НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

НОВІКОВ Владислав Олександрович

УДК 351.74 + 342.95

ІНСТИТУЦІЙНІ МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ІНФОРМАЦІЙНО-ГІБРИДНИХ ВІЙН

Спеціальність 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку
Галузь науки: Публічне управління та адміністрування

Подається на здобуття наукового ступеня кандидата наук з державного управління

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

Науковий керівник: Помаза-Пономаренко А.Л., доктор наук з державного управління, старший дослідник

Харків – 2024

АНОТАЦІЯ

Новіков В. О. Інституційні механізми публічного управління в умовах інформаційно-гібридних війн. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата наук в галузі науки «Публічне управління та адміністрування» за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. Національний університет цивільного захисту України, Харків, 2024.

У дисертації запропоновано розв'язання актуального науково-прикладного завдання, що полягає у визначенні науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

Забезпечити розв'язання цього науково-прикладного завдання дозволило вперше запропоноване визначення шляхів розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни. Серед цих шляхів основними визнано такі: 1) створення єдиного координаційно-аналітичного центру/ради в Україні, на зразок Бюро протидії гібридній війні, яке функціонує в США та напрацювало дієві управлінські практики реагування на інформаційні загрози; 2) налагодження результативної взаємодії України з іншими державами та міжнародними організаціями в напрямку вчасного протистояння цим загрозам.

Висловити вищевказані авторські пропозиції дозволило вдосконалене визначення головної небезпеки інформаційно-гібридної війни як потенційної можливості цільового інформаційного, у т.ч. негативного, впливу на об'єктивно закладені та наявні суперечності практично на всіх рівнях державного та суспільного устрою в будь-якій країні чи регіоні, з метою примусового прояву цього впливу із заданим рівнем інтенсивності

та в завідомо окресленому напрямку.

Виявлено позитивні закордонні публічно-управлінські практики щодо протидії інформаційним загрозам (у Франції, Казахстані, США та ін.). Аналіз цих практик дав підстави стверджувати, що запорукою успішності їхньої реалізації є застосовувані ризик-орієнтовані підходи. На цій підставі в дисертації доведена необхідність застосування таких підходів під час забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни. Ці підходи, у свою чергу, дозволили обґрунтувати сценарії реагування на ці війни: 1) проактивний сценарій, який рекомендовано реалізовувати під час стратегічного планування та поступального забезпечення сталого розвитку; 2) реактивний сценарій, що передбачає оперативне реагування на інформаційні загрози, зокрема, у межах уточненої концепції протидії ним.

Крім того, удосконалено концептуальні засади щодо прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління на пострадянському і вітчизняному просторі. Доведено, що на ці механізми впливають зовнішні та внутрішні фактори (політичні, соціальні, економічні та ін.). Аргументовано, що серед них найбільш загрозливими на сучасному етапі є соціальні, оскільки вони безпосередньо пов’язані з рівнем міграції громадян, їхнього добробуту, безробіття, демографічного розвитку та ін., що суттєво знижується в Україні через вплив інформаційних загроз і гібридної війни. Дані обставини надають переваги для держави-агресора, яка розпочала інформаційно-гібридну війну проти України.

Окремий блок дисертації становлять положення, у межах яких дістало подальшого розвитку, зокрема, визначення асиметрії як основоположної властивості інформаційно-гібридних війн. Акцентовано, що вона відзначається латентністю та спрямованістю на найбільш вразливі місця в інформаційній обороні противника, наслідки недосконалості якої порівнянні із застосуванням нетрадиційної зброї, покликаної значно

зменшити витрати на використання традиційної зброї й отримати інформаційну перевагу над противником.

У дисертації здійснено структуризацію інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни з позиції виокремлення в складі цих механізмів організаційного та правового механізмів публічного управління. Вони приводять у рух його відповідну суб'єктну підсистему. На сьогодні цю підсистему охарактеризовано як незадовільно функціонуючу, на підставі чого обґрунтовано шляхи підвищення її результативності із наведенням конкретних нормотворчих пропозицій щодо усунення дублювання функцій органів державної влади у сфері інформаційної безпеки.

Крім того, визначено ризики функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни. Уважаємо, що унеможливити трансформацію цих ризиків у небезпеки інформаційного характеру може реалізація комплексу заходів, а саме: 1) протидія поширенню неправдивої та видозміненої інформації з боку країни-агресора, що впливає на розвиток українського суспільства й держави; 2) формування цілісної інформаційної концепції й стратегії поширення об'єктивної інформації та протидії загрозам інформаційного характеру; 3) підвищення рівня медіа-культури суспільства та його цифровізованого розвитку тощо. З цією метою згруповано інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни, серед яких технологіям «м'якої сили» відведено особливе місце. Доведено, що нейтралізувати їхній негативний вплив може застосування ризик-орієнтованих підходів. З'ясовано, що їх активно застосовують як економічно розвинені країни, так і ті, що тільки стали на шлях забезпечення власного сталого розвитку. Такий досвід є цінним для України, відтак, рекомендовано його врахування під час визначення шляхів розвитку інституційних механізмів публічного управління в умовах інформаційно-гібридної війни.

Об’єкт дослідження – публічне управління у сфері забезпечення інформаційної безпеки.

Предмет дослідження – інституційні механізми публічного управління в умовах інформаційно-гібридних війн.

Дисертаційне дослідження побудовано на концептуальному, системному, синергетичному й інституціональному підходах, а також сукупності методів: логічного узагальнення, синтезу й абстрагування; теоретизування й історичної формалізації; системного аналізу, порівняння, вибірки й опису; індукції та дедукції; групування та прогнозування.

Інформаційно-фактологічною базою дослідження є закони України, укази Президента України, нормативні акти Кабінету Міністрів України, аналітичні матеріали центральних органів виконавчої влади, статистична інформація Державної служби статистики України тощо.

Ключові слова: публічне управління та адміністрування, інституційні механізми публічного управління в умовах інформаційно-гібридних війн, органи публічної влади, національна безпека, інформаційна безпека.

ANNOTATION

Novikov V.O. Institutional mechanisms of public administration in the conditions of information and hybrid wars. – Manuscript.

The dissertation on competition of a scientific degree of the Candidate of Science in Public Administration, speciality 25.00.05 – Public Administration of State Security and Enforcement of Public Order. National Civil Defence University of Ukraine, Kharkiv, 2024.

The thesis introduces solution for an essential scientific and applied task consisting in determination of scientific and theoretical principles of institutional mechanisms of public administration in the conditions of information and hybrid wars, as well as in elaboration of practical recommendations for the development

for improving such mechanisms in Ukraine.

It became possible to solve an applied science task with the help of the first proposed definition of the ways of development of an institutional system of public administration in Ukraine under the conditions of hybrid and information warfare. Among these ways, the following were defined as the main ones: 1) establishing the coordination and analytical centre / council in Ukraine similar to the Centre on Combating Hybrid Threats, which functions in the USA and has already created effective administrative practices aimed at the response to information threats; 2) building effective relationships between Ukraine and other countries and international organizations aimed at countering these threats in time.

The above-mentioned author's proposals were given based on the improved definition of the main threat of hybrid and information warfare as a potential possibility of purposeful informational, particularly negative influence on the objectively established and available contradictions practically at all levels of state and public system in any country or region with the purpose of forced manifestation of this influence at the predetermined level of intensity and in the predetermined direction.

Positive foreign public and administrative practices in the field of countering information threats (in France, Kazakhstan, the USA, etc.) were defined. The analysis of these practices made it possible to state that the applied risk-oriented approaches guarantee their successful implementation. On this ground, the thesis proves the necessity to apply these approaches for the development of institutional system of public administration in Ukraine under the conditions of hybrid and information warfare. These approaches, in turn, made it possible to prove the following scenarios of response in this war: 1) a proactive scenario, which is recommended to implement for strategic planning and progressive achievement of sustainable development; 2) a reactive scenario, which stipulates prompt response to information threats, in particular within the framework of specified conception of counteraction.

In addition, the conceptual framework for forecasting hybrid and information warfare in the context of the development of institutional mechanisms of public

administration in the post-Soviet and local area was improved. It was proved that both external and internal factors (political, social, economic, etc.) influence these mechanisms. It was proved that the most threatening among them at the current stage are the social ones, as they are directly connected with the level of migration of citizens, their well-being, unemployment, demographic development, etc., which significantly declines in Ukraine due to the influence of information threats and hybrid warfare. These circumstances provide advantages for the aggressor state, which has launched an information-hybrid war against Ukraine.

A special part of the thesis contains the provisions, within which the definition of asymmetry as a fundamental characteristic of hybrid and information warfare obtained its further development. It was emphasized that it is characterized by abeyance and focus on the most vulnerable aspects in the enemy's informational defence, the consequences of imperfection of which may be compared with the use of unconventional weapon aimed at significant reduction of conventional arms expenditures and at gaining information advantage over the enemy.

The thesis structurizes the institutional mechanisms of public administration in Ukraine under the conditions of hybrid and information warfare from the point of view of distinction of organizational and legal mechanisms of public administration out of these mechanisms. They trigger its relevant subjective subsystem. As of today, this subsystem is characterized as the one that functions inadequately. Based on this, the effectiveness improvement ways were substantiated by providing the specific regulatory proposals concerning the elimination of doubling of functions of the state authorities in the field of information security.

Moreover, the risks of functioning of institutional mechanisms of public administration in Ukraine under the conditions of hybrid and information warfare were determined. We consider that the implementation of the set of certain measures prevents the transformation of these risks into information threats. These measures include: 1) prevention of the spread of untruthful and altered information by the aggressor state, which influences the development of Ukrainian society and the state; 2) formation of the comprehensive information

conception and the strategy of objective information spreading, as well as combating information threats; 3) increasing the level of media culture of the society and its digital development, etc. With this purpose, the tools of dysfunctionalization of institutional mechanisms of public administration under the conditions of hybrid and information warfare were grouped (among which the special place belongs to the technologies of "soft power"). It was proved that it is possible to neutralize their negative impact by using the risk-oriented approaches. It was established that they are actively used by both the economically developed countries and the ones that have recently chosen sustainability practices. This experience is valuable for Ukraine, therefore, it is recommended to take it into considerations when defining the ways of development of institutional mechanisms of public administration under the conditions of hybrid and information warfare.

The object of the research is public administration in the field of ensuring information security.

The subject of the study is the institutional mechanisms of public administration in the conditions of information and hybrid wars.

The dissertation research is based on conceptual, systemic, synergistic, and institutional approaches, as well as a set of methods: logical generalization, synthesis, and abstraction; theorizing and historical formalization; system analysis, comparison, sampling and description; induction and deduction; clustering and forecasting.

The informational and factual basis of the study is the laws of Ukraine, decrees of the President of Ukraine, normative acts of the Cabinet of Ministers of Ukraine, analytical materials of central executive bodies, statistical information of the State Statistics Service of Ukraine, etc.

Keywords: public management and administration, institutional mechanisms of public management in the conditions of information-hybrid wars, public authorities, national security, informational security.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Статті у фахових наукових виданнях з державного управління:

1. Новіков В.О. Ризик-орієнтований підхід до формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн: досвід Франції, Казахстану й України // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2020. Вип. 1 (12). С. 300–308. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18672/1/journal12.20.pdf.

2. Новіков В.О. Дисфукнціоналізація інституційної системи та механізмів публічного управління в умовах інформаційно-гібридних війн // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2020. Вип. 2 (13). С. 345–354. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18688/1/vdu13.pdf.

3. Новіков В.О. Theoretical and institutional features of the modern definition of the concept of hybrid war // *Вісник Національного університету цивільного захисту України. Серія: Державне управління.* 2023. Вип. 2 (19). С. 207–212.

4. Новіков В.О. Аналіз сучасної концепції інформаційно-гібридної війни // *Державне управління: удосконалення та розвиток:* елек. журнал. 2023. № 9. URL: https://www.nayka.com.ua/index.php/dy/article/view/2133.

5. Новіков В.О. Information and hybrid wars in the current environment: public-administrative aspect // *Public administration and state security aspects.* 2023. Vol. 2. P. 43–51.

6. Помаза-Пономаренко А.Л., Новіков В.О. Шляхи трансформації інституційних механізмів публічного управління в Україні: від інформаційних загроз до гібридних війн // Державне будівництво: елек. журнал. 2023. № 1 (33). URL: https://periodicals.karazin.ua/db/article/view/22921.

Статті в закордонних виданнях за напрямком:

7. Novikov V. Approaches to improvement of the institutional system and mechanisms of public administration in the conditions of information-hybrid wars // *Eurasian Academic Research Journal*. 2020. Vol. 37. Pp. 75-80.

Тези конференцій:

8. Новіков В.О. Особливості сучасного концепту інформаційно-гібридної війни по відношенню до України // Публічне управління в системі координат: демократія, децентралізація, місцеве самоврядування: матеріали Всеукраїнської науково-практичної конференції (18.10.2019 р., м. Мелітополь) / відп. ред. Ортіна Г.В. Мелітополь: ФОП Однорог Т.В., 2019. С. 410–411.

9. Новіков В.О. Аналіз інституційних особливостей формування сучасної концепції інформаційно-гібридної війни // Modern research in science and education: матеріали І Міжнародної науково-практичної конференції (14-16.09.2023 р., м. Київ). Київ: Науково-видавничий центр «Sci-conf.com.ua». 2023. С. 286–289. URL: https://sci-conf.com.ua/wp-content/uploads/2023/09/MODERN-RESEARCH-IN-SCIENCE-AND-EDUCATION-14-16.09.23.pdf.

10. Новіков В.О. Напрями вдосконалення інституційних механізмів публічного управління в умовах інформаційно-гібридних війн // Наука і вища освіта : матеріали XXXII Міжнародної наукової конференції здобувачів вищої освіти і молодих учених (08.11.2023 р., м. Запоріжжя). 2023. С. 263–264.

11. Новіков В.О. Особливості розвитку механізмів публічного управління в умовах інформаційно-гібридних війн // Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття : матеріали Всеукраїнської науково-практичної конференції (07-08.12.2023 р., м. Житомир). С. 276–278.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВРУ – Верховна Рада України.

ЄЦПГЗ – Європейський центр з протидії гібридним загрозам.

ЄС – Європейський Союз.

КМУ – Кабінет Міністрів України.

КНР – Китайська Народна Республіка.

ЗМІ – Засоби масової інформації.

ІКТ – Інформаційно-комунікаційні технології.

МВС України – Міністерство внутрішніх справ України.

МЗС України – Міністерство закордонних справ України.

НКО – некомерційні організації.

НУО – неурядові організації.

ООН – Організація Об’єднаних Націй.

ОМС – органи місцевого самоврядування.

ПАРЄ – Парламентська Асамблея Ради Європи.

СБУ – Служба безпеки України.

СУАР – Сіньцзян-Уйгурський автономний район.

США – Сполучені Штати Америки.

ЦОВВ – Центральні органи виконавчої влади.

HRW – Human Rights Watch.

HWRB – Hybrid warfare resistance Bureau.

NIC – National Intelligence Council.

RAND – research and development.

StratCom – Strategic Communications Centre of Excellence.

UCC – United Cyber Caliphate.

ВСТУП

Актуальність теми. Актуальність дослідження обумовлена постійно зростаючою роллю інформації для суспільства та системи публічного управління. У сучасних умовах цифрового простору інформація та відповідні комунікації набули комплексного характеру, передбачаючи їх вплив на виникнення, ведення та характер війн нового типу – інформаційно-гібридних. Зважаючи на це, увага до забезпечення безпековості інформаційного простору набуває все більш важливого значення для національної безпеки загалом і для інституційної системи України. Ці зміни знайшли відповідний практико орієнтований відгук на найвищому рівні, зокрема, у межах указу Президента України від 25.02.2017 р. № 47/2017, що затвердив Доктрину інформаційної безпеки. Цей правовий документ передбачає створення єдиної системи забезпечення контролю та безпеки, а також протидії загрозам на всіх рівнях управління. Розробці цієї доктрини передувало схвалення Стратегії розвитку інформаційного суспільства в Україні (розпорядження Уряду України від 15.05.2013 р. № 386-р). Така стратегія передбачала гарантування законності та розумної достатності при зборі, накопиченні та поширенні інформації про громадян й організацій, а також забезпечення державного захисту інтересів українських громадян в інформаційній сфері.

У той же час, наукове осмислення як самого феномену інформаційно-гібридної війни, так і його впливу на всі аспекти життєдіяльності соціуму та функціонування інституційної системи публічного управління за умов цієї війни продовжує змінюватися, набуваючи ознак парадигмальності. Відзначимо, що теоретичні основи визначення інформаційної війни були закладені на початку XX ст., а з 2000-х років розпочався новий етап її дослідження – через сутнісні зміни цього феномену в умовах сучасних локальних конфліктів, а також трансформації світових війн у гібридні. Дане ж

дослідження передбачає, що через збільшення викликів і загроз, зумовлених цими змінами, інституційна система публічного управління потребує розвитку з урахуванням появи нових концепцій і стратегій ведення глобальних інформаційно-гібридних війн.

Отже, сучасне положення міжнародної безпеки є нестабільним, що зумовлює збільшення кількості конфліктів і зміну підходів до ведення війни нетрадиційними засобами. Останніми роками Україна та її населення змушені відчувати на собі всі ці зміни, а також інформаційно-гібридні загрози. Тому одним із найбільш важливих завдань для нашої держави є створення дієвої інституційної системи публічного управління, із визначенням координуючого суб'єкта. Гарантування безпеки для населення – це підтримка на належному рівні безпеки, яка виходить від нього. Такий рівень відображає стан задоволення соціальних інтересів, і тому важливо забезпечувати безпечний розвиток інформаційного суспільства. Зважаючи на це, актуальним є визначення теоретичних й організаційно-правових засад дієвого функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни.

Питання дослідження змісту системи публічного управління та вплив її на національну й інформаційну безпеку неодноразово порушувались у працях зарубіжних і вітчизняних науковців У. Бека, С. Бєлая, З. Бжезінського, О. Бондаренка, У. Вакко, Т. Воропаєвої, А. Гідденса, В. Горбуліна, М. Девідсона, Д. Деннінг, О. Довганя, С. Домбровської, А. Едельштайн, І. Кекіш, А. Кларк, О. Копанчук, О. Кравчука, О. Крюкова, Є. Магди, Ф. Майлза, О. Машкова, О. Мережко, Дж. Найа, Н. Нижник, Г. Ортіної, О. Пархоменко-Куцевіл, А. Помази-Пономаренко, Г. Почепцова, О. Радченка, І. Рущенко, Г. Ситника, В. Скуратівського, В. Торічного, Е. Тоффлера, Ф. Хоффмана, Е. Щепанського, Т. Ярового та ін. [11; 12; 13; 24–26; 33; 40; 42; 46; 66; 73; 79; 84; 95; 97; 102; 105–108; 122–124; 128; 131; 143–145; 161; 162; 181–182; 189; 190; 202; 209; 213; 219; 222; 223; 225]. В аналізованих наукових працях основна увага зосереджена на організаційних, правових, економічних,

ресурсних та інших аспектах державної політики у сфері національної безпеки загалом й інформаційної зокрема.

У той же час, вимагають комплексного відображення питання формування та функціонування інституційної системи публічного управління України в умовах інформаційно-гібридних війн. Це можливо зреалізувати за допомогою дослідження інструментарію «м'якої сили» і «жорсткої сили», виважене та вчасне реагування на які дозволяє унеможливити трансформацію інформаційних загроз у базис для виникнення та поширення інформаційно-гібридної війни. Отже, потреба у теоретичному, методичному та практико орієнтованому вирішенні окреслених завдань підтверджує актуальність дисертаційної роботи, її важливість, наукову новизну, зумовлює мету, завдання, предмет й об'єкт дослідження, а також апробацію та практичне впровадження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проведено в межах науково-дослідних робіт, які виконувались Національним університетом цивільного захисту України, а саме: за темою «Розробка наукових основ державного управління у сфері безпеки ринку соціально-економічних послуг України з точки зору цивільного захисту» (ДР № 0115U002035), у межах якої здобувачем визначено формування інституційних механізмів публічного управління невизначеностями в умовах інформаційно-гібридних війн.

Мета та завдання дослідження. *Метою* дисертаційної роботи є визначення науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розроблення практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

Зважаючи на поставлену мету дисертаційного дослідження, визначено такі науково-теоретичні та практико орієнтовані *завдання*:

– узагальнити теоретичні засади інформаційно-гібридних війн як інструменту соціогуманітарного протиборства в системі публічного управління;

– дослідити особливості функціонування структурно-функціонального механізму виникнення інформаційних війн та механізми формування інформаційних технологій в умовах інформаційно-гібридних війн;

– структуризувати інституційні механізми публічного управління України в умовах інформаційно-гібридної війни;

– охарактеризувати особливості та ризики функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни;

– проаналізувати інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни;

– обґрунтувати ризик-орієнтовані підходи до вдосконалення інституційної системи публічного управління України в умовах інформаційно-гібридної війни;

– запропонувати шляхи розвитку інституційної системи публічного управління України в умовах інформаційно-гібридних війн;

– визначити концептуальні засади прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління.

Об’єкт дослідження – публічне управління у сфері забезпечення інформаційної безпеки.

Предмет дослідження – інституційні механізми публічного управління в умовах інформаційно-гібридних війн.

Методи дослідження. Методологічну основою дисертаційного дослідження становить сукупність способів наукового пізнання та загальнонаукових принципів проведення дослідження, що враховують фундаментальні положення й праці вчених щодо аспектів публічного врядування й адміністрування, інституціоналізму, конфліктології тощо.

Дисертаційне дослідження побудовано на *концептуальному, системному, синергетичному й інституціональному підходах*, а також сукупності методів, а саме:

– *логічного узагальнення, синтезу й абстрагування* (під час розкриття сутності феномену інформаційно-гібридної війни як інструмент соціогуманітарного протиборства в системі публічного управління);

– *теоретизування й історичної формалізації* (для визначення механізмів формування інформаційної реальності як чинника забезпечення безпеки);

– *системного аналізу, порівняння, вибірки й опису* (з метою дослідження особливостей і ризиків функціонування інституційних механізмів публічного управління в Україні в умовах інформаційно-гібридної війни);

– *індукції та дедукції* (під час визначення концептуальних засад формування інституційних механізмів публічного управління невизначеностями в умовах інформаційно-гібридних війн);

– *групування та прогнозування* (з метою обґрунтування шляхів удосконалення інституційної системи публічного управління України в умовах інформаційно-гібридних війн).

Інформаційно-фактологічною базою дослідження є закони України, укази Президента України, нормативні акти Кабінету Міністрів України, статистична інформація Державної служби статистики України тощо.

Наукова новизна одержаних результатів полягає у визначенні науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

Наукова новизна результатів конкретизується в таких положеннях:

уперше:

– запропоновано шляхи розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, серед яких основними визнано, зокрема, створення єдиного координаційно-аналітичного центру/ради в Україні, на зразок американського Бюро протидії гібридній війні, яке напрацювало дієві управлінські практики реагування на

інформаційні загрози, а також налагодження результативної взаємодії України з іншими державами та міжнародними організаціями в напрямку вчасного протистояння цим загрозам;

удосконалено:

– визначення головної небезпеки інформаційно-гібридної війни як потенційної можливості цільового інформаційного впливу, зокрема негативного, на об'єктивно закладені та наявні суперечності практично на всіх рівнях державного та суспільного устрою в будь-якій країні чи регіоні, з метою примусового прояву цього впливу із заданим рівнем інтенсивності та в завідомо окресленому напрямку;

– ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, що (підходи) дозволили обґрунтувати сценарії реагування на ці війни – проактивний сценарій, який рекомендовано реалізовувати під час стратегічного планування та поступального забезпечення сталого розвитку, і реактивний сценарій, що передбачає оперативне реагування на інформаційні загрози, зокрема, у межах уточненої концепції протидії ним;

– концептуальні засади щодо прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління на пострадянському і вітчизняному просторі, на які впливають зовнішні та внутрішні фактори, серед яких найбільш загрозливими на сучасному етапі визнано соціальні, пов'язані з рівнем міграції громадян, їхнього добробуту, безробіття, демографічного розвитку та ін.;

дістало подальшого розвитку:

– визначення асиметрії як основоположної властивості інформаційно-гібридних війн, що відзначається латентністю та спрямованістю на найбільш вразливі місця в інформаційній обороні противника, наслідки недосконалості якої порівнянні із застосуванням нетрадиційної зброї, покликаної значно зменшити витрати на використання традиційної зброї й

отримати інформаційну перевагу над противником;

– структуризація інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, яка (структуризація) дозволила: 1) виокремити в складі цих механізмів організаційний, правовий і структурно-функціональний, які приводить у рух відповідна суб'єктна підсистема; 2) уточнити визначення поняття інформаційної безпеки як об'єкту державного впливу; 3) обґрунтувати шляхи підвищення результативності функціонування цих підсистем із наведенням конкретних нормотворчих пропозицій щодо усунення дублювання функцій органів державної влади у сфері інформаційної безпеки;

– визначення ризиків функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, унеможливлення трансформації яких (ризиків) у небезпеки інформаційного характеру рекомендовано здійснювати шляхом: протидії поширенню неправдивої та видозміненої інформації з боку країни-агресора, що впливає на розвиток українського суспільства й держави; формування цілісної інформаційної концепції й стратегії поширення об'єктивної інформації та протидії загрозам інформаційного характеру; підвищення рівня медіа-культури суспільства та його цифровізованого розвитку тощо;

– класифікація інструментів дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни, серед яких технологіям «м'якої сили» відведено особливе місце, тому що вони передбачають здійснення щодо держави-об'єкта (держави-мішені) неоголошеної гібридної війни з боку держави-актора, нейтралізувати негативний інформаційний вплив якої рекомендовано із застосуванням ризик-орієнтованих підходів, напрацьованих за кордоном.

Практичне значення одержаних результатів полягає в можливості їхнього застосування в діяльності органів публічної влади, що сприятиме підвищенню результативності інституційної реалізації публічного управління у сфері національної й інформаційної безпеки України.

Пропозиції щодо застосування ризик-орієнтованих підходів до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни використані в організаційно-аналітичній роботі Управління Служби безпеки України в Харківській області (довідка № 70/4-8859-1 від 14.11.2022 р.) і Черкаської районної ради (довідка № 10/01-13 від 06.02.2024 р.).

Крім того, пропозиції дисертації щодо концептуальних засад прогнозування інформаційно-гібридних війн на пострадянському та вітчизняному просторі використовувалися в навчальному процесі Національного університету цивільного захисту України, зокрема, при викладанні здобувачам вищої освіти другого (магістерського) рівня вищої освіти (спеціальність 281 «Публічне управління та адміністрування») таких дисциплін, як «Інформаційна політика в Україні» і «Сучасні геополітичні процеси: світ і Україна» (акт № 22-20 від 28.11.2023 р.).

Дисертація є самостійною науковою працею, теоретичні та прикладні результати якої отримано особисто здобувачем. Конкретний внесок здобувача в наукових працях, підготовлених у співавторстві, зазначений у списку опублікованих праць за темою дисертації [6].

Апробація результатів дисертації. Основні теоретичні положення та висновки дисертації були апробовані на міжнародних і всеукраїнських науково-практичних конференціях, зокрема, тези було опубліковано за результатами: Всеукраїнської науково-практичної конференції «Публічне управління в системі координат: демократія, децентралізація, місцеве самоврядування» (м. Мелітополь, 2019 р.); І Міжнародної науково-практичної «Modern research in science and education» (м. Київ, 2023 р.); XXXII Міжнародної наукової конференції здобувачів вищої освіти і молодих учених «Наука і вища освіта» (м. Запоріжжя, 2023 р.), Всеукраїнської науково-практичної конференції «Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття» (м. Житомир, 2023 р.).

Публікації. Основні положення дисертаційної роботи опубліковано у 11 наукових працях, із них: 6 статей у вітчизняних наукових фахових виданнях, включених до категорії Б; 1 стаття у закордонному науковому виданні за напрямком дослідження; 4 тез доповідей на конференціях. Загальний обсяг публікацій автора відповідно до теми дослідження становить 4,86 друк. арк.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ СОЦІОГУМАНІТАРНИХ ТЕХНОЛОГІЙ СУЧАСНИХ ІНФОРМАЦІЙНО-ГІБРИДНИХ ВІЙН У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

1.1. Феномен інформаційно-гібридної війни як інструмент соціогуманітарного протиборства в системі публічного управління

Розширення інформаційного простору та прискорення обігу інформації на основі нових технологій сприяє накопиченню реальних та штучно створюваних суперечностей у сфері інформаційної політики.

У зв’язку з цим в сучасних умовах все більше поширення отримує таке явище, як інформаційні та гібридні війни, які, у свою чергу, ведуть до загострення суперечностей інформаційного характеру [21, с. 140–143].

Українська держава в останнє десятиліття XXI століття зіткнулася з серйозними викликами в сфері національної безпеки (конфлікт на Донбасі, пандемія Covid-19, агресія Росії проти України, конфлікт, що розпочався в 2023 р. на Близькому Сході) тощо. У зв’язку з цим особливого уваги та докладного вивчення вимагає така форма конфлікту, як інформаційно-гібридні війни.

На наш погляд, ці явища – не однакові за змістом, але досить часто війни, що відбуваються у світі в останнє десятиліття, використовують механізми як з інформаційною складовою, так і є гібридними за формою реалізації. У зв’язку з цим логічним, на наш погляд, було б розглядати механізми реалізації сучасних загроз в інформаційній сфері як інформаційно-гібридні конфлікти (війни), оскільки ці явища перешкоджають не тільки розвитку інформаційного суспільства, але й зачіпають буквально всі сторони соціальної життя в масштабі всієї планети.

Зазначаючи в цілому позитивну роль переходу до інформаційного суспільства, що виражається у використанні нових сучаснихметодів і засобів обробки та передачі інформації з метою підвищення ефективності функціонування багатьох сфер діяльності, необхідно вказати й на важливу обставину в цьому зв’язку.

Насамперед слід мати на увазі, що позитивні властивості інформації та інформаційних технологій, які створюються на благо цивілізації, однаково доступні й часто використовуються в міжнародній політиці як механізми інформаційно-гібридних війн [222, с. 74].

Хвиля технічного прогресу внесла суттєві зміни в методи вирішення військових, економічних, торгових та інших конфліктів. Прямі силові методи уступають (або використовуються поряд з інформаційними механізмами) місце інформаційним. У сучасних умовах усе частіше ці методи використовуються комплексно. Яскравим прикладом ведення інформаційно-гібридних методів війни стала розпочата в 2022 р. війна Росії проти України.

Проблема гібридних війн (і гібридності в цілому) виходить на перший план у сучасній соціальній і політико-управлінській практиці. Дана проблематикавидається особливо важливою для державно-управлінського аналізу задля більш глибокого розуміння сутності, природи та розвитку війни як однієї з форм насильства [20, с. 67–69].

Сучасні дослідники інтерпретують інформаційно-гібридну війну як соціальне явище, породжене суспільством, як інструмент міждержавного військового протиборства, складову системи регулювання політичного конфлікту та інструмент державної політики.

Різні аспекти зазначеної проблематики досліджували зарубіжні вчені, такі як Е. Тоффлер [142], О. Васюта [19, с. 24–26], Ф. Хоффман [182] та деякі інші. В Україні проблематикою інформаційних війн займалися, зокрема, В. Горбулін [33], Г. Почепцов [106;108], І. Жаровська та Н. Ортинська [48] й багато інших науковців.

Поняття сучасної війни (не лише інформаційної, а й війни загалом) піддається серйозним трансформаціям, а саме еволюціонує в сучасних умовах [20].

Розуміння сутності трансформаційних процесів сучасних воєн уможливить створення та застосування адекватних важелів впливу на ці процеси, що неминуче позначиться на питаннях національної безпеки. Водночас розуміння руйнівної сили інформаційної війни (війн) потребує глибокого дослідження цього феномена.

Інформаційні взаємодії, контакти, конфлікти та різні форми їх вирішення є основою розвитку суспільства [64, с. 300]. Проблема інформаційних війн має кілька аспектів, що визначають інформаційну війну в контексті категорії «війна» взагалі.

Вся історія людства насичена конфронтаціями різних держав, які переростають у військові конфлікти та битви. Цей вид воєн вивчається воєнною історією. Руйнівні результати двох світових воєн привели міжнародне співтовариство до висновку про заборону збройних конфліктів [135, с. 70–72].

В історії військових зіткнень, заснованих на застосуванні збройних сил, інформація виконує роль ресурсу (план, розвідка тощо). Аналогічна ситуація складається з інформацією в економічних, політичних та управлінських конфліктах, які в певній мірі можуть бути віднесені до різновидів війн. Аналогічні процеси відбуваються і в економічному житті суспільства.

У розроблюваних західними вченими концепціях інформаційної війни значна увага приділяється поширенню інформаційними каналами противника або у світовому інформаційному просторі дезінформації або тенденційної інформації для впливу на оцінки, наміри та орієнтацію населення, державних і управлінських рішень з метою формування суспільної думки, вигідної для впливової сторони (це сьогодні досить яскраво проявляється в розпочатій у жовтні 2023 р. війні на Близькому

Сході).

Інформаційні війни (часто гібридні за методом реалізації) в сучасному світі в переважній більшості є формами соціальної взаємодії різних суб'єктів глобалізації, які керуються у своїх діях стандартами відповідних моделей світу (західний світ, православний світ, ісламський світ, теорія боротьби цивілізацій за С. Хантінгтона) [71, с. 128].

Саме тому діє- і життєздатність процесів глобалізації передбачає класифікацію агресивних інформаційних впливів з урахуванням їх характеру, спрямованості та адресності.

Будь-які маніпуляції та пропагандистські кампанії засновані на «ефекті резонансу», коли «імплантована» інформація, спрямована на зміну поведінки спільності людей, маскується під знання та стереотипи, вже існуючі в конкретній соціальній спільності, на яку спрямована пропагандистська кампанія [71, с. 129].

Розвиток засобів і технологій інформаційної війни робить все більш актуальним розробку засобів протидії маніпуляційним технологіям, а також розвиток методів публічного управління й захисту інформаційного простору держави, заснованих на демократичних нормах.

Процеси глобалізації, що відбуваються, супроводжувані конкурентною боротьбою світових і регіональних держав у геополітичному просторі, сприяють появі нових викликів і загроз безпеці національним інтересам всіх держав.

Однією з таких загроз є «інформаційно-гібридні війни», тому дослідження феномена «інформаційно-гібридних війн», характеристика їх найважливіших аспектів викликає науковий інтерес і знаходиться в центрі уваги сучасних наукових досліджень.

Слід підкреслити, що «інформаційно-гібридні війни» є доволі складним явищем, оскільки за своєю природою передбачають використання воєнних і невоєнних технологій одночасно або послідовно, залежно від об'єкта впливу.

До воєнних технологій відноситься використання сил спецпідрозділів, приватних військових компаній, терористичних і екстремістських угрупувань тощо. До невоєнних технологій або інструментів відносяться розвідувально-підривна діяльність спецслужб, «інформаційні війни», «кібервійни», «санкційні війни», медіа-ресурси, Інтернет-простір, соціальні мережі і т.д.

У ході «інформаційно-гібридної війни» можуть відбуватися й звичайні бойові дії, терористичні акти, кримінальне насильство та примушення. Вся ця різноманітна діяльність може здійснюватися різними методами, або навіть одним підрозділом, але з однією метою – отримання найбільшого, синергетичного (позитивного) та психологічного ефекту [64, с. 299–302].

Яскравими прикладами цього є події останніх років в Афганістані, Сирії, Іраку, Україні та в інших гарячих точках,в яких задіяні терористичні угруповання різної орієнтації, приватні військові компанії, криміналітет, протестний потенціал інтереси третіх країн та ін.

На сучасному етапі в рамках своїх геополітичних і геоекономічних інтересів світові та регіональні держави ведуть між собою «інформаційно-гібридні війни», причому на чужій території, тобто в окремому регіоні або в конкретній країні, чужими руками, при цьому заперечуючи свою причетність до всього.

Основним принципом «інформаційно-гібридних війн» є те, що вони ніколи не оголошуються, поєднують у собі різні види комбінацій явних і прихованих дій, провокацій та диверсій [48, с. 58].

У цьому плані країни пострадянського простору, включаючи Україну, як самостійні суб’єкти міжнародних відносин не є винятком і знаходяться в зоні геополітичних і геоекономічних інтересів світових та регіональних держав.

У контексті наведеного особливості прояву даної проблеми в реальній практиці публічного управління полягають у тому, що кожній

країні необхідно, в першу чергу, визначити види технологій/інструментів «інформаційно-гібридних війн», що використовуються, їх загрози, умови реалізації (внутрішні та зовнішні) у геополітичному просторі, в кожній країні – об'єкті таких війн, а потім вжити заходи протидії.

Різноманітність технологій інформаційно-гібридних війн вимагає адекватного протидії з боку органів публічного управління в контексті забезпечення ефективної роботи системи національної безпеки.

Серед сучасних зарубіжних дослідників з даної проблематики слід виділити таких вчених і військових експертів: румунського генерала спецслужб І. Пачепу, американських вчених Б. Гарта, М. Лайнбарджера, А. Сибровського, Дж. Гарстка, С. Манна, Е. Фишмана, С. Хеннесі, Дж. Ная, Д. Перцеффа, Дж. Кучера, М. Калдора, Е. Корибко, Д. Франклина, Дж. Ендрюса, грецького політолога І. Іліопулоса, шведського вченого Г. Саймонса, фінського вченого Р. Нюберга, президента Центру стратегічних досліджень Італії Г. Джузеппе, нідерландського генерала Ф. В. Каппа, Р. Триведі та ін. [74].

Інформаційна боротьба зазнала значних кількісних і якісних змін у міру створення єдиного світового інформаційного простору. Сучасна науково-технічна революція здійснила справжній переворот в інформаційній боротьбі.

Насамперед це характеризується тим, що психологічні операції стали проводитися більш активно та глобально, радіоелектронна боротьба розвивається, а нові інформаційні технології інтенсивно впроваджуються.

Сьогодні в інформаційну боротьбу залучається все більше сил і засобів, і її наслідки стають все більш масштабними. Наочним прикладом цього є війни та збройні конфлікти останніх десятиліть XX ст. та першої чверті XXI ст. (Югославія, Україна, Близький Схід та ін.). Їх аналіз з усією очевидністю свідчить про те, що результат військових дій будь-якого масштабу в сучасному світі визначається мистецтвом ведення інформаційної боротьби.

Інформаційна політика передбачає всеохоплюючий підхід, який враховує взаємовідносини між категоріями «загальне» та «особливе»[19, с. 163]. Цей факт набуває особливої ролі в умовах глобалізації. Розуміння інформаційної реальності доводиться представниками різних наукових напрямків.

З огляду на це аналізована нами проблематика наразі не мала прецеденту ні в історії науки, ні в світовій політиці. Це пов'язано з тим, що сутнісні характеристики інформаційно-гібридних війн у їх категорійному вираженні досі не були в повній мірі актуалізовані під спеціальні та масштабні дослідження сучасних проблем.

Як зазначають дослідники, дана проблема має низку особливостей:

1. По-перше, основні уявлення про глобалізацію тривалий час були підпорядковані концептуально-ідеологічному протистоянню матеріалізму ідеалізму, тому значно спрощували дослідницьку ситуацію, що позначається на сучасному мисленні.

2. По-друге, в силу стрімко складних соціокультурних і соціально-гуманітарних параметрів сучасної науки на перший план як «інноваційні» предметні області дослідження вийшли вивчення науки як самостійного джерела дослідження та методологія науки [20, с. 18].

З іншого боку, відсутність чітких, адекватних понять, які використовуються при аналізі сутності інформаційно-гібридних війн, не надає в повній мірі об'єктивної оцінки тих чи інших сучасних явищ міжнародного життя, що, у свою чергу, представляє широкий діапазон дій для суб'єктів глобалізаційного тиску.

Говорячи про одиніз проявів глобалізації – інформаційно-гібридні війни, український дослідник Г. Почепцов зазначає, що «... шлях базового підходу в цій галузі може спиратися на цілі у вигляді суттєвої зміни картини світу, що отримується в результаті комунікативного впливу. Когнітивна психологія, когнітивна психотерапія можуть дати підказки в цьому напрямку»[106, с. 21].

Тобто, різка зміна цілей, картини світу може розглядатися як певне інформаційне вторгнення, що становить небезпеку для отримувача цієї інформації. І це відчуття небезпеки значно зростає при переході його впливу від індивідуальної на масову свідомість.

Сучасна науково-технічна революція здійснила справжній переворот в інформаційній боротьбі. Психологічні операції стали проводитися більш активно й глобально, а нові інформаційні технології інтенсивно впроваджуватися. Сьогодні в інформаційну боротьбу залучається все більше сил і засобів, й її наслідки стають все більш масштабними.

Наприклад, у США, Японії, Німеччині, Франції, Ізраїлі та в інших розвинених країнах пильна увага приділяється інформації, яка вважається одним із головних факторів володіння сучасним світом [74].

В останній час все частіше в політико-управлінській практиці вживається термін «інформаційна війна». На думку декана Школи інформаційної війни та стратегії при Вашингтонському університеті національної оборони Д. Еджера, викладену в швейцарському журналі «Jane’s International Defense Review», саме поняття та концепція «інформаційної війни» залишаються предметом жвавої дискусії у військових і наукових колах Заходу [144, с. 193].

Однак західні спеціалісти вже одностайно визнали інформаційну війну вищою формою інформаційного протиборства. Так, у розробленій Комітетом начальників штабів Збройних сил США «Єдиній доктрині протиборства в галузі управління та зв’язку» термін «інформаційна війна» визначається як сукупність заходів, що вживаються з метою досягнення інформаційної переваги над противником шляхом впливу на його інформаційні системи, процеси, комп’ютерні мережі, суспільну та індивідуальну свідомість і підсвідомість населення та особового складу Збройних сил, при одночасному захисті своєї інформаційної середовища [98].

Таким чином, у цьому терміні поєднано два види інформаційної

боротьби – інформаційно-технічна та інформаційно-психологічна. Поняття інформаційна війна є широким поняттям і включає в себе безліч аспектів.

Сьогодні деякі фахівці, які займаються питаннями інформаційної безпеки, виділяють такі аспекти інформаційної війни:

– діяльність різних благодійних міжнародних фондів, клубів, сект;

– використання у відповідних цілях нейролінгвістичного програмування тощо.

Концептуальним стрижнем більшості робіт, що досліджують сутність інформаційних війн, стала теорія відчуження – відчуження сутності людини від її існування [64, с. 302].

