 1 (17). С. 95–109.
14. Захаренко К. Особливості формування ефективної державної інформаційної політики // Політичне життя. 2019. №3. С. 71–76.
15. Захаренко К. Партії і політичні рухи в інформаційному вимірі сучасної держави // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 116. С. 285–289.
16. Захаренко К. Правовий супровід інформаційної безпеки суспільства // Державо і право. 2019. Вип. 83. С. 128–138.
17. Захаренко К. Протидія маніпулятивним впливам (засоби, технології, можливості) // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 137. С. 181–189.
18. Захаренко К. Роль громадських організацій і рухів у формуванні національної інформаційної безпеки // Гілея: науковий вісник: зб. наук. пр. 2016. Вип. 115. С. 426–430.
19. Захаренко К. Специфіка позиціювання політичної партії в інформаційному просторі держави і суспільства // Державо і право. 2019. Випуск 85. С. 338–348.
20. Захаренко К. Стратегія формування ефективної системи державної інформаційної безпеки // Гілея: науковий вісник. 2018. Вип. 131. С. 268–272.

21. Захаренко К. Теоретичні засади дослідження інформаційної безпеки // Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 2 (4). С. 107–116.
22. Захаренко К. Чинники здійснення державної інформаційної політики України // Регіональні студії. 2019. № 17. С. 15–19.

Наукові праці, що засвідчують апробацію матеріалів та додатково відображають наукові результати дисертації:

23. Захаренко К. До питання про розвиток національної системи інформаційної безпеки: досвід сусідів // Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія. 2018. Вип. 50. С. 176–189.
24. Захаренко К. Засоби масової інформації як інструмент та механізм розвитку інформаційного суспільства // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2018. Вип. 39. С. 79–87.
25. Захаренко К. Засоби масової інформації як чинник розвитку суспільства // Вісник Інституту розвитку дитини. Серія: Філософія, педагогіка, психологія. 2015. Вип. 38. С. 29–36.
26. Захаренко К. Категорія «інформаційної безпеки» у вітчизняному науковому дискурсі // Гуманітарний вісник державного вищого навчального закладу «Переяслав-Хмельницький державний педагогічний університет ім. Г. С. Сковороди». Серія: Філософія. 2015. Вип. 37. С. 106–117.
27. Захаренко К. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі // Гуманітарний вісник ЗДІА. 2018. Випуск 72. С. 44–52.
28. Захаренко К. Місце політичних партій в системі інформаційної безпеки // Політологічні читання імені професора Богдана Ярошa: зб. наук. пр. / за заг. ред. В.І. Бортнікова, О.Б. Ярош, Я.Б. Ярошa. Луцьк: Вежа-Друк, 2020. Вип. 9. С. 44–49.

29. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки // Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Серія: Філософія. 2017. Вип. 48 (1). С. 212–219.
30. Захаренко К. Проблеми консолідації субєктів інформаційної безпеки // Проблеми соціальної роботи: філософія, психологія, соціологія. 2018. № 1(11). С. 36–43.
31. Захаренко К. Проблеми формування ефективної державної інформаційної політики // Науковий часопис НПУ імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2016. Вип. 36. С. 202–209.
32. Захаренко К. Розвиток системи інформаційної безпеки: досвід зарубіжних країн // Вища освіта України. 2018. № 3. С. 71–77.

Відомості про апробацію результатів дисертації

1. Друга міжнародна науково-практична конференція «Управлінські компетенції викладача вищої школи» (28 лютого 2014 р., м. Київ, очна форма участі).
2. Міжнародна науково-практична конференція «Політика і духовність в умовах глобальних викликів» (2 квітня 2014 р., м. Київ, очна форма участі).
3. IV міжнародні Драгоманівські читання: до 180-річчя НПУ імені М. П. Драгоманова (16–17 квітня 2015 р., м. Київ, очна форма участі).
4. Одинадцяті юридичні читання «Форма сучасної національної української держави: реалії та перспективи» (21–22 травня 2015 р., м. Київ, очна форма участі).
5. Міжнародна науково-практична конференція «Формування державної освітньої політики: філософські, теоретичні та прикладні аспекти» (25–26 лютого 2016 р., м. Київ, очна форма участі).
6. Міжнародна науково-практична конференція «Сутність та перспективи впровадження електронної демократії в Україні» (15 листопада 2016 р., м. Вінниця, очна форма участі).
7. Різдвяні педагогічні читання «Новий вчитель для нової української школи» (23–25 грудня 2016 р., м. Київ, очна форма участі).

8. Науково-практична конференція «Ціннісний дискурс у суспільстві та освіті» (1–2 березня 2018 р., м. Київ, очна форма участі).
9. Міжнародна наукова конференція «Тринадцяті юридичні читання «Українська державність: крізь призму часу (до 100-річчя Української національно-демократичної революції 1917–1921 рр.)»» (24–25 травня 2018 р., м. Київ, очна форма участі).
10. Наукова конференція «Культурологічна практика в системі підготовки майбутнього вчителя» (5–6 жовтня 2018 р., м. Київ, очна форма участі).
11. Тиждень філософії в НПУ імені М. П. Драгоманова «Майбутнє філософської освіти в Європі: виклики та перспективи» (14–17 травня 2019 р., м. Київ, очна форма участі).
12. Науково-практична конференція «Значення культурної практики в освітянському процесі університету» (31 травня – 1 червня 2019 р., м. Київ – м. Новгород-Сіверський, очна форма участі).
13. Політологічні читання імені професора Богдана Яроша (14 квітня 2020 р., м. Луцьк, заочна форма участі).