В епоху телекомунікаційної революції цей «розрив» «ситуації людини» зумовлений насамперед засобами масової інформації, залученими у відносини влади та власності.

«Система», як прояв раціональної сторони людської природи, агресивно наступає на «життєвий світ» – спонтанні, унікальні прояви людської індивідуальності. Тому зняття відчуження в інформаційному суспільстві можливе, на нашу думку, лише як індивідуальнасамозаміна, що передбачає здатність учасників комунікації до відповідальності.

Відтак, західна думка в цілому означає відхід від того цінного, що мало місце в православній традиції, – від діалектики та принципу гуманізму. У ній спостерігається або схематизація проблеми, певне знеособлення несвідомого (Е. фон Гартман, А. Шопенгауер), або надмірна біологізація (З. Фрейд) [19, с. 172].

У цьому контексті для аналізу інформаційного простору може бути використаний потужний апарат сучасних соціологічних і політико-управлінських концепцій. Слід визначити основні напрямки такого аналізу.

Перший напрямок – розгляд інформаційного простору як специфічного соціального ресурсу, володіння яким дозволяє реалізовувати різні позаінформаційні цілі.

Другий напрямок – розгляд інформаційних відносин як соціальних. Інакше кажучи, опис та осмислення інформаційного простору як сукупності соціальних зв'язків і відносин. Наприклад, інформаційний простір можна розглядати з урахуванням ідей французького соціолога П. Бурдьє – як розподіл різного виду благ і послуг, а також агентів та їх груп [19, с. 84].

Третій напрямок пов'язаний з використанням при аналізі інформаційного простору апарату нової галузі соціології, яка так і називається – «соціологія простору».

Для можливості оцінити розстановку сил у тому чи іншому інформаційному просторі, а також управляти процесами, що відбуваються в ньому, слід увести в обіг поняття інформаційного поля.

Під інформаційним полем будемо розуміти карту інформаційного простору, на якій позначені соціальні групи, що цікавлять дослідника, а також їх оточення, зв'язки, характер взаємодії, обрані за певним ознакою.

Такими ознаками можуть бути територія, сфера дії, принцип утворення, характер поведінки групи.

При описі конкретного інформаційного поля на особливу увагу заслуговує поняття вектора інтересів соціальної групи. Вектор інтересів є одним з основоположних факторів згуртування групи, основою її існування та діяльності.

Крім того, чим чіткіше будуть визначені рамки вектора інтересів соціальної групи, тим точніше можна прогнозувати поведінку групи в майбутньому [108, с. 236].

Як уже зазначалось, між соціальними групами відбувається інформаційний обмін. Можливість такого обміну зумовлена наявністю інформаційних каналів, тобто управлінською системою універсального кодування-розшифровки символів і засобів їх доставки від однієї групи до іншої.

Інформаційні канали, які зв'язують дві або більше соціальні групи, є

динамічними, вони можуть розширюватися та звужуватися. Властивість динаміки застосовується до багатьох розглянутих у цій роботі понять, оскільки сама інформація є тонкою матерією і її обробка пов'язана з постійними змінами.

Інформаційні канали є основою для взаємодії, яка на практиці набуває конкретної форми. Окремий етап взаємодії, як правило, не вимагає використання всієї широти інформаційного каналу. У зв'язку з цим для опису інформаційної взаємодії доцільно використовувати вектор (спрямованості) взаємодії.

Даний термін призначений для опису спрямованості волі взаємодіючих суб'єктів, бажаних ними результатів, міри зацікавленості, використовуваних ними засобів, часу тощо. Вектор взаємодії слід відрізняти від вектора інтересів групи.

Перший характеризує систему відносин між досліджуваною групою та групами-контрагентами.

Другий більш повно розкриває відносини досліджуваної групи до багатьох факторів власного існування. Одним із видів інформаційної взаємодії є інформаційне вплив – передача інформаційного повідомлення одного суб'єкта інформаційного простору іншому з метою викликати в останнього певну реакцію. Інформаційне вплив можна класифікувати за такими підставами.

За способом – прямий і непрямий. За активністю – інтенсивний і пролонгований. За роллю в системі управління та комунікації – основний, додатковий і підготовчий. За цілями – конструктивний і деструктивний. За спрямованістю – вибірковий, широкий і спрямований.

Карту інформаційного простору можна складати щодо однієї групи стосовно різних ситуацій, що відбуваються в один і той же час: сприяння, конфлікт, накопичення інформації, досягнення цілей тощо.

Розглядаючи безпосередньо сферу політики та управління, а саме політичний інформаційне простір, оберемо в якості соціальних груп –

суб'єктів інформаційного простору – політичні спільноти як суб'єкти публічного управління – партії, рухи, прихильники конкретних політичних поглядів. Особливо слід відзначити поділ всіх суб'єктів політичного інформаційного простору на інформаційну еліту та інформаційні маси.

Еліта більшою мірою формує інформаційний простір: створює прецеденти, розставляє акценти на конкретних фактах і подіях, тим самим збільшуючи або зменшуючи їх значення. Маси підтримують саме існування інформаційного простору і, в силу представлення інтересів самих різних груп, – баланс його стану.

При цьому політико-управлінська еліта та еліта політичного інформаційного простору часто не збігаються, оскільки друга включає в себе, поряд з першою, ще й той прошарок населення, на думку якого орієнтується більшість.

Український учений Г. Почепцов вводить поняття «лідери думок», яким і позначає таку верству людей [108, с. 117]. Оскільки доступ до інформації є одним із найважливіших факторів конструювання інформаційних ієрархій, тож дуже важливою проблемою стає легітимність порядку доступу до інформації.

Легітимність у широкому розумінні слова – це правомірність, допустимість, виправдання певної дії на основі її відповідності загальноприйнятим нормам і цінностям. Це поняття має як юридичний, так і психологічний компонент. Так, М. Вебер виділив три типи легітимного порядку, спираючись на механізми його підтримки:

– порядок, підтримуваний «чисто аффективно: емоційною відданістю»;

– порядок, спирається на ціннісно-раціональні механізми, тобто на «віру в абсолютну значимість порядку як виразу найвищих незаперечних цінностей (моральних, естетичних або будь-яких інших»;

– порядок, підтримуваний релігійною вірою, тобто «вірою в залежність блага і спасіння від збереження даного порядку».

Ідеальний тип легітимного порядку – це порядок, що не потребує захисту, оскільки порядок забезпечується визнанням його всіма громадянами. Тому один із способів виміряти легітимність доступу до інформації – подивитися, скільки людей контролюють цей процес [74].

Залежно від доступу до інформації в інформаційному просторі можна виділити два протилежних ідеальних типу механізму конструювання інформаційної ієрархії.

Моноцентричний інформаційний простір має один яскраво виражений центр, який конструює основні інформаційні позиції, контролює їх функціонування, коригує статуси.

Звичайно, цей центр стикається з опором, оскільки кожна, навіть найслабша інформаційна позиція, наділена здатністю до пасивного опору, саботажу, імітації підпорядкування тощо.

Але в моноцентричному інформаційному просторі чітко виділяється центр, якому можна пасивно протистояти, але з яким неможливо конкурувати.

Таким чином, у багатьох визначеннях інформаційно-гібридної війни підкреслено, що метою такого роду війн є інформаційна перевага над противником.

Певною мірою використання цього поняття виправдано в кожній із теорій інформаційно-гібридних війн. По-перше, інформаційна перевага означає більш високу швидкість збору, обробки інформації та прийняття рішень на основі її аналізу.

Як наслідок, до переваги можна віднести вичерпне знання обстановки та можливість передбачити дії противника як у наступі, так і в обороні. Крім того, більш повне знання ситуації, як правило, дає можливість розглядати більшу кількість варіантів поведінки, з яких можна вибирати найефективніші та несподівані для протилежної сторони.

Розглянувши різні трактування концепцій інформаційних війн, можна дійти таких висновків. Основоположною властивістю

інформаційних (у даному випадку – інформаційно-гібридних війн) є їхня асиметрія, тобто латентність і спрямованість на найбільш вразливі місця в інформаційній обороні противника. Крім того, на даний час їхні наслідки можуть бути порівнянні із застосуванням кінетичної зброї, коли витрати на її використання можуть бути меншими в тисячі разів [98].

Американські вчені, які вважають себе основоположниками сучасної концепції ведення інформаційної війни, спочатку виходили з домінанти ведення інформаційних операцій у ході збройних конфліктів, і в цьому, на нашу думку, вони звузили для себе діапазон застосування власної інформаційної зброї [225, с. 4]. Особливо слід відзначити, що у США вперше на урядовому рівні було вироблено й закріплено поняття інформаційної війни, яке достатньою мірою відображає погляди сучасних теоретиків інформаційно-гібридних війн.

1.2. Структурно-функціональний механізм виникнення інформаційних війн у глобалізованому світі

Інформаційне протиборство завжди присутнє в найрізноманітніших сферах міждержавних відносин як у мирний, так і в період воєнного стану, як одна із форм вирішення неминучих суперечностей.

Однак завдяки появі новітніх засобів його ведення через активно освоєну інформаційну сферу утворилася нова фаза такого протиборства – інформаційна війна як одна із вищих і критичних форм його прояву.

Як ми вже зазначали в попередньому підрозділі, логічніше використовувати поняття інформаційно-гібридна війна. У зв’язку з цим важливим у розумінні інформаційно-гібридних війн є вивчення структурно-функціонального механізму формування інформаційних війн у сучасному глобалізованому світі.

Сам термін «інформаційна війна» з’явився приблизно в середині

сімдесятих років XX ст. На Заході «батьком» цього терміна називають вченого-фізика Томаса Рона, який у 1976 р. (у розпал холодної війни) назвав інформацію найслабшою ланкою збройних сил і оборони [31, с. 24–26, 41–46].

Практично всі сторони, які здійснюють інформаційний вплив у своїх інтересах, формують стратегію і тактику інформаційної війни, конкретний зміст і характер інформаційних операцій відповідно до своїх інтересів, цілей, завдань і наявних можливостей.

Основним смисловим призначенням інформаційної війни є використання всіх основних якостей і властивостей інформаційної сфери, заснованих на певних властивостях і законах створення, поширення, обробки і використання інформації з метою її трансформації у завідомо заданому напрямку [1, с. 31].

На нашу думку, головною небезпекою інформаційної війни є потенційна можливість цільового інформаційного, у тому числі негативного, впливу на об’єктивно закладені та наявні суперечності практично на всіх рівнях державного та суспільного устрою у будь-якій країні чи регіоні з метою їх примусового прояву із заданим рівнем інтенсивності та у завідомо визначеному напрямку.

В умовах глобалізації структурно-функціональних змін у системі світових взаємовідносин у всіх сферах, їхньої сильної взаємопов’язаності та взаємозалежності, коли проблеми публічного управління та державного регулювання вийшли на принципово інший рівень, а визначення перспектив політики будь-якої країни перетворилося на найскладніше багатостороннє завдання, роль інформаційної війни набуває особливої важливості [1; 2].

При виявленні сучасних форм і методів проведення інформаційних війн необхідно враховувати сучасні міжнародні реалії.

Так, наприклад, у глобалізаційних процесах і створенні єдиного інформаційного простору головну роль, на нашу думку, відіграє

економічна складова, яка значною мірою реалізується через інтереси транснаціональних корпорацій і неурядових організацій, що об'єднують осіб, які мають безпосереднє відношення до світового капіталу [24, с. 63–66].

Сьогодні термін «інформаційна війна» все ще носить публіцистичний характер і наразі не отримав повсюдного визнання у вітчизняних і зарубіжних наукових колах – про це свідчать безперервні дискусії з приводу того, що ж насправді ховається під цим поняттям, в чому сутність явищ, що відносяться до інформаційних війн, а також суперечки з приводу коректності та принципової застосовності даного терміна до тієї сфери соціальних взаємовідносин, яку прийнято називати інформаційним протиборством або конфліктом інтересів в інформаційній сфері соціальних систем [25, с. 156–158].

Як наслідок, ми можемо спостерігати використання в науковій літературі декількох десятків різних визначень терміна«інформаційна війна», явні переваги й настільки ж явні недоліки яких не дозволяють віддати абсолютну перевагу жодному з них.

Однак всі разом ці визначення досить повно й однозначно виділяють з усього можливого різноманіття існуючих у сучасному соціальному суспільстві взаємовідносин ті соціальні явища, взаємовідносини і процеси, які можна виділити в окрему групу з умовною назвою «інформаційна війна» [26, с. 18].

Наразі погляди багатьох представників наукового співтовариства на інформаційну війну, агресію і протиборство остаточно ще не сформовані. Усі існуючі терміни та поняття ще не пройшли перевірку часом і знаходяться в стані динамічного розвитку, вдосконалення і коригування, що, можливо, в недалекому майбутньому призведе до появи зовсім інших базових визначень.

У цілому підходи до визначення і сутності інформаційної війни можна поділити на три основні групи. Автори першої групи зводять

поняття інформаційної війни до окремих інформаційних заходів і операцій, інформаційних способів і засобів корпоративної конкуренції або ведення міждержавного протиборства, або ж збройного протиборства [142; 21; 75].

Найбільш відомим фахівцем, який відносить інформаційну війну до інформаційних способів і засобів ведення протиборства, є український вчений Г. Почепцов. Так, він зазначає: «Інформаційна війна – це комунікативна технологія впливу на масову свідомість з короткостроковими та довгостроковими цілями» [108, с. 43]. До комунікативних технологій дослідник відносить пропаганду, рекламу, виборчі технології, паблік рилейшнз.

Однак, на його думку, трактування поняття «інформаційна війна» через її засоби і методи повністю не розкриває сутності даного явища. Г. Почепцов вважає, що проблему засобів і методів інформаційної війни слід розглядати через призму поняття «інформаційна зброя».

Західний фахівець у галузі теорії інформаційного протиборства Е. Тоффлер визначає поняття інформаційної війни як «відкриті та приховані цілеспрямовані інформаційні впливи інформаційних систем одна на одну з метою отримання певного виграшу в матеріальній сфері» [142, с. 312].

При цьому він вважає, що поки противник усуває отриманий збиток, тобто зайнятий тільки собою, протилежна сторона має певну перевагу. Інформаційна війна не відрізняється від звичайної війни в частині ознак поразки. Агресор добивається перемоги, виключно підкоривши собі структури управління противника, які є інформаційною мішенню.

Звідси випливають й основні напрямки організації захисту: зменшення розміру мішені; захист мішені; регулярне знищення «інформаційних бур'янів»; встановлення жорсткого контролю за власною системою публічного управління.

Учений стверджує, що стратегія застосування інформаційної зброї носить виключно наступальний характер. На його думку, цей дуже

важливий результат, який ще не до кінця осмислений науковим співтовариством, дозволяє дійти до твердження про те, що наступальний характер інформаційної зброї значною мірою визначає обличчя інформаційної війни й дозволяє визначити потенційного агресора.

На думку ряду фахівців (Е. Тоффлер [142], Г. Почепцов [106] та ін.), інформаційну війну можна визначити як нову форму боротьби двох і більше сторін, яка полягає в цілеспрямованому використанні спеціальних засобів і методів впливу на інформаційні ресурси противника, а також у захисті власних інформаційних ресурсів для досягнення призначених цілей.

З цієї точки зору, в мирний час інформаційна війна носить переважно прихований характер. Її основним змістом є ведення розвідувальних і політико-психологічних дій щодо противника, а також здійснення заходів щодо власної інформаційної безпеки. Тому в період реальних загроз можуть з’являтися додаткові завдання, що вирішуються в інтересах забезпечення потрібної ефективності планованих бойових дій [37; 51].

До особливостей ведення інформаційної війни в цей період можна віднести:

– граничну обмеженість у використанні її сил і засобів;

– дотримання існуючих норм міжнародного права (наприклад, заборона радіоелектронного придушення певних частот і систем, передбачених Статутом Міжнародного союзу електрозв’язку та Регламентом радіозв’язку) та ін.

З початком військових дій сили і засоби інформаційної війни вирішують такі завдання:

– масоване вплив на інформаційний ресурс противника і запобігання зниження бойових можливостей своїх сил;

– проведення заходів щодо зниження рівня морально-психологічної стійкості військ противника і забезпечення нейтралізації інформації, що впливає на морально-психологічний стан свого особового складу тощо.

Англійські фахівці з інформаційних війн вказують на можливість того, що інформаційна складова воєнних дій у майбутньому стане переважаючою (підтвердження цьому це можемо спостерігати у воєнних конфліктах 2022–2023 років між Україною та Росією, між Ізраїлем і Палестиною та ін.) [179; 209].

Також вони підкреслюють, що інформаційну перевагу однієї армії над іншою завдяки революції у військовій справі з часом можна буде здобувати перемогу над противником, уникаючи фізичного зіткнення особового складу противників або роблячи це зіткнення дуже коротким і успішним.

На їхню думку, війни майбутнього зможуть вигравати шляхом застосування виключно або практично виключно віддалених засобів ураження військових і цивільних електронних систем противника.

Подібних поглядів дотримуються також китайські військові фахівці [189, с. 226]. Аналіз підходів до поняття «інформаційна війна» німецьких і канадських фахівців показує, що вони мало відрізняються від американських, англійських і китайських точок зору [178, с. 119].

Разом з тим, на думку аналітиків французького Центру досліджень стратегічних технологій (Centre de recherche etd'études sur les stratégies technologiques), діяльність європейських держав щодо збільшення власного потенціалу інформаційної зброї натикається на серйозну протидію США [47, с. 175].

Прагнучи дещо загальмувати власні розробки європейців, США навіть йдуть на продаж за демпінговими цінами космічних систем стеження та контролю ліній зв'язку, надають доступ до накопичених баз даних.

В якості прикладу можна навести угоди з Великою Британією і низку пропозицій, зроблених Німеччині. Експерти французького Інституту міжнародних відносин і стратегічних досліджень (Institut de relations international eset strategiques) вважають, що сьогодні союзники Сполучених

Штатів Америки по НАТО знаходяться в серйозній військовій залежності від США, оскільки у своїх системах озброєнь широко використовують американське програмне забезпечення (зокрема, вказують на систему позиціонування французьких ракет) [47, с. 182].

Аналізуючи нові аспекти американської воєнної доктрини, спрямовані на досягнення перемоги безкровними методами з мінімумом втрат, французькі фахівці звертають увагу на те, що головним засобом є не контроль над територією, а повне панування в «інформаційній сфері», що являє собою сукупність інформаційних систем і мереж зв'язку на планеті [35, с. 94]. При цьому війна набуває віртуального і невидимого характеру, що дозволяє отримати вирішальну перевагу, не розгортаючи бойових дій.

Аналогічні погляди на інформаційну війну стосовно воєнного часу висловлюють і вітчизняні фахівці. Так, український учений Г. Почепцов виділяє такі напрямки:

– фізичні атаки на елементи інфраструктури державного і військового управління (знищення центрів управління і управління);

– електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (радіотехнічна боротьба);

– отримання розвідувальної інформації шляхом перехоплення та аналізу великих обсягів інформації (радіотехнічна розвідка);

– здійснення несанкціонованого доступу до інформаційних ресурсів шляхом використання програмно-апаратних засобів прориву систем захисту інформаційних і телекомунікаційних систем противника з подальшим спотворенням, знищенням або викраденням інформації чи порушенням нормального функціонування цих систем (кібервійна);

– формування та масове поширення інформаційними каналами противника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри та орієнтацію населення і осіб, які приймають управлінські рішення [108, с. 374].

З огляду на з викладене вище, інформаційну війну у воєнний час можна визначити як комплекс інформаційної підтримки, інформаційних контрзаходів, заходів інформаційного захисту, що здійснюються відповідно до єдиного плану і спрямовані на досягнення й підтримку інформаційної переваги над противником під час бойових дій.

Важливо при цьому розуміти, що для збройних сил поняття «інформаційна війна» має чотири основні аспекти:

– визначення заходів для отримання інформації про противника і умови бою (засоби РЕР, погода, інженерне обладнання тощо) для збору інформації про свої та взаємодіючі війська;

– визначення заходів щодо блокування процесу збору противником інформації про наші війська;

– планування заходів щодо дезінформації на всіх етапах бойових дій;

– здійснення заходів щодо організації взаємодії з іншими військовими контингентами, що беруть участь у конфлікті [37].

Деякі американські експерти також пропонують називати інформаційну війну стосовно сфери сучасного збройного протистояння інформаційною боротьбою.

Фактично інформаційній складовій сучасних збройних конфліктів більше відповідає поняття «інформаційна боротьба», а не поняття «інформаційна війна».

На нашу думку, стосовно відкритих збройних конфліктів між державами термін «інформаційна війна» зможе повною мірою використовуватися тільки в майбутньому, коли збройна боротьба між державами здійснюватиметься виключно або переважно засобами і методами нанесення шкоди інформаційній сфері противника практично без фізичної участі особового складу збройних сил безпосередньо в зоні бойових дій.

Автори третьої групи визначення інформаційної війни вважають її явищем зовнішньо мирного періоду міждержавного протиборства, що

дозволяє вирішувати зовнішньополітичні завдання не силовим у традиційному розумінні шляхом [37]. Як об’єкти впливу інформаційних війн вони визначають:

– владні, управлінські, інформаційні системи;

– збройні сили;

– процеси прийняття управлінських рішень;

– свідомість населення;

– громадська думка;

– критична інфраструктура.

Як цілі інформаційної війни називають досить близькі положення:

– нав’язування необхідного для сторони, що впливає, рішення;

– нав’язування противнику своїх духовно-моральних і культурологічних цінностей;

– встановлення контролю над діями противника і напрямок його діяльності у вигідному для сторони, що впливає, руслі;

– цілеспрямований вплив на противника через свою і його інформаційну інфраструктуру;

– гуманітарне поневолення;

– нав'язування протиборчій стороні своєї політичної волі [51].

На концептуальному рівні інформаційну війну можна визначити як організацію інформаційного та психологічного впливу на потенційних противників з метою вчинення впливу на процеси прийняття ними таких рішень, які були б вигідні для своєї сторони [47].

Основна мета такої війни – не знищення противника, а «встановлення контролю над його діями і спрямування їх у вигідному для себе руслі». Тобто, інформаційна війна в класичному розумінні являє собою ідеологічну, психологічну обробку збройних сил, населення, військово-політичного керівництва противника з метою створення необхідної громадської думки або їх дезінформації і, таким чином, нав’язування протиборчій стороні своєї політичної волі.

Отже, при розробці заходів протидії сучасним акціям інформаційної війни доцільно виходити з наступного визначення інформаційної війни: інформаційна війна є найбільш жорсткою формою інформаційного протиборства між державами, що здійснюється насильницькими засобами і способами впливу на інформаційну сферу противника з метою вирішення стратегічних завдань.

Суть інформаційної війни в сучасний період полягає у прихованому управлінні політичними, економічними, воєнними та іншими процесами держави-противника.

Найважливішою властивістю інформаційної війни є відсутність доказових свідчень причетності сторони, що впливає, до заподіяння шкоди протиборчій стороні. Головною відмінною ознакою дій інформаційної війни є підривні дії щодо інформаційної сфери держави-противника зі стратегічними цілями [131, с. 324–326].

Об’єктами поразки в інформаційній війні є:

– свідомість, воля і почуття населення країни-противника, особливо в періоди виборів, всенародних референдумів, кризових ситуацій;

– системи прийняття управлінських рішень у політичній, економічній, соціальній, науково-технічній сферах, у сферах забезпечення безпеки і оборони;

– інформаційна інфраструктура країни-противника.

Основними суб’єктами ведення інформаційної війни виступають зовнішньополітичні відомства та спецслужби зарубіжних держав, а також інформаційно-пропагандистські структури.

Проведені дослідження дозволяють також виділити основні й характерні риси інформаційної війни, які відрізняють її від інших форм ведення воєнних дій, висувають нові проблеми перед її учасниками та заслуговують на особливу увагу, а саме:

– незначні витрати на розробку та застосування інформаційної зброї. Вартість розробки високоякісних засобів ведення інформаційної війни

відносно невелика й доступна широкому колу її учасників. На відміну від уже наявних технологій створення ефективних озброєнь, нові потенційні засоби інформаційної війни можуть бути створені окремими фахівцями або групами фахівців, що входять до «Глобальної інформаційної інфраструктури» (далі – ГІП) незалежно від їх географічного розташування;

– розмитість традиційних кордонів (географічних, між приватними та державними структурами, між протиправними діями та діями військового характеру). Традиційні кордони між державами, між структурними елементами суспільства та публічного управління і навіть концептуальні визначення для таких утворень, як, наприклад, «національне держава», стають досить умовними. Відмінності між суспільними та особистими інтересами поступово згладжуються як наслідок процесу, що посилюється, їх взаємопов'язаності в рамках інформаційної інфраструктури. Бурхливий розвиток інформаційної мережі Інтернет і розширення числа її користувачів у глобальному масштабі пояснюється вільним, відкритим і нерегульованим доступом до можливостей цієї інформаційної системи. В рамках цієї інформаційної мережі, характерними рисами якої стали плюралізм і зростаюче число протиріч між інтересами груп користувачів, з'являються широкі можливості злочинної або військової діяльності;

– підвищення ролі управління сприйняттям. Управління сприйняттям людей може прийняти набагато більші масштаби. Незважаючи на те, що організовані та систематичні заходи з дезінформації в історичному плані не так ужей нові, розроблені засоби інформаційної війни можуть стати зовсім новим потужним інструментом маніпуляції сприйняттям;

– нові виклики стратегічної розвідки. Перед стратегічною розвідкою постають фундаментально інші завдання. Усвідомлення нових загроз і вразливості системи забезпечення національної безпеки у зв'язку з інформаційною війною настійливо вказують на необхідність ретельного перегляду класичних розвідувальних методів збору та аналізу

розвідувальних відомостей;

– велика складність завдань тактичного попередження та оцінки збитків. Тактичне попередження та оцінка збитків також стають завданнями особливого роду. З урахуванням різноманіття та хитромудрості способів і засобів впливу й захисту в рамках інформаційної інфраструктури виникає необхідність створення нової системи тактичного попередження та оцінки збитків, здатної виявляти й розпізнавати випадкові збої в роботі інформаційних мереж, помилки програмного забезпечення, а також внесення програмних закладок, що забезпечують ведення шпіонажу, або завчасне розгортання бойових програмних засобів;

– уразливість території держави. Зростання залежності економіки та суспільства в цілому від високопродуктивних комп'ютерних систем перетворює інформаційну інфраструктуру країни на сукупність нових «стратегічних» цілей. Загроза ключовим елементам національної інформаційної інфраструктури може чинити серйозний тиск на процес прийняття управлінських рішень, тоді як безпосередній інформаційний вплив здатний повністю дезорганізувати всю систему державного управління.

В умовах такого конфлікту державні кордони для забезпечення безпеки країни особливого значення вже не мають. Об'єктами нападу можуть бути інформаційні системи, які є «нервовими» центрами адміністративного та військового управління. Однак можливі й інші об'єкти, на яких зосереджена або циркулює інформація, що має важливе значення для нормального функціонування різних структур держави та суспільства [131, с. 345–346].

Ці особливості інформаційних воєн дозволяють визначити основні відмінності між інформаційною війною та звичайною (традиційною), які полягають, на наш погляд, у такому:

1. Звичайна війна має відомий і чіткий арсенал впливу. Через його передбачуваність можлива побудова у відповідь певних оборонних систем

і проведення захисних заходів. Ситуація стає іншою у разі інформаційних війн. Арсенал впливу в них характеризується достатньою часткою гнучкості та непередбачуваності. У більшості випадків в інформаційній війні відсутня можливість передбачити напрямок та інструментарій можливої атаки.

2. У разі звичайної війни територія захоплюється повністю, тоді як за інформаційної війни можливе поетапне захоплення. Імовірна окрема робота з лідерами думок, з молоддю тощо, тобто при збереженні загальної норми окремі зони можуть виводитися з-під інформаційного впливу. Інформаційна війна в цьому плані виглядає як «мирна війна», оскільки може проходити на тлі загального миру та благополуччя.

3. Можливість багаторазового захоплення одних і тих же людей. У рамках війни звичайною є логіка «так – ні», у разі інформаційної війни є варіант нечіткої логіки, коли оцінки можуть даватися з певною ймовірністю (на 40, 60% і т.д.). Більше того, одночасно на людину можуть впливати різні «противники», фактично захоплюючи різні тематичні зони її свідомості. У війні ті, хто захоплює територію, і ті, хто потім її освоює, є різними людьми й виконують різні соціальні ролі. У разі інформаційної війни ці позиції збігаються. Інформаційна війна багато в чому стирає чітке розмежування типу «друг/ворог». Можна вважати когось союзником, хоч насправді він є ворогом.

4. Людина не в змозі реагувати на невидимий вплив, подібний до радіації. Ця дія може приймати доброзичливу форму, на яку навіть чисто біологічно людина не готова відповідати агресивно.

5. На відміну від звичайної війни, в якій фізична зброя, що застосовується, руйнує в межах зони поразки все, інформаційна зброя діє вибірково, охоплюючи різні верстви населення. Звичайна зброя впливаєна будь-яку частину населення однаково.

6. Головною небезпекою інформаційної війни є відсутність чітко ідентифікованих (видимих) ознак руйнівного впливу, характерного для

звичайних воєн. Населення навіть не відчуває, що воно зазнає впливу. У результаті суспільство не приводить у дію захисні механізми, що є в його розпорядженні. Почуття небезпеки, яке в інших ситуаціях діє безвідмовно, у цьому разі не реагує. На відміну від звичайної війни, в якій фізична зброя, що застосовується, руйнує в межах зони поразки все, інформаційна зброя діє вибірково, охоплюючи по-різному різні верстви населення. Звичайна зброя впливає на будь-яку частину населення однаково.

1.3. Механізми формування інформаційних технологій в умовах інформаційно-гібрідних війн

Як уже зазначалося в попередньому підрозділі, поширення інформаційних технологій різко змінює відносну цінність ресурсів, висуваючи на перший план механізми формування інтелекту та фінансів як найбільш мобільних факторів в умовах сучасної економіки та управління, для яких зростаюче значення має час і швидкість інформатизації суспільства.

Найважливішим практичним наслідком цієї тенденції є відносне знецінення традиційних технологій і продуктів їх застосування по мірі поширення технологій, що втілюють нові принципи, цінні знання та оброблені інформаційні ресурси.

У руслі цієї тенденції США та технологічно розвинені країни останнім часом проводять політику «скидання» за межі країни не тільки екологічно, але й «інтелектуально брудних» і примітивних виробництв з низьким обсягом наукоємної продукції та прибутковості [32].

Основними наслідками розвитку та поширення інформаційних технологій є:

– поглиблення сформованого розриву між розвиненими та розвиваються країнами, а також поява нового розриву між

постіндустріальними країнами та країнами з традиційними індустріальними економіками;

– виділення в усіх країнах світу груп людей, пов’язаних з інформаційними технологіями, та їх відокремлення в автономне «інформаційне співтовариство»;

– перетікання інтелектуальних ресурсів у найбільш розвинені країни з поступовою концентрацією інформаційно-комунікаційного потенціалу в корпораціях і державах постіндустріального типу;

– уповільнення та/або припинення науково-технічного прогресу в неінформатизованих суспільствах з наростанням у них фінансових труднощів і соціальної деградації за межами країн з інформаційними економіками [52].

Серед іншого серйозної уваги заслуговує поява соціально орієнтованих інформаційних технологій. Це особлива різновидність високих технологій (high-tech), які отримали за аналогією назву «highhume». Розробка та поширення таких технологій пов’язані з великими спокусами та небезпеками. Ефективність впливу інформаційних технологій на свідомість породжує спокусу вирішувати реальні проблеми не шляхом коригування дійсності, а методами зміни індивідуальних і масових уявлень про ситуацію, що склалася [62, с. 5].

Використання комп’ютерів може бути як благом, так і злом для суспільства. Для інформаційних технологій це має особливе значення, оскільки вони за своєю соціальною та психологічною суттю не є традиційними засобами взаємодії з матеріальним світом, а комплексами з перетворення живої людської свідомості. Дана обставина визначає специфіку генерування небезпек інформаційно-технологічної природи, а саме:

– можливість перенесення психології конфлікту в інформаційний простір та розв’язання руйнівної комп’ютерної війни з перспективою розвалу систем громадського управління та технологічної деградації

інформатизованих сфер;

– маніпулювання світовими фінансами та дестабілізація фондового ринку, що загрожує небезпечним зниженням якості інвестицій та виникненням неприйнятного ризику для всієї глобальної валютно-фінансової системи;

– масове культивування серед окремих груп (на основі врахування їх соціальних та національних особливостей) певного способу життя та стилю соціальної поведінки, що може розвинути «погані схильності» (типу вживання наркотиків) у суперсучасний різновид етнічної та класової зброї [157, с. 186].

Наведені та інші небезпеки, виклики інформаційного розвитку сучасного світу спричинили постановку на порядок денний, як уже наголошувалось, проблеми так званої інформаційно-гібридної війни, яка визначається сьогодні як прихована діяльність з метою забезпечення інформаційного домінування, що набуває значення не менше важливіше, ніж традиційне військове домінування. Воно спрямоване на формування інформаційно-залежних відносин від суб’єкта впливу як на технологічному, так і на соціально-психологічному та державно-управлінському рівнях.

Одним із головних досягнень сучасної цивілізації в умовах глобалізації, яка на даний момент вважається основною тенденцією історичного розвитку, є Інтернет-революція [161, с. 44].

Процес поширення інформаційних технологій пов’язаний як з новими досягненнями, так і з появою цілої низки нових проблем. Користь від цієї Інтернет-революції може позначитись у політичній, економічній та соціальній сферах [130, с. 234].

Проблема пошуку механізмів взаємодії традиційної політичної структури суспільства та нового інформаційного простору вже достатньою мірою привертає підвищену увагу вчених, які представляють різні галузі знання.

Проблематика, пов’язана з особливостями функціонування політичних інститутів за умов формування інформаційного суспільства, є новою для сучасної науки. Серед авторів, які займаються цими питаннями, слід передусім назвати Д. Белла [8-9], З. Бжезинського [13], П. Друкера [44], Р. Кана [188], М. Кастельса [54], Р. М. Маклюєна [156], Й. Масуді [77], М. Пората [199], Д. Рісмена [205], Т. Стоуньєра [52], Д. Тапскотта [216], Е. Тоффлера [142] та ін.

Інтенсивне впровадження інформаційно-комунікаційних технологій (далі – ІКТ) в органи публічного управління дає можливість наблизити їх до громадян, розширити послуги населенню, підвищити ефективність та скоротити витрати на держсектор, стимулювати створення нових інформаційних продуктів і послуг приватним сектором шляхом адекватної державної політики [216].

Використання до органів громадського управління ІКТ – складний процес, зумовлений низкою чинників, зокрема:

– вертикальної структурою адміністрації, яку потрібно замінювати на горизонтальну;

– недостатнім розумінням із боку державних службовців (потрібні інтенсивні програми навчання);

– браком баз даних для публічного доступу.

За допомогою Інтернету держава може інформувати громадян, суттєво просунути формування інформаційного суспільства. Роль держави, на наш погляд, має полягати у знаходженні балансу між конкуренцією та регулюванням, свободою персональних комунікацій та необхідністю захищати суспільні інтереси від терористів, свободою слова та захистом моральності та інтересів неповнолітніх. Сюди відноситься ідея універсального доступу до мережевих послуг та інформації, доступ до урядової інформації [125].

Водночас анонімність подібних акцій насправді є великою ілюзією. Справа в тому, що підключення до Інтернету у будь-якій точці світу

можливе лише через сервер компанії-провайдера, який здійснює докладний запис того, хто, з якого телефону, коли і до яких ресурсів Мережі звертався.

З цього випливає, що уникнути попадання в так звані лог-файли неможливо. У разі розміщення сайту з компроматом на так званих публічних західних сайтах, що надають на умовах анонімної реєстрації в принципі будь-який дисковий простір для розміщення в Мережі будь-якої інформації, реальних механізмів виявлення авторів сайтів зараз офіційно не існує [56, с. 21–24].

Мабуть, усі відомі на сьогодні «зливи негативної інформації» – ланки одного ланцюга:

– проводяться експерименти з вивчення того, як компромат поширюється з Інтернету в традиційні ЗМІ – в газети, на радіо та ТБ;

– яким може бути індекс цитування;

– які ЗМІ будуть готові тиражувати прочитане на анонімному сервері;

– чи вдасться через мережу впровадити в суспільну свідомість нові ідеї [59, с. 173].

Експериментально зібрані таким чином відомості можуть бути використані для планування та здійснення інших акцій чорного PR. Подібні сайти, як правило, не потребують систематичного оновлення. Вони створюються для разового застосування, а потім – «вмирають». Але життєздатність самого явища використання Інтернет-сайтів для «вкидання» компромату є фактом, і ця аж ніяк нечиста технологія існуватиме, доки на неї існує політичне «замовлення» [68, с. 87].

З формальної точки зору цей спосіб відрізняється відносною дешевизною в порівнянні з традиційними способами. Використання Інтернету для цієї мети можливе й під час проведення виборчої кампанії будь-якого рівня. З одного боку, з Мережі політико-управлінська еліта черпає інформацію, а з іншого, оскільки оперативно встановити джерело

такого роду імпульсу практично неможливо, – звернення до суду як засобу захисту від таких дій є малоефективними [68, с. 51].

Як найефективніший засіб підвищення рейтингу політика-управлінця-початківця політичні технологи широко використовують конфлікти й скандали, а також «технології» спеціально створених анекдотів і чуток, що формують певний електоральний настрій [93, с. 120].

Факт включення до рейтингу маловідомих кандидатів чи політичних партій сам по собі підвищує їхні шанси на виборах, оскільки потенційні виборці таким чином знайомляться з ними через публікації результатів опитувань у ЗМІ. Отже, цілком можливо використовувати опитування у виборчих кампаніях для маніпулювання громадською думкою.

Інтернет має свою особливу специфіку, завдяки якій він відрізняється від ЗМІ – його неможливо «інформаційно монополізувати», на відміну, наприклад, від центральних телеканалів [76, с. 32]. Ця особливість Мережі є одним із пояснень її зростаючої популярності. Крім того, аудиторія Інтернету, що збільшується, досить незалежна: на відміну від телебачення і преси, що не залишають споживачеві права самостійно вибирати новини, Мережа дозволяє «фільтрувати» інформацію на свій розсуд і почуватися більш обізнаним про те, що відбувається у світі. Користувачі мають можливість отримувати інформацію саме тоді, коли щось трапляється; у цей момент зростає інтерес до найбільш оперативних і повних джерел, серед яких очевидні технологічні переваги мають мережеві ЗМІ, що стають серйозним конкурентом традиційним медіа.

До переваг Мережі слід також віднести нульову вартість тиражування та простоту виробництва електронних документів. Впровадження нових технологій інформаційного суспільства починає істотно впливати на соціально-економічну та державно-управлінську сфери суспільства в напрямку як політичної стабілізації, так і можливої дестабілізації суспільства [50, с. 9].

Корисною особливістю Інтернету є звична структура електронних

текстів – гіпертекст. Якщо при традиційному викладі поняття зв'язуються лінійно в тексті документа, то гіпертекст створює багаторівневі зв'язки між словом і його докладнішим тлумаченням: кожен термін одночасно може бути «посиланням», тобто логічно пов'язаний з рядом контекстів і за їх допомогою описаний, проілюстрований або забезпечений коментарями будь-якого обсягу та глибини [152, с. 68].

Посиланнями можуть бути будь-які елементи електронної сторінки (веб-сторінки) – текст, картинки, кнопки. Якщо натиснути на них мишкою, програма перегляду сторінок (браузер) відправить серверу, вказаному в посиланні, запит на документ, який у ній і позначений.

Таким чином, можна переходити від документа до документа, від сервера до сервера, користуючись тим, що Інтернет є гігантською мережею, що зв'язує документи і сервери один з одним нитками гіперпосилань.

Серед інших проблем Мережі є й суто технологічна: недостатня поки що ступінь інтеграції Інтернет-служб, що не дозволяє повною мірою скористатися глобальними ресурсами Інтернету. Принципову доступність будь-якої інформації через мережу не слід плутати з реальними можливостями роботи з нею. У результаті віддача від доступу до глобального океану інформації багато в чому є ілюзорною [43, с. 26].

Освоєння Мережі означає насамперед реальну можливість знайти необхідну інформацію. У результаті користувач (навіть який сплатив доступ до платних баз даних) змушений самостійно шукати в численних «чорних ящиках» локальних баз даних, не маючи можливості систематичного глобального пошуку.

За масштабами впливу на електорат Інтернет поки що поступається традиційним друкованим й електронним ЗМІ. Однак ті переваги, якими він володіє, дозволяють розглядати його як важливу складову частину всього ідеологічного та політико-управлінського інструментарію формування суспільної свідомості.

Найнебезпечнішою рисою ЗМІ (й Інтернету як ЗМІ), як вважають багато фахівців, є їхня здатність подавати інформацію таким чином, щоб за видимою об'єктивністю у великої маси людей формувалася необхідна (замовлена) картина реальності [53, с. 25].

Формування такої віртуальної картини підтримується всією потужністю технологій пропаганди й контрпропаганди, що реалізуються за допомогою ЗМІ та Інтернету, який часто виступає цілком конкурентоспроможним інструментом ЗМІ, незважаючи на їх поки що незрівнянно більшу доступність для більшості населення країни. Наприклад, висвітлення бойових дій РФ в Україні чи Ізраїлю на кордоні з Палестини тощо.

Сила та результативність інформаційно-психологічних впливів (далі – ІПВ), здійснюваних за допомогою ЗМІ і, перш за все, телебачення, пояснюються сильним психологічним ефектом причетності до подій, коли людина занурюється в них «тут і зараз» [108, с. 70].

Цей своєрідний ефект, що отримав назву «ефект CNN» (найбільша американська служба новин), оцінюється багатьма дослідниками як головна умова ефективності ІПВ за допомогою ЗМІ. Оскільки більшість радіомовних станцій і телевізійних каналів, новинних та політичних програм представлено в Інтернеті, ефект CNN спрацьовує також і для користувачів Інтернету [106, с. 72–74]. При цьому не можна не відзначити такий фактор, як відсутність офіційної (політичної чи моральної) цензури, свободи розповсюдження та отримання інформації в Інтернеті.

Сьогодні групи різної політичної орієнтації та неурядові організації можуть використовувати Інтернет для мобілізації політичних сил проти своєї та інших держав у кризових ситуаціях, що загрожують невизначеними наслідками.

Неврегульованість правових відносин при поширенні інформації в Інтернеті тягне за собою свободу розповсюдження наклепницької та недостовірної інформації.

Кампанії подібного роду ставлять серйозні проблеми не лише перед державою та системою управління, а й перед суспільством, зацікавленим у об'єктивній інформації [125, с. 76]. При цьому може виявитися так, що вище керівництво країни, як і суспільство в цілому, можуть не знати, що ж відбувається насправді.

Дана проблема посилюється відсутністю в Інтернеті загальновизнаних правил поведінки, простотою вчинення правопорушень (розголошення таємниць, незаконного копіювання інформації персонального характеру, порушення авторських прав та ін.), анонімною присутністю в Мережі без небезпеки піддатися покаранню за поширення хибної інформації, відсутністю самоцензури.

У розвинених країнах відзначається тенденція кращого отримання інформації з Інтернету, ніж у вигляді звичайних ЗМІ. Пояснюється це суттєвим скороченням часу на пошук інформації. Користувач сам відбирає потрібну йому інформацію. Звичайні ЗМІ націлені на нав'язування інформації та максимально можливе управління подачею інформації для досягнення політичних чи інших цілей [108, с. 23].

Цілком легальним способом ІПВ для користувачів Інтернету є поширення пропагандистських інформаційних матеріалів за допомогою різних технологій залучення уваги, організації віртуальних груп за інтересами, збору адрес електронної пошти для організації масових розсилок.

Існує два шляхи розповсюдження інформації в Інтернеті. Перший – користувач відвідує сайт із необхідною інформацією. Другий – користувач отримує інформацію на адресу своєї електронної пошти. Збільшення відвідуваності конкретного сайту досягається за допомогою включення його Інтернет-адреси до різних популярних пошукових систем. Іншою технологією привернення уваги є розміщення банерів на різних часто відвідуваних сайтах [108, с. 23].

Створення різних віртуальних груп за інтересами в Інтернеті також є

легальним способом просування тих чи інших ідей. Постійна віртуальна група, що утворилася, свідчить про наявність людей, здатних до сприйняття ідей, що просуваються, а зростання чисельності групи показує ефективність ІПВ. Віртуальна спільність людей, що склалася, може стати основою для утворення реальних організацій терористичного або кримінального спрямування з важко виявляється структурою і системою зв'язку.

Технології швидкого поширення інформації через комп'ютерні мережі будуть набувати все більшого значення, оскільки дозволяють цілком легально проводити цілеспрямовані інформаційно-пропагандистські заходи без контролю з боку системи управління.

Сьогодні ступінь довіри населення до інформації, розміщеної в Інтернеті та поширюваної традиційними ЗМІ, однаковий [107, с. 25]. Суть справи в тому, що більшість населення звикла до маніпулятивного характеру ІПВ, визнає їх цивілізованими засобами політико-психологічної боротьби і вже виробила політичний імунітет та прийоми особистісного психологічного захисту, проте щодо анонімних повідомлень, запущених Інтернетом, справа складніша.

Хоча використання глобальної комп'ютерної мережі в політичних цілях лише набирає сили, в Інтернеті вже вільно розташувалися політичні авантюристи, провокатори-пропагандисти, розпалювачі чуток, які позбавлені доступу до державних ЗМІ.

Очевидно, що політичні маніпуляції через Інтернет слід розглядати як об'єкт міжнародно-правового регулювання. Рано чи пізно доведеться вирішувати питання електронної цензури на міжнародному рівні, незважаючи на всі проголошені декларації про свободу інформації.

Сила ІПВ в Інтернеті збільшується багаторазово завдяки новим технологіям мультимедіа та віртуальної реальності (далі – ВР) [125, с. 87]. Ці технології підтримують емоційну складову ІПВ, залучаючи користувача до нових переживань щодо прочитаного чи почутого.

Знаходження у віртуальному просторі взагалі небезпечне для людини, оскільки імітація дійсності є своєрідним психологічним інструментом, що впливає на свідомість і підсвідомість людини.

Можуть виникати й нові форми опосередкованого соціального контролю, які базуються на замаскованому маніпулюванні свідомістю, м'якому придушенні психіки [53, с. 88].

З практичної точки зору технології ВР дозволяють зробити ІСВ індивідуальним, орієнтованим на маніпуляцію свідомості конкретної особистості. Часто це відбувається за допомогою витонченої реклами тієї чи іншої особи чи ідеї, що супроводжується продуманим візуальним фоном. Технології ВР можуть використовуватися для створення будь-якої реальної ситуації, поєднуючи елементи реального відео та елементи, створені комп'ютерною графікою.

У своєму розвитку Інтернет постійно вбирає в себе нові й нові функції та послуги, при цьому майже не втрачаючи функції та послуги попереднього етапу, особливо ті з них, які встигли обрости аудиторією прихильників і користувачів.

Інтернет починався і входив у життя своїх адептів із двох вихідних видів мережевого сервісу. Обидва вони можуть бути віднесені до асинхронних видів спілкування, що не потребує одночасного перебування у спілкуванні, що спілкуються в єдиному середовищі. Це, насамперед, обмін електронною поштою (e-mail), як правило, між двома співрозмовниками, хоча можливе множинне розсилання якогось повідомлення або підключення до мікросередовища спілкування деяких (взагалі – небагатьох) партнерів зі спілкування [54, с. 39].

При масовому підключенні партнерів зі спілкування виникає інший сервіс асинхронних обговорень, що включає в себе електронні дошки оголошень, листи розсилки (комп'ютерні телеконференції) або ехоконференції, а згодом і веб-форуми [76, с. 231].

Функції Інтернету не обмежуються комунікацією – одна з найбільш

масових функцій (пізнавальна) є розміщення на сайтах та сторінках WWW інформаційних матеріалів, а також пошук інформації.

Ігрові функції Інтернету знову-таки включають безліч азартних, настільних, реальних (наприклад, фінансових) або спеціалізованих ігор з комп'ютерною програмою, з віддаленим партнером, з безліччю гравців, що одночасно або асинхронно беруть участь у грі та ін. [53, с. 89].

Так, широко поширені електронні казино, електронні біржі для реальних трансакцій – купівлі-продажу акцій, сайти прихильників поширених інтелектуальних (шахи, го, реверс та ін.) або карткових ігор.

Величезною популярністю користуються так звані комп'ютерні ігрові, пізнавальні та комунікативні функції Інтернету, що поділяються на загальнодоступні та закриті. Останні включають у себе платні чи внутрішньо-фірмові (тобто доступні для всіх або відібраних співробітників), або доступні лише передплатникам ресурси – такими ресурсами можуть бути форуми для спілкування, інформаційні матеріали, віртуальні ігрові «кімнати» тощо [53, с. 88].

Як уже зазначалося, незважаючи на всю різноманітність активності користувачів Інтернету, можна виділити три основні види діяльності, яку вони здійснюють: пізнавальну, ігрову та комунікативну. Цим різновидам діяльності відповідають глобальні трансформації особистості, серед яких:

1. Захопленість пізнанням у сфері програмування та телекомунікацій чи, як крайній варіант, хакерство.

2. Захопленість комп'ютерними іграми та, зокрема, іграми з Інтернету чи, як крайній варіант, так звана ігрова наркоманія.

3. Захоплення мережевою комунікацією чи, як крайній варіант, так звана Інтернет-адикція – своєрідна «(нарко)залежність» від Інтернету [66, с. 288].

Термін «комунікація» походить від латин. «Communico» – роблю спільним, пов'язую, спілкуюся. Комунікативна діяльність – це система дій, що послідовно розгортаються, кожна з яких спрямована на вирішення

приватного завдання і може бути розглянута як деякий «крок» у напрямку до мети спілкування [17, с. 518]. Під комунікацією в суспільстві мають на увазі спілкування, обмін думками, знаннями, почуттями, схемами поведінки тощо.

Комунікативна діяльність, здійснювана з допомогою Інтернету, дуже різноманітна. Існують такі основні види спілкування в Мережі:

– спілкування в режимі реального часу («чат»): з одним співрозмовником або з великою кількістю людей одночасно;

– спілкування, при якому повідомлення до адресата надходять із відстрочкою: з одним співрозмовником (електронна пошта), з багатьма людьми – учасниками телеконференції (ньюсгрупи).

Крім того, підставою для класифікації видів спілкування в Інтернеті можуть бути такі параметри:

– відкритість спільноти для всіх бажаючих почати спілкування або закритість її для сторонніх;

– наявність/відсутність контролю над діяльністю учасників, причому окремими випадками контролю може бути модерування, негласне проникнення закритий для сторонніх канал спілкування, «підслуховування» (lurking);

– обмеження вербальними текстами або мультимедійне [76, с. 279].

Класифікація могла б бути проведена і за параметром «ступінь анонімності при спілкуванні в Інтернеті», але зробити це не так просто, оскільки зараз відбувається інтенсивне експериментування з анонімністю – від граничного саморозкриття з елементами ексгібіціонізму до обману, схильності до маніпулювання та спроб «фактично управляти думкою про себе».

Подібна можливість варіювати ступінь анонімності у спілкуванні має чималу привабливу силу. Часто ховаються справжнє ім’я, вік та соціальний статус, стать, справжні факти біографії, замість реальних описуються соціально схвалені особисті якості, в тому числі схвалені лише

у вузькому соціумі [76, с. 281].

Слід пам’ятати, що всі функції та послуги Інтернету застосовуються з метою політико-управлінської діяльності. Серед різновидів політичної діяльності, що реалізуються за допомогою Інтернету, слід розрізняти політико-інформаційну активність і політичну рекламу, вільний або регламентований обмін думками на політичні теми, передачу політичної інформації, зондування громадської думки, протидію діям політичних противників, що вживаються в Мережі, політична активність (проповідництво, вербування)) та ін. [216, с. 25].

Важливою особливістю політичного застосування Інтернету слід визнати відносну дешевизну розміщення інформації, оперативність оновлення, можливість аргументованого та оперативного пояснення позицій при полеміці (що не завжди вдається при жвавій усній полеміці), швидкість розсилки інформаційних матеріалів прихильникам, нові перспективи політичної реклами.

Таким чином, підбиваючи підсумки можливості використання мережевих технологій в інформаційному протиборстві, слід зазначити таке:

1. Державна політика Української держави щодо мережі Інтернет ґрунтується на визнанні необхідності використання інформаційних ресурсів, доступних через мережу Інтернет, відповідних засобів інформаційного обміну, а також надання державної підтримки розвитку українського сегменту мережі Інтернет.

2. Органи державного управління зобов’язані надавати населенню безкоштовні інформаційні послуги. Загальнодоступна інформація виборчих комісій має бути подана в Мережі для забезпечення умов відкритості та гласності, а також можливості розвитку методів громадського контролю виборчого процесу.

Висновки до розділу 1

1. Інформаційна війна – вища форма міждержавного інформаційного протистояння, конфлікт інтересів суб'єктів геополітичної конкуренції (протиборства) в інформаційному просторі з метою вирішення протиріч щодо влади та здійснення політичного керівництва, а також щодо перерозподілу їх ролі, місця та функцій у політико-управлінській системі сучасного суспільства, в якому зіткнення конфліктуючих сторін відбувається у формі інформаційних та інформаційно-психологічних операцій із застосуванням інформаційної зброї.

Сутність такої інформаційної війни полягає у завданні військової поразки противнику шляхом досягнення та використання інформаційної переваги над ним.

2. Інформаційно-гібридна війна може здійснюватися і в умовах відсутності силового конфлікту, що виводить цей різновид до числа найбільш застосовних та універсальних засобів забезпечення реалізації зовнішніх інтересів. У відносно мирних умовах інформаційні війни цього типу можуть застосовуватися як спеціальні механізми управління кризами та провокування варварства на території противника.

Ця обставина визначає асиметричний характер інформаційних воєн і наявність потенційних можливостей у свідомо слабшої сторони щодо завдання цілеспрямованими точковими ударами серйозної шкоди технологічно розвиненому противнику.

3. У постіндустріальному і очевидно інформаційному світі, що формується, найважливішим ресурсом виявляється не традиційний географічний простір із закріпленими в ньому фізичними людьми та виробничими потужностями, а інтелект, інформація та фінанси.

При цьому за допомогою високих технологій інформація, що містить дані про результати інтелектуальної діяльності, легко переміщується у просторі. Відсутність територіальної «прив'язки» ключових ресурсів

дозволяє інформаційно-комунікаційним лідерам опановувати їх і використовувати у своїх цілях без будь-якого фізичного втручання.

4. Ефективне освоєння чужих територій стає можливим без урахування стану кадрового потенціалу та добробуту основної частини населення країни, що освоюється шляхом використання для досягнення поставлених цілей інформаційно-технологічної локалізації та фактичного вилучення із соціально-економічного простору носіїв інтелекту та розпорядників фінансових ресурсів.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ФУНКЦІОНУВАННЯ ІНСТИТУЦІЙНИХ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ІНФОРМАЦІЙНО-ГІБРИДНИХ ВІЙН

2.1. Особливості та ризики функціонування інституційних механізмів публічного управління в Україні в умовах інформаційно-гібридної війни

Термін «гібридна війна» спочатку використовувався для характеристики поняття «збройні конфлікти», які не можуть бути віднесені ні до традиційних, ні до іррегулярних, оскільки в них використовуються різні форми та методи ведення збройної та неозброєної боротьби. За слушним свідченням Ф. Хоффмана, нова тенденція ведення війни усуває межі між відомими раніше типами воєн, і ключову роль у цьому відіграють інституції – легітимізовані чи створені в неправовій формі [181, с. 7; 182]. На цій підставі можна стверджувати про важливість дослідження особливостей і ризиків реалізації публічного управління в Україні в умовах інформаційно-гібридної війни з позиції функціонування інституційних механізмів.

Як відомо, посилення уваги до гібридних та інформаційних війн відбулося після Другої ліванської війни (2006 р.) між Ізраїлем та «Хізбаллою», коли цей термін увійшов в обіг і став використовуватися як політиками, так і військовими. Після 2014 р. (через анексію Криму) термін гібридної війни отримав ще ширше вживання. Саме цим терміном все частіше користуються під час характеристики повномасштабної агресії рф. При цьому термін «гібридна війна» застосовується як до визначення конкретних епізодів таких, як «кольорові революції», так і під час характеристики зовнішньої політики держав (власне, російську політику щодо України чи країн Балтії дедалі частіше називають інформаційно-

гібридною війною) [168].

На Варшавському саміті НАТО (2016 р.) інформаційно-гібридна війна активно обговорювалася, і навіть було оголошено про створення в перспективі особливої стратегії та предметних планів щодо її реалізації, які стосуються ролі НАТО у протидії гібридній війні [там само]. Щоправда, при цьому обговорювалося, що основні обов'язки протидії інформаційним гібридним загрозам поки що залишаються на нашій державі. Альянсу пропонували розглянути питання щодо застосування ст. 5 Договору про колективну оборону для таких випадків.

Таким чином, у країнах Заходу спостерігається тренд на поступове прирівнювання понять «війна», «інформаційно-гібридна війна» і «військова агресія». Якщо це вдасться, то з'являться легітимні підстави для застосування сили проти держави, що створює інформаційно-гібридну загрозу або гібридну війну. Звідси постають питання, як визначити ємно поняття «інформаційно-гібридна війна, наскільки це поняття нове у військовій справі та суспільно-політичному управлінні, як трактується поняття гібридної війни на рівні військових доктрин, яке місце займає інформаційно-гібридна війна у сучасній політиці (рис. 2.1). Усе це визначає актуальність обраної проблематики дослідження.

Проблематика забезпечення національної безпеки у воєнний період загалом і під час впливу інформаційно-гібридних загроз досліджувалася вітчизняними та зарубіжними вченими В. Абрамовим, У. Ваккою, О. Василишин, М. Девідсоном, С. Домбровською, І. Кекішем, О. Крюковим, Ф. Майлзом, Н. Нижник, О. Пархоменко-Куцевіл, А. Помазою-Пономаренко, Г. Ситником, В. Торічним, Ф. Хоффманом та ін. [42; 66; 97; 131; 181; 182; 193; 219]. Разом із тим зовнішня агресія рф набула таких масштабів, що загрожують усій системі безпеки України, (соціальній, економічній, інформаційній, екологічній тощо), відзначаючись нетиповістю, гібридністю. Зважаючи на це, важливим є дослідження особливостей формування концепції інформаційно-гібридної війни.

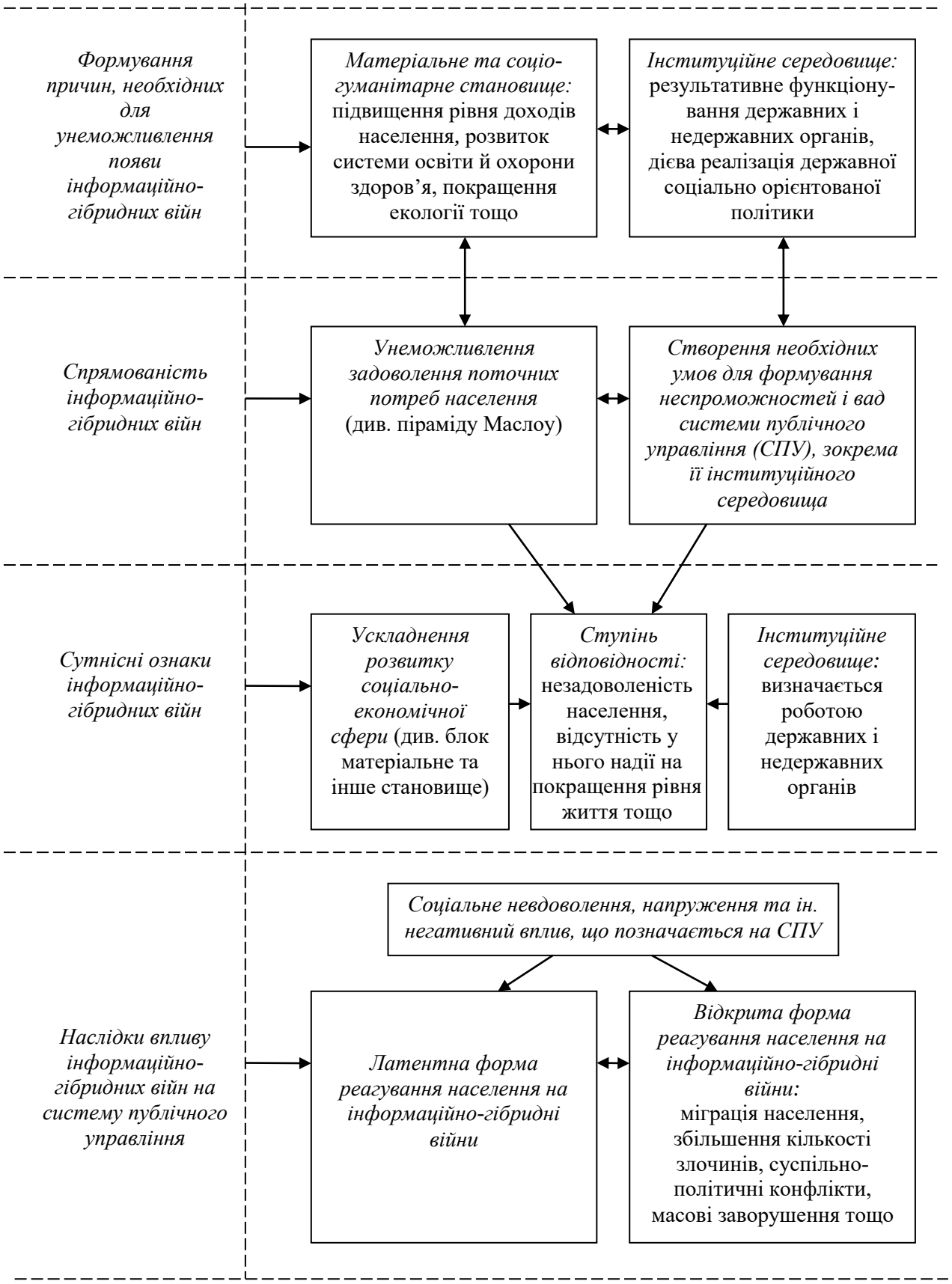

Рис. 2.1. Причини та наслідки виникнення інформаційно-гібридних війн і їхній вплив на систему публічного управління

Джерело: складено на підставі [11-12; 66; 202]

Отже, з рис. 2.1 видно фактори й умови, що формують державну соціально орієнтовану політику, рівень довіри населення до системи публічного управління (органи якого є відповідальними за таку політику) під час впливу інформаційно-гібридних ризиків і загроз. У той же час, ці ризики та загрози можуть створити необхідні умови для виникнення та поширення інформаційно-гібридних війн. Це зумовлює необхідність у дослідженні інституційних механізмів публічного управління в умовах інформаційно-гібридних війн. З огляду на галузь науки, у межах якої проводиться дослідження, підкреслимо, що це варто робити крізь призму визначення, з одного боку, ролі органів публічної влади в забезпеченні системи безпеки. А з другого – наслідків впливу інформаційно-гібридних війн на діяльність цих органів і на стан соціально-економічного розвитку населення в масштабах держави в цілому.

У цьому контексті варто наполягати на важливості більш детального розгляду будови інституційних механізмів публічного управління в умовах інформаційно-гібридних війн в Україні (рис. 2.2). Аналіз наукових напрацювань у галузі науки публічного управління та адміністрування [5; 10; 36; 65] дає підстави стверджувати, що ці механізми включають до своєї структури насамперед організаційні та правові механізми публічного управління. Адже ключовими для них є поняття «інститут» та «інституція», довкола яких і будується методологія дослідження. Власне кажучи, слід говорити про правові інститути, що становлять підґрунтя функціонування правової бази, яка, у свою чергу, визначає особливості державної політики та системи органів (інституцій). Останні як раз розробляють, організують і координують реалізацію державної політики, забезпечуючи задоволення потреб населення (див. рис. 2.1). Ці інституції формують інституційне середовище, що покликане підвищувати рівень і якість життя населення, забезпечувати розвиток системи освіти й охорони здоров’я, покращення екології тощо. Публічні інституції прямо або побіжно підтримують на належному рівні національну безпеку в умовах впливу інформаційно-

гібридних ризиків і загроз. Тому спектр нашого дослідження бути масштабнішим і спрямованим на дослідження процесу функціонування інституційних механізмів публічного управління в умовах таких ризиків і загроз.

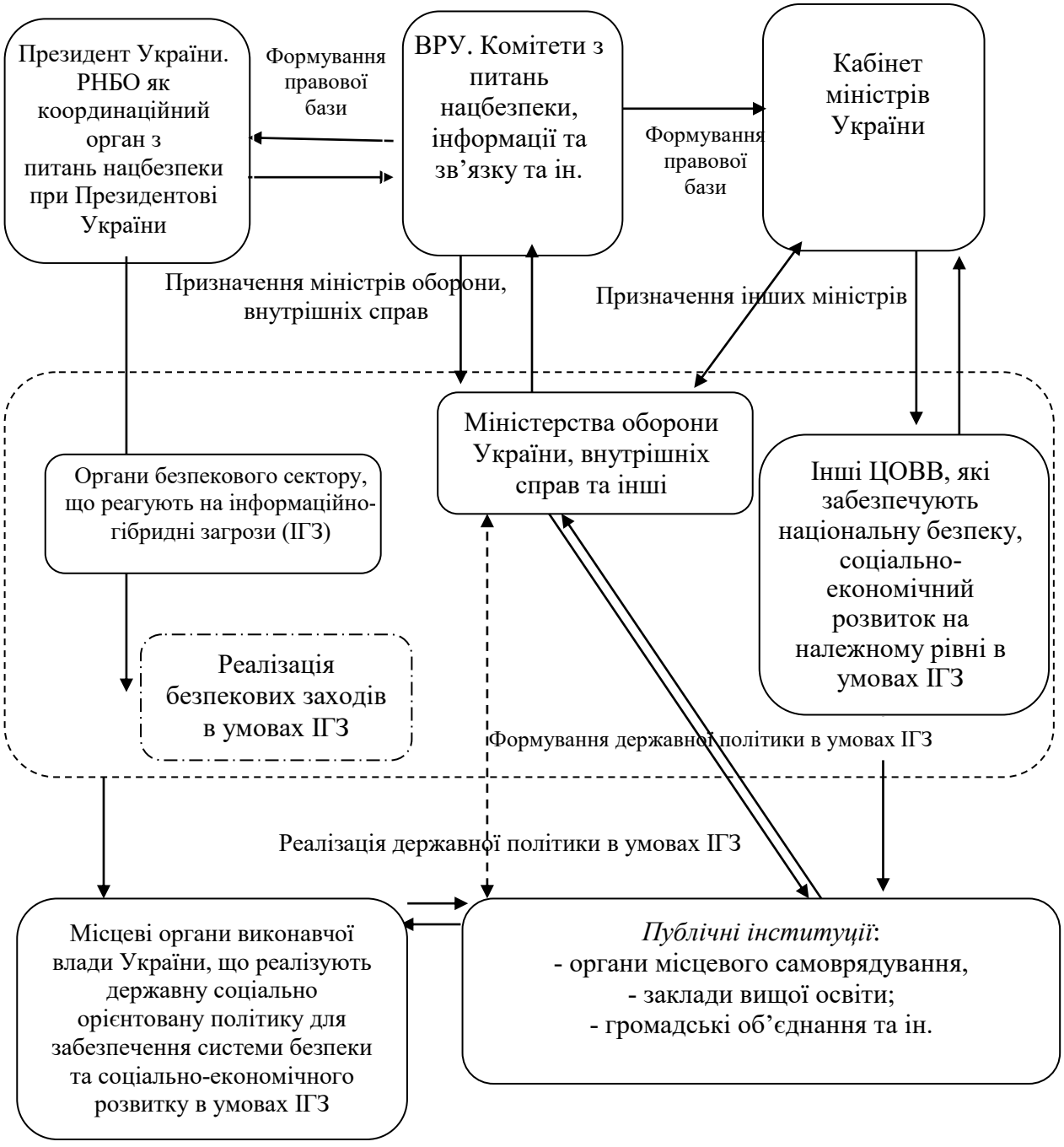

Рис. 2.2. Схема функціонування інституційних механізмів публічного управління в умовах інформаційно-гібридних загроз і війн в Україні

Джерело: авторська розробка

Крім того, публічне управління за умов значного впливу інформаційно-гібридних загроз і війн має відзначатися комплексністю (тобто застосуванням публічно-управлінських методів заборони, координації та попередження).

Як видно з рис. 2.2, функціонування інституційних механізмів публічного управління в умовах інформаційно-гібридних загроз і війн в Україні безпосередньо пов'язане з ключовими категоріями «правовий інститут» та «інституції» (органи публічної влади), а також з процесами щодо формування правових інститутів, удосконалення структури та діяльності цих органів тощо. На цій підставі можемо зазначити, що інституційні механізми публічного управління в умовах інформаційно-гібридних загрозі війн є динамічним елементом системи публічного управління, співвідносячись як часткове та загальне. Ураховуючи загальні засади побудови системи публічного управління, можемо стверджувати, що інституційні механізми публічного управління в умовах інформаційно-гібридних загроз і війн приводять у рух усі інші елементи, що включає така система. Серед них варто виокремити мету, принципи, завдання (дерево цілей), суб'єктів впливу, об'єкт впливу, функції, методи тощо. У цьому контексті важливим є визначення наскільки враховані положення фундаментальної науки на вітчизняних теренах під час побудови інституційних механізмів публічного управління в умовах інформаційно-гібридних загроз і війн.

У продовження зауважимо, що інституційні механізми публічного управління в умовах інформаційно-гібридних загроз і війн представляють собою ніщо інше як сукупність елементів системи, що можуть бути статичними та динамічними, і саме механізми приводять забезпечують її результативне функціонування. Аналіз загальних положень галузі науки публічне управління та адміністрування дає підстави наполягати, що серед статичних елементів системи публічного управління варто виділяти такі: мету, принципи, завдання та функції публічного управління, його методи та

засоби, що застосовують суб'єкти, а також необхідні для цього ресурси (матеріально-технічні, фінансові, кадрові, інформаційні та ін.). Щодо динамічних елементів системи публічного управління, то вони передбачають забезпечення її якісно-кількісної трансформації. До них можна віднести такі: 1) суб'єктів публічного управління; 2) об'єкт публічного управління. Ці два блоки елементів взаємодіють у межах відповідних суб'єктно-об'єктних відносин, і передбачають налагодження зворотного зв'язку з метою визначення стану функціонування об'єкту впливу (чи досягнуто оптимальності такого стану) [89; 90]. Зважаючи на умовний план дослідження, відзначимо, що виникнення, трансформація та припинення таких суб'єктно-об'єктних відносин відбувається в межах правового поля й інституційного середовища (тобто в рамках правового й організаційного механізмів публічного управління). Вони, у свою чергу, передбачають обов'язкову участь органів публічного управління – державних і недержавних інституцій (див. рис. 2.1 і 2.2).

Отже, *перша група* елементів інституційних механізмів публічного управління в умовах інформаційно-гібридних війн є статичною та формує підґрунтя для взаємодії елементів *другої групи*, представленої суб'єктами й об'єктом публічного управління. При цьому мета такого публічного управління полягає в забезпеченні належного стану функціонування об'єкту такого управління, тобто населення. Досягнення такої мети відбувається через здійснення цілеспрямованого, організуючого впливу суб'єктів публічного управління [5; 40; 46; 78]. Очевидно, що базис їхньої діяльності становлять загальні та спеціальні принципи публічного управління (науковості, системності, результативності, ефективності, прозорості, відкритості, відповідності структури суб'єкта державного впливу його об'єктові тощо) [там само].

Слід підкреслити, що врахування цих принципів є завданням усіх органів публічної влади, незалежно від рівня їхнього функціонування (центрального, регіонального чи місцевого). З огляду на це можемо визнати

важливість визначення цілої *суб'єктної підсистеми* публічного управління в умовах інформаційно-гібридних війн, одним з основних завдань якої (підсистеми) є унеможливлення трансформації інституційних ризиків функціонування органів публічної влади в загрози для соціального й економічного розвитку України.

Чинне законодавство України [96] визначає, що суб'єктів публічного управління в залежності від сфери їхнього впливу на такий розвиток. У той же час, він не можливий без гарантування системи безпеки (соціальної, економічної, інформаційної, екологічної тощо). Адже безпекова функція є основною для будь-якої держави, що визначається в її конституції (життя, здоров'я, честь і гідність людини є найвищою цінністю). На цій підставі можемо зауважити, що сектор безпеки й оборони України є суб'єктною підсистемою публічного управління в умовах інформаційно-гібридних війн.

Закон України «Про національну безпеку України» установлює, що сектор безпеки й оборони охоплює чотири взаємопов'язані складові, а саме: 1) сили безпеки; 2) сили оборони; 3) оборонно-промисловий комплекс; 4) громадян і громадські об'єднання, які добровільно приймають участь у забезпеченні нацбезпеки [96, ч. 1 ст. 12]. Ці суб'єкти в різній мірі реагують на загрози інформаційного характеру, забезпечуючи інформаційну безпеку держави та суспільства. З огляду на предмет нашого дослідження можемо підкреслити, що визначати особливості реалізації інституційних механізмів публічного управління варто саме з позиції характеристики формування органами публічної влади інформаційної безпеки. Відтак, поза увагою нашого дослідження залишуться сили оборони й оборонно-промисловий комплекс.

У чинному законодавстві України у сфері нацбезпеки не міститься визначення інформаційної безпеки, є «національна безпека», «воєнна безпека», «державна безпека», «громадська безпека та порядок» (див. ст. 1 Закону України «Про національну безпеку України» [там само]). Проте аналіз цього законодавчого акту дає підстави стверджувати, що

інформаційній безпеці відводиться не остання роль. Так, у ч. 4 ст. 3 визначено, що «державна політика у сфері національної безпеки спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями» [96]. Разом із тим, чинне законодавство України у сфері нацбезпеки не конкретизує, які ж органи публічної влади забезпечують той чи інший напрям безпеки. Як зазначалося в роботі вище, законодавець окреслив сектор безпеки, сектор оборони тощо. Розгляд визначень «сектору безпеки», «сектори оборони» тощо дозволив наполягати на тому, що саме перший сектор (безпековий) покликаний гарантувати та підтримувати інформаційну безпеку в умовах впливу загроз інформаційного характеру (див. ст. 1 Закону України «Про національну безпеку України» [там само]).

Згідно з ч. 2 ст. 12 Закону України «Про національну безпеку України» [96] можемо виділити органи публічної влади, що входять до сектору безпеки та покликані забезпечувати інформаційну безпеку, а саме:

– МВС України;

– СБУ;

– Нацполіція;

– Державна служба спеціального зв’язку та захисту інформації України;

– Апарат Ради національної безпеки і оборони України [там само].

У ст. 13 аналізованого закону визначено, що керівництво у сферах нацбезпеки здійснює Президент України, який:

1) забезпечує таку безпеку;

2) очолює РНБО України;

3) видає укази та інші підзаконні акти, реалізує право законодавчої ініціативи у ВРУ щодо законодавчого врегулювання питань нацбезпеки;

4) вносить до ВРУ подання щодо призначення Міністра оборони України та ін. [96].

Відповідно до ч. 1 ст. 14 аналізованого закону координацію у сфері нацбезпеки здійснює Рада національної безпеки і оборони України, що також законодавчо закріплено в ст. 107 Конституції України та Закону України «Про Раду національної безпеки і оборони України» [96]. Крім того, у ч. 2 ст. 14 аналізованого закону вказано, що під час дії воєнного або надзвичайного стану тощо, що загрожує національній безпеці України, РНБО України координує діяльність органів виконавчої влади, розглядає пропозиції щодо застосування спеціальних обмежувальних заходів [там само].

Дослідження положень Закону України «Про Раду національної безпеки і оборони України» [96] дає підстави наполягати, що РНБО України є спеціалізованим органом публічної влади, який формує та реалізує державну політику щодо гарантування національної безпеки. Профільний комітет Ради національної безпеки і оборони України (як власне і сама Рада) здійснюють таке:

1) моніторинг і дослідження загальнодержавного рівня загроз інформаційній безпеці;

2) вивчення стану й ефективності реалізації стратегій та програм, спрямованих на підвищення рівня інформаційної безпеки;

3) надають пропозиції щодо нейтралізації загроз інформаційного характеру, що можуть трансформуватися в небезпеки виникнення інформаційно-гібридних війн.

Зважаючи на наведене на рис. 2.2, відзначимо, що особливу роль у гарантуванні інформаційної безпеки України за умови впливу загроз у цій сфері відіграє взаємодія Президента України, РНБО України із законодавчим органом. Верховна Рада України, зокрема, Комітет з питань національної безпеки, оборони та розвідки, Комітет з питань інформації та зв’язку та інші комітети ВРУ, формують і розглядають пропозиції щодо внесення законодавчих змін у таких сферах:

1) національної й інформаційної безпеки;

2) електронного обігу;

3) телекомунікацій;

4) розвитку інформаційного суспільства;

5) національної програми інформатизації;

6) захисту системи електронних інформаційних ресурсів тощо [96].

Варто погодитися з ученими В. Антонюк, І. Березовською, В. Зайцевим, О. Крюковим, Р. Правим та ін. [5; 10; 49; 66; 109], що діяльність суб'єктів публічного управління у сфері забезпечення інформаційної безпеки спрямована на вчасне визначення, прогнозування та нейтралізацію ризиків і загроз інформаційного характеру. Унеможливлення їхньої трансформації в небезпеки та війни – головне завдання вищевказаних суб'єктів публічного управління. Вони, зокрема, повинні реагувати на такі найбільш актуальні наразі загрози інформаційної безпеки України, як інформаційно-психологічна війна, приниження української мови і культури, формування російськими ЗМІ альтернативної до дійсності викривленої інформаційної картини світу тощо [там само].

На підставі вищенаведеного можна наполягати на необхідності розгляду *інформаційної безпеки* як сукупності суб'єктно-об'єктних взаємовідносин, що виникають між суб'єктами інформаційного середовища (простору), які здійснюють цілеспрямований, організуючий вплив на різні сфери суспільної життєдіяльності загалом і на об'єкти інформаційної інфраструктури зокрема, що відбувається за допомогою комплексу правових, організаційних, інформаційних, економічних та інших заходів (під час формування й оновлення правової бази, удосконалення структури та/або форм діяльності органів публічної влади, стратегічних, урядових і кризових комунікацій тощо) з метою унеможливлення трансформації ризиків і загроз інформаційного характеру у небезпеки та війни. Застосування системного підходу до формування інформаційної безпеки дозволяє стверджувати, що актуальним є розгляд провідної ролі суб'єктів формування та реалізації державної політики такої безпеки.

Крім того, відзначимо, що підтримки інформаційної безпеки є одним із пріоритетних завдань діяльності й інших органів публічної влади. По-перше, державним органом спеціального призначення з правоохоронними функціями, що забезпечує інформаційну безпеку України, є Служба безпеки України. Це положення закріплено в п. 3 ч. 1 ст. 19 Закону України «Про національну безпеку України» [96]. Власне кажучи, СБУ здійснює контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, науково-технічного потенціалу, кібербезпеки, інформаційної безпеки, об'єктів критичної інфраструктури тощо [там само]. По-друге, створена та функціонує Державна служба спеціального зв'язку та захисту інформації України [96, ст. 22]. Ця служба є державним органом, призначеним для забезпечення такого:

а) функціонування державної системи урядового та конфіденційного зв'язку;

б) формування й реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації;

в) криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення та ін. [там само, ч. 1 ст. 22].

Аналіз положень галузі науки публічне управління [5; 46; 78] дав змогу зауважити, що всі вищеперераховані суб'єкти формування та реалізації державної політики інформаційної безпеки покликані реалізовувати основні функції публічного управління. До них варто віднести функції планування та прогнозування, організації, координації, регулювання та контролю. На підставі розгляду наукових напрацювань [там само] можемо стверджувати, що має місце побіжне врахування засадничих принципів публічного управління під час закріплення за органами публічної влади тих чи інших функцій (табл. 2.1). Як результат, має сучасне розбалансування системи публічного управління в умовах актуалізації

загроз інформаційного характеру. При цьому інформаційно-гібридна війна стає «м'яким» інструментом дисфукнкціоналізації такої системи з середини.

Таблиця 2.1

Функціональна карта інституційної реалізації публічного управління в умовах загроз інформаційного характеру й інформаційно-гібридної війни в Україні

№ з/п	Назва функції, що реалізується органом публічного управління	Назва органу публічного управління, що реалізує функцію	Функціональне реагування на вплив інформаційно-гібридної війни	Норма права, що закріплює таку функцію за органом публічного управління
1.	Планування / прогнозування	Президент України	1. Реалізує право законодавчої ініціативи у ВРУ щодо законодавчого врегулювання питань нацбезпеки	Ст. 13 Закону України «Про національну безпеку України»
			2. Доручає РНБО України розробити довгострокові плануючі документи у сфері нацбезпеки. Вносить зміни до таких документів.	Абз. 2, 4 ч. 1 ст. 26 Закону України «Про національну безпеку України». Ч. 2 ст. 31 Закону України «Про національну безпеку України».
		РНБО України, з його апаратом, комітетом та ін.	Апарат РНБО України разом з Національним інститутом стратегічних досліджень, державних органів, інституцій громадянського	Абз. 5 ч. 3 ст. 25 Закону України «Про національну безпеку України». Ч. 5 ст. 33 Закону України «Про

№ з/п	Назва функції, що реалізується органом публічного управління	Назва органу публічного управління, що реалізує функцію	Функціональне реагування на вплив інформаційно-гібридної війни	Норма права, що закріплює таку функцію за органом публічного управління
			суспільства залучаються до розробки довгострокових плануючих документів у сфері нацбезпеки.	національну безпеку України».
2.	Керування (організація, регулювання)	Президент України	Здійснює керівництво у сферах нацбезпеки, забезпечуючи інформаційну та інші види безпеки.	Ст. 13 Закону України «Про національну безпеку України»
		Державна служба спеціаль-ного зв'язку та захисту інформації України	Формування й реалізація державної політики у сферах кіберзахисту критичної інформаційної інфраструктури	Ст. 22 Закону України «Про національну безпеку України»
		СБУ	Забезпечує державну безпеку, у т.ч. захист науково-технічного потенціалу, кібербезпеки, інформаційної безпеки тощо	Ч. 1 ст. 19 Закону України «Про національну безпеку України»
3.	Координація	РНБО України, з його апаратом, комітетом та ін.	Координація за станом реалізації довгострокових плануючих документів у сфері нацбезпеки.	Абз. 5 ч. 3 ст. 25 Закону України «Про національну безпеку України»

№ з/п	Назва функції, що реалізується органом публічного управління	Назва органу публічного управління, що реалізує функцію	Функціональне реагування на вплив інформаційно-гібридної війни	Норма права, що закріплює таку функцію за органом публічного управління
4.	Контроль	Президент України, ВРУ, Уряд України	Контроль за сектором безпеки як безпосередньо, так і через створювані ними у разі необхідності консультативні, дорадчі та інші допоміжні органи і служби	Ст. 5, 6, 7 Закону України «Про національну безпеку України»
		Громадські організації та інші НУО	Громадський контроль за сектором безпеки та станом забезпечення безпеки	Ст. 10 Закону України «Про національну безпеку України»
		РНБО України, з його апаратом, комітетом та ін.	Координація за станом реалізації довгострокових плануючих документів у сфері нацбезпеки.	Абз. 5 ч. 3 ст. 25 Закону України «Про національну безпеку України»

Джерело: складено на підставі [96]

Можна по-різному класифікувати суб’єктів публічного управління у сфері інформаційної безпеки. Науковець В. Негодченко пропонує класифікувати вказаних суб’єктів, виокремлюючи дві групи: державні та недержавні [87]. З такою класифікацією, безперечно, можна погодитися з огляду на позицію законодавця у визначенні суб’єктів забезпечення системи безпеки (див. Закон України «Про національну безпеку України» [96]). Крім того, недержавні суб’єкти (НУО) мають доступ до значної частки інформаційної інфраструктури, а тому можуть суттєво впливати на

державну інформаційну політику.

Іншої, але не менш важливої думки є О. Довгань, який класифікує суб'єктів публічного управління в інформаційній сфері, покликаних забезпечити її безпечне функціонування, на:

1) суб'єктів з інформаційно-аналітичними функціями щодо аналізу загроз;

2) суб'єктів з організаційно-управлінськими функціями (прийняття рішень, програмування й планування);

3) суб'єктів із безпосередньо виконавчими функціями [40].

При цьому О. Довгань [там само] вказує на рівні формування органами державної влади системи інформаційної безпеки: 1) законодавчий; 2) адміністративний; 3) процедурний; 4) програмно-технічний. Щоправда не зовсім зрозумілою є позиція автора з приводу виокремлення таких рівнів, адже загально прийнятим є визначення вищого, центрального, регіонального та місцевого рівнів управління [5; 10].

Крім того, дослідник Р. Прав слушно визначає серед суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері:

а) органи державної влади України (різних рівнів та сфер життєдіяльності, органи місцевого самоврядування);

б) суб'єкти, що функціонують «поза» системою державного управління (підприємства, організації й установи різних форм власності, громадські об'єднання, асоціації та інші НУО) [109].

На погляд законодавця, варто виділяти таких суб'єктів національної системи інформаційної безпеки: КМУ, Міністерство інформаційної політики України, МЗС України, Міністерство оборони України, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, СБУ, Державна служба спеціального зв'язку та захисту інформації України, розвідувальні органи України. Така

інституційна класифікація наведена в Доктрині інформаційної безпеки України та Законі України «Про основні засади забезпечення кібербезпеки України» [96; 113].

Вищенаведені науково-теоретичні інституційні класифікації у сфері інформаційної безпеки жодним чином не протирічить наведеним даним у табл. 2.1, навпаки, дозволяють наполягати на розмежуванні функцій суб'єктів публічного управління в інформаційній сфері на основні та допоміжні. Щодо основних функцій, то до них належать планування, організація, мотивація та контроль, про які йшлося в роботі вище.

У той же час, виникає проблемне питання щодо уніфікації підходів до правового визначення суб'єктів публічного управління в умовах впливу інформаційно-гібридної війни. Власне кажучи, слід привести у відповідність такі нормативно-правові документи: Закон України «Про національну безпеку України», Доктрину інформаційної безпеки України та Закон України «Про основні засади забезпечення кібербезпеки України» [96; 113]. Оскільки в межах зазначених правових документів відсутнє єдине визначення суб'єктів публічного управління, покликаних гарантувати інформаційну безпеку України.

Отже, формування сучасної системи інформаційної безпеки в Україні потребує вирішення низки завдання, а саме: поширення неправдивої та видозміненої інформації з боку країни-агресора, що впливає на розвиток суспільства, відсутність цілісної інформаційної концепції та стратегії поширення об'єктивної інформації та щодо протидії загрозам інформаційного характеру, недостатній рівень медіа-культури суспільства та його цифровізованого розвитку тощо. Погоджуємося з вченими В Антонюк, В. Негодченко, О. Олійник, Р. Правим, В. Федченко та ін. [5; 10; 94; 109; 150], що вирішення цих проблемних питань вимагає дієвої співпраці суб'єктної підсистеми публічного управління в умовах інформаційно-гібридної війни.

Уважаємо, що має місце правова диференціація у визначенні

суб'єктної підсистеми публічного управління в умовах інформаційно-гібридної війни в Україні. Зважаючи на це, можемо наполягати на необхідності внесення відповідних змін до чинного законодавства у сфері національної й інформаційної безпеки шляхом уточнення суб'єктного складу системи, покликаної її забезпечити на належному рівні. У цьому контексті доцільним є уточнення суб'єктного складу системи забезпечення національної й інформаційної безпеки України, що буде здійснено в роботі далі.

2.2. Аналіз сучасної концепції інформаційно-гібридної війни

Обговорюючи гібридні методи боротьби, американські експерти наголошують на якісно новому етапі в еволюції воєн. Ця новизна полягає, за визначенням Ф. Хоффмана, у тому, що конфлікти майбутнього матимуть змішаний характер з погляду використання традиційних й іррегулярних методів ведення війни [181-182]. Проте аналіз доктринальних документів Сполучених Штатів Америки показує, що говорити про появу концепції гібридних воєн як нової форми протиборства передчасно, оскільки Пентагон не виробив офіційного визначення. У Статуті сил спеціальних операцій 2008 р. термін «гібридний» використовується при тлумаченні змісту іррегулярних воєн, визначаючи ідею поєднання іррегулярних, підривних актів дії, щоб підірвати або завдати шкоди впливу США та їх стратегічних партнерів [177, с. 1-5]. Отже, термін «гібридний» у поєднаннях з термінами «загроза», «протиборство» і «війна» згадується й у інших документах під час опису складності сучасних конфліктів та необхідності адаптації до них збройних сил [90; 91].

Крім того, у чотирирічному огляді оборонної політики за 2010 р. термін «гібридна війна» використовується для позначення таких особливостей сучасного військового конфлікту, як збільшена складність, множинність

учасників, включаючи терористичні та кримінальні угруповання, асиметричність дій супротивника та в цілому розмивання традиційних уявлень про форми конфліктів [201, с. 8]. На цій підставі можемо зазначити, що «гібридна загроза» вживається у найзагальнішому вигляді – як антонім конвенційної загрози.

Отже, самостійного та специфічного значення термін поки не має, але за багатьма ознаками є близьким до визначення поняття «іррегулярні війни». Вони як якраз і визначені в доктринальних документах як «силова боротьба між державою та недержавними акторами за легітимність і вплив над населенням. Іррегулярна війна віддає перевагу непрямим й асиметричним діям, хоча може включати повний спектр військових та інших засобів, аби завдати шкоди владі, впливу та політичній волі противника» [186, с. 6].

Термін «іррегулярна війна» має неоднозначне трактування, тому що використовується у двох значеннях: 1) як вид прямого збройного конфлікту (синонім конфлікту малої інтенсивності); 2) як менш інтенсивний, ніж збройний конфлікт, прийом протиборства (тероризм, контртероризм тощо). В останньому випадку не завжди можна довести їх приналежність до конкретної держави, а самі ці дії можуть виходити за межі міжнародного права [там же].

Невизначеність терміну «гібридна війна» призводить до того, що той самий конфлікт різні військові та цивільні відомства оцінюють по-різному. Як відомо, війну Росії з Грузією у 2008 р. представники сил спецоперацій та сухопутних військ називають традиційною, а представники військово-повітряних сил – гібридною, розуміючи під гібридними війнами комбінацію традиційних і нетрадиційних засобів та методів боротьби. Крім того, уважають, що гібридні війни – це складніший та інтенсивний варіант іррегулярної війни. У цьому контексті на даному етапі дослідження можемо зауважити, що доречним буде трактування «гібридної війни» крізь призму тріади «нетрадиційної війни», «іррегулярної війни» і «особливого різновиду конфліктів». За свідченням дослідників, істотних відмінностей між

іррегулярними та гібридними війнами немає, можна говорити лише про різночитання, пов'язані з різною інтерпретацією тих самих ознак. Можна зробити проміжний висновок, що «гібридність» означає деякі інноваційні поєднання прийомів протиборства, які насамперед співвідносили переважно з іррегулярною війною [91].

Паралельно з терміном «гібридна війна» можливо також використовувати відповідний термін «операції повного спектру» [185, с. 14-15]. Ідея «операцій повного спектру» (full spectrum operations) було запропоновано ще наприкінці 1990-х років як один із напрямів реформ збройних сил США, які потім активно просував міністр оборони Д. Рамсфелд [там же]. «Повний спектр» передбачає такі якості:

• здатність регулярних сил проводити операції різного масштабу;

• однаково ефективне використання військових та невійськових інструментів;

• готовність до відображення непередбачуваних загроз;

• здатність досягати комплексної переваги над будь-яким потенційним противником [91].

Такі універсальні функції «операцій повного спектру» здатні набути за умови впровадження у військову справу досягнень високоточної зброї та інших компонентів, що належать до так званої «революції у військовій справі». Тим самим, поняття «повного спектра» застосовується і для характеристики загроз, і для способів реагування на них саме у тих аспектах, які сьогодні вкладаються у поняття гібридних загроз і війн. Надалі концепція операцій повного спектру стала складовою концепції «спільних/міжвидових операцій» (joint operations). У межах останньої концепції робиться акцент на поєднання міжвидової взаємодії і на нейтралізації фактично необмеженого кола загроз. Втім, таке амбітне завдання поки що не вирішено на практиці.

Таким чином, у наукових публікаціях можна зустріти різних прибічників тієї чи іншої концепції гібридних війн, які звертають увагу на те, що використання цього терміну ускладнює військово-політичний аналіз,

військове планування й особливо вивчення досвіду минулих війн. До цього можна додати проблему інклюзивності: гібридна війна потенційно включає будь-які методи і засоби боротьби, що ускладнює визначення специфіки гібридної війни на противагу політиці або іншій діяльності. Зауваження американських експертів викликають не лише термін «гібридна війна», а й «іррегулярна війна» як протиставлення традиційній війні. Іррегулярність асоціюється з рідкістю, відхиленням від норми, несистемністю відносно меншою важливістю. Проте це дещо умовне протиставлення, що можливе лише в аналітичних побудовах, оскільки історія чітко показує, що у більшості воєн століттями використовувалися разом як традиційні, так й іррегулярні методи боротьби [219]. Їх протиставлення на кшталт «або–або» ускладнює визначення взаємозв'язку у практичному використанні, а запровадження чергового, при цьому нечітко певного терміну «гібридні війни», тільки посилює таку проблему. На цій підставі можемо рекомендувати застосування синергетичного й інституційного підходів до визначення поняття «гібридна війна». Зазначені підходи дозволяють стверджувати про важливість розгляду такого виду війни з позиції впливу тих чи інших факторів, що становлять загрозу для системи безпеки окремо взятої держави або певної групи держав, гарантування та підтримка якої (системи безпеки) є пріоритетним завданням різних публічних інституцій за будь-яких умов їх функціонування.

Слід підкреслити, що особливий інтерес представляє «Біла книга» США щодо протидії нетрадиційним війнам (unconventional), опублікована командуванням спеціальних операцій сухопутних військ у вересні 2014 р. Саме в цьому закордонному документі кримські події розглядаються крізь призму гібридних воєн. Ці дії російських військових у Криму стали синтезом досвіду залучення Ірану по лінії ХАМАС і «хізбалли» в близькосхідні конфлікти і китайською доктриною «необмеженої війни», що виникла 1990-х роках [90; 91]. Сутнісно китайська концепція «необмеженої війни» зводиться до того, що слід неочікувано атакувати супротивника,

який має значну перевагу, шукаючи вразливі місця та використовуючи недоліки в системі національної безпеки, уряді та суспільстві. Інструментарій нападу принципово нічим не обмежується та включає, наприклад, хакерські атаки, створення проблем у фінансовій системі, використання засобів тероризму, вплив через ЗМІ, озброєну боротьбу у міських умовах тощо [202].

У «Білій книзі» гібридна війна визначена як «комбінування традиційних, іррегулярних та асиметричних засобів для безперервної маніпуляції політичним та ідеологічним конфліктам» [70; 73; 91; 122; 181]. Воно близьке до консенсусного тлумачення. Однак у документі наводиться уточнення, пов'язане з гібридною війною Росії проти України. Йдеться про те, що підготовка спеціальної операції проводилася на загальнодержавному рівні, що означає комбінування дипломатичних, інформаційних, економічних, фінансових і правових інструментів [там само].

Принагідно зауважимо, що основна увага зосереджується на «нетрадиційній», а не на «гібридній» війні. Справа в тому, що згідно з аналізованим документом, рф у гібридних діях зробила акцент на методи саме нетрадиційної війни, яка, у свою чергу, є найважливішою частиною іррегулярної війни. Місце нетрадиційної війни в ряді інших видів операцій іррегулярної війни показано на рис. 2.3.

У «Білій книзі» наголошується, що дії рф в Україні (у 2014 р.) повністю відповідають прийомам нетрадиційної війни: використання сил спеціальних операцій, співробітників розвідки, політичних провокаторів, представників ЗМІ транснаціональних злочинних елементів на сході та півдні України. Цілі цієї діяльності полягали у створенні хаосу, дестабілізації громадського порядку, провокуванні невідповідної силової реакції влади для її дискредитації в очах українців. Відносно рф доводиться її різнохарактерна підтримка сепаратистських угрупувань на території України [91; 133; 140; 190]. Так, у «Білій книзі» військове відомство використовує посилання на матеріали держдепартаменту (зокрема, оцінки

С. Нуланд), які мають незангажований характер.

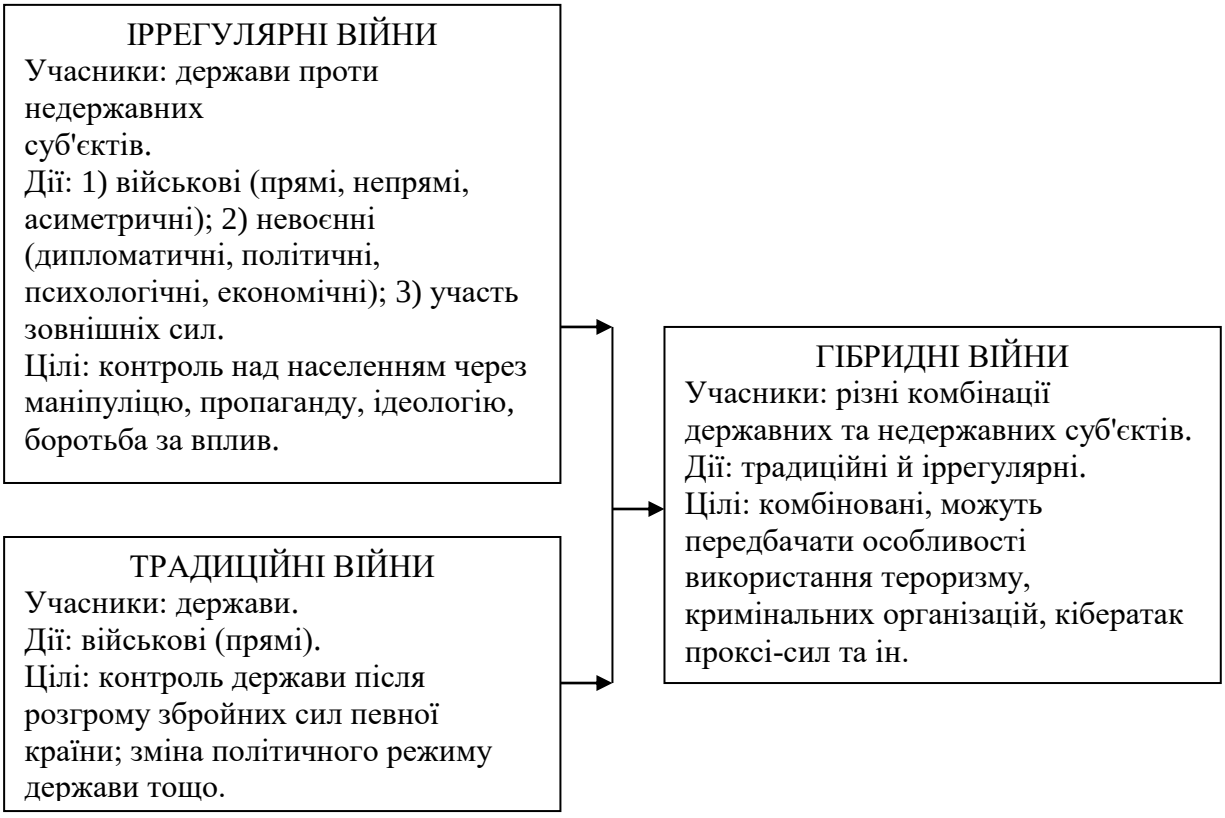

Рис. 2.3. Види війн

Джерело: складено на підставі [70; 73; 122-124; 133; 140; 190]

Таким чином, на доктринальному рівні новації у методах нетрадиційної війни пов'язані зі зміною спектру загроз та акторів конфлікту, які формують ту якість дестабілізуючих заходів, що робить війну вже не просто іррегулярною, а гібридною. Ще одна особливість гібридних воєн – це їхній тривалий характер, що вимагає превентивної та тривалої політики протидії, організованою на державному рівні. Однак на рівні планування та проведення операцій ключовими залишаються учасники, методи та засоби нетрадиційної війни, що зайвий раз говорить про те, що концепція «гібридної війни» поки перебуває на стадії становлення. Відтак, спосіб протидії США гібридним загрозам з боку Росії, Ірану та Китаю пропонується називати «Протидія нетрадиційним війнам» [70; 73; 122; 133; 140; 190]. З урахуванням того, що гібридні загрози носять довготривалий

характер, пропонується на кілька десятиліть уперед додати доктрині протидії нетрадиційним війнам «актуальний» статус у межах забезпечення системи безпеки [там само].

У вітчизняній військовій доктрині концепція гібридної війни почала актуалізуватися, на жаль, в останні роки, а сам термін увійшов у вжиток вже після того, як став популярним на Заході останнім часом. Проте проблематика (не)насильницької зміни влади та широкого застосування (не)військових методів протистояння має багату традицію у зарубіжній військовій практиці. Так, можемо навести цитату з ідейної спадщини Е. Месснера: «Певний час у війнах важливим визнавалося завоювання території. Згодом найважливішим було завоювання свідомості широкого загалу умовного противника. Раніше лінія фронту, що розділяла ворогів, була як розпливчастою, та к і ні. У майбутніх війнах воювати будуть не на лінії, а на всієї поверхні територій обох супротивників, тому що позаду збройного протистояння виникнуть політичний, соціальний та економічний фронти. Вони передбачають протистояння не на двовимірній поверхні, як у давнину, не в тривимірному просторі, як було з моменту народження військової авіації, а в чотиривимірному, де свідомість воюючих народів є четвертим виміром» [80]. Ці ідеї потім знайшли розвиток у наукових дискусіях щодо природи сучасної війни.

У фундаментальній науці комплекс теоретичних і практичних проблем, пов'язаних із змінами у характері війни, обговорювався дослідниками на тлі осмислення тривалої боротьби з бандформуваннями та сепаратистськими угрупуваннями, зокрема, у Грузії (2008 р.), під час серії «кольорових революцій» у північній Африці (2014 р.), в Україні (2014 р. і по теперішній час), а також під час сирійської кампанії (2011–2018 рр.). Фахівці насамперед стурбовані ризиками, що виникають для збройних сил зазначених держав при використанні противником гібридних методів. Так, «кольорові революції» втілюють головний засіб досягнення політичних цілей гібридної війни – ненасильницьку зміну влади інших державах [30].

Увага вчених [11; 30; 58; 121; 146] спрямована на ситуації, коли досить стабільні держави несподівано швидко залучалися до збройного конфлікту, стрімко руйнувалися або дискредитовувалися державні інститути, а потім суспільство поринало в хаос. Найважливішою складовою гібридної війни вважається інформаційне вплив, що опосередковано підтверджується кількісними оцінками їхньої спільної зустрічальності в текстах [66; 82; 202]. Як зазначають дослідники, гібридна дія створює можливість привести до влади потрібне політичне, військово-політичне та ін. угруповання без прямого силового впливу та захоплення території, а лише за рахунок маніпулятивних засобів. У цьому контексті слушним твердження, що стали менш помітними межі між станом світу та війною, причому зростає роль невійськових способів протиборства. Згідно з оцінками фахівців, співвідношення між військовими та невоєнними методами боротьби складає 1:4 [7, с. 6; 45].

Отже, назріла необхідність розуміння умов війн, що змінилися та передбачають традиційні, нестандартні форми протиборства. У вітчизняній науці, на жаль, не приділялося достатньої уваги розробці нестандартних форм протиборства, включаючи асиметричні дії. У той же час, формуються нові особливості війни, по відношенню до яких доречно вживати термін «гібридна війна». Акцент методів протиборства зміщується у бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів, що реалізуються із залученням протестного потенціалу населення. Усе це доповнюється військовими заходами прихованого характеру, у тому числі реалізацією заходів інформаційного протистояння та діями сил спеціальних операцій [11; 12; 66]. До відкритого застосування сили найчастіше під виглядом миротворчої діяльності та кризового врегулювання переходять лише на якомусь етапі максимальної готовності [45]. У межах цього твердження фахівці визначили таку особливість концепції гібридної війни, яка була реалізована під час кризи в Україні та у сирійському конфлікті.

Аналіз наукових напрацювань дав змогу розуміти під гібридними війнами – комплексне застосування політичних, економічних, інформаційних та інших військових або невійськових заходів, що реалізуються з нахилом на військову силу. Очевидно, що йдеться про зміни у плануванні, проведенні та використанні специфічних інструментів під час сучасних військових, суспільно-політичних та інших конфліктів.

Показово, що як синонім «гібридні методи війни» використовуються терміни «непрямі методи впливу», «асиметричні дії», відомі з часів сунь Цзи та в різних варіаціях відтворені як у практиці війни, так і в зарубіжній науковій думці XX – початку XXI ст. [84; 193]. Трактуючи цей термін, слід зазначити, що якщо так звані гібридні методи протиборства (впливу) можуть використовуватися й без відкритого застосування військової сили, але сьогодні класичних бойових дій уже немає без гібридних методів впливу. Яскравим прикладом на підтвердження цієї думки є конфлікт у Сирії. У цьому контексті сучасні військові, суспільно-політичні та інші суспільні конфлікти відрізняє прагнення досягти владно-політичних цілей із мінімально відкритим збройним впливом на супротивника. Іншими відмінними рисами гібридних війн є відсутність формального оголошення війни та малопередбачувані далекі наслідки, оскільки оптимальне функціонування суспільства можна дестабілізувати та дезорганізувати в усіх аспектах життя [11; 12].

Якщо говорити більш конкретно, у гібридних діях акцент робиться на швидку внутрішню дестабілізацію держави за рахунок такого:

1) підриву військового, соціально-економічного та іншого потенціалу;

2) масштабних інформаційно-психологічних операцій із максимально широким охопленням населення;

3) підтримки внутрішньої опозиції й екстремістських організацій різного виду;

4) використання методів повстанської, диверсійної та терористичної боротьби [168; 170; 173].

Даючи оцінку концепції гібридної війни, експерти підкреслюють, що не йдеться про її принципову новизну, у цьому сенсі під гібридною війною слід розуміти сукупність конкретних рішень щодо комбінування методів, продиктованих конкретними обставинами [168; 170; 173]. Реалізуючись на практиці, ці рішення показують мінливий образ війни, який при цьому не зраджує своїй природі – наносити втрат. Звичайно, використовувані при цьому інструменти розширюються й удосконалюються в міру еволюції військового справи, і особливо щодо впровадження досягнень науково-технічної революції. Проте це не змінює самої сутності питання, адже ідея «троянського коня» залишається й у час поширення інтернету, зростання швидкості передачі інформації та створення високоточного зброї [45; 202]. Остання ознака є свідченням швидкої трансформації війни загалом і гібридної війни зокрема в напрямку інформатизації та діджиталізації.

Водночас змінний образ війни вимагає особливої уваги, зокрема, експерти відзначають таку особливість, як наростання нелінійності у разі гібридних дій. Цей ефект, помічений ще К. фон Клаузевицем, означає, що можуть виникнути умови, які здатні так посилити наслідки від малих подій, що радикально зміниться перебіг військової кампанії [7; 91]. У продовження цієї думки А. Бартош до таких «каталізаторів» відносить організацію техногенних катастроф, здійснення терактів на житлово-комунальних комунікаціях, вбивства політичних лідерів та ін. [7, с. 10]. Перед теоретиками та практиками публічного управління постає завдання не лише адаптувати оборонну політику держави до загроз гібридних воєн, а й військово-політичні та суспільно-політичні механізми, які б не дозволили перерости незначним, периферійним конфліктам у масштабну війну [82, с. 86; 92].

На жаль, одним із сучасних прикладів гібридної війни є спеціальна операція збройних сил рф у Криму (26–28.02.2014 р.) і повномасштабна агресія проти України (24.02.2022 р.), причому успіх операції закордонні експерти пов'язують саме із гібридністю дій російських військових. На

думку експертів, «гібридність» полягала в швидкому розгортанні військової сили рф у Криму, веденні масштабних інформаційних операцій, спрямованих на російсько-орієнтовану масову аудиторію, а також у широкому використання сил спецоперацій – «ввічливих людей» без розпізнавальних знаків, одночасної дії повстанських і регулярних елементів [30].

Таким чином, гібридна війна пов'язується з новим типом загроз, що потребують реагування НАТО та окремих країн ЄС, які виявилися не готові до подібних агресивних дій. Гібридна війна визначається серйозним викликом системи колективної безпеки, оскільки перебуває у «сірій зоні» дій (а це очевидний акт агресії), ускладнюючи пряму апеляцію до ст. 5 Північноатлантичного договору [60]. Більше того, в альянсі слушно наголошували, що рф стала ще небезпечнішою, ніж у роки холодної війни, тому що використовує методи гібридної війни [60]. Експерти RAND Corporation вбачають сліди гібридної війни рф мало не по всьому світові [91; 92; 203]. Цю позицію як ніхто поділяє Україна, країни Балтії, Велика Британія та ін. До речі, на території країн Балтії у червні 2018 р. пройшли навчання спецназу Trojan Footprint 18 щодо відбиття гібридної загрози. Тоді у навчанні прийняли участь 2 тис. військовослужбовців спеціальних підрозділів із 13 країн [218]. Зважаючи на вищевказане, уважаємо, що слід розібратися, який вплив мають дії російських військових у Криму та всій Україні у світлі доктрини гібридних воєн.

Швидке розгортання. Насправді в Криму російських військовослужбовців було дислоковано ще до 201 року, згідно з додатком 2 до угоди про поділ Чорноморського флоту від 28 травня 1997 р. [91; 147]. Напередодні 2014 р. їхня кількість не перевищувала 25 тис., а додатково перекинуті туди сили також не порушували кількісні ліміти. За оцінкам експертів, додатково було перекинуто більше 1700 осіб [179; 182]. Україна до кінця операції так і не денонсувала згадану угоду, тому ніякого швидкого розгортання не було. Принагідно зауважимо, що з правової точки було

додано достатньо зусиль з боку рф, щоб полегшити введення військ до України, заняття її території та запровадження зовнішнього керування на них.

Масштабні інформаційні операції. З упевненістю можна стверджувати, що напередодні спецоперації на території України велася активна пропаганда, спрямована на масову свідомість. У цьому аспекті дії російських військових не виявилися несподіваними для місцевих мешканців Криму в 2014 р. Відбувалося лише замовчування не суті подій, а строки досягнення «кінцевих цілей». Масова підтримка гасла "Крим – це російська земля» не вимагала переконання чисельної кількості громадян ні в Криму, ні в рф, про що говорили проведені соціологічні опитування ще до загострення ситуації. Пропаганда рф щодо незаконного перевороту в Києві, можливих репресіях, погрозах на адресу мешканців Криму, різні обіцянки зумовили не просто зростання проросійських настроїв, а й до того, що населення півострова готувалося до відкритого конфлікту ще до прибуття «ввічливих зелених чоловічків», які були сприйняті як допомога та захист. Як відомо, у м. Севастополі загони самооборони почали формувати вже 23.02.2014 р. [73; 123; 133; 140].

Щодо українських військових, то вони перші, хто змушений боронити Україну, тому щодо їх діяльності існує багато фейків, дезінформації тощо, що поширюється в рф. Цілком зрозуміло, що це викликає різне сприйняття в населення, і, на жаль, подекуди схвалення та позитивний відгук. Проте цього не має бути з огляду на ті кровопролиття та безчинства, які чинить рф як країна-агресор.

Кібероперації. Військова інфраструктура України в окупованих її регіонах не мала значної інформаційної складової у плані розвідки, спостереження, управління та командування військами. Тому про кіберпростір на території кримського півострову, Донецької та Луганської областей як поля протистояння між Україною та рф можна говорити, що він наче був, але його не було. Аналіз структури організаційного механізму

державного управління у сфері інформаційно-гібридної війни (див. рис. 2.2) дає підстави стверджувати, що в Україні функціонує ціла система публічних інституцій, покликаних протистояти загрозам інформаційного характеру. Це і РНБО України, Нацполіція, СБУ, Державна служба спеціального зв'язку та захисту інформації України тощо [96]. Проте всі ці інституції дозволили відмежуватися від подій інформаційного впливу, який чинився тривалий час з боку рф на території кримського півострову, Донецької, Луганської, Херсонської та інших областей. За умови дієвого функціонування зазначених інституцій деструктивний і дестабілізуючий вплив було вчасно нейтралізовано, а, отже, збережено територіальну цілісність України. Проросійська пропаганда – це справа не одного місця та дня. На цій підставі потрібно говорити про те, що важливим є оптимізація діяльності публічних інституцій, покликаних гарантувати та підтримувати інформаційну, соціальну та іншу безпеку в Україні [91; 92].

Одна справа, коли блокується зв'язок під час захоплення українських військових об'єктів, а інша – це збереження спецзв'язку з базами та військовими частинами та відсутність протидії проросійській пропаганді. На наш погляд, проблема у зв'язку, у тому числі в зворотному, який наразі складніше налагодити під час введеного правового режиму стану війни. Фронт може бути не тільки відокремлений географічно, а й умовним, як-то інформаційний. Українське керівництво та публічні інституції у сфері забезпечення інформаційної безпеки повинні брати на себе відповідальність, більше того, вони всі мають необхідні повноваження для інформаційного захисту (див. ст. 19, 22 тощо Закону України «Про національну безпеку України» [96]).

Широке використання спеціальних сил, комбінування регулярних та повстанських сил. Вище ми дійшли висновку, що ефективність дій російських військових у 2014 році пояснюється підтримкою місцевого населення, серед якого активно поширювали проросійську пропаганду (щодо блокування режиму київської влади,

непогодження з методами її роботи тощо). Усе це завдало удару з середини країни, паралізувало дії українських військових тощо. Проте комбінованість і вагомість дій регулярних Збройних Сил України, включаючи загони територіальної оборони, можна побачити у низці ситуацій, за яких військовослужбовці своїми зусиллями спростовували проросійські фейки та дезінформацію, що поширювалася роками. Тож, у цьому плані можна вказати на особливу концептуальну новацію – спроможність публічної влади тільки за кризових умов.

Таким чином, після подій, які відбулися в 2014 р. на території України і зумовили окупацію низки її територій можна наполягати на важливості розгляду цих подій у контексті, по-перше, гібридності війни, яка ведеться проти неї. А по-друге, недооцінювання ролі пропаганди, ідеології та сили інформаційного впливу. Противник України, на жаль, зумів скористатися вмінням урахувати специфіку конфлікту та вразливі місця, як наслідок, за декілька місяців до повномасштабної агресії вміло її приховав, використовуючи добре відомі прийоми боротьби, а не міфологізоване ноухау. Сьогодні інформаційно-гібридна війна проти України вимагає адекватного сприйняття країни-агресора як зовнішнього чинника, що зумовив загибель українців, втрату ними роботи, руйнацію цивільної, соціальної, енергетичної, критичної та іншої інфраструктури тощо. Інакше, загрози інформаційного характеру, автором яких є рф, трансформуються в небезпеки для України. За найгіршого сценарію, рф може домогтися розколу українського суспільства, розвалу державних інститутів, а також Збройні Сил України [11; 12; 140]. Усе це помножено на розгубленість державно-владного режиму, призведе до втрати суверенітету України та нації як такої. Необхідним є активне вкидання теми інформаційно-гібридної війни у політичний, суспільно-управлінський дискурс, тому що слід забезпечити висвітлення справжнього становища справ в Україні з метою протистояння подальші дезінформації, що має тенденцію до посилення у певні періоди функціонування нашої держави. Ці періоди стосуються

реалізації її євроінтеграційних прагнень, як демократичної, соціальної, правової держави. Достатньо тільки подивитися на новини в російських ЗМІ у 2019 році (коли було конституційно закріплено євро інтеграційний курс України) або у 2022 році (коли їй було надано статус країни в члени ЄС). Крім того, варто вказати на те, що під час нових періодів функціонування України вибуховий інтерес до теми інформаційно-гібридної війни в англомовній науковій літературі збільшувався [86; 220].

Отже, потрібно говорити про актуалізацію сучасної концепції гібридної війни, яку можна розглянути як спробу країн Європи та США переглянути якісний ривок у реформі та переозброєнні колективної системи безпеки, про що заявив генеральний секретар НАТО А. Расмуссен [86; 220]. Очевидно, що на тлі кризи НАТО, пов'язаної з вимогою США до країн Європи збільшити свої фінансові внески, тема інформаційно-гібридної війни може забезпечити консолідацію альянсу та колективну безпеку. Крім того, реалізація даного посилу є необхідною для того, щоб забезпечити формування об’єктивної суспільної свідомість – про мілітаризацію російської зовнішньої політики. Розгляд інформаційно-гібридної війни як ноу-хау сьогодні вже не дає особливої переваги, але на яку (війну) важливо реагувати збалансовуючи механізми державної політики, що спрямована на протиборство російській агресії.

З суспільно-політичного погляду, ажіотаж навколо інформаційно-гібридної війни пов'язаний не лише з кон'юнктурними міркуваннями окремих держав або їх коаліцій, але й з об'єктивною тенденцією до зростання частки таємної інформації, дипломатії, методів іррегулярної війни, активізації діяльності спецслужб. У свою чергу, ці процеси є наслідком перерозподілу сил у світовій безпековій політиці, що неминуче супроводжується кризою міжнародних організацій, міжнародного права та превалюванням двосторонніх відносин над багатосторонніми. Нові форми інформаційного протиборства також виникають під впливом процесів глобалізації, яка сприяє зростанню розмитості міждержавних кордонів для

переміщення людей, товарів, фінансів, технологій тощо. Ці форми негативно позначаються на суверенітеті держав (Грузії, України, Молдови та ін.), роблячи їх вразливим, що вимагає усунення в напрямку протистояння інформаційно-гібридній війні [92; 103].

Інформаційно-гібридна війна поки що не отримала остаточного оформлення як самостійний вид протиборства. Водночас, тенденція до використання інформаційно-гібридних методів у сучасних конфліктах зберігається. Американські експерти у сфері інформаційної безпеки вважають, що ці методи потрібні на десятиліття вперед, тому необхідно розробляти особливу стратегію, що дозволяє мобілізувати необхідні ресурси до державних масштабах, ураховуючи багатоаспектність інформаційно-гібридної дії. Аналогічне розуміння проблеми має сформуватися і на вітчизняних теренах, про що буде свідчити програма вжитих заходів щодо функціонального удосконалення організаційного механізму державного управління в умовах інформаційно-гібридної війни. У цьому контексті важливим є об'єднання міжвідомчих зусиль щодо інституційного забезпечення інформаційної безпеки України (див. табл. 2.1). Поки що зміст цієї доктрини зводиться до комбінування вже відомих засобів, способів та методів протиборства військового, напіввоєнного та невоєнного характеру.

Отже, феномен інформаційно-гібридної війни еволюціонує у двох напрямах. З одного боку, інформаційно-гібридна війна залишається «парасольковим» поняттям, що дозволяє проаналізувати особливості сучасних військових і суспільно-політичних конфліктів, а також здійснити пошук оптимальних шляхів для адаптації мистецтва керування державою до мінливих умов та способів протиборства [11; 45; 78]. Другий напрямок еволюції, що заслуговує на окреме вивчення, пов'язаний із суспільно-політичним дискурсом. Йдеться про сприйняття та реагування суспільством загроз інформаційного характеру, адже вони (процеси сприйняття та реагування) не завжди відзначаються виваженістю й об’єктивністю. На військово-доктринальному рівні концепт інформаційно-гібридної війни

остаточно не сформований, як і в суспільно-політичній полеміці він нерідко використовується як засіб маніпуляції та пропаганди, тому він розглядається викривлено, включити все що завгодно. На цій підставі можемо стверджувати про важливість дослідження ролі соціально-політичного забезпечення інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни.

2.3. Інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни

Розглядаючи термін «інформаційно-гібридна війна», варто наголосити, що на сьогодні немає єдиного визначення такого типу війни. Це пов'язано з багатозначністю терміну «information warfare», що зумовило безліч різночитань при його перекладі. Цей термін трактується як «інформаційна війна», «інформаційне протиборство», «інформаційно-психологічна війна» та ін. [14; 15; 36; 73; 79; 105-108; 126; 141-142; 143-145; 158; 160]. Якщо у фундаментальній науці немає єдиного визначення поняття інформаційна й інформаціно-гібридна війна, то, очевидно, що це додає складності визначенню інструментів ведення такої війни, які необхідно більш детально розглянути. Адже вони спрямовані на дестабілізацію у функціонуванні певної держави, її апарату та населення.

За свідченням К.С. Грей, сьогодні в міжнародних відносинах усе складніше (ніж це було в минулому сторіччі) використовувати безпосередньо жорстку військову силу. З одного боку, це надзвичайно витратно, а з другого – зростає значення універсального міжнародного гуманітарного права [180] тощо. Відповідно, держави для досягнення своїх зовнішньополітичних та інших цілей повинні застосовувати гнучкіші технології – інструменти «м'якої сили». Вони також спрямовані на дестабілізацію функціонування державних органів, що формують

відповідну інституційну систему публічного управління. Проте з огляду на інноваційність таких інструментів, їх використання набуває поширення, оскільки значна частина країн світу має низький рівень соціального, економічного й інформаційного розвитку, що унеможливлює протистояння таких держав перед зовнішніми та внутрішніми загрозами.

На погляд К.С. Грей [180], ці інструменти «м'якої сили» активно застосовуються під час ведення інформаційно-гбіридної війни. Зважаючи на її масштабність і загрозливість, доцільним є проведення наукових досліджень щодо особливостей інструментів «м'якої сили» і шляхів протистояння їм. Це необхідно для того, щоб убезпечити держави від руйнування, перетворення їх на дисфункціональні чи неспроможні до функціонування та розвитку [89; 90].

Уперше термін «м'яка сила» («soft power») було запроваджено у 1990 році вченим Джозефом С. Най молодшим (Joseph S. Nye, Jr.) [84]. Як відомо, з грудня 1995 р. до червня 2004 р. він обіймав посаду декана Школи державного управління ім. Кеннеді Гарвардського університету. Науковець зазначає, що «м'яка сила» має інтерпретуватися в різних цілях, руйнівних і не тільки. За цих умов «м'яка сила» представляє собою форми цілеспрямованої діяльності щодо формування та підтримки соціально-культурної, ідеологічної та іншої привабливості держави-об'єкта. Саме таким терміном позначається держава, на яку спрямовано зовнішній вплив з боку держави-актора. Вона застосовує «м'яку силу», у свою чергу, цілеспрямовано чи ненавмисно для досягнення своїх стратегічних цілей. У продовження вчені стверджують, що така привабливість «м'якої сили» ґрунтується на принципах, яких дотримується держава-актор, або на цінностях, які є основними в будь-якій конкретній країні [202; 207; 208]. За свідченням дослідників, наразі концепт «м'якої сили» активно реалізується Китаєм, зокрема, за допомогою проведення агресивної торговельної політики по відношенню до Заходу, шляхом надання на пільгових умовах кредитів для латиноамериканських та африканських держав, а також

здійснення дипломатичного тиску на своїх партнерів. Крім того, прикладом того, що Китай активно використовує інструменти «м'якої сили» є таке: 1) надання можливостей для іноземних громадян на безкоштовне їхнє навчатися за китайськими програми у різних сферах суспільної життєдіяльності [83]; 2) проведення найширших культурних кампанії; 3) надання найбільшої кількості солдатів для проведення миротворчих місій ООН [178; 179; 203; 208].

Аналіз наукових напрацювань у сфері інформаційної безпеки та гібридних війн дав підстави наполягати, що «м'яка сила» має визначатися як комплексний інструментарій вирішення зовнішньополітичних завдань, що базується на можливостях залучення громадянського й інформаціного суспільства, інформаційно-комунікаційних технологій, гуманітарних та ін. альтернативних класичній дипломатії методів. Наразі застосування інструментів «м'якої сили» відбувається в умовах посилення глобалізації, конкуренції та накопичення кризового потенціалу. Це, у свою чергу, зумовлює появу ризиків і загроз, які з часом здійснюють деструктивний вплив на державу-об'єкта, який передбачає: 1) політичний, економічний та інший тиск на суверенну державу, втручання у її внутрішні справи, дестабілізацію внутрішньо-державної обстановки та суспільного життя; 2) маніпулювання громадською думкою та свідомістю, у тому числі в межах фінансування гуманітарних проектів та ін. проектів, начебто пов'язаних із захистом прав людини [89; 90].

Варто погодитися з вченими [178; 179; 202; 208], що управлінську практику застосування «м'якої сили» залежно від цілей її застосування та спрямованості можна умовно розділити на такі підвиди:

1) «м'яка сила» як засіб просування державою своїх національних інтересів за кордоном або на міжнародній арені без поєднання з агресивними руйнівними діями щодо інших суверенних держав та загрозами їх стабільності та їх громадському порядку;

2) «м'яка сила» як засіб дестабілізації та дисфункціоналізації системи

публічного управління та держави в цілому, неконституційної зміни її влади, її руйнування. У цьому дослідженні розглядатиметься «м’яка сила» як засіб дестабілізації або дисфункціоналізації інституційної системи публічного управління [там само].

Крім того, слід констатувати, що зміст концепту «м'якої сили» набагато ширший за такі форми інформаційної та політичної діяльності: 1) пропаганда державою своїх цінностей; 2) формування нею власного позитивного іміджу. Для характеристики цих форм можуть бути використані інші слова, що не мають настільки явних негативних асоціацій, що притаманні інформаційно-гібридній війні. Це зумовлено тим, що пропаганда, ідеологія, формування міжнародного іміджу країни тощо становлять передумови для поширення інформаційно-гібридній війни. Невчасне та недієве реагування на такі форми зовнішнього впливу стимулюють виникнення такого виду війни [89; 90].

Сьогодні для України надзвичайно актуальною є проблематика технологій «м’якої сили», які застосовуються проти неї з метою її руйнування,трансформації її у слабку державу-сателіт, що має повністю субмісивну політичну й економічну сфери. Використання цих технологій значно посилюється, свідчення чого є масштаби агресивного застосування інформаційних технологій з боку рф, Китаю та інших держав [83; 89; 178; 202; 208]. Так, в умовах прогресуючого зростання кількості випадків публічних заяв щодо «бандерівського» українського народу, принизливого ставлення до нашого народу варто зазначити, що, на жаль, ці інструменти «м’якої сили» отримали розвитку шляхом поширення національної ненависті та ворожнечі. Це, так зване, нове націєбудування примусовими методами [89; 90]. На цій підставі вважаємо, що проблеми, пов’язані із загрозами агресивного застосування «м’якої сили» з боку Росії набувають особливого значення й актуальності.

Вище в роботі згадувалися інструменти «м'якої сили» і «жорсткої сили». На різницю між ними вказують закордонні вчені, зауважуючи, що інструменти «жорсткої сили» спираються на матеріальні та людські військові

ресурси і, як правило, використовуються із поєднанням насильницьких методів [181-182]. На погляд учених, використання інструментів «м'якої сили» вимагає розробки та використання різних стратегій і дій, спрямованих на формування симпатії (антипатій) у населення не до своєї Батьківщини, а до іншої держави-актора [там само]. Вона, у свою чергу, вживає всіх заходів щодо впровадження в суспільне життя факторів саморуйнування держави-об'єкта, її органів державної влади та суспільства.

Отже, аналіз наукових напрацювань [178; 181; 202; 208] дає підстави стверджувати, що концепт інформаційно-гібридної війни з її інструментами запропонований Дж.С. Наєм та ін., не є беззаперечним [84; 193]. Так, дослідник Е. Ліаропулос, Т. Лоуренс та ін., будучи ще одними з критиків концепту «м'якої сили», констатують, що така сила є відображенням жорсткої та сильної влади з боку держави-актора, що не погоджується з політикою держави-об'єкта [189]. Держава-актор може застосовувати «м'яку силу» тільки за наявності своєї жорсткої влади, але не тільки через неї. Очевидно, що держави-актори мають значний військовий потенціал, економічну могутність і промислову потужність, щоб можуть претендувати на ефективне застосування «м'якої сили» [там само]. Саме так відбувається по відношенню до України, яка є державою-об'єктом для застосування Росією інструментів «м'якої сили».

Ще однією особливістю концепту «м'якої сили» називають те, що надзвичайно складно оцінити (а точніше виміряти) вплив держави-актора та застосовану нею «м'яку силу» [там само]. Так, слушним є зауваження К. Хермана, Т. Лоуренса та ін., що за своєю природою виникнення та поширення «м'яка сила» – це відносне та нематеріальне поняття, що важко піддається кількісній оцінці [188; 189]. На думку науковців, яку ми поділяємо, для вимірювання елементів потенціалу та застосування «жорсткої сили» можуть бути використані кількісні показники, а саме: 1) чисельність населення; 2) обсяги витрат на оборону; 3) військовий потенціал; 4) ВВП та наслідки економічних санкцій тощо [там само]. Проте вкрай складно

виміряти інструменти «м'якої сили», і найімовірніше під час їхнього оцінювання можуть застосовуватися якісні показники такі, як імідж держави, її репутація, культурний вплив тощо.

Отже, відсутність чіткої концепції визначення «м'якої сили» є очевидною, і він аплікується на публічну дипломатію, стратегічні комунікації, внутрішній порядок у державі-об'єкті та ін. При цьому траєкторія дії «м'якої сили» формується залежно від потенціалу держави-актора, яка використовує технології «м'якої» сили». Крім того, ця траєкторія залежить також від типу комунікативного месенджу, який передається від держави-актора, а також залежно від характеру цілей, що переслідує така держава [89; 90].

Отже, при всіх недоліках оцінювальної конструкції «м'якої сили», вона є дескриптивно атрибутована, адже передбачає застосування цілого комплексу технологій. У цьому контексті вважаємо, що концепт «м'якої сили» верифікується державами-акторами, насамперед, для дисфункціоналізації, дестабілізації та припинення функціонування держав-об'єктів [84; 180; 190; 217].

Розгляд закордонних практик застосування інструментів «м'якої сили» на Європейському й Азійському континентах дав змогу стверджувати, що і країни з високим соціально-економічним рівнем, і країни, що тільки стали на шлях сталого розвитку, здатні дієво реагувати на такі інструменти. Досвід таких країн є корисним для дослідження й аплікування на вітчизняних теренах. Дане твердження висловлено з огляду на два моменти: 1) євроінтеграційні прагнення України; 2) стан її соціального й економічного функціонування, що характеризується поки що як не стабільний.

Під час дослідження виявлено, що та ж Франція й Казахстан – країни з різним соціально-економічним рівнем розвитку, успішно впроваджують управлінські практики реагування на інструменти «м'якої сили». Це відбувається за допомогою застосування ризик-орієнтованих підходів,

зокрема, під час розробки та реалізації стратегій управління ризиками та загрозами інформаційного характеру [89].

Цей підхід до побудови стратегій управління ризиками передбачає виділення таких інтегральних способів управління ризиками (не включаючи етап моніторингу та оцінки ризиків):

1) превенція ризиків;

2) прийняття та адаптація ризиків;

3) редукування ризиків;

4) переведення чи каналізація ризиків;

5) трансформація та деконструкція ризиків [89; 90; 95; 166].

Уважаємо за необхідне вказати на пропозиції науковців, які здійснили оцінювання ступеня відображення в законодавстві Казахстану та Франції імперативу обліку ризиків у публічному управлінні [89; 195]. Це абсолютно різні країни за станом соціально-економічного розвитку, але є умовно зразковими. Безумовно, що Франція вже досягла в цьому ризик-орієнтованому напрямі більш значних результатів. Казахстан упроваджує даний підхід з 2012-2013 рр. Однак ця країна також має певні вагомі здобутки, на які варто звернути увагу.

Так, публічне управління ризиками та загрозами (у тому числі інформаційного характеру) у Франції відбувається в різних сферах суспільної життєдіяльності. Таке управління отримало назву (мовою оригіналу) «gestion des risques», «management des risques». Воно є важливим пріоритетом і дієвим інструментом державного управління (див. [215]). Проведений аналіз низки нормативно-правових актів Франції дав змогу зазначити, що в цих документах окреслено імперативи обліку ризиків і загроз у публічному управлінні. Зокрема, розроблена та впроваджується Національна стратегія управління ризиками повеней (Stratégie nationale de gestion des risques d'inondation), Декрет № 2010-515 від 18.05.2010 «Про регіональні багаторічні програми управління ризиками» та ін. [215].

Крім того, на території Франції активно впроваджуються міжнародні

стандарти ISO 31000:2009 «Управління ризиками – керівні принципи та напрямки», ISO 73: 2009 «Управління ризиками» та ін., що були затверджені Міжнародною організацією зі стандартизації [138]. Крім того, у Франції дотримуються положень Директиви № 2006/48/ЕС Європейського Парламенту та Ради щодо технічних положень, які стосуються управління ризиками. До речі, цієї Директиви також мають дотримуватися й вітчизняні управлінці [41].

Принагідно відзначимо, що в структурі Міністерства екології, сталого розвитку та енергетики Франції створено та діє нині спеціальний орган – Загальна дирекція з попередження ризиків і загроз інформаційного характеру (Direction Générale de la Prévention des Risque) [215]. Крім того, у Франції функціонують такі інституції, що впроваджують ризик-орієнтований підхід:

1) Національний комітет з управління ризиками у сфері сільського господарства (Comité national de gestion des risques en agriculture) при Уряді Франції;

2) Фонд попередження великих природних ризиків (Fonds de prévention des risques naturels majeurs);

3) Центр з вивчення та експертизи ризиків, стану навколишнього середовища, мобільності та розвитку (Centre d'études et d'expertise sur les risques, l'environnement, la mobilite et l'aménagement (CEREMA));

4) Національний комітет з управління ризиками у сфері лісових ресурсів (Comité National de la gestion des risques en forêt) та ін.

Усі ці інституції реалізують публічне управління з мето унеможливлення трансформації ризиків інформаційного характеру у загрози. Керівництво цих інституцій призначається урядовими декретами. Крім того, існує комісар Уряду Франції з громадських інтересів групи планування та управління ризиками (commissaire du Gouvernement auprès du groupement d'intérêt public «Aménagement du territoire et gestion des risques») [164].

В Україні деякі підзаконні акти також закріплюють норми, що передбачають аналіз, оцінку, прогнозування та мінімізацію ризиків і загроз у

системі публічного управління. На наше переконання, базовим спеціальним нормативно-правовим документом у цій сфері мав би стати проект закону «Про державне стратегічне планування» (оприлюднений ще у 2017 р.) [115]. Цей законопроект повинен був урегулювати відносини, які виникають між учасниками стратегічного планування у процесі цілепокладання, прогнозування, планування та програмування соціально-економічного розвитку України, і на які (відносини) впливають ризики та загрози інформаційного характеру. Згідно з положеннями зазначеного проекту закону, прогнозування визначається діяльністю учасників стратегічного планування щодо розробки науково обґрунтованих уявлень про ризики соціально-економічного розвитку, про загрози національної безпеки України, про напрями, результати та показники її соціально-економічного розвитку [89; 90]. Розробники проекту закону вважають, що стратегічний прогноз є документом стратегічного планування, який містить систему науково обґрунтованих уявлень щодо стратегічних, інформаційних та інших ризиків і загроз соціально-економічного розвитку та безпеці України. Відтак, поділяємо думку дослідників, що до принципів стратегічного планування (із застосуванням ризик-орієнтованого підходу) можна віднести принципи публічності, реалістичності, результативності, ефективності, комплексності тощо. Їхній зміст визначається таким чином: при визначенні цілей і завдань соціально-економічного розвитку та забезпечення безпеки учасники стратегічного планування повинні виходити з можливості досягнення цілей і вирішення завдань у встановлені терміни з урахуванням ресурсних обмежень та ризиків [42].

Зважаючи на вищенаведене, уважаємо, що необхідно оновити вітчизняне законодавство, окресливши перспективи застосування ризик-орієнтовано підходу під час функціонування інституційних механізмів публічного управління в умовах загроз інформаційного характеру. При цьому слід звернути увагу на важливість проведення оцінки ризиків несприятливих наслідків застосування запропонованого правового регулювання. Таке

оцінювання має включати перелік ризиків вирішення виявленої проблеми одним з таких способів правового регулювання:

– ризики невідповідності запропонованого правового регулювання заявленим цілям регулювання;

– ризики недостатності механізмів реалізації запропонованого правового регулювання для вирішення проблеми;

– ризики відсутності належного контролю дотримання вимог, що вводяться;

– ризики відсутності необхідних ресурсів та кадрів;

– ризики невідповідності запропонованого способу правового регулювання рівню поширення необхідних технологій;

– ризики погіршення інвестиційного клімату;

– ризики зниження темпів розвитку малого та середнього підприємництва;

– ризики зниження конкуренції;

– ризики зниження безпеки та якості продукції;

– екологічні ризики;

– соціальні ризики [11; 16; 42; 90].

Природа всіх цих ризиків складна, але зумовлена виникненням і поширенням інформації, відомостей, баз даних тощо. Тому важливим є здійснення результативного та повсюдного застосування ризик-орієнтованого публічного управління потоками цієї інформації, що вимагає оновлення вітчизняного законодавства [89] та врахування відповідного позитивного закордонного досвіду.

Перш ніж розглядати світові тенденції, які деструктивно впливають на державу-об’єкт, необхідно звернутися до фундаментальних філософських підстав деструктивізму [38]. Видається, що перераховані вище проблеми деструктивного впливу держав існують у цифрову епоху, яку переживає людство сьогодні. Тому їх (проблеми) можна віднести вже не до передумов, а до логічного висновку про кульмінацію періоду постмодернізму та

початок метамодерну. Важливим аспектом у цьому контексті є прогрес саморуйнування, починаючи від поглядів на божественне й абсолютне і закінчуючи суспільно-політичними рішеннями, які відображаються на інформаційно-цифровому суспільстві [117].

Найчастіше приклади глобального деструктивізму можна побачити у вигляді прийнятих суспільно-політичних рішень, а також протиборства та домінування одного державного устрою над іншим. За цих умов Україні та її громадянам складно протистояти багаторічному деструктивному впливу, що обумовлено багатьма факторами, починаючи від географічного розташування та закінчуючи міжкультурними відносинами на стику Азії й Європи. Феномен саморуйнування породжується у різних місцях [там само]. Проте погоджуємося з Е. Афоніним, О. Крюковим, О. Радченко та ін., що останнім часом через зміну конституційне закріплення інтеграційного курсу можемо спостерігати самодостатність українців на фоні деструкту з боку країни-агресора. Це проявляється у механізмах, задіяних проти сучасного українського суспільства. Разом із тим, важливим аспектом є реагування інших держав на такий деструкт, що (реагування) може проявлятися в санкціях, обмеженнях та заборонах на участь у міжнародних організаціях, присутність на світовому ринку [89; 202].

Елементи деструктивізму можна спостерігати також і на Сході, наприклад, коли у серпні 2021 року в Афганістані владу захопив «Талібан» (заборонена організація), рівень прав і свобод, а також соціальний статус цивільного населення був переглянутий у бік радикалізму [85]. Це викликало еміграцію частини суспільства до більш світських країн. Однак такі деструктивні феномени надають вплив виключно внутрішній безпеці або спрямовані на локальних сусідів. Глобальний чи світовий деструктивізм властивий могутнішим країнам (Китаю, Росії тощо).

Яскравим прикладом є індекс цитування світових друкованих видань. За даними 4intermediationalmedia&newspapers –б перші дев'ять позицій серед газет та журналів займають або англійські, або американські видання, на

десятому рядку знаходиться єдина китайська газета ChinaDaily [163]. Азіатські, близько східні та інші ЗМІ йдуть з нижчим рейтингом після європейських передових мас-медіа. При цьому згідно з дослідженням міжнародного інституту маркетингових досліджень GFK, перші три номінації в рейтингу найбільш читаючих країн світу займають Китай, Росія й Іспанія [175].

Варто відзначити, що лідера деструктивізму у рейтингу світових ЗМІ немає, але цей феномен є свідченням біполярного світу, в якому бажання чути інших учасників цього міжнародного процесу не цікавить інформаційне суспільство, яке формується західними й азійськими медіамагнатами.

Повертаючись до критичного аналізу та проблем деструктивних тенденцій у сфері інформаційної безпеки вважаємо що, подібний безпосередній перетин і вплив однієї сфери людської діяльності на інші у сфері політики та правових норм у цифровому світі чинить негативний вплив на інформаційне суспільство, яке вимушене мігрувати чи пристосовуватися до таких важких процесів. Наведені вище приклади є далеко не єдиними. Подібні події відбувалися під час президентських виборів у США 2016 р. і під час виборів до конгресу у 2018 р., звинувачення у дезінформації, у тому числі надходили від руху Black Lives Matter (BLM) на адресу російських спецслужб та агентства інтернет-досліджень [176; 221].

Відзначимо, що з’явився спеціальний термін – астротурфінг, процес штучного маскування громадських ініціатив чи підтримки [120]. У такому разі будь-яка соціальна проблема зводиться в абсолют і потребує негайного вирішення. Звичайно, в астротурфінгу немає нічого деструктивного, проте, коли це переростає в жорсткі дискусії та протести не лише в інформаційному середовищі, а й проявляється у реальному житті суспільства, то за цих умов астротурфінгможе представляти небезпеку [там само]. На початку дослідження було розглянуто феномен інформаційних

воєн та їх негативний вплив на розвиток цифрової цивілізації з кінця XX та початку XXI століть. У цьому підрозділі розглядаються деструктивні тактики, в яких реальні події як перетинаються, так і не перетинаються з бойовими діями. Проте їх можна легко використовувати у застосуванні проти супротивника із незахищеним цифровим суспільством. Далі звернемося до блокування інформаційних ресурсів, соціальних мереж та інших медіаплатформ, з метою виявлення критерію, наскільки можливо протидіяти подібним інформаційним загрозам [36; 43; 62; 63; 66; 68; 99; 125; 130].

У 2013 році було представлено доктрину війни нового покоління, що передбачає комплексний підхід у веденні бойових дій за умов гібридних війн. У цій концепції приділяється особлива увага інформаційному протиборству. Так, події «арабської весни» та їх медійний супровід можна прогнозувати та протистояти їм, важливою умовою для чого буде створення системи відстеження інформаційних загроз. Війни, конфлікти, протестні рухи та інші акції [11; 62; 63; 66; 68; 99; 125; 130], пов'язані з насильством і поширені з використанням засобів масових інформацій та онлайн-медіа, дедалі більше сигналізують, що термін «інформаційне протиборство» переріс у повноцінну інформаційно-гібридну війну проти України та інших держав. Тому під час перегляду стратегії інформаційної безпеки України необхідно також це враховувати [там само]. Медіа, ЗМІ, соціальні мережі та інші онлайн-ресурси – усі вони є інструментами інформаційного поля чи простору (війни). Це нове середовище впливає на людство останні десятиліття. Поштовхом даному геополітичному процесу послужило дослідження людиною космосу та розвиток Інтернету. Сучасне інформаційне суспільство є «зобов'язаним», оскільки сьогодні, по суті, навіть без простої реєстрації на порталі «Дії» громадянин стає ізольований від інструментів, доступних для українського суспільства, а відтак, не може повноцінно існувати в інформаційному середовищі. Якщо раніше це здавалося дивним, то сьогодні суспільство вже не дивується такому рівню

цифровізації, доступності матеріалів та персональних висловлювань у медіа [66; 198].

Такий значний стрибок у розвитку та становленні інформаційного поля у світі й Україні не просто створив систему з метаданими, соціальними мережами та іншими можливостями спрощення життя суспільства, а й почав створювати прецеденти для формування етики, цінностей, моралі та поведінки в інформаційних екосистем. Крім того, було сформовано цілу правову базу і підвищено рівень відповідальності з метою підтримання «чистоти» нових інформаційних екосистем. У дослідженні не планується масштабний аналіз питань щодо конструктивних зв'язків між інформаційним середовищем та державою. Варто визнати, що такий зв’язок існує, і передбачає здійснення контролю за дотриманням прав і свобод громадян. У цьому контексті планується розглядати виключно інформаційні загрози та методи боротьби з ними, піддаючи об’єктивній критиці певні механізми публічного управління, вибрані в якості аксіом.

До речі, на веб-сайті Державної служби статистики України є рубрика «інформаційне суспільство». Через повномасштабну агресію проти нашої країни інформація на цьому веб-сайті не оновлюється з міркувань безпеки. І це зрозуміло. У той же час, у межах цієї рубрики містилася така інформація: 1) кількість засобів фіксованого телефонного зв’язку; 2) обсяг реалізованих послуг у сфері телекомунікацій та поштового зв’язку; 3) кількість абонентів зв’язку; 4) кількість поштових відправлень; 5) кількість поштових відправлень (1980-2018); 6) стан і розвиток зв’язку; 7) використання інструментів електронної демократії органами державної влади та місцевого самоврядування [97].

Аналіз інформації, наведеної на сайті Держстату [97] дає підстави стверджувати, що розуміння «інформаційного суспільства», яке закладено практичними фахівцями, дещо відрізняється від науково-теоретичної характеристики цього терміну. На наше переконання, практико орієнтоване визначення інформаційного суспільства є вужчим. Власне кажучи, воно

розглядається з позиції використання застарілих комунікаційних засобів зв’язку (поштові відправлення, телекомунікації тощо). У той же час, наскрізно в роботі ми акцентуємо на загрозливому характері насамперед новітніх ІКТ. Адже вони пришвидшують процеси передачі та ретрансляції негативної, викривленої та іншої небажаної інформації. Очевидно, що недостатньо відображати, скільки е-петицій, е-звернень було розглянуто органами державної влади, або, скільки коштів виділено на, так званий, громадський бюджет, як це зроблено фахівцями Державної служби статистики України [97] (див. Додаток А, Додаток Б).

Відтак, уважаємо, що у післявоєнний період одним з пріоритетних завдань України буде формування її інституційної спроможності з урахуванням актуалізації питання цифровізації всіх сфер суспільної життєдіяльності, а також розвитку інформаційного суспільства. Серед нього має бути якомога більше цифровізовано грамотних громадян, які здатні об’єктивно сприймати фальсифіковану та фейкову інформацію держав-акторів, держав-агресорок та ін.

Варто відзначити, що з моменту початку спеціальної військової операції рф на території України щодо держави-агресора справедливо були прийняті обмежувальні санкційні вимоги Заходу. Після їхнього уведення влада рф вжила низку заходів, у т. ч. щодо блокування різних медіаресурсів. Прецедентами стали матеріали із закликами до насильства по відношенню до російських військовослужбовців, опублікованими, зокрема, компанією Meta. Як відомо, у країні-агресорці ця компанія визнана екстремістською організацією. Важливе уточнення, перегляд цих соціальних мереж, як і раніше, можливий з території рф, але виключно з використанням VPN-серверів.

Очевидно, що відбувається зіткнення з епохою нових інформаційних викликів та загроз, але не в звичній нам формі, а більш комплексній і гібридній, що покладає на користувача більше відповідальності. Межі прав людини та свободи слова у медіасвіті починають розмиватись, а медіа

ресурси набувають усе більшого значення в системі публічного управління, вимагаючи посилення уваги на процеси формування медіа грамотності населення, його інформаційної культури. Якщо повернутися до питання про деструктивні тенденції у сфері інформаційної безпеки, то йдеться не про такі очевидні всім цінності, а про протиріччя та можливості неоднозначного розуміння. Так, країна-агресор створила список заборонених джерел, діяльність яких визнана екстремістською. При цьому переглядати ці ресурси з території рф можна через VPN-сервіси. І якщо раніше такі можливості були не надто популярними, то з блокуванням соціальних мереж компанії Meta, до якої входять Instagram та Facebook, радіус можливостей користувача з відвідування «екстремістських сайтів», зрозуміло, збільшуються. Кількість користувачів обох вищевказаних соцмереж становить 40 мільйонів (на момент травня 2022 року) [66; 68; 99; 125; 130; 186; 192; 204].

Визнання діяльності компанії Meta «екстремістською» на території країни-агресора і тим самим примус великої кількості користувачів до використання VPN в постійному режимі, розширює можливість доступу і до інших, більше неоднозначних, у т.ч. небезпечним ресурсам. На приклад формування системи заборонених джерел інформації країною-агресором, на наш погляд, має бути звернута увага вітчизняних управлінців з метою застосування комплексного підходу до створення цифрового суспільства. У 2022 році в рф створено прецедент щодо блокування цілої компанії, до якої входять дві світові соціальні мережі. Раніше схожі події відбувалися щодо Telegram, Youtube та інших онлайн-медіа. Однак, як показує практика, більшість користувачів все одно будуть обирати зарубіжні платформи, навіть з умовою заборони на них та необхідності використання VPN з поганим трафіком [там само].

Ще одним суперечливим моментом у блокуванні онлайн-медіа є ізоляція. У цьому контексті йдеться про те, що в соціальних мережах публікується значний обсяг матеріалів, присвячених військово-технічним

аспектам та інноваціям у оборонній сфері тих чи інших держав. Здійснення аналізу та збору розвідувальних даних із відкритих джерел (OSINT) у цьому випадку ускладнюється [197]. Цитата Сунь-дзи, про те, що ворога потрібно тримати ще ближче до себе у його осмисленні філософії війни добре описує саме цю ідею [139]. Переосмислювати та розмірковувати на тему безпечного медіаполя для всіх ечасників цього глобального геополітичного процесу можна довго. Однак видається, що сьогодні в України існують лише два можливі шляхи вирішення проблеми: створення внутрішньоукраїнської національної мережі, розробці якої можна повчитися у тих же китайських колег [99; 125; 130; 223], і реалізація Стратегії розвитку інформаційного суспільства України [96]. Видається, що обидва шляхи позитивно позначаться на майбутньому українського суспільства в Інтернет-просторі, а також на забезпеченні його (суспільства) захищеності і на безпеці кожного користувача. Однак подібні вчасно й науково обґрунтовано стратегії необхідно переглядати та вносити корективи щорічно, виходячи з нових інформаційних викликів і загроз, локальних конфліктів та інших політичних проблем [89; 66; 68; 99; 125; 130; 223].

Сучасне міжнародне суспільство об'єктивно стає свідком деструктивних тенденцій у сфері інформаційної безпеки, що відбуваються в Україні, Ізраїлі та ін., через сформовані монополії та дуополії ЗМІ, а вже наслідки цього деструктивізму відчувають безпосередньо громадяни. Відтак, у межах забезпечення інформаційної безпеки України необхідне прийняття якнайшвидше управлінських рішень щодо блокуваннями деструктивного інформаційного впливу країни-агресора з метою забезпечення безпеки українського інформаційного суспільства. Провівши аналіз закордонних наукових напрацювань у сфері інформаційної безпеки, можна виявити, що не всі важелі у формуванні такої безпеки є дієвими, але певні можуть бути враховані на вітчизняних теренах. Крім того, у найближчі роки, швидше за все, VPN-сервіси будуть реформовані для запобігання їхнього визнання як екстремістських [68; 99; 125; 130].

На завершення міркувань щодо підстав формування деструктивних тенденцій у сфері інформаційної безпеки необхідно ще раз відзначити комплексний характер збитків, які в результаті завдаються інформаційному суспільству, – негативному впливу піддається середовище проживання та спосіб життя сучасної людини, трансформуються основи її раціонального мислення. Тому майбутнє розвитку цифрового світу та інформаційного суспільства, у якому зможе безпечно себе відчувати кожен користувач, залежить від створення організаційно-правових, духовно-культурних, інтелектуально-світоглядних, раціонально-смислових та інших засад, які потребують окремого визначення й обґрунтування.

Висновки до розділу 2

1. Проаналізовано ризики та загрози функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, яка ведеться проти нашої держави. Це здійснено крізь призму визначення ролі суб'єктів державної політики у сфері національної й інформаційної безпеки. Виявлено, що серед теоретиків і практиків державного управління відсутній єдиний підхід до групування суб'єктів державної політики у цій сфері. Тому систематизовано класифікацію суб'єктів політики державної безпеки у сфері національної й інформаційної безпеки: 1) зважаючи на рівень формування та реалізації державної політики (державні суб'єкти різних рівнів та недержавні); 2) зважаючи на функціональне навантаження та спектр повноважень (суб'єкти, що виконують дослідницько-інформаційні, організуючі та координуючі функції); 3) залежно від статусу суб'єктів (органи публічної влади, що включають державні інституції та організації недержавного сектору, що залучаються до формування державної політики). Крім того, виявлено, що суб'єктів державної політики у сфері національної й інформаційної безпеки,

на яку деструктивно впливає інформаційно-гібридна війна, можна розділити на дві основні категорії: 1) органи державної влади України (різних рівнів управління та сфер суспільної життєдіяльності, на які це управління спрямоване, органи місцевого самоврядування та ін.); 2) суб'єкти, що функціонують поза системою публічного управління: підприємства та організації різних форм власності і господарювання, громадські об'єднання, асоціації та інші організації громадянського суспільства.

2. Аналіз наукових напрацювань у межах обраної проблематики дав підстави стверджувати про виокремлення у структурі інституційних механізмів публічного управління в умовах інформаційно-гібридної війни таких підсистем – організаційної та правової. Дана гіпотеза висловлена, з одного боку, з огляду на роль правових та соціальних інститутів у забезпеченні належного функціонування всіх сфер суспільної життєдіяльності. А з другого – зважаючи на місце інституцій як органів публічної влади у такому забезпеченні. З'ясовано, в умовах інформаційно-гібридної війни визначальне місце серед таких інституцій займають координуючі суб'єкти публічного управління, що формують і реалізують державну політику у сфері національної й інформаційної безпеки. Акцентується, зокрема, на функціях і повноваженнях Ради національної безпеки і оборони України, її апарату та профільного комітету, що здійснюють таке: 1) моніторинг та дослідження рівня інформаційних загроз; 2) вивчення стану та результативності реалізації стратегій і програм щодо гарантування національної й інформаційної безпеки; 3) підвищення її рівня; 4) надають пропозиції щодо нейтралізації інформаційних загроз, кіберзагроз тощо. Установлено, що РНБО України безпосередньо взаємодіє з Президентом і Парламентом України, його Комітетами з питань нацбезпеки, інформації та зв'язку. Ця взаємодія відбувається в межах наданих пропозиції щодо внесення законодавчих змін у сферах: електронного обігу, телекомунікацій, розвитку інформаційного суспільства, національної програми інформатизації, захисту системи електронних інформаційних

ресурсів тощо. Крім того, наголошується на особливій ролі інших спеціалізованих органів: СБУ, Нацполіції, Державної служби спеціального зв'язку та захисту інформації України тощо. Зважаючи на правову диференціацію у визначенні суб'єктного складу підсистем, що покликані гарантувати та підтримувати систему безпеки України в умовах інформаційно-гібридної війни, запропоновано внести зміни до чинного правового поля з метою усунення такої диференціації. Власне кажучи, рекомендується узгодити між собою положення Закону України «Про національну безпеку України», Доктрини інформаційної безпеки України та Закону України «Про основні засади забезпечення кібербезпеки України» [96; 113].

3. Доведено, що інформаційна безпека України представляє собою сукупність суб'єктно-об'єктних взаємовідносин, що виникають між суб'єктами інформаційного середовища (простору), які здійснюють цілеспрямований, організуючий вплив на різні сфери суспільної життєдіяльності загалом і на об'єкти інформаційної інфраструктури зокрема, що відбувається за допомогою комплексу правових, організаційних, інформаційних, економічних та інших заходів (під час формування й оновлення правової бази, удосконалення структури та/або форм діяльності органів публічної влади, стратегічних, урядових і кризових комунікацій тощо) з метою унеможливлення трансформації ризиків і загроз інформаційного характеру у небезпеки для країни та війни. Запропоноване визначення поняття «інформаційна безпека» передбачає застосування системного підходу до формування інституційної системи публічного управління в умовах інформаційно-гібридної війни. Ключовим завдання такої системи є нейтралізація негативного впливу інформаційно-психологічної війни, пропаганди щодо нівелювання української мови та культури, унеможливлення формування російськими ЗМІ альтернативної інформаційної дійсності шляхом викривленої справжньої картини світу, підвищення позитивного іміджу України на міжнародній арені.

4. Виявлено особливості сучасної концепції інформаційно-гібридної війни, що дозволили визначити таке: ця концепція не набула ще єдиної загально визнаної характеристики ні в теоретичній, ні в практичній площинах. З’ясовано, що на доктринальному рівні новації у методах визначення нетрадиційної війни пов'язані зі зміною спектру інформаційних загроз та акторів конфлікту, що формують ту якість, яка робить війну вже не просто іррегулярною, а інформаційно-гібридною. Іще однією особливістю інформаційно-гібридних воєн визнано їхній тривалий характер, який вимагає превентивної та тривалої політики протидії, організованої на державному рівні. Однак на рівні планування та проведення операцій ключовими залишаються учасники, методи та засоби нетрадиційної війни, що зайвий раз говорить про те, що концепція інформаційно-гібридної війни поки знаходиться на стадії становлення. Відтак, спосіб протидії США інформаційно-гібридним загрозам з боку Росії, Ірану та Китаю дослідники пропонують називати «протидія нетрадиційним війнам». З урахуванням того, що інформаційно-гібридні загрози мають складну природу виникнення та відзначаються масштабністю та довготривалістю, можна спрогнозувати, що через кілька десятиліть доктрина протидії нетрадиційним війнам суттєво видозміниться. Крім того, пропонується застосовувати синергетичний та інституційний підходи до характеристики поняття «інформаційно-гібридна війна».

5. Установлено, що ризики в системі публічного управління чинять істотний вплив на всі сфери суспільної життєдіяльності, позначаючись негативно на соціальній свідомість інформаційної безпеки. На цій підставі рекомендовано розглядати ризик-орієнтоване публічне управління як підвид інституційного публічного управління, що реалізується системою органів державної влади та недержавним сектором у напрямку системної інтеграції (імплементації) концептів, стратегій і механізмів стратегічного та поточного прогностичного оцінювання існуючих ризиків і загроз інформаційного характеру. Порівняльний аналіз досвіду України, Казахстану та Франції щодо

оцінювання таких ризиків у публічному управлінні дав змогу наполягати на:

1) важливості впровадження нових, у тому числі ризико-орієнтованих підходів у систему публічного управління, що, по-перше, відбувається на рівні формування та реалізації державної політики, а, по-друге, повинно відображатися в ключових правових документах стратегічного планування (у тому числі в рамках побудови так званої «нової моделі» публічного управління);

2) актуалізації питань управління ризиками інформаційного характеру через їхню трансформацію в загрози, що становлять у подальшому базис для виникнення та поширення інформаційно-гібридних війн;

3) постійній реалізації (на системній основі) заходів попередження, прогнозування, реагування на вплив інформаційних загроз. Для цього має функціонувати диверсифікована система профільних органів, що реалізують науково-обґрунтоване профільне ризик-орієнтоване публічне управління в конкретних сферах суспільних відносин, за наявності також і централізованої структури, що оцінює якість реалізації ризик-орієнтованого публічного управління в масштабах усієї держави. Зважаючи на положення чинного законодавства України щодо національної безпеки, акцентується на особливі ролі спеціалізованих органів, покликаних гарантувати таку безпеку в умовах впливу інформаційних загроз. Завданням таких інституцій є гарантування інформаційної безпеки України й унеможливлення трансформації інформаційних загроз у небезпеки та війни;

4) проектуванні інструментів ризик-орієнтованого публічного управління України в умовах інформаційно-гібридної війни з урахуванням позитивно верифікованої багаторічної закордонної практики реагування на інструменти «м’якої сили».

6. З’ясовано, що інструменти «м’якої сили» представляють собою сукупність інституційних, проектно-ідеологічних, міжнародно-правових, організаційних, фінансових, інформаційно-пропагандистських, розвідувальних та інших механізмів проектування, алгоритмізації,

реалізації, забезпечення та контролю процесів дисфункціоналізації, дискредитації або тотальної руйнації іншої суверенної держави (держави-об'єкта) з метою трансформації цієї держави в неспроможну, що веде до повного її знищення у межах колишньої території або примусової її трансформації у субмісивні форми з редукованим або повністю втраченим суверенітетом, а також для досягнення інших цілей на користь держави-актора. Застосування «м’якої сили» завжди передбачає агресивні дії противника, тому актуальним є визначення заходів з випередження і припинення впливу противника держави-актора на державу-об'єкт, що повинна находити можливості для захисту від запланованих агресивних дій із боку держави-актора. На цій підставі застосування інструментів «м’якої сили» обґрунтовано може інтерпретуватися як здійснення щодо держави-об’єкта неоголошеної гібридної війни, як-то відбувається по відношенню до України [89-91].

РОЗДІЛ 3
НАПРЯМИ ВДОСКОНАЛЕННЯ ІНСТИТУЦІЙНИХ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ІНФОРМАЦІЙНО-ГІБРИДНИХ ВІЙН

3.1. Ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління в умовах інформаційно-гібридних війн

Динаміка розвитку військово-політичної обстановки у світі показує, що розв'язані в різних країнах гібридні й інформаційно-гібридні війни негативно впливають на національну безпеку цих держав. Зрозуміло, що гібридні й інформаційно-гібридні війни – це реальність, яку важко заперечувати, і яка змушує проводити подальше системне дослідження цього феномена.

Як відомо, згідно зі статтею 3 Резолюції Генеральної Асамблеї ООН від 14 грудня 1974 року [23], використання однією державою проти іншої збройних банд, груп, іррегулярних сил та ін., які є військовою складовою «гібридних воєн», визнається агресією. Однак непоодинокими є випадки, коли ці норми не дотримуються геополітичними гравцями світового та регіонального рівнів, що вдаються в «гібридних й інформаційно-гібридних війн» за допомогою приватних військових компаній, терористичних угруповань тощо. Свідченням цього є відповідні події в Афганістані, Україні, Сирії, Венесуелі та інших регіонах, де поширення набули гібридні й інформаційно-гібридні війни. Певні труднощі під час дослідження викликає відсутність конкретного нормативно-правового закріплення «гібридних й інформаційно-гібридних воєн» в міжнародному масштабі в цілому та в Україні зокрема, що ускладнює застосування ризик-орієнтованих підходів до їх нейтралізації та попередження.

Аналіз нормативно-правової бази щодо визначення «гібридних й інформаційно-гібридних війн» переважно регламентує їх як протидію інформаційним технологіям, що залучаються в межах інформаційних війн, кібервійни, терористичної війни та інших видів війн. З огляду на це доцільно спочатку показати, як дана обставина подається в наукових та експертних колах на загально світовому та регіональному рівнях, а потім висвітлити це питання на прикладі України.

Сучасний світоустрій вимагає, щоб всі види воєн/конфліктів мали відповідне правове поле. Якщо війна – це організоване насильство, то складно говорити про організацію та організованість, якщо не визначати правові межі цього насильства. Війна, будучи виявом реальності, передбачає використання певних аморальних, не етичних норм, які порушують чинні правові норми, про які потрібно пам’ятати. Одне з визначальних місць займають норми військового права, а також міжнародного права. Вони дозволяють визначити, хто та за яких обставин може застосовувати зброю і стосовно кого можна застосувати військове насильство. Поки не визначено правове поле та його межі, не можна говорити про організацію та проведення війни, а насильство може стати неконтрольованим, нескінченним та спрямованим проти всіх. За відсутності урегульованості суспільних відносин нормами військового та міжнародного права, застосовуються процедури формального оголошення війни та підписання мирного договору, але вони не визначають початку війни, як-то має місце з боку рф по відношенню до України. Як результат, отримуємо військове насильство, але не війну.

Як відомо, після руйнівної для всього людства Другої світової війни 1939-1945 років, з метою підтримки міжнародного миру та безпеки у майбутні роки, позбавлення майбутніх поколінь від військових лих, у жовтні 1945 року було створено Організацію Об'єднаних Націй [19; 107]. Прийнятий того ж року її Статут заборонив країнам надалі ведення будь-якої війни, визнавши останню злочином проти людства і зобов’язав усіх

країн-членів вирішувати свої міжнародні суперечки мирними засобами, щоб не наражати на загрозу міжнародний мир, безпеку та справедливість, утриматися від загроз застосування сили як проти територіальної недоторканності чи політичної незалежності будь-якої держави, так і будь-яким іншим чином, несумісним з Цілями Організації Об'єднаних Націй [19].

Однією з актуальних проблем при вивченні й осмисленні феномену гібридних й інформаційно-гібридних воєн, розроблення заходів щодо відображення збройного, економічного, інформаційного та іншого впливу є проблема правового забезпечення протидії таким війнам і унеможливлення легітимного застосування ризик-орієнтованого підходу. У цьому контексті правове забезпечення доцільно розглядати як сукупність методів правового й організаційного впливу за допомогою юридичних засобів, спрямованих на забезпечення розвитку суспільних відносин, що складаються у сфері протидії гібридним й інформаційно-гібридних війнам, а також управлінських заходів щодо протидії таким війнам [87; 88].

Слід зазначити, що в обхід цих обмежень світовими акторами для реалізації своїх геополітичних та геоекономічних амбіцій було розроблено та впроваджено різні технології ведення «гібридних й інформаційно-гібридних воєн», які успішно використовуються й досі. Виходячи з цілей/інтересів, яких кожна світова та регіональна спільнота дотримується, можна вказати на застосування суб'єктивних підходів до ведення гібридних й інформаційно-гібридних війн. Аналіз сучасного протистояння у Афганістані, Сирії, Україні, Венесуелі та інших «гарячих» точках світу вказує на те, що цей вид війни не обмежений міжнародними правовими рамками, і надає можливість реалізувати глобальні цілі, не допускаючи відкритого великомасштабного зіткнення армій [88; 103].

У цьому питанні думки більшості вчених-теоретиків і практиків, військових стратегів й експертів збігаються. Усі вони одностайні в тому, що «гібридні й інформаційно-гібридні війни» плануються та реалізуються протягом багатьох років поза правовим простором [87; 108]. На цій підставі

можемо зазначити, що інформаційно-гібридна війна в Україні є нелегітимною як і, власне, гібридна війна.

Закони війни розроблені, і, як правило, передбачають виникнення конфліктів між двома воюючими сторонами, зазвичай державами, які переслідують власні інтереси, які кожна зі сторін конфлікту вважає законними. Для характеристики традиційної війни ООН використовує поняття «агресія», окреслила закони її здійснення, захисту прав комбатантів, військовополонених та цивільного населення, забороняючи використання певних видів зброї по відношенню до них. Існуюча нормативно-правова база є інструментом для осіб, які приймають політичні рішення та здійснюють керівництво військовими діями. Нічого такого для гібридної війни та й інформаційно-гібридної війни немає [19].

У цьому контексті можна зазначити, що для гібридних воєн унікальною рушійною силою є повна відсутність легітимності, підпорядкованості міжнародним нормам та правилам, що робить допустимим на цій основі проведення найбрудніших провокацій із залученням терористичних груп, організованої злочинності, фейкових маніпуляцій з даними, здійснюваних державному рівні [66; 68; 99; 130].

З цього випливає, що з правової точки зору «гібридні й інформаційно-гібридні війни» не мають законної сили, але методи реагування та протистояння ним повинні бути легітимними. Інакше одне насильство буде породжувати інше. Сьогоднішні протистояння держав, світових і регіональних спільнот у «гарячих» точках світу з використанням різних технологій «гібридних й інформаційно-гібридних воєн» супроводжуються величезними людськими жертвами, гуманітарними/екологічними лихами, вимушеною міграцією населення та іншими негативними для нього наслідками. Усі ці обставини становлять безпосередню загрозу міжнародній безпеці та миру, про що говорять усі основні протиборчі сили, одночасно не визнаючи свою причетність до цього, як наприклад, рф.

Колишній радник НАТО, відставний голландський генерал Франк

Ванн Каппа слушно зазначає, що держава, яка веде гібридну й інформаційно-гібридних війну, укладає угоду з недержавними виконавцями (бойовиками, групами місцевого населення, організаціями та ін.), зв'язок із якими формально повністю заперечується. Ці виконавці можуть робити такі речі, які сама держава-агресор зробити не може, оскільки будь-яка держава зобов'язана слідувати Женевській конвенції та Гаазькій конвенції про закони сухопутної війни, домовленості з іншими країнами. Усю, так би мовити, брудну роботу можна перекласти на плечі вищенаведених недержавних формувань. З цієї причини терористичні угруповання, приватні військові компанії не пов'язані з міжнародними конвенціями, законами, що забороняють ведення традиційної війни, і вигідні для використання у «гібридних й інформаційно-гібридних війнах» [103; 108].

В останні три роки терміни гібридна й інформаційно-гібридна війна активно застосовуються в військово-політичній та суспільно-політичній площинах та відповідному науковому середовищі. Проте правові аспекти цього явища поки що залишаються недостатньо вивченими. На даний час ведеться жвава дискусія про допустимість використання цього терміну у правовому контексті та про можливості його подальшого включення до міжнародно-правової термінології. Гібридна й інформаційно-гібридна війна стали суспільними кліше для позначення дій держав, які не вписуються в рамки традиційної військово-силової парадигми, і це вкрай негативно позначається на перспективах нормативно-правового регулювання цього явища [87].

Варто констатувати, що перспективи нормативного (звичаєво-правового чи договірно-правового) врегулювання проблематики «гібридної й інформаційно-гібридної війни» поки що є дуже туманними. Оскільки прийняття міжнародно-правових документів має супроводжуватись обговоренням серед широкого загалу та консенсусом, якого з розглянутої проблематики сьогодні немає.

У цьому контексті можна погодитися з ученими [66; 87; 108; 136;

202], що поки що відсутня згода між головними геополітичними гравцями, провідними акторами гібридних й інформаційно-гібридних війн. З огляду на це виникають сумніви в тому, що у найближчій перспективі вдасться унеможливити появу гібридних й інформаційно-гібридних війн у міжнародному чи національному законодавстві. Адже це, у свою чергу, ускладнює реалізацію геополітичних і геоекономічних інтересів держав, які самоствердjуються за допомогою гібридних й інформаційно-гібридних війн.

За результатами дослідження характеру сучасних гібридних й інформаційно-гібридних війн в усіх наявних «гарячих» точках, де перетинаються інтереси світових та регіональних спільнот, можна помітити, що військовий компонент (у більшості випадків) таких війн використовується під прикриттям миротворчої діяльності (наприклад, «руського миру»), або під егідою надання гуманітарної допомоги, врегулювання кризи, що початково регламентовано відповідними міжнародними нормативно-правовими актами у межах ООН [19; 104; 136].

З цього приводу можна зазначити, що одне з провідних місць у пошуках нового світу «гібридних й інформаційно-гібридних війн» займає формулювання стратегії ведення таких війн [88; 103; 136]. Вона, на нашу думку, ще протягом багатьох десятиліть буде визначати вигляд суспільно-політичних, військово-політичних та інших конфліктів майбутнього. При цьому важливою відміною ознакою гібридної й інформаційно-гібридної війни буде відкрите застосування нелегітимної сили, що зумовлює появу суспільно-політичних, військово-політичних та інших конфліктів [там само].

З цією метою деякі держави використовують існуючу нормативно-правову базу миротворчої діяльності й операцій з кризового врегулювання. Зазначений тренд є важливим фактором, що призводить до зміни основних ідей (постулатів) війни та появи нових вимірів сучасних конфліктів, базис яких становлять інформаційні загрози.

В Україні, поряд з іншими державами пострадянського простору, як зазначалося вище, «гібридні й інформаційно-гібридні війни» декларативно регламентовані законодавчо. Так, чинна Стратегія інформаційної безпеки України (2021 р.) містить тільки таку вказівку на гібридність, не розкриваючи її: 1) рф застосовує технології гібридної війни проти України, у т.ч. моделі й механізми інформаційного втручання, що поширюються на територію нашої держави; 2) її завданням є створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам [96; 136; 137]. Не сприяє полегшенню розуміння гібридних й інформаційно-гібридних війн, внесені зміни до деяких законодавчих актів України, зокрема, щодо протидії засобам кримінально-правового впливу ворожим інформаційним впливам в умовах триваючої гібридної війни Російської Федерації з Україною [110].

Обставина щодо декларативного законодавчого визначення гібридних й інформаційно-гібридних війн в Україні пояснюється такими причинами:

По-перше, Україна сама є жертвою аналогічних війн.

По-друге, Україна не веде ворожу політику відношенню до інших країн і всі проблеми ще на початковому етапі їхнього виникнення намагається вирішувати мирними шляхами.

По-третє, вітчизняна нормативно-правова база, що регламентує сферу забезпечення системи безпеки, має насамперед оборонний характер, а не наступальний (достатньо подивитися Стратегії національної безпеки України 2007, 2015 і 2020 років [96; 136]). Стратегічні цілі та завдання України, на жаль, не мають глобальної ознаки, як це спостерігається у світових і регіональних спільнотах, які прагнуть домінування над державами й в окремо взятому регіоні з використанням засобів ведення гібридних й інформаційно-гібридних війн.

По-четверте, Україна є членом міжнародних організацій, у межах яких також відсутній конкретний правовий документ, що регламентує протидію гібридним й інформаційно-гібридним війнам. При цьому

підписано та реалізується безліч угод, концепцій, стратегій боротьби з різними технологіями/інструментами «гібридних воєн», наприклад, таких, як «кібервійни», «інформаційні війни», «терористичні війни» чи боротьба з міжнародним тероризмом, екстремізмом, які передбачають боротьбу з різними видами злочинів транснаціонального характеру, які трактуються як «гібридні й інформаційні загрози» [103; 202].

З цієї причини Україна не веде і не має наміру вести гібридні й інформаційно-гібридні війни або інші війни проти інших держав. Разом з тим, Україна, як й інші держави, відчуває гібридні й інформаційні загрози. Навпаки, проти неї реалізуються окремі технології гібридних й інформаційно-гібридних війн із використанням таких негативних явищ, як міжнародний тероризм та екстремізм; незаконний обіг наркотиків, незаконна торгівля зброєю та людьми, засоби інформаційної війни та ін.

Усі ці загрози становлять військові та невійськові компоненти «гібридних й інформаційно-гібридних війн», і спрямовані на підрив політичних, військових та економічних засад України (спочатку шляхом мінімального збройного впливу, але так було до 2014 року) [66; 68; 104]. Ці компоненти «гібридних й інформаційно-гібридних війн» мають конкретні визначення, наприклад, «інформаційні війни», «терористичні війни», «наркотичні війни», «кібервійни», «прикордонні війни», «санкційні війни» та інші. При цьому може виникнути питання про неприйнятність таких визначень для нашої країни. Вітчизняне бачення цього питання виходить з того, що вже в ужиток міцно увійшли поняття «гібридні війни», «інформаційні війни», «кібервійни». Виходячи з цього, не можна заперечувати й актуальність для України проблематики терористичної війни. Адже загрози, які виникають у межах останньої, ще тривалий час будуть становити небезпеку для України.

З огляду на це на даний час на її теренах сформовано систему правових норм щодо протидії зазначеним технологіям «гібридних й інформаційно-гібридних війн», що здійснюється державою самостійно, а

також у рамках таких міжнародних та регіональних організацій, як ООН, ОБСЄ та ін.

З метою протидії «гібридним й інформаційним війнам» проти України основний акцент має робитися на забезпеченні і інформаційної безпеки. Базовим нормативно-правовим документом, що регламентує діяльність у сфері інформаційної безпеки України (окрім чинної Стратегії), може вважатися Концепція інформаційної безпеки України. Наразі розроблено проект такої концепції [96; 116].

Сьогодні сфера інформаційної безпеки розглядається як одна з найбільш важливих для України, що засвідчує Стратегії її національної й інформаційної безпеки. У той же час, в Україні поки не створена достатня законодавча база для протидії терористичним війнам та інформаційним загрозам, як одним із технологій «інформаційно-гібридних війн». З цією метою прийняті та реалізуються такі нормативно-правові документи або їхні поки проекти:

– Закони України «Про боротьбу з тероризмом» (2003 р.), що передбачає й боротьбу з екстремізмом;

– Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» (2019 р.);

– Закон України «Про протидії торгівлі людьми» (2011 р.);

– проект закону «Про зброю» [96].

Крім того, діє Указ Президента країни № 53/2019 від 05.03.2019 року «Про Концепцію боротьби з тероризмом в Україні» [96].

Аналіз чинного законодавства України у сфері протидії гібридній війні дає дозволив стверджувати про актуальність його доповнення. На нашу думку, слід розробити та прийняти таке:

1) Закон України «Про гібридні війни в України»;

2) Концепцію щодо протидії гібридним війнам.

Крім того, необхідно вжити такі заходи: 1) удосконалити систему захисту об’єктів, що можуть становити інтерес для інформаційних загроз; 2) забезпечити систематичний моніторинг за станом безпеки цих об’єктів; 3) провести комплекс заходів, що спрямовані на формування правової та цифрової культури в усьому суспільстві з метою протистояння інформаційним загрозам.

Наразі продовжується вдосконалення нормативно-правової бази у сфері протидії гібридним війнам. Так, відповідно до внесених змін до чинного законодавства, що регламентує цю галузь, установлено кримінальне покарання за публічні заклики до скоєння та виправдання злочинів терористичного та екстремістського характеру. Проте управлінська практика протистояння інформаційним загрозам в Україні засвідчує, що недостатньо вжити правових й організаційних заходів у зазначеній сфері.

Україна у сфері боротьби з тероризмом, екстремізмом, радикалізмом та іншими загрозами й інформаційними викликами сучасності такими, як незаконний обіг наркотиків та зброї, транснаціональна організована злочинність та кіберзлочини, є тригером і проблемою для всіх держав світу, а також міжнародних та регіональних організацій. У сучасних складних та суперечливих умовах ми повинні налагодити зворотний зв’язок та співпрацювати, а не конкурувати.

До речі, боротьба зі злочинами у сфері інформаційних технологій означає протидію «кібервійнам», з яким ведуть боротьбу практично всі держави. Наприклад, у США створено «Кіберкомандування», яке наразі перетворено на самостійну структуру Збройних сил США щодо протидії загрозі з боку рф у кіберпросторі [56].

Сьогодні всі ми стаємо свідками стрімкого розвитку інформаційно-технологічних комунікацій. Світові та регіональні спільноти та держави-лідери, на жаль, бачать майбутнє за «кібервійнами», які стають важливою технологією гібридних та інформаційно-гібридних війн. При цьому понятійний апарат «кібервійн» практично щодня поповнюється новими

термінами такими, як «кіберзагрози», «кіберкомандування», «кіберзброя», «кібероперації», «кіберзавдання», «кіберпроблеми», «кіберсистеми», «кіберінфраструктури», «кібератаки», «кіберзломи», «кібербомби», «кібербезпека», «кібероблаштування» та ін. У США, КНР та інших розвинених у технологічному відношенні країнах протягом кількох років йде протистояння негативному впливу віртуального простору, Україні, безперечно, слід ураховувати цей закордонний досвід [56; 103; 136; 144-145; 220].

Кібербезпека є однією з найбільш стратегічних проблем державного значення. Актуальність протидії «кіберзлочинам» на цьому етапі обґрунтовується тим, що останніми роками інформаційні простори країн та їхнього інтересу активно почали використовувати різні злочинні групи, включаючи терористів та екстремістів, для отримання прибутку, пропаганди своїх ідей, найму нових бойовиків та інших протиправних акцій, спрямованих на ослаблення національної безпеки. Такі методи активно впроваджує рф по відношенню до України. Тому «кібервійни» становлять для неї «гібридну загрозу», як у цілому й для будь-якої держави.

Для ефективної боротьби з кіберзлочинами до Кримінального кодексу України [96; 136] постійно вносяться зміни та доповнення залежно від виявлення/появи нових видів злочинів із використанням інтернет-ресурсів. Так, відповідно до внесених змін установлено кримінальну відповідальність та покарання за публічне виправдання терористичної та екстремістської діяльності.

Слід підкреслити, що активне використання Інтернету в терористичних та екстремістських цілях почалося з дня появи ІГІЛ. До ІГІЛ злочинні організації обмежувалися програмними заявами та документами, які передавалися безпосередньо журналістам чи вивішувалися на не відомих Інтернет-сайтах [53; 54; 59; 62; 63; 68; 77; 99; 120; 130; 150; 159]. Це пов’язано з тим, що найчастіше світові новини дізнаються не з традиційних медіа, а з тих же Facebook та Twitter.

Україна приділяє відповідну увагу протидії «гібридним й інформаційним загрозам» із використанням біологічних, екологічних та інших природно-техногенних компонентів «гібридних війн», які отримали такі назви, як «біотероризм», «екотероризм» або «гібридний біотероризм», «гібридний екотероризм» тощо. Ці види «гібридних й інформаційних війн» становлять серйозну загрозу національній безпеці України, оскільки розраховані не на одиночні терористичні акції, а на масовий терор населення з використанням різних вірусів, заразних захворювань тварин, комах, радіоактивних, хімічних відходів та інших (сибірка, пташиний грип, свинячий грип, гепатит С, ВІЛ/СНІД тощо), окремі спалахи яких трапляються й досі. Із цією метою прийнято відповідні нормативно-правові документи, наприклад, рішення Ради національної безпеки і оборони України «Про біологічну безпеку» у 2009 році [111].

Україна приєдналася до Орхуської конвенції 1998 року, також підписала у цьому ж році Кіотський протокол з обмеження викидів промислових відходів у довкілля, що визначають міжнародні норми з охорони та використання навколишнього середовища. Крім того, наша держава підтримала декларацію «Цілі тисячоліття» та інші міжнародні документи, що регламентують цю сферу [96].

На наш погляд, подальша участь України в роботі ООН, ОБСЕ, СНД та ін. із питань протидії «гібридним й інформаційним війнам» буде перспективним у плані забезпечення національної безпеки та національних інтересів України.

Вищевикладене дозволяє зробити деякі проміжні висновки:

1. «Гібридні й інформаційні війни» у міжнародному масштабі та на національному рівні самостійних суб'єктів міжнародного права, включаючи Україну, не розроблені в рамках окремого нормативно-правового документа. Власне кажучи, зараз відсутній законодавчий вимір «гібридних й інформаційних війн», що виникають поза міжнародним правовим простором. Ситуація в Афганістані, Іраку, Сирії, Україні та інших «гарячих»

точках свідчить про те, що цей вид війни дає країнам-агресорам можливість вирішувати свої глобальні цілі, не вступаючи у великомасштабне зіткнення із використанням своїх армій (до певного часу). Сьогодні «гібридні й інформаційні війни» стали реальністю, яку важко заперечувати, на що вказують усі й експертна спільнота, й учені, й військові тактики та стратеги, й політики та ін.

2. Виявлено, що поки відсутня перспектива правого врегулювання «гібридних й інформаційних війн» та широкий консенсус серед держав, які ведуть ці війни. З огляду на це викликає сумнів те, що в найближчій перспективі вдасться заборонити «гібридні й інформаційні війни» на законодавчому рівні. Адже деякі світові та регіональні спільноти, що реалізується за допомогою «гібридних й інформаційних війн», зокрема, свої геополітичні та геоекономічні інтереси.

3. Відсутність правового регулювання сприяє безкарному веденню «гібридних й інформаційних війн», локальних бойових дій із залученням найманців, терористичних груп, організованої злочинності, партизанських загонів, застосуванням біологічних, екологічних, природних компонентів тощо, у поєднанні з фейковими маніпуляціями кіберпросторі. Усі зазначені сили та засоби не пов’язані з міжнародними конвенціями, законами, що забороняють ведення традиційної/глобальної війни, і вигідні для використання в гібридних й інформаційних війнах.

4. Основні міжнародні геополітичні силові центри, з одного боку, виступають за дотримання фундаментальних міжнародних норм, зокрема, Статуту ООН про заборону класичних війн. А з другого боку, прагнуть обійти ці заборони під час гібридних й інформаційних війн, реалізуючи свої геостратегічні інтереси. На наш погляд, перспективи вироблення компромісних рішень складно реалізовані, але можливі, адже дозволяють попередити традиційне військове зіткнення, що не регламентовано у правовому вимірі. Якогось широкого консенсусу серед держав, що ведуть «гібридні й інформаційні війни», з прийняття міжнародно-правових

обмежень даних дій у процесі дослідження не досягнуто. Тому мають рацію ті вчені, які відзначають, що шанси на встановлення міжнародної відповідальності за даний вид діяльності не надто великі, оскільки, з погляду сучасного міжнародного права, подібне втручання довести складно.

5. Незважаючи на те, що в Україні «гібридні й інформаційні війни» також не оформлені належним чином законодавчо. У той же час, наша держава має вирішити цю проблему, адже на Україну спрямовані всі види «гібридних й інформаційних загроз». У межах глобальних і регіональних організацій – ООН, ОБСЄ, СНД та ін., членом яких є наша країна, також відсутні нормативно-правові документи щодо протидії «гібридним й інформаційним війнам». Вони поки присутні у вигляді декларативних заяв та розглядаються у поєднанні з іншими загрозами, які мають гібридний й інформаційний характер.

На наш погляд, майбутнє за мирними та несиловими способами боротьби, а не за глобальними воєнними діями й агресією. Проте досі не вироблено єдиний понятійний апарат щодо визначення гібридних й інформаційних війн. З метою вирішення ситуації у цьому напрямі рекомендується:

1. На вітчизняних теренах прийняти додаткові заходи щодо подальшого вдосконалення національного законодавства щодо своєчасного виявлення «гібридних й інформаційних загроз», основних об’єктів впливу (політичні й економічні засади держави, населення) та протидії їм із урахуванням безперервного розвитку інформаційно-комунікаційних технологій, визнаних найважливішими технологіями чи інструментами «гібридних й інформаційних війн». Уніфікувати національний нормативно-правовий вимір із аналогічними документами міжнародних та регіональних організацій з безпеки, членами яких є Україна.

2. Введення заборони на «гібридні й інформаційні війни» у глобальному масштабі. Це складно реалізувати, але необхідною є розробка та прийняття, зокрема, такого документа в межах ООН. Це обумовлюється,

насамперед, тим, що в результаті «гібридних й інформаційних війн», які можуть трансформуватися у військові протистояння, знищується цивільне населення.

3. ООН, ОБСЕ, антитерористичний центр СНД та ін. необхідно розглядати в зоні своєї відповідальності існуючі загрози як гібридних, так й інформаційних загроз, а також відповідним чином на них реагувати із застосуванням ризик-орієнтованого підходу.

У цьому контексті стратегічний план і прогноз розвитку України має розумітися як документ антикризового управління, що містить систему науково обґрунтованих уявлень про стратегічні ризики соціально-економічного розвитку та про загрози системі безпеці. Серед принципів антикризового управління можна виділити принцип реалістичності та протистояння інформаційно-гібридній війні, зміст якого визначається наступним чином: при визначенні цілей та завдань розвитку України та забезпечення її національної безпеки учасники стратегічного планування й антикризового управління повинні виходити з можливості досягнення цілей та вирішення завдань у встановлені терміни з урахуванням ресурсних обмежень та ризиків [42; 90].

Визначення ризиків при досягненні цілей розвитку України та цільових показників на довгостроковий період, з урахуванням завдань забезпечення національної безпеки, має бути встановлено як вимогу, що підлягає виконанню кожні 5 років в межах реалізації Стратегії сталого розвитку України [90; 103]. Стратегічний прогноз, що розробляється на 10 і більше років Урядом України, так само має включати оцінку інформаційних ризиків і загроз безпеці, а також розробку оптимального сценарію подолання таких ризиків і загроз із врахуванням національних інтересів. Серед основних завдань моніторингу реалізації документів стратегічного планування й антикризового управління має бути заявлено «проведення аналізу, виявлення можливих інформаційних загроз та своєчасне вжиття заходів щодо їх запобігання» [90; 103].

Крім того, допрацьований проект закону має передбачати необхідність управління ризиками, зокрема, «Систему управління ризиками». Зрозуміло, що наразі в цьому напрямі дуже розвинулось митне регулювання в Україні. Проте важливо, щоб її система публічного управління мала системний характер у межах всіх інституційних механізмів державного впливу у сфері інформаційної безпеки [90; 103].

У рамках обраної проблематики також привертають увагу міжнародні стандарти ISO 73:2009 «Менеджмент ризику. Терміни та визначення», про які вказано було вище в роботі під час дослідження досвіду Франції щодо впровадження ризик-орієнтованого підходу. У цьому стандарті визначено поняття ризику як наслідків впливу невизначеності на досягнення поставленої мети. Під наслідком впливу невизначеності необхідно розуміти відхилення від очікуваного результату чи події (позитивне та/або негативне). Цілі можуть бути різними за змістом і призначенням (стратегічні, загально-організаційні, що належать до розробки проекту правового документу, конкретної продукції та процесу) [16]. Ризик часто характеризують шляхом опису можливої події та його наслідків або їх поєднання [42].

Як відомо, менеджмент ризику допомагає у прийнятті рішень в умовах невизначеності та можливості виникнення подій чи обставин (планових та непередбачених), що впливають на досягнення цілей організації [11; 95]. Менеджмент ризику включає застосування логічних та системних методів для: обміну інформацією та консультацій у сфері ризику; встановлення сфери застосування при ідентифікації, аналізі, оцінці та обробці ризику, що відповідає будь-якій діяльності, процесу, функції чи продукції; моніторингу та аналізу ризику; реєстрації отриманих результатів та складання звітності [90; 95].

Менеджмент ризику у сфері публічного управління передбачає проведення оцінювання рівня та масштабів впливу тих чи інших ризиків. Основною метою оцінки ризику є подання на основі об'єктивних свідчень інформації, необхідної для ухвалення обґрунтованого рішення щодо способів

обробки ризику [42; 44; 90]. Оцінка ризику забезпечує таке: 1) розуміння потенційних небезпек та впливу їх наслідків для досягнення встановлених цілей організації; 2) отримання інформації, яка потрібна на прийняття рішень; 3) розуміння небезпеки та її джерел; 4) ідентифікацію ключових факторів, що формують ризик, уразливих місць організації та її систем; 5) можливість порівняння ризику з ризиком альтернативних організацій, технологій, методів та процесів; 6) обмін інформацією про ризик та невизначеності; 7) інформацію, необхідну ранжування ризику; 8) запобігання нових інцидентів на основі дослідження наслідків інцидентів; 9) вибір методів обробки ризику; 10) відповідність правовим та обов'язковим вимогам; 11) отримання інформації, необхідної для обґрунтованого рішення про прийняття ризику відповідно до встановленими критеріями; 12) оцінку ризику усім стадіях життєвого циклу продукції [16; 95].

Представляє значний інтерес для аналізу управління ризиками Наказ Антимонопольного комітету України «Про затвердження Методичних рекомендацій щодо оцінки впливу нормативно-правових актів та проектів актів на конкуренцію» (2017 р.). [112] Аналізований документ фактично окреслює напрямки застосування методичних підходів до оцінки регулюючого впливу. Разом із тим, далі сфери конкуренції, або оцінювання підзаконних актів за гендерно-правовими ознаками вітчизняний законодавець не пішов [16; 81].

Отже, уважаємо, що необхідно оновити вітчизняне законодавство, окресливши перспективи застосування ризик-орієнтовано підходу до інституційних механізмів публічного управління в умовах загроз інформаційного характеру та гібридних війн. При цьому слід звернути увагу на важливість проведення оцінки ризиків несприятливих наслідків застосування запропонованого правового регулювання. Така оцінка повинна містити перелік ризиків вирішення виявленої проблеми одним із таких способів правового регулювання, спрямованих на визначення та нейтралізацію інформаційних загроз гібридних війн:

1) ризики відсутності належного контролю дотримання вимог, що вводяться;

2) ризики відсутності необхідних ресурсів та кадрів;

3) ризики невідповідності запропонованого способу правового регулювання рівню поширення необхідних технологій;

4) ризики зниження рівня безпеки та ін. [42; 90; 95].

Отже, природа всіх вищевказаних ризиків складна, і зумовлена виникненням і поширенням інформації. Відтак, важливим є дієве та повсюдне застосування ризик-орієнтованого публічного управління потоками цієї інформації, що вимагає оновлення вітчизняного законодавства, зокрема, прийняття Закону України «Про гібридні війни в України», Концепції щодо протидії гібридним війнам тощо [90; 103].

3.2. Шляхи вдосконалення інституційної системи публічного управління України в умовах інформаційно-гібридних війн

На Україну чинять значний вплив інформаційні загрози (традиційні та нетрадиційні), а також проти неї ведеться інформаційно-гібридна війна. До традиційних загроз належать існуючі століттями військові загрози з використанням армій. Із розвитком людства й технологій ці загрози продовжують розвиватися й удосконалюватися, розрізняючись лише у формах та методах застосування зброї. Наразі вони набули глобального та більш загрозливого характеру через появою ядерної, хімічної та інших видів зброї масового знищення, наявних у розпорядження тих чи інших держав. До нетрадиційних загроз належать міжнародний тероризм, релігійний екстремізм, незаконний обіг наркотиків, торгівля людьми, контрабанда зброї, піратство, екологічні злочини та інші злочини транснаціонального характеру.

На наш погляд, сьогодні нетрадиційні загрози переважають над

традиційними. Це пояснюється двома причинами, а саме: забороною на їх ведення та надмірними витратами на них. Властивістю багатовимірності повною мірою володіють гібридні конфлікти некласичного характеру з участю у бойових діях збройних формувань недержавних суб'єктів, серед яких міжнародний тероризм, для якого характерна розмита національна та ідеологічна приналежність. Протистояння армій є надзвичайно затратним і зумовлює непоправні втратами як людського, і матеріального характеру. Їм на зміну приходять війни нового типу – гібридного. Можна з упевненістю констатувати, що процеси глобалізації підвищили ефективність нетрадиційних загроз системі безпеці.

Сьогодні проти України використовуються різні технології й інструменти інформаційно-гібридних війн. На наш погляд, найважливішими з них слід визнати «інформаційні війни», «терористичні війни», «кібервійни», «когнітивні війни», «мігрантські війни», «прикордонні війни», «біологічні війни» та інші [103]. Усі зазначені технології залежать від форми протистояння між державами.

Основу інформаційно-гібридних війн проти України складає дезінформація. Цей тип війни є дезінформаційним, а не інформаційним. Іноді її називають також «фейковою війною», що передбачає використання фальшивих новин, які не всі здатні відрізнити від правди. У цифрову добу такі новини іноді називаються «скидами», «качками» тощо, що мають єдину мету: вплинути на ситуацію у світі, не вдаючись до кровопролиття та протистояння армій світу [120; 198].

Слово «дезінформація» увійшло в науковий обіг завдяки спецслужбам. Як відомо, вони умовно характеризують дезінформацію як наркотичну речовину. Якщо вдихати її один чи два рази, то вона, можливо, і не змінить суспільного життя, але якщо ж вживати таку речовину щодня, то вона перетворить людину на повністю залежну.

Технології інформаційно-гібридних війн, засновані на маніпулятивному управлінні суспільно-політичною свідомістю і поведінкою

громадян, є виключно небезпечними: їхнє головне завдання – розділити і поляризувати суспільство, сегментизувати його, змусивши фрагменти ненавидіти один одного, органи державної влади, для того, щоб потім зіштовхнути населення між собою, або, щоб вони ініціювали боротьбу зі знищення існуючої влади [103]. Власне кажучи, метою технологій інформаційно-гібридних війн є об'єднати агресію людей в єдиний потік і направити його проти чинної державної влади.

Глобальні соціальні платформи (Facebook, Twitter, YouTube тощо) є світовими монополістами у своїх форматах подання інформації чи дезінформації. Формати функціонування зазначених мереж не тільки передбачають контроль за інформацією, що проходить через них, володіючи можливістю і правом «банити» будь-які акаунти, але також вбудовування у трафік будь-яких інформаційних матеріалів без попередження про це користувачів [53; 54; 59; 62].

Інформаційно-гібридна війна проти населення України, що триває, переслідує лише одну мету: погіршити місце нашої держави на міжнародній арені, зганьбивши українську націю і, зрештою, поширивши серед неї песимізм щодо свого майбутнього і недовіру до системи державного управління.

Проти України також ведеться «когнітивна війна» (від слова cognitio – сприйняття, пізнання) як один із компонентів інформаційно-гібридних війн. «Когнітивна війна» передбачає вплив на свідомість людей та контроль над нею. Свідомість населення можна контролювати не тільки через засоби масової інформації, а також в Інтернет-просторі, шляхом поширення вигідної інформації/дезінформації [59; 62; 63].

На територію України поширює дію низка міжнародних неурядових організацій. Окремі з них мають на меті вплив на свідомість переважно молоді, формуючи в її частини відчуттів недовіри до чинної державної влади, що зумовлює зниження рівня інтелектуальної безпеки країни. Інформаційно-гібридна війна проти України ведеться з 90-х рр. минулого

століття, тобто з моменту набуття республікою незалежності. Цю війну можна розділити на два етапи: 1) мирний період, що відзначається латентним впливом інформаційних загроз на систему безпеки нашої держави (часові межі цього етапу припадають на 1991 р. – 2011 р.); 2) військовий період (2014 р. – по теперішній час). Другий період характеризується активністю терористичних та інших груп, які використовують протиборчі сили для реалізації певних суспільно-політичних цілей [92; 103].

Розглядаючи особливості «терористичних та інформаційно-гібридних війн», слід зважати на те, що вони є причинами багатьох проблем практично всіх держав, оскільки супроводжуються збройними конфліктами, масовою міграцією, руйнуванням життєво важливих інфраструктур, поширенням наркоманії, небезпечних захворювань та інших негативних явищ.

У цьому плані науково доведено, що основна загроза походить від тих партій та рухів, які дотримуються вкрай радикальних ідеологій тероризму та екстремізму. При цьому ідеологи тероризму й екстремізму вміло використовують усі недоліки суспільного життя, поширюючи серед своїх прихильників думки про необхідність виправлення ситуації в кращий бік.

Якщо провести хронологічний аналіз виявів інформаційно-гібридних загроз проти України (починаючи з 90-х років XX ст. і по теперішній час), то можна дійти висновку, що характер та методи терористичних дій та інформаційних вкидів зазнали поступальних змін (і в джерелі походження, і в масштабах) [67; 77]. Їх основу, як і раніше, становлять фізичне усунення неугодних осіб та інфраструктурних об’єктів. Особливе занепокоєння викликає тенденції збільшення терористичних актів або спроб вчинення аналогічних діянь в останні роки, про що свідчать статистичні дані силового блоку. Беручи до уваги цю обставину, можна припустити, що тенденція зростання інформаційно-гібридних терористичних та екстремістських загроз зберігає присутність терористичних війн. На сьогодні вони викликають стурбованість у багатьох країнах світу, включаючи й Україну, через

проблему участі їхніх громадян у складі міжнародних терористичних угруповань у збройних конфліктах гарячих «місць» – Афганістану, Сирії, Іраку та інших. Ця тенденція зберігається й сьогодні, активно проявляючись у «терористичних війнах» [103; 202].

На наш погляд, певну тривогу викликає питання щодо виявлення та відстеження коштів, спрямованих на фінансування тероризму, що загрожує інформаційній безпеці країни. Це пояснюється тим, що поки що не вдається повністю перекрити канали фінансування тероризму й екстремізму. Досі не уточнено фінансових цілей і завдань суб'єктів терористичної діяльності, витрати на популяризацію ідеології тероризму (екстремізму), зміст легальних структур, що становлять інтереси терористичних організацій (благодійні фонди, релігійні організації, інформаційні агенції тощо).

Тероризм супроводжується інформаційними загрозами, виступаючи однією з технологій інформаційно-гібридних війн, тому паралельно з ними мають розглядатися «терористичні війни», як складова. Ще однією складовою інформаційно-гібридних війн є кібервійни. Адже на сучасному етапі активна боротьба між світовими та регіональними спільнотами розгорнулася у кіберпросторі [53; 54; 59; 62; 63; 67; 77; 79]. Сьогодні наявність високотехнологічного потенціалу в передових країнах дає їм можливість із використанням даного простору проводити підривні акції, що міцно утвердилися як «кібервійни». Такі війни, на жаль, набули значного поширення проти України. Як відомо, протягом останніх років російським хакерським атакам були піддані сайти вітчизняних урядових відомств (Міністерства освіти і науки України, Посольства України у Франції, Митної служби України та ін.) [154].

За даними американської дослідницької інтернет-компанії Рапід та інших дослідницьких установ, що займаються питаннями безпеки інтернету та комп’ютерних систем, у 2023 році Україна посіла перше місце у світі в списку країн, чиї комп’ютери найбільше схильні до хакерських атак (зокрема, 29 таких атак). Наприклад, ті ж США пережили 14 кібератак,

більшість з яких були на замовлення Ірану та КНР [79; 148]. Для цього використовуються різні шкідливі програми, віруси такі, як «Троянський кінь», «Петя» тощо.

Бурхливий розвиток інформаційно-комунікаційних технологій, особливо віртуальний інтернет-простір, що активно використовуються всіма кримінальними структурами та злочинними угрупованнями у своїх цілях. Україна випробувала на собі дії «кібертерористів» ІГІЛ, які через інтернет-ресурси за короткий проміжок часу здійснили вербування у свої ряди декілька десятків представників несвідомої частини української молоді. Сьогодні створений ІГІЛ («кіберхаліфат») становить загрозу не тільки для України, а й усьому світу. У 2016 році це хакерське угруповання та ще десятки інших об'єдналися під загальною назвою «Об’єднаний кіберхаліфат» (United Cyber Caliphate, або UCC), до яких зараховують усіх кіберзлочинців, які діють від імені терористів ІГІЛ [85; 187].

Крім того, проти України ведуться «мігрантські війни». Починаючи з 80-х років минулого століття, наша держава відчувала наплив афганських біженців-мігрантів через ускладнення обстановки в північних прикордонних провінціях Афганістану, які продовжується й досі. Сьогодні варто також говорити про імігрантські війни, що пов’язують зі збільшенням міграційних процесів за кордон України, у тому числі міграції її громадян до Республіки Польща, Німеччини та ін. Основою цього є проблема нелегальної міграції, з якою ведеться боротьба на міжнародному рівні. Тому будь-які негативні моменти (депортація громадян, урегулювання порядку перебування мігрантів та інші питання), що викликають невдоволення в іноземних країнах, подаються як «мігрантські війни».

Складності ситуації додає повномасштабна агресія проти України. Україною вже докладаються зусилля для позитивного вирішення питань нелегальної міграції, але війна триває. Відтак, державна міграційна політика є пріоритетним завданням для нашої країни, оскільки до значного відтоку трудових мігрантів-українців додалися вимушені переселенці з зон ведення

активних бойових дій і окупованих територій. Крім того, зважаючи на все, процеси трудової міграції в найближчому майбутньому будуть значно посилені. Це має під собою об'єктивне та суб'єктивне підґрунтя, оскільки досі не врегульовані прикордонні питання між Україною та Республікою Польща, що періодично зумовлюють необґрунтовані затримки під час перетину кордону.

Таким чином, можна констатувати, що Україна схильна до інформаційно-гібридних загроз, які будуть з'являтися і в подальшому. Вищевикладене дозволяє зробити такі проміжні висновки:

1. Тенденції та динаміка злочинів проти інформаційної безпеки України наочно свідчать про зростання нетрадиційних загроз такій безпеці, насамперед, це стосується діяльності релігійно-екстремістських організацій.

2. Усе більше здійснюється злочинів, пов'язаних із сучасними інформаційними технологіями.

3. Рф, ісламські республіки, Китай та ін. залишаються в найближчій перспективі сприятливим плацдармом для ведення інформаційно-гібридних війн, у т.ч. проти України. Це обґрунтовується тим, що геополітичні інтереси світових та регіональних спільнот надзвичайно переплетені, що розв'язати їх у найближчому майбутньому складно. У цьому контексті ще більше активізуються інформаційні атаки проти України у рамках інформаційної війни як складової «гібридної війни». У 2023 році Україна очолила рейтинг держав, по відношенню до яких було зреалізовано хакерські атаки [154].

4. При веденні та реалізації інформаційно-гібридних війн проти України активно буде використаний протестний потенціал українських громадян, які входять до різних міжнародних терористичних та екстремістські організації, що підтримуються країною-агресором.

За цим підрозділом пропонуються такі рекомендації:

1. В обстановці, що складається, жодна держава самостійно не здатна ефективно протистояти різним технологіям інформаційно-гібридних війн,

зокрема, й Україна. З огляду на це їй необхідно координувати зусилля щодо протидії інформаційно-гібридним війнам. У цьому плані зростає роль міжнародних і регіональних організацій, механізми функціонування яких передбачають захисні заходи щодо протидії інформаційно-гібридним війнам.

2. Сили міжнародного тероризму та релігійного екстремізму, незаконного обігу наркотиків, зброї та інші транскордонні злочинні угруповання, задіяні в інформаційно-гібридних війнах, реалізують свої злочинні наміри та цілі, використовуючи новітні інформаційно-комунікаційні технології, мережу інтернет, соціальні мережі тощо. Ці обставини змушують постійно вдосконалювати нормативно-правову базу щодо протидії всім використовуваним технологіям інформаційно-гібридних війн.

3. Окремого підходу потребує діяльність із протидії інформаційним війнам проти України. У цьому контексті видається доцільним створення самостійної структури по відстеженню/моніторингу інформаційного та ідеологічного простору. На наше переконання, необхідно опрацювати питання про адміністративне чи кримінальне покарання за поширення фейкової інформації.

4. У плані протидії незаконному фінансуванню тероризму пропонується надалі акцентувати увагу на виявленні таких моментів:

– каналів можливого впровадження терористів у державні структури з метою підкупу та вербування нових членів;

– залучення коштів/пожертв від третіх осіб;

– інтегрування коштів у фінансову систему держави, шляхом внесення на розрахункові рахунки організацій-посередників, залучених до фінансування злочинної діяльності;

– переказу коштів в інші організації-посередники, розташовані на місцях здійснення терористичної діяльності та ін.

Незважаючи на те, що поняття інформаційно-гібридні війни у

міжнародному масштабі поки що не знайшло належного закріплення, загрози такої війни проти будь-якої держави існують. Питання про протидію інформаційно-гібридним війнам також мало досліджено в наукових та експертних колах. Як результат, поряд з різними визначеннями інформаційно-гібридних війн, деякими вченими, військовими фахівцями та експертами надані роз'яснення щодо заходів протидії цим війнам [103].

Проблема протидії інформаційно-гібридним війнам через свою складність та актуальність передбачає розробку цілої низки ефективних заходів, без яких неможливо буде досягти прогресу з цього питання. Питання протидії інформаційно-гібридним війнам як новій формі міждержавного протистояння повинні бути виділені як один із пріоритетних напрямів наукових досліджень [64; 66; 82; 100; 108; 133; 170].

З цієї причини слід зазначити, що сукупність нормативно-правового впливу на суспільні відносини, що складаються в галузі протидії інформаційно-гібридним війнам, включає:

1) підсистему правових норм, що регулюють відносини в галузі протидії інформаційно-гібридним війнам;

2) підсистему організаційно-правових заходів, спрямованих на запобігання, виявлення, ліквідацію чи локалізацію загроз, пов'язаних з інформаційно-гібридними війнами [40; 87; 118].

Наше бачення цієї проблеми полягає в тому, що кожній країні необхідно, насамперед, визначити види використовуваних технологій/інструментів «інформаційно-гібридних війн», їх загроз, умов реалізації (внутрішні та зовнішні) у геополітичному просторі, у кожній країні-об'єкті таких війн, а потім вжити заходів щодо протидії їм.

На даний час відомі заходи протидії традиційним класичним війнам, чого не скажеш про «інформаційно-гібридні війни». Різновид технологій таких війн вимагає адекватної протидії кожній з них (наприклад, щодо недостовірної інформації як інструменту інформаційної війни, кібератак у межах кібервійни та ін.) [79].

Питання протидії інформаційно-гібридним війнам перебувають у центрі уваги США, ЄС, рф, Китаю та інших країн. У зазначеному напрямку рівень протидії інформаційно-гібридним війнам у цих країнах не однаковий через ступінь їхнього розвитку у технологічному плані. Зважаючи на це, доцільно розкрити стан вирішення цього питання у вказаних країнах.

Світові та регіональні спільноти керуються своїми геополітичними інтересами у геополітичному просторі, що включає географічний, економічний, ідеологічний, інформаційний простір. Тому необхідна розробка нових міжнародно-правових документів для протидії способам ведення інформаційно-гібридних війн у кожному конкретному типі геополітичного простору [47; 133].

Слід зазначити, що в ході міждержавних протистоянь у різних сферах, практично щодня з’являються нові військові та невійськові технології інформаційно-гібридних війн, утворюючи своєрідний гібрид. За цих обставин протидія інформаційно-гібридним війнам вимагає використання всіх військових та невійськових технологій із боку державних органів влади будь-якої країни-мішені інформаційно-гібридних війн. Так, виявлення всіх невійськових технологій інформаційно-гібридних війн, їх сутності, напрямів із подальшою їхньою ліквідацією є завданням спеціальних служб та правоохоронних органів. Їхня роль важлива у зв'язку з тим, що інформаційно-гібридні війни пов’язані безпосередньо із розвідувально-підривною діяльністю спецслужб країни-агресора, яка використовує власну агентуру, різні неурядові та некомерційні організації (далі – НУО та НКО) та інші можливості, завдаючи шкоди національній безпеки країни-об’єкта інформаційно-гібридних війн [94].

Саме розвідка надає вихідний матеріал для прогнозування інформаційно-гібридних загроз та планування заходів протидії ним. Стратегічний прогноз інформаційно-гібридних загроз дозволяє передбачати рішення противника щодо вибору стратегії реагування на такі загрози. Розробка заходів щодо протидії ним повинна здійснюватися з урахуванням

важливої ролі внутрішніх і зовнішніх факторів в інформаційно-гібридних війнах. Загальні способи протидії інформаційно-гібридним загрозам зводяться до надійного перекриття каналів фінансування підривних сил, використання дипломатичних засобів для ізоляції та покарання держав-спонсорів, націлювання всіх видів розвідки на ідентифікацію лідерів, розташування таборів підготовки та складів як першочергових об'єктів нейтралізації [93]. Діяльність розвідки має враховувати побудову за мережевим принципом сил і засобів противника, усієї системи управління. Першочергова увага має приділятися вдосконаленню територіальної оборони з урахуванням даних розвідки та контррозвідки щодо планів дій противника.

Акцентуючи увагу на важливій ролі розвідки в протидії інформаційно-гібридним війнам, слід зауважити, що в США функціонує Національна рада розвідки (National Intelligence Council, NIC) [194]. Починаючи з 1997 року, Національна рада розвідки США готує звіт під назвою «Глобальні тенденції» кожні 4 роки, для Президента Сполучених Штатів і політиків. Робота цієї ради ґрунтується на розвідувальних даних із різноманітних джерел, зокрема експертів із наукових кіл та приватного сектору [там само]. На наш погляд, в Україні також слід створити аналог такої Національної ради з розвідки. Крім того, слід ураховувати ту особливість, що в США функціонує потужний аналітичний центр з урахуванням бібліотеки конгресу, аналітичні структури, як RAND Corporation [203] тощо. Ця пропозиція заслуговує на увагу. Уважаємо, що на вітчизняних теренах також необхідно створити таку Національну раду з розвідки при Президентові України.

Крім того, можна рекомендувати створення власних інформаційних пропагандистських структур, орієнтованих на конкретну аудиторію населення, створення наукових організацій, які розроблятимуть технології протидії ворожій пропаганді у вітчизняному суспільстві з використанням сучасних інформаційних технологій. Одним із заходів протидії таким

загрозам може виступити зміцнення економіки, підвищення рівня життя в Україні, а також усунення явних проблем у державі, які могли б спричинити невдоволення її громадян.

Системна та цілеспрямована нейтралізація операцій інформаційно-гібридної війни, що проводяться проти України, вимагає, у тому числі створення нової організаційної структури, наприклад, Бюро контргібридної війни. Поки що Україна, як завжди, «довго запрягає», хоча зовнішня агресія проти неї триває з 2014 року, і в 2022 році вона набула ознак повномасштабності. До речі, подібна структура функціонує в США – це Бюро протидії гібридній війні (Hybrid warfare resistance Bureau, HWRB) [184]. Воно створене у грудні 2015 р. та має офіційний статус суспільної організації [там само]. Цікаво, що власного сайту в Інтернеті дана організація не має, розміщуючи свою інформацію виключно у соціальних мережах. У будь-якому випадку, Україна не повинна обмежуватися лише визначенням інформаційних загроз, що виникають у гібридній війні з боку рф. Одні лише оборонні дії та реагування на кроки противника не дадуть бажаного результату; доцільним є реалізація комплексу заходів щодо прогнозування, протидії на випередження тощо.

Україна ще у 2014 році мала прийняти закони про протидію інформаційно-гібридним війнам. Однак це питання залишається не вирішеним й досі. Держава, що страждає від гібридних й інформаційних атак, має докладати комплексу зусиль з метою відновлення власної системи безпеки у піднапрямах політика, економіка та суспільство. У цьому контексті доцільним є створення організацій, діяльність яких сприятиме проведення контргібридних дій, а також упровадження в державну систему та структуру Збройних сил спеціальних підрозділів, призначених для проведення відповідних та превентивних інформаційних та психологічних операцій [103].

США та їх західні союзники стали приділяти особливу увагу питанням протидії інформаційно-гібридним війнам та їхнім загрозам,

здійснюючи заходи щодо протидії ним. Важливе місце також відведено проведенню навчання для відпрацювання дій у інформаційно-гібридній війні. У Латвії, зокрема, з метою підготовки та координації таких навчань створено спеціальний центр – Центр передового досвіду стратегічних комунікацій (Strategic Communications Centre of Excellence, StratCom) [214].

Водночас деякі політики вважають, що на сьогодні ЄС та її військова безпекова структура – НАТО точно знає, як протистояти конвенційними (традиційними) загрозами, але ця організація немає необхідних інструментів боротьби з невоєнними прийомами .

Надалі Парламентська Асамблея Ради Європи (ПАРЄ) також ухвалила відповідну резолюцію, в якій зазначається: «Сьогодні держави все частіше стикаються із явищем «гібридної війни», яка представляє собою новий тип загрози, і заснована на поєднанні військових та невійськових засобів таких, як кібератаки, кампанії з дезінформації, які поширюються, зокрема, через соціальні мережі, що можуть вразити стратегічну інфраструктуру країни таку, як система управління повітряним рухом чи атомні станції» [86; 101].

ЄС у плані протидії гібридним й інформаційним війнам, можливих зі сторони рф, у вересні 2017 року у столиці Фінляндії місті Гельсінкі відкрив Центр боротьби з гібридними загрозами. За свідченням його експертів рф є однією з головних країн, за якою вестиметься спостереження (що зумовлено, зокрема, виступом президента рф на Безпековій конференції у Мюнхені) [102]. На даний час у діяльності центру бере участь 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, Німеччина, Великобританія, Іспанія, Польща, Естонія, Латвія та Литва. Як раніше заявили представники центру, його метою не є пряме протистояння атак, а дослідницька, прогнозна, інформаційно-аналітична робота. Центр також організовуватиме спільні дослідження та проекти щодо покращення способів обміну інформацією [174]. Україні слід напрацьовувати дієву практику взаємодії з Європейським центром з протидії гібридним загрозам.

Слід зазначити, що у військових та офіційних документах КНР поняття «інформаційно-гібридна війна» розглядається крізь призму «нових обставин». КНР за прикладом своїх основних опонентів – США та рф – також веде інформаційно-гібридні війни. Наразі розв'язана безкомпромісна «торговельна війна» між КНР та США. Спостерігається використання різних технологій інформаційно-гібридних війн з боку Китаю. Так, в останні роки для повернення своїх раніше втрачених територій по периметру Азіатсько-Тихоокеанського регіону, КНР активно використовує риболовлю на даному просторі. На цій підставі в складі військово-морських сил Китаю створено озброєну рибальську армаду або «морські воєнізовані формування Народно-визвольної армії Китаю», які перетворилися на різновид китайських нерегулярних військових формувань [22]. Американська сторона називає їх «морським ополченням» чи «морською міліцією». Воно забезпечує відмінне маскування для Пекіна. Якщо припустити, що «рибалок» спіймали та заарештували, скажімо, японці, за те, що вони займають спірні об'єкти в Східно-Китайському морі, немає жодних доказів, що вони є частиною Китайської армії та беруть участь в операціях з розширення зони впливу Китаю.

Останніми роками КНР поступово перетворюється на епіцентр інформаційно-гібридної війни, ґрунтуючись на терористичній активності, що зберігається в СУАР [132]. Інформаційно-гібридна війна в СУАР – це приклад боротьби проти енергетичної незалежності Китаю, оскільки саме в цьому районі діють найбільші його нафтопереробні заводи. Так, нафтопереробний завод у м. Душаньзці переробляє близько 16 млн. тонн нафти (переважно з Казахстану). Річна потужність НПЗ у Карамаї – 10 млн. тонн, у м. Урумчі – 1 млн. тонн, м. Куче – 5,7 млн. тонн.

Останніми роками КНР активно реалізує «кібервійни». У цьому контексті особливу небезпеку стали представляти китайські хакери, які бзпосередньо співпрацюють із державною розвідкою КНР. Вони шпигують за військовими з інших держав і крадуть їх стратегічні розробки, а також

стежать за великими бізнес-компаніями та захоплюють інтернет-мережі. Їх уже спіймали за крадіжкою американських розробок у сфері озброєння та при зломах системи космічних супутників. Міністерство державної безпеки КНР керує величезною армією китайських хакерів, яка організовано атакує цілі за кордоном [79; 211; 221].

Сьогодні опір України інформаційно-гібридним війнам здійснюється силовими та несиловими методами. Силові методи застосовуються в основному з метою ліквідації терористичних угруповань, що проникають ззовні [79]. При цьому основний наголос має бути зроблено на протидію України інформаційним технологіям, на забезпеченні кібербезпеки, а також ведення безперервної розвідки та її безпосередньої взаємодії зі структурами політичного та військового управління з метою оперативного створення та використання переваг в загрозливому середовищі інформаційної безпеки.

Протидія інформаційно-гібридним війнам та її різним компонентам з боку України також здійснюється в межах гібридних загроз. Аналіз наукових напрацювань показує, що на сучасному етапі основним інструментом під час протистояння таким загрозам є соціальні мережі, що пов’язано з інформатизованістю суспільства, через захоплення цифровими технологіями.

Соціальні мережі сьогодні є одним із ключових та найбільш ефективних інструментів інформаційного впливу, у т. ч. засобом для маніпулювання особистістю, соціальними групами та суспільством загалом. Не дивно, що вони все частіше використовуються як майданчики для ведення інформаційно-гібридних війн. У сучасному світі через соціальні мережі регулярно поширюється інформація, яка часто не відповідає дійсності та наносить шкоду інтересам особистості, суспільства та держави.

З метою протидії інформаційно-гібридним війнам в Україні визначено кримінальну відповідальність за вчинення злочинів у цифровому світі. Виходячи з інтересів національної безпеки України, періодично здійснюється блокування відомих шкідливих сайтів ворожих сил, що ззовні

здійснюються контрпропагандистські заходи та дезінформаційні атаки проти України [202].

Разом з тим, у наукових та експертних колах існують суперечливі думки щодо шляхів реагування на провокації в мережі інтернет, до чого вдається значна частина країн. Спроби встановлення в сучасних умовах адміністративного контролю за поширенням інформації в соціальних мережах шляхом блокування переданих повідомлень, відключення від мережі Інтернет і тому подібні методи видаються дієвими, але не єдиними. Оскільки дана тактика не може бути довгостроковою і зумовить з часом соціальну напругу. Прикладом упровадження такої практики є досвід блокування деяких соцмереж у рф [53; 54; 62; 63; 67; 77].

Блокування в Інтернеті дедалі більше доводить свою неефективність. Рано чи пізно від блокувань потрібно буде відмовитись, оскільки все більше користувачів обходять блокування, навіть не помічаючи їх. Уважаємо, що зусилля управлінців, працівників правоохоронних органів мають бути сконцентровані на результативному моніторингу Інтернет-активності, а не на безуспішному протистоянні Telegram-каналам. За умов виваженої й науково обґрунтованої «проактивної» державної інформаційної політики можна зберегти життя та здоров’я громадян, які постраждали внаслідок повномасштабної агресії з боку рф [там само]. Ця обставина вимагає додаткового вивчення та дослідження нових способів протидії інформаційним атакам з боку країни-агресора, зокрема, тих, що застосовуються в межах «реактивної» державної інформаційної політики. Слід підкреслити, що «проактивна» державної політики передбачає застосування принципів стратегічного планування та реалізацію довгострокових проектів, наприклад, стратегії сталого розвитку, стратегії національної безпеки тощо. «Реактивна» же державна політика спрямована на оперативне реагування на наявні загрози, тобто «тут і зараз». Однак за цього підходу складно говорити про далекоглядність державної політики, а лише про її антикризовість [118]. У той же час, можливі різні сценарії

розвитку подій, за яких можуть видатися більш дієвими або заходи «проактивної» державної політики, або заходи «реактивної» державної політики. Наразі для України актуальними є останні заходи, але вони не унеможливлюють паралельного застосування стратегічного та системного підходів, що передбачають реалізацію «проактивної» державної політики. Власне кажучи, на сучасному етапі функціонування України обґрунтовуємо необхідність створення підґрунтя для її стратегічного розвитку, що має відбувається за умов трансформації наявних неочікуваних інформаційних загроз у стан контрольованих. Уважаємо, що для цього слід розробити та прийняти низку правових документів, а саме: Стратегію сталого розвитку України, концепцію протистояння інформаційним загрозам й інформаційно-гібридним війнам.

На наш погляд, організація розумного моніторингу Інтернет-активності та посилення контрпропаганди як способів протидії інформаційно-гібридним війнам є актуальним і своєчасним напрямком реалізації інформаційної політики України. На наше переконання, у цьому контексті слід забезпечити розвиток її інституційної системи публічного управління шляхом такого (рис. 3.1):

1. Створення власної інформаційної контргібридної пропагандистської структури, орієнтованої на конкретну аудиторію українського населення, яке не може протистояти інформаційним загрозам, у т.ч. з боку рф. Ця вітчизняна структура має розробляти технології протидії ворожій пропаганді на українське суспільство з використанням сучасних інформаційних технологій. На нашу думку, створення аналогічних контргібридних структур для України є перспективним і важливим вектором її інституційного розвитку в найближчому майбутньому. Аналогом такої інформаційної контргібридної пропагандистської структури для України визнається Бюро протидії гібридній війні, що функціонує в США.

2. Налагодження дієвої взаємодії України з іншими міжнародними та

регіональними організаціями, а саме: Європейським центром з протидії гібридним загрозам, Парламентською Асамблею Ради Європи, Центром передового досвіду стратегічних комунікацій (StratCom) та ін. [214; 225].

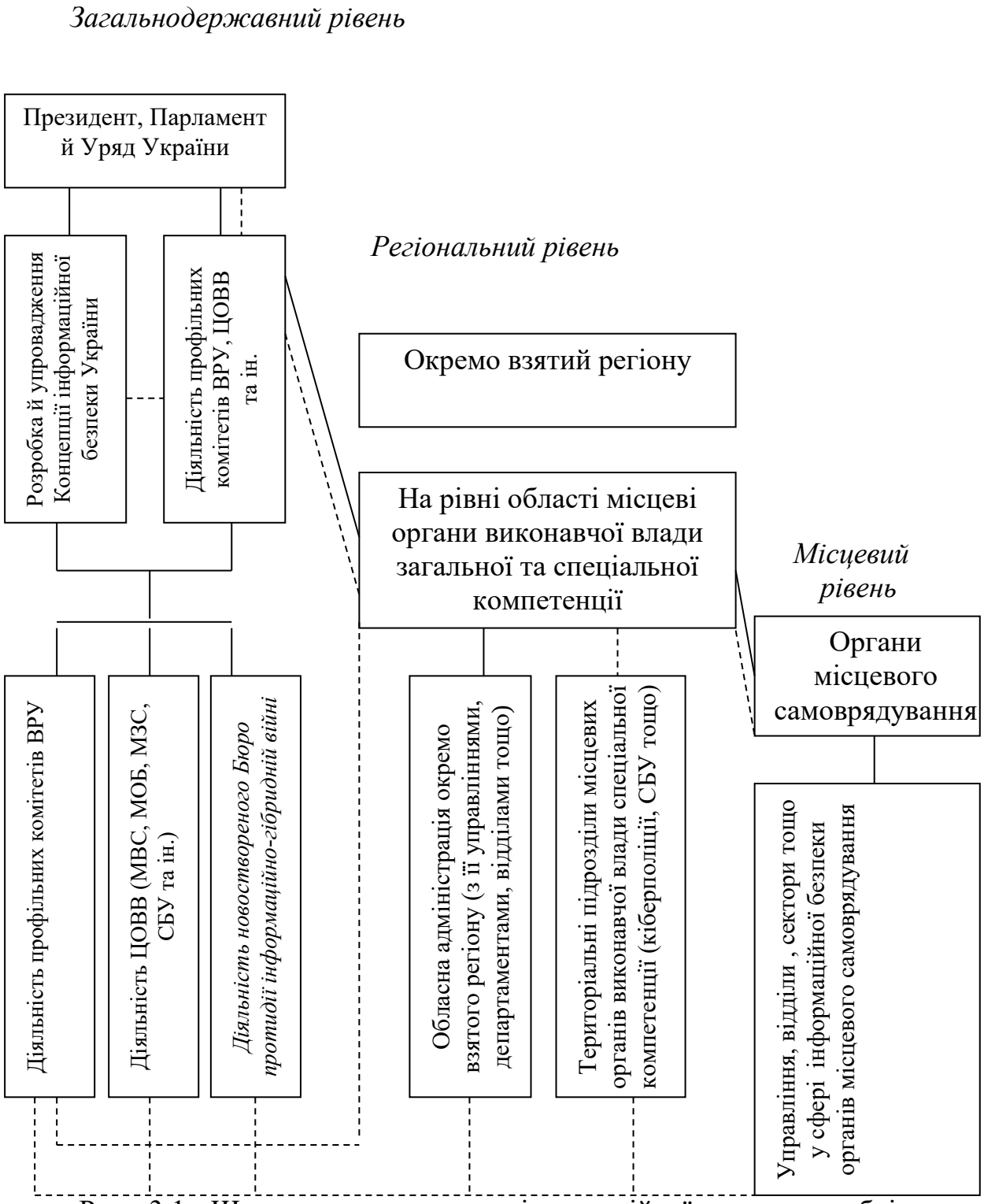

Рис. 3.1. Шляхи вдосконалення інституційної системи публічного управління України в умовах інформаційно-гібрідних війн

Джерело: авторська розробка

На наш погляд, одночасно мають реалізовуватися заходи щодо належного забезпечення інформаційної безпеки України й іншими публічними інституціями – НУО, НКО. Вони мають залучатися до реального формування та контролю за державною інформаційною політикою України. Зокрема, під час розробки Концепції інформаційної безпеки України. Крім того, уважаємо, що в цій концепції інформаційно-гібридна війна має бути визначена як одна із загроз інформаційній безпеці нашої країни.

У продовження також відзначимо, що розвиток вітчизняної інституційної системи публічного управління в умовах інформаційно-гібридних війнах має бути забезпечений шляхом створення Державного унітарного підприємства «Центр технічного захисту інформації, сертифікації та експертизи». На наше переконання, такий центр має протидіяти іноземній технічній розвідці. Діяльність цієї організації рекомендуємо регламентувати в межах: 1) постанови Уряду України «Про положення про вимоги, умови та правила захисту інформації від іноземної технічної розвідки»; 2) державної програма забезпечення інформаційної безпеки України на період до 2030 року. Підкреслимо, що реалізація таких правових документів повинна відзначатися використанням у повній мірі методу «інформаційно-правового домінування», що передбачає наявність позицій щодо максимально результативної взаємодії з міжнародними організаціями під час протистояння інформаційно-гібридним війнам, особливо кіберзагрозам з огляду на масштаби їхнього значного поширення [103].

Україна, як й інші держави Східного європейського регіону, є вразливою до впливу кіберзагроз і кібервійн. Як відомо, «кібервійни» – це один із компонентів інформаційно-гібридних війн, що реалізуються у цифровому просторі. Основна мета кібервійн передбачає підрив існуючого державного ладу в країні-жертві шляхом «хакерських атак» [79; 154]. Кібервійни можна розділити на дві групи. Перша група підтримується на

офіційному державному рівні з боку світових та регіональних спільнот й організацій, які мають у своєму розпорядження кіберкомандування, кібервійська та інші аналогічні формування. Друга група використовується терористичними організаціями глобального та локального значення, супроводжуючись вчиненням кіберзлочинів у віртуальному просторі. Цей напрямок протиправної діяльності отримав назви «кібертероризм», «кіберекстремізм», «кіберхаліфат» та ін. [там само].

Сьогодні основними учасниками кібервійн може бути визнано найбільш розвинені в технологічному відношенні країни: рф, Китай, Індію, Іран, Північну Корею та ін., які мають передову кіберзброю. Наприклад, найвідомішим фактом вважається американська хакерська атака на іранські ядерні об’єкти з використанням вірусу «Stuxnet», який вивів з ладу центрифуги зі збагачення урану [3; 79; 103].

Отже, кібервійни відрізняються тим, що вони дають можливість досягти бажаного ефекту, установлюючи контроль над країною-об’єктом без кровопролиття, тобто із застосуванням новітньої технології. Кібероперації першої групи в основному спрямовані на добування закритої інформації військового, економічного та політичного характеру, тому до них віднесено кібершпигунство, економічне шпигунство, промислове шпигунство, політичне шпигунство та ін. З цією метою використовуються різні віруси-шпигуни, шкідливі програмні забезпечення, звукові атаки та ін. [там само].

На нашу думку, Україна може протидіяти кібервійнам у двох напрямках, а саме:

1. Удосконалення власної нормативно-правової бази, включаючи канал двостороннього та багатостороннього співробітництва із зарубіжними країнами.

2. Створення відповідних організаційних і технічних структур щодо захисту важливої інформації.

З метою протидії кібервійнам із використанням Інтернету, соціальних

мереж на вітчизняних теренах створено Кіберполіцію як департамент Національної поліції України [57]. Його завданням є боротьба з кіберзлочинами, тобто протидія хакерській діяльності, термінації міжнародних дзвінків стільникових компаній, вербування українців до терористичних груп у цифровому світі та ін.

У контексті вдосконалення заходів щодо протидії «кібервійнам» Україна бере участь у міжнародних форумах, конференціях та інших науково-практичних заходах. Крім того, у межах двостороннього та багатостороннього співробітництва України з іншими державами також здійснюється низка заходів. Практично у всіх підписаних чи підписуваних нормативно-правових документів передбачається співробітництво сторін у сфері боротьби з кіберзлочинами. Багатосторонній формат співпраці з протидії кібервійнам передбачає спільну боротьбу в рамках міжнародних та регіональних організацій за прикладом ООН, ОБСЄ, СНД, ПАРЄ та ін.

В останні роки Україна стала поступово перетворюватися на одну з сприятливих політичних площин щодо обговорення та розгляду проблем боротьби із терористичними й інформаційно-гібридними війнами. Висловлюємо переконання, що створений Центр по боротьбі з тероризмом в Україні при МВС надасть додатковий позитивний імпульс для розробки заходів з протидії таким війнам. Відтак, спеціальним службам та правоохоронним органам першорядне значення має бути приділено питанням забезпечення інформаційної безпеки українських громадян.

При цьому слід наголосити на важливості плідної співпраці державних органів України з Інтерполом щодо питань розшуку терористів, контрабандистів та інших категорій злочинців, які ховаються за межами нашої держави. З цією ж метою має бути створено Центр боротьби з тероризмом, екстремізмом та сепаратизмом при МВС України.

З метою запобігання подальшій радикалізації української молоді за кордоном, уважаємо, що має проводитися робота щодо повернення на батьківщину такої молоді. У цьому контексті важливо, щоб Україна

підтримувала розумні та конструктивні ініціативи, спрямовані на протидію дезінформації та впливу інформаційних загроз. Проте, перебуваючи в епіцентрі протидії інформаційно-гібридних війн, Україна й досі не вирішила питання щодо створення відповідного антигібридного центру під егідою однією із зазначених регіональних та міжнародних організацій. Крім того, у зазначеному напрямку наявні недоліки, основним з яких, на наш погляд, уважається недостатня взаємодія спеціальних та правоохоронних органів України, дублювання ними процесів реагування на дезінформацію тієї ж рф. З цієї причини назріла необхідність, на наш погляд, у концентрації та децентралізації всіх питань щодо протидії інформаційно-гібридним війнам і відповідним загрозам шляхом функціонування одного компетентного органу.

Крім того, архіважливим завданням України є протидія нелегальній міграції її громадян за кордон, що можна охарактеризувати як «мігрантська війна». Уважаємо, що вона має бути розв'язана на міжнародному рівні шляхом укладення двосторонніх угод, що повинні окреслити заходи щодо впорядкування міграційних процесів.

У той же час, забезпечити «проактивність» розвитку інституційних механізмів публічного управління в умовах інформаційно-гібридних війн може застосування системного підходу, що передбачає здійснення стратегування та прогнозування. На цій підставі вважаємо, що перспективним напрямком досліджень є обґрунтування засад щодо реалізації зазначених управлінських функцій, які охоплює планування.

3.3. Концептуальні засади прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління

Аналізуючи перспективи прогнозування особливостей виникнення та

розвитку інформаційно-гібридних війн на пострадянському та вітчизняному просторі, зазначимо, що його здійснення знову ж таки залежить від публічної політики економічно розвинених держав і міжнародних організацій, їхніх стратегій та тактики щодо світового домінування з використанням різних технологій інформаційно-гібридних війн, про які йшло в роботі вище. Практика показує, що процес глобалізації змушує держави та міжнародні організації діяти неординарно, періодично змінюючи правила гри. Це насамперед, відноситься до США, що продовжують політику щодо збереження однополярного світу, без урахування інтересів Росії, яка прагне затвердити себе як світову державу, а також амбітних прагнень КНР. В останні роки інформаційно-гібридне протистояння цих країн набуває очевидного характеру. З огляду на це геополітичну обстановку пострадянського та вітчизняного простору варто характеризувати з позиції першорядного впливу на цей простір протиборства країн і міжнародних спільнот у всьому світі.

Крім того, на сучасному етапі спостерігається загострення обстановки на Близькому та Середньому Сході, Південній Азії, Азіатсько-Тихоокеанському регіоні, Латинській Америці та інших країнах, де перетинаються приватні інтереси з публічними. На цій підставі варто констатувати, що світ перебуває у стані невизначеності, тому складно робити прогнози на далеке майбутнє. Учорашні вороги стають друзями, у свою чергу, теперішні друзі стають ворогами. Наприклад, важко було уявити, що КНР погодиться на мирні переговори зі своїми історичними ворогами – США та Південною Кореєю, відтак стає неясно, як у перспективі розвиватимуться події на Корейському півострові [221].

Складності ситуації додає особливості сучасного розвитку країн Центральної Азії, яка з давніх-давен була об’єктом уваги світових і регіональних спільнот та іноземних держав. Зважаючи на це, можемо відзначити, що ці сили в майбутньому також не відмовляться від використання інформаційно-гібридних війн на пострадянському, а , відтак,

вітчизняному, просторі. Україна, як і раніше, залишається ареною зіткнення інтересів рф, США, Китаю та інших зацікавлених держав, у зв'язку з чим весь спектр інформаційно-гібридних загроз пов’язаний з їхнім протистоянням на вітчизняних теренах. Тому прогнозування майбутніх перспектив розвитку інформаційно-гібридних війн в Україні та на пострадянському просторі є ускладненим, але важливим.

На наше переконання, основний зміст протистояння інтересів рф, США, Китаю та інших зацікавлених держав полягає в тому, що всі вони хочуть лише одного – позбутися один одного як вагомих гравців на міжнародній арені та політичного життя окремо взятого регіону, у т.ч. України. На жаль, для цього ними використовуються всі наявні важелі впливу із застосуванням різних технологій/інструментів інформаційно-гібридних війн. У цьому плані доречно навести тезу, що важко спрогнозувати розвиток подій навіть на найближчі роки, не кажучи вже про кілька десятиліття.

Прикладом, на наш погляд, може бути нездійснений прогноз про ускладнення військово-політичної обстановки в Центральній Азії після виведення іноземних сил з Афганістану у 2014 році. Про цей процес говорили багато вчених, експертів, різних міжнародних аналітичних центрів/організацій через призму інтересів світових та регіональних спільнот у цьому регіоні. Нова адміністрація США прийняла нову стратегію щодо Афганістану, на підставі якої присутність США та НАТО, навпаки, було посилено в Афганістані [86; 221].

На даному етапі на пострадянському просторі зберігається стабільно негативна обстановка, здебільшого це стосується України та пов’язаних із нею подій. Так, своєчасно поширюються фейкові новини, здійснюється регулярне вливання дезінформації щодо російсько-української війни та участі в цьому європейських країн та ін. Ці заходи інформаційного впливу спрямовані на масовий прорив або захоплення територій України, або тих територій, які з нею межують, для здійснення інших великомасштабних

акцій чи ескалації ситуації, що може наразі лише прогнозуватися.

Ключем для прогнозування виникнення інформаційно-гібридної війни є визнання того, що вона є результатом спровокованих ззовні асиметричних конфліктів, покликаних підірвати державну та соціальну цілісність, геоекономічні та геополітичні інтереси тощо. Ґрунтуючись на цьому факті, слід вказати на напрям ймовірного удару інформаційно-гібридної війни.

Беручи до уваги цю тезу, у цьому дослідженні спрогнозовано перспективи інформаційно-гібридних війн на пострадянському та вітчизняному просторі. При цьому ставиться мета розкрити дану тему крізь призму можливого впливу основних зовнішніх та внутрішніх факторів на реалізовані Україною інтеграційні прагнення, а також на пострадянський простір у цілому тих чи інших технології/інструментів інформаційно-гібридної війни.

Як відомо, пострадянський простір формується протягом останніх тридцяти років (тобто з моменту розвалу СРСР). Колишні радянські республіки перетворилося на арену «великої гри» світових країн-лідерів і регіональних спільнот. Про це ще на початку 90-х мм. згадував американський політолог і стратег З. Бжезінський, який, зокрема, зазначав таке: «Хоча про кожного із суперників можна сказати, що він прагне отримати сферу впливу, проте, амбіції Москви набагато ширші, ураховуючи її зовсім нещодавні прагнення про імперський контроль і повернення Росії статусу однієї з великих держав глобального масштабу. Зовнішньополітичні заяви Москви явно свідчать, що вона розглядає увесь простір колишнього Радянського Союзу як площину для своїх особливих геостратегічних інтересів, за яких будь-який політичний і навіть економічний вплив ззовні неприпустимий» [13; 27; 167].

Ці висловлювання американського стратега ще раз засвідчують, що пострадянський простір, включаючи й вітчизняний, традиційно входив і буде входити до зони інтересів рф, яка буде відстоювати свої інтереси за

будь-яких обставин на території України як суверенної держави. До речі, у стратегії національної безпеки США закріплено положення, що США можуть вести війну проти російських і китайських збройних сил на віддалених територіях, тобто на території третіх країн та за інтенсивності, що не допускає перевищення ядерного порога [28; 165].

Саме така війна і називається інформаційно-гібридною війною. Тому варіантів розв’язання військових конфліктів між США та рф, США та КНР, НАТО та рф на віддалених театрах бойових дій таких, як Україна, Придністров'я, Сирія, Центральна Азія чи Кавказу, може бути безліч. Як випливає із зазначеної стратегії США, Україна також, на жаль, значиться у списку країн-об'єктів інформаційно-гібридних війн, ініційовані тими чи іншими державами.

Окрім рф, КНР і США, свою гру на пострадянському та вітчизняному просторі ведуть також Європейський Союз, Туреччина, Іран, Саудівська Аравія, Індія, Японія та інші країни, кожна з яких має власні геополітичні/геоекономічні інтереси. З метою їхнього досягнення використовуються різні технології/інструменти інформаційно-гібридних війн. Не можна забувати, що протягом останніх десятиліть робилися неодноразові спроби дестабілізації обстановки в Україні на основі міжетнічних, релігійних та інших зовнішніх і внутрішніх факторів (міжетнічні російсько-татарські, україно-татарські протистояння 1990 р., 2010 і 2014 р., або надумане обмеження прав російськомовних українців та ін.). Усі вказані події підігрівалися безпосередньо ззовні певними світовими та регіональними спільнотами та державами, що (події) мали гібридний характер. При цьому зовнішніми силами вміло було використано внутрішні проблемні чинники окремо взятих регіонів України – АР Крим, Донецької та Луганської областей.

Ця ж думка підтверджується за кордонними експертами, які зауважують, що не можна виключати можливості використання пострадянського регіону як одного з плацдармів про інформаційно-

гібридних війн [165; 211]. Тим більше, що деякі її прийоми (наприклад, штучне розпалювання міжетнічних та соціальних конфліктів) є вміло апробованими [там само].

До речі, на основі аналізу інформаційно-гібридних війн у Сирії та Україні, американські політичні аналітики прогнозують аналогічну війну на просторі Центральної Азії за участю рф та КНР [165; 211]. Зокрема, дослідники зазначають, що, зважаючи на викладені моменти, а також апробацію запропонованої методології на прикладі аналізу ситуацій у Сирії та Україні, слід перейти до практичної реалізації вчення про «інформаційно-гібридну війну» і визначити наступні можливі напрями її удару. Найважливіші багатополярні транснаціональні проекти реалізуються рф та Китаєм, при цьому значущими проектами в «портфелях» зазначених країн вважаються Євразійський економічний Союз та «Один пояс – один шлях» («Новий шовковий шлях»), який формують рф і Китай. Зона перетину даних проектів знаходиться в країнах з родючими ґрунтами та іншими значними природними ресурсами (лісами, водоймами, корисними копалинами, нафтою, газом тощо). Вони наявні в Україні, країнах Середньої та Центральної Азії, а це означає, що масштабна дестабілізація цих регіонів може завдати удару «дуплетом» - одним сильним геополітичним ударом стримати амбіції наддержав, серед яких наразі ключовим тригером є США. Саме тому існує високий ризик розв’язування повномасштабної інформаційно-гібридної війни в азійському регіоні, як ми це вже бачили в Україні останніми роками. Крім того, варто вказати на пряме й доволі масштабне перетинання інтеграційних проектів у межах російсько-китайського стратегічного партнерства, що поширило дію на Балкани. На цій підставі можна підкреслити, що настільки щільного та розвиненого перетину/переплетення інтересів обох наддержав, якими себе вважають рф і КНР, як у Східно- і Південно-європейському регіонах, а також регіоні Середньої та Центральної Азії, немає.

Розвиваючи цю думку, можна з упевненістю стверджувати, що на

рубежі XX-XXI століть, не вдаючись до прямого великомасштабного зіткненню регулярних армій, США та НАТО реалізують стратегію інформаційно-гібридних війн для поетапних багатовимірних конфліктів на території України, Закавказзя та Центральної Азії. Кінцева мета стратегії хаотизація рф та євразійського простору. Це реалізується з метою оточення рф поясом русофобних режимів за одночасного нарощування всіх видів тиску на цю країну-агресора.

У свою чергу, не слід забувати, що кожна країна (європейська, центральноазійська та ін.) мають свої специфічні особливості розбудови, і відповідно, вимагають відповідного етатичного підходу до характеристики «геополітичних ігор». У цьому контексті слушною є наукова позиція, згідно з якою протягом тривалого часу багато західних експертів розглядали пострадянський регіон як монолітне ціле, хоча після розпаду СРСР кожна з країн цього регіону рухалася своєю траєкторією політичного, суспільного й економічного розвитку, маючи різний ступінь відкритості до зовнішнього світу. Україна спромоглася до посередніх результатів у цій сфері, але хоча б не на папері забезпечила власний демократичний розвиток, як-то відбувається в Білорусії та рф [167].

Учені З. Бзежинський, С Грей, Дж. Саймон та ін. справделиво зазначають, що в пострадянських державах вже давно йде «інформаційно-гібридна війна» [13; 167; 180; 211]. Україна є великою державою за розмірами й історією становлення, але інформаційно-гібридна війна (що ведеться рф) використовується як засіб територіального переділу нашої країни. Тому вітчизняні та закордонні ЗМІ, правозахисники та політичні лідери – це інституційні інструменти протистояння України впливу інформаційно-гібридної війни. І якщо хтось апелює в країні-агресорці до закону, свободи слова та прав людини, для початку цій країні слід навчитися їх дотримуватися та поважати суспільство сусідньої держави, як, власне її суверенність. Ті, хто розв’язав інформаційно-гібридну війну проти України і розпочали брудні політичні ігри повинні усвідомити, що за рамками правого

поля, де вони виявились самі і намагаються втягнути туди всю Україну, жодних правил уже не існує.

З публікацій деяких незалежних засобів масової інформації випливає, що сьогодні у списку країн із високим ризиком суспільно-політичної нестабільності, де можуть бути використані ті чи інші технології/інструменти інформаційно-гібридних війн, уважаються не тільки Україна, а й Туркменістан і Казахстан. Загроза Туркменістану виражається більше у формі «не кольорової революції» (як-то було в Казахстані, Україні), а у вторгненні терористів з Афганістану. І практика ведення «кольорових революцій» дає підстави стверджувати, що для успішної реалізації такий операцій не обов'язково захоплювати адміністративну столицю певної країни. Достатньо завоювати або, як мінімум, серйозно розкачати велике стотисячне (мільйонне) місто. У Казахстані існує значний ризик цілеспрямованої робота деяких НУО, фінансованих ззовні, з метою загострення «національного питання» до рівня екстремістських виявів соціального невдоволення з боку як казахів, і росіян.

На наш погляд, під вплив аналогічної інформаційно-гібридної загрози можуть потрапити й інші держави Центральної Азії. В умовах нового світопорядку всі вони стикаються з економічними, екологічними, етнічними, демографічними та іншими проблемами. Вони, у свою чергу, можуть бути супутніми факторами при виборі та реалізації різних технологій/інструментів інформаційно-гібридних війн.

Головною прихованою метою будь-якої інформаційно-гібридної війни є перешкода побудови багатополярної системи міжнародних відносин шляхом зовнішнього провокування конфліктів ідентичності (етнічної, релігійної, регіональної, політичної тощо) у державі-мішені перехідного типу, як-то відбувається в Україні. При цьому слід зазначити, що на пострадянському просторі в результаті національно-територіального розмежування, що склалося при колишньому Радянському Союзі, утворилися і, надалі, остаточно сформувалися деякі зовнішні та внутрішні

фактори, які не раз призводили до різних конфліктів між цими державами, навіть під час функціонування могутнього СРСР. Тому з урахуванням зазначених факторів стосовно кожної пострадянської країни сьогодні визначаються основи застосування різних технологій/інструментів ведення інформаційно-гібридних війн.

Той же З. Бжезінський [13; 167] включив до списку держав-мішеней до таких війн Україну, усі п’ять держав Центральної Азії й Балканські країни, через їхню вразливість, в основному, до міжетнічних, релігійних та інших проблем, що викликають соціальне невдоволення та протистояння. З цієї причини пострадянський простір є спокусою для втручання з боку іншої країни, кожна з яких сповнена рішучості чинити опір домінуючій ролі іншої держави-сусіда.

До основних зовнішніх факторів, що становлять підґрунтя для інформаційно-гібридних війн, можна віднести: міжнародний екстремізм та тероризм; незаконний обіг наркотиків та зброї; незаконна торгівля людьми, та інші види транснаціональної злочинності, які, в основному, виходять із нестабільної сусідньої країни – рф. Основними ж внутрішніми факторами можна вважати такі: релігійна ситуація; міжетнічні відносини; нелегальна міграція; не до кінця вирішені прикордонні питання; водно-енергетична проблематика; низький рівень добробуту певних категорій населення та соціально-економічного становища загалом; екологічні та демографічні питання тощо.

Кожен із зазначених факторів служить детермінантою для застосування тих чи інших технологій/інструментів інформаційно-гібридних війн на пострадянському просторі. Будь-яке протистояння цим факторам подається в різних засобах масової інформації як різновид «гібридної війни» [27].

Таким чином, сьогодні у світі послуговуються поняттями батьківщина, віра, релігія тощо, насамперед, за умов дестабілізації соціального розвитку. Проте наразі у світі йде справжня війна з тероризмом

та екстремізмом, для чого задіяні всі наявні ресурси окремих держав, коаліцій країн, регіональних та міжнародних організацій з питань безпеки. Для опору терористичній діяльності в Афганістані, Сирії, Іраку та інших країнах, поряд з несиловими методами, використовуються й силові (приватні військові компанії, спецпідрозділи та інші).

На сучасному етапі світо порядку «терористичні війни» безпосередньо виходять із діючих на території Афганістану, Сирії, Іраку та інших держав сил міжнародного тероризму, до яких належать: ІГІЛ, Рух Талібан, Ісламський Рух Туркестану та ін. У їхньому складі присутні громадяни з пострадянських держав. Усі вони беруть участь в інформаційно-гібридних війнах, розв'язаних державами-агресорами на зазначених територій із застосуванням сил тероризму.

Слід наголосити, що в Україні йде справжня інформаційно-гібридна війна, і наша держава сьогодні перетворилася на плацдарм для ведення такої й аналогічних війн. У той же час, багато залежатиме від врегулювання російсько-української війни, у межах якої зростає кількість зазначених інформаційно-гібридних загроз. Однак у найближчій перспективі представляється малоймовірним врегулювання даної ситуації в Україні, оскільки стратегічні інтереси держави-агресора рф сильно переплетені з геополітичним і геоекономічним вектором.

Російсько-українська війна багато в чому збігається із сучасними розробками «асиметричних війн» (інформаційно-гібридних війн), базис яким становлять «досягнення» щодо якомога більшої кількості жертв серед мирного населення, масових переміщень громадян, гуманітарної катастрофи тощо. Держава-агресор рф загалом намагатиметься створити ситуацію «керованого хаосу» на вітчизняних теренах через організацію інформаційно-гібридних війн. На прикладі України, на жаль, можна простежити поступову активізацію технологій/інструментів інформаційно-гібридної війни, яка передбачає використання хаосу і сама створює «керований хаос». При цьому слід зазначити, що практично за всі досконалі терористичні акції у

світі, включаючи і на пострадянському просторі, рф не бере на себе відповідальність.

Терористичні угруповання використовують військові та невоєнні технології інформаційно-гібридних війн. Так, вони ведуть локальні бойові дії проти урядових сил й один проти одного, використовують іноземних найманців, роблять терористичні акти через поділ сфер впливу. До невійськових технологій слід віднести «інформаційну війну», «кібервійну» та інші. Зокрема, відомі хакерські атаки ІГІЛ на ряд урядових та військових об'єктів провідних світових держав, що діють під назвою «Електронні привиди халіфату» [79; 154].

Як відомо, жодна терористична організація, у тому числі ІГІЛ, не може проіснувати без підтримки ззовні. Тому слід погодитися зі сформованою в експертному суспільстві думкою про те, що закриття «кураторами» проекту «Ісламська держава» на території Іраку та Сирії, може спричинити її виникнення в новому вигляді, але в іншому місці для ведення інформаційно-гібридних війн. У цьому плані Україна не є винятком. Прикладом наявності «сплячих осередків» є численні арешти і засудження терористів-одинаків або учасників груп, що діють на території республіки. Підтвердженням сказаного є затримання останнім часом правоохоронними органами злочинних угруповань, які виношували плани вчинення терористичних актів у прикордонних районах та всередині пострадянських країн [79; 154].

Широке поширення дезінформаційних повідомлень про ускладнення військово-політичної обстановки в Україні, Афганістані, Центральній Азії, про зміцнення в них сил міжнародного тероризму, екстремізму, незаконного обігу наркотиків тощо також можна віднести до технологій інформаційно-гібридних війн. При цьому активно використовуються Фейсбук, Твіттер та інші соціальні мережі, де діє безліч «фабрик тролів», подачі рейкових новин тощо.

«Мігрантські війни» також мають перспективу для розвитку і

становлять загрозу для України. Вони можуть набути ще більшого розмаху у зв'язку з повномасштабною агресією рф, що дестабілізує соціально-економічне становище України, зумовлюючи виникнення масової міграції її населення в інші країни. Отже, головна проблема створення спрямованого міграційного потоку полягає в тому, чим він спровокований. Ні локальні теракти, ні напади загонів бойовиків на кордон не здатні викликати масову еміграцію, оскільки не зачіпають безпеку більшої частини населення. У цьому контексті цю масовість забезпечує війна, як-то відбувається в Україні. Виходячи з цього, можна допустити, що й у перспективі вище-перелічені зовнішні та внутрішні чинники будуть актуальними для неї, залишаючись детермінантами для застосування різних технологій/інструментів інформаційно-гібридних війн на цьому просторі. Одним із важливих внутрішніх факторів, який може бути детермінантою інформаційно-гібридної війни на найближчу перспективу, визнається міграційна та демографічна ситуація в Україні, знищується її цвіт нації, гине багато військового та цивільного населення.

Пострадянські країни, крім економічної залежності, також слабкі й у ідеологічному плані. В Україні й досі тривають протистояння на релігійному підґрунті, тривалий час була заборонялася єдина релігійна концепція. І так було до томасу про автокефалію Православної церкви України, що може об'єднати людей. Вони не повинні жити за чужими концепціями (західними, російськими та іншими).

До речі, як відомо, у США функціонує відомство, яке визначає зовнішню релігійну політику. Зважаючи на це, можемо стверджувати, що сьогодні країни переходять на нову стадію інституційного розвитку – ментальні інформаційні війни, кінцевою метою яких є розкол певного суспільства та замовлення появи суспільно-політичних конфліктів. У пострадянських державах спостерігається непослідовний процес формування релігійної політики, адже десь вона продовжує передбачати застосуванням методів прямого впливу, а не ліберального. Це дозволяє

наполягати на продовженні використання релігії як опіуму для народу, механізму маніпулювання ним. З кожним роком, для значної частини пострадянських держав проблема релігійного контролю, екстремізму тощо стає все більш актуальнішою. Доречно лише поглянути на списки заборонених екстремістських організацій у рф, і можна виявити, що серед них насамперед релігійні організації. У рф активно реалізується механізм «формування загального релігійного розуміння світопорядку», що передбачає протистояння наявним екстремістським і «західним» загрозам, наприклад, одностатевим відносинам. Вони якимось чином становлять небезпеку для політичної системи рф, її соціуму та державних інститутів.

Аналіз наукових напрацювань дає підстави стверджувати, що, дійсно, у пострадянських державах відсутній єдиний підхід до релігійних партій та рухів, але цього й не повинно бути, тому що загально визнаним є принцип свободи релігійного віросповідання. Відтак, не коректно наполягати на необхідності здійснення уніфікації підходів щодо вирішення релігійних питань. Інакше, можна стикнутися з проблемою радикалізації суспільства в пострадянських державах, з можливість розв’язання на їхніх територіях релігійних та інформаційно-гібридних війн.

У перспективі ще одним супутнім внутрішнім фактором інформаційно-гібридної війни на пострадянському просторі може стати енергетична проблематика чи питання ефективного використання природних ресурсів. Із розвитком національних економік проблема споживання енергії та природних ресурсів тільки зросте, що не може не відбиватися на соціально-економічному потенціалі країн, адже нестача природних ресурсів багато в чому обмежує економічний розвиток. З огляду на це існують побоювання, що виконавцями інформаційно-гібридних війн на пострадянському просторі енергетична сфера може бути використана як основний дестабілізуючий фактор.

На даний час проблема раціонального використання енергетичних ресурсів на пострадянському просторі не вирішено. Деякі країни активно

включаються до вирішення однієї з стратегічних цілей України щодо забезпечення енергетичної незалежності, однак це можливо шляхом залучення до будівництва нових енергосистем, що наразі ускладнює повномасштабна агресія рф. Крім того, перспективний напрям для України становить перехід на інші альтернативні джерела споживання електроенергії. Це певною мірою знизить градус соціальної напруженості і зменшить рівень конфліктності в Україні, який зумовлений рф.

Що стосується проблеми міграції, то вона виникає і через дестабілізацію економічної й енергетичної безпеки. На наш погляд, слід звернути увагу на те, що у разі погіршення економічної обстановки в Україні, як це зараз спостерігається і не результативність міжнародних санкцій проти рф, кількість українських мігрантів може зрости і вони змушені будуть залишити постійне місце свого мешкання. Це може викликати зростання рівня безробіття, злочинності та соціальну напруженість у вітчизняному суспільстві. Тоді безробітні, більшу частину яких складає молодь, шукатимуть інші джерела існування, утворивши цим протестний (невдоволений) потенціал у своїй країні. Цим можуть скористатися вербувальники різних міжнародних терористичних і злочинних організацій радикального проросійського спрямування, які всебічно підтримуються зацікавленими регіональними спільнотами для поповнення своїх рядів. Як не прикро, але перспективність використання цієї обставини в найближчому майбутньому для дестабілізації ситуації в Україні аж ніяк не є примарною. Аналогічними супутніми факторами послужать також неврегульовані на її території прикордонні питання.

У продовження відзначимо, що в перспективі міжнародні спільноти та держави можуть також скористатися, як ще одним інструментом реалізації інформаційно-гібридних війн, багатовекторну політику пострадянських держав. Щодо України, то ще донедавна вона була в списку держав з багатовекторною політикою, але після внесення змін до Конституції України у 2019 році ситуація змінилася діаметрально у бік

закріплення євроінтеграційних і євроатлантичних прагнень нашої держави. Відтак, уважаємо, що для рф складно буде використати цей інструмент для розхитування інформаційно-гібридної війни в Україні.

Щодо інших пострадянських країн, то ним необхідно рішуче відмовитися від спроб всидіти на двох стільцях. А тому, з одного боку, намагатися загравати із Заходом, а з іншого боку, розраховувати на підтримку рф. У певний момент така багатовекторна політика може дати збій, і держава з такою політикою виявиться віч-на-віч із серйозними противниками [103].

Культурний аспект інформаційно-гібридної війни також зберігатиме свою актуальність на пострадянському просторі. У наш час глобальної інформатизації важливою складовою інформаційно-гібридних війн стають «культурні війни», які мають на меті зміну культурного коду нації країни-мішені. Інтервенція у культуру представляється вторгненням в епісистему конкретного народу чи етносу, створення чужих йому соціальних інститутів, статусів, цінностей, традицій тощо. На підтвердження можемо навести ситуацію з підміною рф справжніх історичних фактів щодо місця походження Київської Русі [19; 36].

Таким чином, метою країни-агресора в подібній війні є відчуження людини від культури, в якій вона вкорінилася, а точніше – від її культурної ідентичності. Інакше кажучи, «культурна війна» – це викликане культурними протиріччями зіткнення акторів міжнародних відносин, наслідком якого є повна або часткова руйнація культурних кодів залучених до нього товариств. Знищення духовної самобутності і морального духу противника уможливлює досягнення економічних, політичних та інших цілей без масштабного залучення збройних сил та тривалих дипломатичних процедур. Особливості культурних війн полягають у тому, що вони охоплюють основні сфери життя суспільства. Слід зазначити, що «культурні війни» ведуть як держави, так і міжнародні та регіональні спільноти. Яскравим прикладом може бути поширеність турецьких серіалів на

пострадянському просторі.

Ще одним сприятливим фактором для реалізації інформаційно-гібридних війн є правове поле суверенних держав, що окреслює шляхи захисту прав і свобод людини. Слід констатувати, що інформаційно-гібридні війни в цьому напрямі вже ведуться давно. Щорічно публікуються звіти різних міжнародних аналітичних центрів таких, як Human Rights Watch (HRW), ООН та ін. щодо стану дотримання прав і свобод людини, на основі чого складаються рейтинги держав [183].

Наявність корупції, лобізм, непотизм («кумівство») та інші негативні суспільно-політичні явища також є детермінантами інформаційно-гібридних війн і сьогодні, і в майбутньому [97; 162]. Для держав пострадянського простору ці негативні суспільно-політичні явища становлять загрозу ефективному функціонуванню інституційних систем публічного управління, а також економічній безпеці таких країн. У зв'язку з цим з'явилися нові технології ведення інформаційно-гібридних війн, які ЗМІ вже названі «санкційними війнами», «митними війнами», «торговими війнами» та ін.

Безперечно, «санкційні війни» між США та рф сьогодні негативно впливають практично на всі країни, хоча зорієнтовані насамперед на державу-агресора, з метою витіснення її з глобальної економічної системи. У той же час, це зумовлює появу негативної реакції з боку країн, проти яких не ведуться «санкційні війни», але вони змушені їх відчувати на собі. Україна має безпосередні політичні, торговельні, економічні зв'язки з такими державами, але вони (зв'язки) наразі є крихкими. На цю дестабілізуючу обставину слід зважати Україні. Щодо «митних війн», то на них також звернути увагу вітчизняним посадовцям з огляду на їхню загрозливість для системи безпеки. Як зазначалося в роботі вище, під «митними війнами» маються на увазі значні зіткнення, коли обидві сторони шляхом виняткового підвищення мита, зборів та ін., аж до заборони ввезення, а іноді й вивезення товарів, намагаються порушити товарообмін та змусити іншу державу піти на поступки [103].

Отже, можемо зробити такі проміжні висновки в межах даного підрозділу:

1. Пострадянський простір загалом і вітчизняний зокрема в перспективі продовжуватиме залишатися об'єктом реалізації державами та міжнародними спільнотами інформаційно-гібридних війн.

2. Україна буде основним плацдармом для ведення інформаційно-гібридних війн, ініціатором якої є рф. У цьому контексті не можна виключити використання як військового компоненту «гібридних війн» сил США, ЄС, КНР та ін.

3. Незважаючи на позитивні тенденції, що намітилися в останні п'ять роки в суспільно-політичних процесах, пов'язаних, насамперед, із відмовою України від багатовекторної й ізоляційної політики, наша держава поки що тільки стала на шлях забезпечення готовності до інтеграційних процесів у масштабі ЄС і НАТО. Це робить її вразливою до впливу інформаційно-гібридних війн. Завданням України є формування прагнення пов'язувати свій розвиток із всебічним розвитком усієї Європи за всіма сферами життєдіяльності, на основі єдиної регіональної самоідентифікації.

4. Досі зберігаються зовнішні та внутрішні фактори, що загрожують системі безпеки країн пострадянського простору. У разі невирішеності таких проблемних питань у перспективі вони трансформуються в детермінанти інформаційно-гібридних війн.

На цій підставі можемо надати такі рекомендації як завдання для України:

1. Необхідно якомога скоріше долучитися до єдиного конкурентоспроможного в економічному плані інтеграційного об'єднання, та нарешті навчитися визначати свій майбутній розвиток, щоб спільними зусиллями протистояти загрозам інформаційно-гібридних війн.

2. Повністю врегулювати або звести до мінімуму наявні основні спірні/невирішені міждержавні відносини, що є складовими цілого комплексу зовнішніх і внутрішніх загроз системі безпеки України. Для того,

щоб запобігти їх використанню як технологій/інструментів ведення інформаційно-гібридних війн. У цьому контексті Україні доречно долучитися до процесів уніфікації підходів щодо спільного врегулювання зазначених проблем на регіональному рівні.

3. Внести відповідні коригування у сферу зовнішньої політики з основою на реальну світову й європейську політичну систему, здатну захистити від значної кількості технологій/інструментів інформаційно-гібридних війн сучасності.

4. Удосконалювати систему власної безпеки, яка, на жаль, не відповідає сучасним вимогам. Це пов’язано з тим, що Україна не інтегрована належним чином до різні міжнародних і регіональних безпекових структур, які впевнено протистоять технологіям/інструментам інформаційно-гібридних війн для досягнення своїх цілей геополітичного/геоекономічного характеру. З огляду на це доцільно якомога швидше приводити вітчизняну систему безпеки під міжнародні стандарти з метою здійснення спільної протидії інформаційно-гібридним війнам.

Висновки до розділу 3

1. З’ясовано, що значна частина військових конфліктів, які відбуваються у світі, наразі набула гібридного характеру та передбачає обов’язковий вплив інформаційних загроз. Дослідження міжнародного та вітчизняного законодавства дає підстави стверджувати, що в ньому слід закріпити визначення поняття «інформаційно-гібридна війна». Щодо розвитку вітчизняного законодавства в означеному напрямку, то перспективним визнано прийняття Концепції інформаційної безпеки України.

2. Виявлено, що Україна самостійно та спільно з ООН, ОБСЄ, СНД та іншими міжнародними організаціями й об’єднаннями протидіє таким

реалізованим проти неї технологіям інформаційно-гібридної війни: «кібервійни», «терористичні війни», «міграційні війни», «прикордонні війни», «екологічні війни» та інші. Водночас визнано, що протидія інформаційно-гібридним війнам, особливо з використанням глобальної мережі Інтернет, соціальних мереж вимагає постійного вдосконалення системи безпеки у зв'язку з розвитком інформаційно-комунікаційних технологій, який практично неможливо зупинити.

3. Установлено, що управлінські заходи, що реалізуються Україною, на жаль, носять запізнілий характер, адже здебільшого ґрунтуються на фактах, що вже відбулися. У цьому контексті наполягається на необхідності розробки комплексу управлінських заходів «на випередження», тобто стратегічного реагування, виходячи зі тенденції щодо зростання кількості зовнішніх і внутрішніх загроз. Щодо проблем протидії інформаційно-гібридним війнам, то пропонуються такі рекомендації:

1. З урахуванням актуальності проблеми протидії інформаційно-гібридним війнам у перспективі створити єдиний координаційно-аналітичний центр/раду, на зразок Бюро протидії гібридній війні. Таке Бюро функціонує в США та напрацювало дієві управлінські практики реагування на інформаційні загрози. Уважаємо, що до складу вітчизняної інформаційної контргібридної структури слід включити окрему наукову установу, яка має займатися розробкою механізмів дослідження даної проблематики (наукове вивчення, підготовку аналітичних документів щодо виявлення вразливих місць та можливого складу інформаційно-гібридних загроз, надання пропозицій). Ці рекомендації важливі для вироблення політичних рішень і вжиття дієвих заходів протидії з протидії інформаційно-гібридній війні.

2. Для того, щоб уникнути в перспективі дублювання функцій між безпековим і силовим блоком України з питань протидії окремим технологіям інформаційно-гібридних війн таких, як «терористичні війни» та «кібер війни», уважаємо, що доцільно здійснити аналіз і корегування обсягу обов'язків і компетенцій.

3. Обґрунтовано розробити та впровадити Концепцію інформаційної безпеки України з урахуванням нових викликів та загроз, у т.ч. пов'язаних із розвитком інформаційних технологій, що становлять базис для виникнення та масштабування інформаційно-гібридних війн. Дана позиція висловлена з урахуванням основоположних засад науки «Публічне управління та адміністрування» щодо особливостей планування та стратегування.

4. Підкреслено на важливості дослідження досвіду економічно розвинених країн світу щодо дієвих механізмів протидії інформаційно-гібридним війнам й активізації співробітництва з цими країнами. Зважаючи на виявлений позитивний закордонний досвід застосування ризик-орієнтованих підходів щодо функціонування таких механізмів, у дисертації обґрунтовано виважене впровадження цих підходів на вітчизняних теренах. Ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни дозволили обґрунтувати сценарії реагування на ці війни: 1) проактивний сценарій, який рекомендовано реалізовувати під час стратегічного планування та поступального забезпечення сталого розвитку; 2) реактивний сценарій, що передбачає оперативне реагування на інформаційні загрози, зокрема, у межах уточненої концепції протидії ним.

Резюмовано, що проти України як самостійного суб'єкта міжнародних відносин реалізуються окремі технології інформаційно-гібридних війн, які чинять негативний вплив на безпеку нашої держави. На сучасному етапі її функціонування інформаційно-гібридні війни визнаються основною технологією реалізації геополітичних/геоекономічних інтересів інших держав, що вдосконалюють механізми свого інформаційно-гібридного пливу. У цьому контексті зроблено окремі висновки, а саме:

1. Аналіз наукових напрацювань показав, що інформаційно-гібридні війни, незважаючи на свою розпливчастість і багатозначне визначення, сьогодні стали реальністю. Між державами велися та наразі ведуться інформаційно-гібридні війни. І не сприяло унеможливленню їхньому

виникненню утворення ООН, яка проголосила перехід до мирного вирішення всіх проблем, що виникають у взаємовідносинах між державами.

2. Виявлено, що інформаційно-гібридні війни набули значного поширення в таких гарячих точках, як Афганістан, Сирія, Україна, Венесуела та ін. Ці країни є вдалим прикладом протистояння основних геополітичних гравців із використанням різних технологій ведення інформаційно-гібридних війн. Констатовано, що політичні, економічні, військові, інформаційні та інші ресурси виступатимуть складовими технологій інформаційно-гібридних війн у перспективі. При цьому процеси глобалізації стимулюватимуть появу нових аспектів інформаційно-гібридних війн.

3. Обґрунтовано, що пострадянський простір, до якого входить й Україна, у перспективі також залишиться об’єктом реалізації інформаційно-гібридних війн, що здійснюються державами-агресорами з використанням зовнішніх та внутрішніх чинників. Визначено, що такі чинники виступають детермінантами інформаційно-гібридних війн.

4. Представники експертного середовища та наукової спільноти поки що не змогли переконати (через діяльність міжнародних організацій) держав-агресорів щодо перспективності застосування мирних і несилових засобів боротьби, а глобальних військових протистоянь. Як виявилося, ООН, ОБСЄ та інші міжнародні організації не мають достатнього впливу на держави, що є ініціаторами ведення інформаційно-гібридних війн. Поки що ці організації обмежуються декларативними заявами щодо протидії інформаційно-гібридним загрозам. На цій підставі акцентовано на необхідності й надалі вдосконалювати вітчизняну правову базу щодо протидії реалізованим проти України окремих технологій інформаційно-гібридної війни. Це можна досягти тільки шляхом прийняття відповідних стратегій, концепцій та інших документів, в яких мають бути враховані питання виявлення, прогнозування, планування, координації та управління, розкриття вразливих для інформаційно-гібридних загроз сфер із метою

своєчасного їх відображення.

2. Міністерствам, відомствам та іншим державним органам України слід розробити відповідні заходи протидії наявним і потенційним технологіям інформаційно-гібридним війнам з урахуванням всіх аспектів. Серед цих заходів першочерговими можуть бути такі:

– постійне нарощування військового/оборонного потенціалу країни;

– проведення безперервного моніторингу досягнення міжнародних організацій та інших держав у сфері військових конфліктів, оперативного реагування на зміни у світі та регіоні, де використовуються технології інформаційно-гібридних війн;

– забезпечення підготовки якісного кадрового потенціалу, насамперед, військового, здатного розробити та реалізувати намічені заходи щодо протидії інформаційно-гібридним війнам;

– досягнення єдності суспільства всередині країни, соціальної стабільності, міжнаціональної згоди, релігійної терпимості, зміцнення суверенітету та територіальної цілісності країни, її іміджу на міжнародній арені;

– підйом на якісно новий рівень діяльності державних інститутів, які забезпечують реалізацію планів/стратегій розвитку країни у мирний/воєнний час;

– розвиток вітчизняної системи та її кооперація з іншими міжнародними організаціями щодо розробки й упровадження технології протидії «кібервійнам»;

– продовження дослідження Інтернет-простору, з метою унеможливлення його використання міжнародними терористичними та іншими злочинними угрупованнями в межах інформаційно-гібридних війн проти України;

– удосконалення контрпропагандистських заходів щодо протидії інформаційно-гібридним війнам, механізмів швидкого та стратегічного реагування на дезінформаційні/фейкові матеріали та раптові інформаційні

атаки (вкиди);

– підвищення ефективності державних засобів масової інформації в контексті протидії інформаційно-гібридним війнам, виходячи з національних інтересів України.

Завданням України є врегулювання або зведення до мінімуму всіх наявних спірних міждержавних відносин із країнами-сусідами з метою запобігання їх використанню в якості тих чи інших технологій/інструментів ведення інформаційно-гібридних війн проти нашої країни. Слід удосконалювати її систему безпеки, а також нормативно-правову базу в рамках протидії інформаційно-гібридним війнам, які ведуться на пострадянському просторі [92; 103].

ВИСНОВКИ

Одержані під час дослідження результати передбачають вирішення актуального конкретного наукового завдання, яке полягає у визначенні науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

На підставі результатів, отриманих під час дисертаційного дослідження, визначено такі висновки та пропозиції:

1. Узагальнено положення про те, що феномен інформаційно-гібридної війни є вищою формою міждержавного інформаційного протистояння, що передбачає конфлікт інтересів суб'єктів геополітичної/геоекономічної конкуренції (протиборства) в інформаційному просторі. З'ясовано, що метою цих протиріч є встановлення зовнішнього політичного керівництва над державою-об'єктом, а також перерозподіл ролі, місця та функцій у політико-управлінській системі сучасного суспільства, в якому зіткнення конфліктуючих сторін відбувається у формі інформаційних та інформаційно-психологічних операцій із застосуванням нетрадиційної зброї, зокрема, інформаційного характеру.

2. Визначено положення про те, що головною небезпекою інформаційно-гібридної війни є відсутність чітко ідентифікованих (видимих) ознак руйнівного впливу, характерного для традиційних війн. Виявлено, що за цих умов ускладненим є приведення захисних механізмів соціального та публічного управління, наявних у розпорядженні, але можливим. На відміну від традиційної війни, що передбачає застосування фізичної, кінетичної та іншої зброї з метою руйнації всього в межах радіусу її дії, інформаційна зброя діє вибірково, охоплюючи по-різному різні верстви населення та публічні інститути. Традиційна ж зброя впливає на будь-яку частину населення однаково. Відтак, наполягається на такій головній небезпеці інформаційно-гібридної війни як потенційна

можливість цільового інформаційного, у т.ч. негативного, впливу.

3. Структуризовано інституційні механізми публічного управління України в умовах інформаційно-гібридної війни, у складі яких виокремлено насамперед організаційні та правові механізми державного впливу. Базис для висловлення такої позиції становили враховані загальні положення фундаментальної науки щодо визначення понять «інститут», «інституція», «організація» та ін. Обґрунтовано, що інституційні механізми публічного управління України в умовах інформаційно-гібридної війни покликані забезпечувати виникнення та розвиток суб'єктно-об'єктних відносин в означеній сфері, що вимагають результативного застосування методів, інструменти та ресурсів публічного управління з метою налагодження зворотного зв'язку й унеможливлення трансформації ризиків інформаційного характеру в загрози, кризи та війни. Зважаючи на таку мету формування та функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, уточнено визначення поняття «інформаційна безпека».

4. Визначено особливості функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни крізь призму виокремлених ризиків їхнього функціонування, а саме: 1) ризику не протидії поширенню неправдивої та видозміненої інформації з боку країни-агресора, що впливає на розвиток суспільства й держави; 2) ризику не формування цілісної інформаційної концепції і стратегії поширення об'єктивної інформації та протидії загрозам інформаційного характеру; 3) ризику не забезпечення підвищення рівня медіа-культури суспільства та його цифровізованого розвитку тощо. З огляду на збільшення виявів цих ризиків охарактеризовано стан упровадження інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни як незадовільний. Цьому сприяли зовнішні та внутрішні фактори, до яких віднесено насамперед зовнішню агресію проти України, посилення з боку рф інформаційного негативного впливу, що наразі вже набув вигляду

інформаційно-гібридної війни, недосконаліть вітчизняної правової бази в досліджуваній сфері на предмет визначення функцій органів державної влади в інформаційній сфері. На цій підставі конкретизовано склад суб'єктної підсистеми у сфері інституційного забезпечення публічного управління в умовах інформаційно-гібридної війни. При цьому здійснено групування складових суб'єктної підсистеми залежно від того, чи є гарантування інформаційної безпеки основною або другорядною функцією, чи їх реалізують державні органи або інші публічні інституції тощо. Усе це дозволило обґрунтувати шляхи підвищення результативності функціонування цих підсистем з наведенням конкретних нормотворчих пропозицій щодо усунення дублювання функцій органів державної влади у сфері інформаційної безпеки.

5. Проаналізовано інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни, які передбачають застосування, зокрема, технологій «м'якої сили». Під ними розуміється сукупність інституційних, проектно-ідеологічних, міжнародно-правових, організаційних, фінансових, інформаційно-пропагандистських, розвідувальних та інших механізмів проектування, алгоритмізації, реалізації, забезпечення та контролю процесів дисфункціоналізації, дискредитації або тотальної руйнації іншої суверенної держави (держави-об'єкта) з метою трансформації цієї держави в неспроможну, що веде до повного її знищення у межах колишньої території або примусової її трансформації у субмісивні форми з редукованим або повністю втраченим суверенітетом, а також для досягнення інших цілей на користь держави-актора. З'ясовано, що застосування «м'якої сили» завжди передбачає агресивні дії противника, зокрема, інформаційного характеру. На цій підставі застосування інструментів «м'якої сили» обґрунтовано інтерпретувати як здійснення щодо держави-об'єкта (держави-мішені) неоголошеної гібридної війни, як-то відбувається по відношенню до України. Аргументовано визначення заходів з випередження негативного

впливу держави-актора на державу-об'єкт шляхом застосування ризик-орієнтованих підходів. Виявлено, що вони активно впроваджується як в економічно розвинених державах (наприклад, у Франції), так і в тих країнах, що тільки стали на шлях забезпечення сталого розвитку (Казахстан). Для обох цих країн характерним є впровадження ризико-орієнтованих підходів в інституційну систему публічного управління, що відображається в ключових правових документах стратегічного планування. Зважаючи на це й інтеграційні прагнення України, рекомендовано здійснити на її теренах проектування інструментів ризик-орієнтованого публічного управління в умовах інформаційно-гібридної війни з урахуванням позитивно верифікованої багаторічної закордонної практики реагування на інструменти «м'якої сили».

6. Обґрунтовано ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, у межах яких (підходів) визначено сценарії реагування на зазначений види війни. Серед цих сценаріїв виокремлені такі: 1) проактивний, який рекомендовано реалізовувати під час стратегічного планування та поступального забезпечення сталого розвитку, що вимагає, у свою чергу, удосконалення стратегії сталого розвитку України; 2) реактивний сценарій, що на відміну від попереднього, передбачає оперативне реагування на інформаційні загрози. У цьому контексті доведена необхідність у розробці та прийнятті концепції протидії інформаційним загрозам та інформаційно-гібридній війні, у якій (концепції) рекомендовано закріпити на рівні правової норми визначення такому виду війни, що наразі відсутнє.

7. Запропоновано шляхи розвитку інституційної системи публічного управління України в умовах інформаційно-гібридних війн, що передбачають, по-перше, створення вітчизняної інформаційної контргібридної пропагандистської структури, на зразок, Бюро протидії гібридній війні, яке функціонує в США та напрацювало дієві управлінські

практики реагування на інформаційні загрози. По-друге, налагодження результативної взаємодії України з іншими міжнародними організаціями в напрямку вчасного визначення та протистояння цим загрозам. Серед таких організацій визначено Європейський центр із протидії гібридним загрозам, Парламентську Асамблею Ради Європи, Центр передового досвіду стратегічних комунікацій (StratCom) та ін. По-третє, доведена необхідність щодо реалізації заходів щодо належного забезпечення інформаційної безпеки України й іншими публічними інституціями – НУО та НКО, що мають залучатися до реального формування та контролю за державною інформаційною політикою. Крім того, що розвиток вітчизняної інституційної системи публічного управління в умовах інформаційно-гібридних війнах має бути забезпечений шляхом створення Державного унітарного підприємства «Центр технічного захисту інформації, сертифікації та експертизи».

8. Визначено концептуальні засади щодо прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління на пострадянському і вітчизняному просторі. Доведено, що на сучасному етапі його розвитку на ці інституційні механізми публічного управління впливають зовнішні та внутрішні фактори, які можуть, у свою чергу, становити підґрунтя для виникнення та посилення інформаційно-гібридної війни. Серед цих факторів загрозливими визнано такі: 1) політичні, що зумовлені багатовекторною й ізольованою політикою країни; 2) економічні, що виникають через «митні», «санкційні» та інші аналогічні війни, що ведеться проти конкретно взятої держави; 3) соціальні, що пов’язані з посиленням міграційних процесів (вимушеного виїзду громадян до інших країн), а, відтак, зростанням рівня безробіття, зниженням добробуту та демографічних показників тощо. На цій підставі уточнено комплекс заходів, що слід реалізовувати в межах досліджених інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, що ведеться проти неї.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Авер'янова Н.М. Гібридна війна: російсько-українське протистояння // Молодий вчений. 2017. № 3 (43). С. 30–34.

2. Авер'янова Н.М., Воропаєва Т.С. Міждержавний збройний конфлікт на теренах України: неоколоніальний вимір // Гілея. 2019. Вип. 145 (№ 6), ч. 2. С. 7–11.

3. Андрєєва О., Мусієнко К. Кіберзброя та аналіз її деструктивної діяльності на прикладі впливу вірусу нового покоління Stuxnet на іранську ядерну програму // Актуальні проблеми міжнародних відносин. 2011. Вип. 103(1). С. 29–34.

4. Антонова Н.Б., Захарова Л.М., Вечір Л.С. Теорія та методологія державного управління: курс лекцій. 2005. 231 с.

5. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці // Державне управління: удосконалення та розвиток. Вип. 8(10). 2014. С. 1–5.

6. Барабаш В.В. Соціальні технології: світовий досвід та тенденції розвитку в Україні : монографія. Херсон, Вид-во: ПП Вишемиський В.С., 2008. 340 с.

7. Бартош А.А. «Тертя» гібридної війни // Військова думка. 2018. № 1. С. 513.

8. Белл Д. Прихід постіндустріального суспільства // Сучасна зарубіжна соціальна філософія. Хрестоматія. Київ : Либідь, 1996.С. 194–250.

9. Белл Деніел Прихід постіндустріального суспільства // Сучасна зарубіжна соціальна філософія. 1996. С. 194–251.

10. Березовська І. Р., Русак Д. М. Державна інформаційна політика та основні напрями її вдосконалення // Міжнародні відносини. Серія «Економічні науки». Вип. 4. 2014. URL: http://journals.iir.kiev.ua/index.php/ec_n/article/view/2488.

11. Бабков Ю.П., Бєлай С.В., Бондаренко О.Г. Підходи до запровадження елементів національної системи стійкості у діяльність органів державного і військового управління // Честь і закон. 2023. № 3 (86). С. 12–20.

12. Бєлай С.В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія. Харків: Національна акад. НГУ, 2015. 349 с.

13. Бжезінський З. Велика шахівниця / пер. з англ. О. Фешовець. Харків :Ранок ; Фабула, 2019. 288 с.

14. Бучин М., Курус Ю. Інформаційна війна та її особливості на сучасному етапі // Політичні науки. 2018. № 2. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/jan/15398/buchinstattya422018.pdf.

15. Валюшко І. Еволюція інформаційних війн: історія і сучасність. Історико-політичні студії. Серія: Політичні науки. 2015. № 2. С. 127–134.

16. Великанова М.М. Ризик у правові доктрині: підходи до визначення сутності // Проблеми цивільного права та процесу. 2017. С. 159-162. URL: https://univd.edu.ua/general/publishing/konf/19-20_05_2017/pdf/47.pdf.

17. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ ;Ірпінь: ВТФ «Перун», 2001. 1440 с.

18. Вєдєнєєв Д. В., Семенюк О. Г. Розвиток концептуальних і науково-практичних поглядів на сутність еконвенційної (гібридної) конфліктності :монографія. Київ : ТОВ «Вид. дім «АртЕк» 2021. 228 с.

19. Вєдєнєєв Д., Сегеда С. Історико-теоретичні витоки поглядів на сутність війн (конфліктів) неконвенційного концептуального типу (1970-і – початок 2000-х рр.) // Воєнно-історичний вісник. 2022. № 1. С. 161–181. https://doi.org/10.33099/2707-1383-2022-43-1-161-181.

20. Вєдєнєєв Д.В., Семенюк О.Г. Розвиток концептуальних поглядів на особливості «гібридних» війн в євроатлантичному воєнно-політичному просторі // Юридичний науковий електронний журнал. 2022. № 8. С. 25–29. https://doi.org/10.32782/2524-0374/2022-6/11.

21. Війна «гібридна» // Політологічний енциклопедичний словник / уклад. : Л. Герасіна, В. Погрібна та ін. ; за ред. проф. М. П. Требіна. Харків : Право, 2015. 816 с.

22. Військово-морські сили Китайської Народної Республіки. URL: https://uk.wikipedia.org/wiki/.

23. Воєнний стан: : спроба відповідей на спірні питання. URL: https://ips.ligazakon.net/document/EA012217#:~:text=%D0%92%D1%96%D0%B4%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%BD%D0%BE%20%D0%B4%D0%BE%20%D0%A0%D0%B5%D0%B7%D0%BE%D0%BB%D1%8E%D1%86%D1%96%D1%97%203314%20(%D0%A5%D0%A5I%D0%A5,%D1%87%D0%B8%D0%BD%D0%BE%D0%BC%2C%20%D0%BD%D0%B5%D1%81%D1%83%D0%BC%D1%96%D1%81%D0%BD%D0%B8%D0%BC%20%D1%96%D0%B7%20%D0%A1%D1%82%D0%B0%D1%82%D1%83%D1%82%D0%BE%D0%BC%20%D0%9E%D0%9E%D0%9D.

24. Воропаєва Т.С. Гуманітарна й інформаційно-психологічна безпека як чинник зміцнення обороноздатності України // Комунікаційно-контентна безпека в умовах гібридно-месіанських агресій Путінської Росії : тезидоп. Міжнар. форуму з кризових / за заг. редакцією В.В. Балабіна. Київ : ВІКНУ. 2016. С. 63–67.

25. Воропаєва Т.С. Національна безпека України: етнопсихологічні аспекти // Проблеми безпеки української нації на порозі XXI ст. 1998. С. 156–158.

26. Воропаєва Т.С. Національна ідентичність громадян України в контексті інформаційної безпеки // Людинознавчі студії. 2009. Т. 20. С. 16–35.

27. Ганус С.О. Українська фігура на «Великій шахівниці» (Збігнєв Бзежинський про сучасне геополітичне становище України) // Науковий вісник УжДУ. Серія: Історія. 2000. № 5. С. 175–187.

28. Геєць В. Куди пливти українському кораблю? // Політика і час. 1995. № 6. С. 62.

29. Гетьманчук М. «Гібридна війна» Росії проти України: інформаційний аспект. URL: http://www.asv.gov.ua.

30. Гиря Г.В. «Кольорові революції» їх сутність та вплив на еволюцію політичних систем на прикладі України та Грузії. URL: http://visnyk-psp.kpi.ua/article/view/32227.

31. Гібридна війна Російської Федерації на Балканах : суспільно-політичне видання. Ч. 2: Сучасні напрями гібридної війни Російської Федерації у балканському регіоні / Д. Ю. Золотухін, В. М. Гребенюк, О. Ю. Іванов. Київ :НА СБУ, 2020. 260 с.

32. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення // Вісник НАДУ. 2015. Вип. № 1. С. 136–141.

33. Горбулін В. Як перемогти Росію у війни майбутнього. К.: Вид-во Брайт Букс. 2020. 256 с.

34. Гребенюк А. В. Антиукраїнська пропаганда: актуальні проблеми визначення поняття та риси // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (м. Київ, 26 берез. 2021 р.). Київ : Нац. акад. СБУ, 2021. С. 24–26.

35. Дементьєва К.В. Інформаційна війна та соціальна відповідальність // Журналістський щорічник. 2014. URL: https:// cyber/article/v/informatsionnaya-voyna-i-sotsialnaya-otvetstvennost-zhurnalistov.

36. Денисенко І. Сучасні війни: нові підходи та інтерпретації. Вісник Харківського національного університету імені В.Н. Каразіна. Серія: «Питання політології». 2008. Вип. 12, № 810. С. 212–218.

37. Денисов В.Н. Агресія військова // Велика українська

енциклопедія. URL: https://vue.gov.ua/Агресія військова.

38. Деструктивізм // Вікіпедія: вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/.

39. Дідківська Л.І., Головко Л.С. Державне регулювання економіки : навч. посіб. К. : Знання-Прес, 2000. 209 с.

40. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави. 2015. Вип. 3 (19). С. 6-17.

41. ДОДАТОК XVII – Нормативно-правове наближення. URL: https://eu-ua.kmu.gov.ua/tekst-uhody-pro-asotsiatsiiu/dodatky-iv-rozdil/normatyvno-pravove-nablyzhennia.

42. Домбровська С.М., Помаза-Пономаренко А.Л., Лукиша Р.Т. Інституціональна державна політика соціально-економічного розвитку регіонів України в умовах ризиків: монографія. Харків: НУЦЗ України, 2018. 216 с.

43. Дорошенко А. С. Гібридна війна в інформаційному суспільстві // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». 2015. № 2 (25). С.21–28.

44. Друкер П. Виклики для менеджменту XXI століття. Київ :КМ-БУКС, 2020. 240 с.

45. Еволюція воєнного мистецтва: навчальний посібник. У 2 ч. Ч. 1. Київ. 2017. URL: https://shron3.chtyvo.org.ua/Viedienieiev_Dmytro/Evoliutsiia_voiennoho_mystetstva_U_2_ch_Ch_1.pdf?PHPSESSID=p68bmuj1tqjeh40je4buj69nh6.

46. Енциклопедичний словник з державного управління / [укл. Ю.П. Сурмін, В.Д. Бакуменко, А.М. Михненко та ін.] за ред. Ю.В. Ковбасюка, Ю.П. Сурміна. К.: НАДУ, 2010. 820 с.

47. Європейський Союз у міжнародних відносинах : навч. посіб. / за ред. В. В. Копійки. Київ : ВПЦ «Київський університет», 2021.

560 с.

48. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище // Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2020. Вип. 2 (26). С. 56–61. https://doi.org/10.23939/law2020.26.056.

49. Зайцев В. В. Суб'єкти забезпечення інформаційної безпеки України // Форум права. Вип. 3. 2013. С. 231-238.

50. Зубарєва М. А. Аналіз інформаційної війни між Росією та Україною в інформаційному суспільстві // Інформаційне суспільство. 2015. Вип. 21. С. 6–11.

51. Ідеологічне та квазіправове обґрунтування Російською Федерацією анексії Автономної Республіки Крим / упоряд. : О. Ф. Бєлов, С. С. Кудінов, В. М. Гребенюк та ін. Київ : Нац. акад. СБУ, 2017. 284 с.

52. Іжутова І. Мартін Лібікі: Що таке інформаційна війна? // Військо України. 2014. URL: http://viysko.com.ua/texnologiji-voyen/martin-libiki-shho-take-informacijna-vijna/.

53. Іщук С. М. Інтернет-комунікації: інформаційний зміст та ігровий характер // Вісник Національного авіаційного університету. 2008. № 2. С. 87–91.

54. Кастельс М. Інтернет-галактика. Міркування щодо Інтернету, бізнесу і суспільства / пер. з англ. Київ : Ваклер, 2007. 304 с.

55. Кислова О. М., Берднік К. О. Нові медіа як комунікативні технології XXI століття: наслідки мережевізації та інтелектуалізації комунікацій // Соціальні технології: зарадичого? Яким чином? З яким результатом? : монографія / за ред. В. І. Подшивалкіна. Одеса :Одеський національний університет імені І. І. Мечнікова, 2015. С. 277–288.

56. Кіберкомандування США. URL: https://uk.wikipedia.org/wiki.

57. Кіберполіція. Кібербезпека України. URL: https://wiki.legalaid.gov.ua/index.php.

58. Кіршенблат С.В. Досвід використання моделі «кольорових революцій» у посткомуністичних регіонах // Політологічні та соціологічні студії. Збірник наукових праць. 2010. № 50 Т. IX. С. 463–474.

59. Кіца М. Особливості реклами в українських Інтернет-ЗМІ в умовах інформаційної війни // Теле- та радіожурналістика. 2015. Вип. 14. С. 170–174.

60. Колективна оборона – Стаття 5. URL: https://www.nato.int/cps/uk/natohq/topics_110496.htm.

61. Комітет з питань інформатизації та зв'язку. URL: http://komit.rada.gov.ua/.

62. Кондратюк М.О. Інформаційнавійна та роль мас-медіа в міжнароднихконфліктах // Вісник Харківської державної академії культури. 2013. Вип. 41. С. 1–6. URL: http://www.ic.ac.kharkov.ua/RIO/v41/15.pdf.

63. Корабльова В. Медіаконструювання соціальної реальності: ідеологічний ракурс // Гуманістичний часопис. 2012. № 4. URL: https://khai. edu.

64. Короход Я.Д. Інформаційно-психологічні війни – зброя XXI // Актуальні проблеми політики. 2013. Вип. 50. С. 299–307.

65. Кравченко В.Ю. Теорія «гібридної війни»: український вимір // Вісник Дніпропетровського університету. Сер. Політологія. 2015. № 2. URL: http://repo.dma.dp.ua.

66. Крюков О.І., Шкурат І.В. Методологія дослідження та механізми формування еліти в умовах глобалізації // Публічне управління: теорія та практика. 2013. Вип. 2. С. 71-77.

67. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. посіб. Київ: ВІКНУ, 2016. 286 с. URL: http://www.mil.univ. kiev.ua/files/222_1044284240.pdf.

68. Курбан О. В. Сучасні інформаційні війни в соціальних онлайн-мережах // Інформаційне суспільство. 2016. Вип. 23. С. 85–90.

69. Лизанчук В. Посилюймо інформаційно-психологічну безпеку в умовах гібридної війни Росії проти України. URL: http://journ.lnu.edu.ua.

70. Лисецький Ю.М., Старовойтенко О.О., Семенюк Ю.В., Павленко Д.Г. Гібридні війни. Компоненти та особливості. URL: http://www.pubadm.vernadskyjournals.in.ua/journals/2021/5_2021/13.pdf.

71. Лісничук О. Гантінґтон (Huntington) Самуель Філіпс // Політична енциклопедія / редкол. : Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. Київ : Парлам. вид-во, 2011. С. 128.

72. Магда Є.В. Виклики гібридної війни: інформаційний вимір. Наукові записки Інституту законодавства Верховної Ради України. 2014. № 5. С. 138–142.

73. Магда Є.В. Гібридна війна: вижити та перемогти. Харків : Віват. 2015. 320 с.

74. Манойло А. В. Інформаційно-психологічна війна як засіб досягнення політичних цілей. URL: http://www.azerilove.net/ articles/85/1/.

75. Маронкова Б. НАТО в новому середовищі гібридної війни // Пропаганда.UA: Ukraine Analytica. 2018. Вип. 1(11), С. 3–10.

76. Маршалл Мак-Люен. Галактика Ґутенберґа: становлення людини друкованої книги / пер. з англ. А. А. Галушки, В. І. Постнікова. Київ: Ніка-Центр, 2015. 388 с. (Серія «Зміна парадигми»).

77. Масуда Й. Комп’ютопія / пер. з англ. В. Ляха // Філософська і соціологічна думка. 1993. № 6. С. 36–50.

78. Мельтюхова Н.М., Набока Л.В. Реалізація державно-управлінських відносин на регіональному рівні: монографія. Х.: Вид-во ХарРІ НАДУ «Магістр», 2014. 180 с.

79. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві. ЮСТІНІАН. 2009. URL: http://www.justinian.com.ua/article.php?id=3233.

80. Месснер Євгеній Едуардович / П.П. Гай-Нижник // Енциклопедія Сучасної України / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. К. : Інститут енциклопедичних досліджень НАН України, 2018. URL: https://esu.com.ua/article-66638.

81. Методичні рекомендації щодо проведення ґендерно-правової експертизи проектів нормативно-правових актів. URL: https://gender.org.ua/images/lib/metodychni_rekomendacii_sho.pdf.

82. Миколайчук І.А. Про сутність гібридної війни у контексті сучасної військовополітичної ситуації // Проблеми національної стратегії, 2016. № 3(36). С. 85–104.

83. Мороз С.А. Досвід Китаю у забезпеченні розвитку галузі освіти як підґрунтя для вдосконалення механізмів державного управління якістю вищої освіти України // Інвестиції: практика та досвід. 2019. URL: http://www.investplan.com.ua/?op=1&z=6658&i=11.

84. Най Дж. Гнучка влада: як досягти успіху у світовій політиці. 2006. 221 с. URL: https://stud.com.ua/55474/filosofiya/perevagi_gnuchkoyi_vladi_informatsiynomu_suspilstvi.

85. Наступ Талібану. URL: https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%81%D1%82%D1%83%D0%BF_%D0%A2%D0%B0%D0%BB%D1%96%D0%B1%D0%B0%D0%BD%D1%83_(2021).

86. НАТО на саміті у Вільнюсі має надати Україні гарантії безпеки – Расмуссен. URL: https://www.ukrinform.ua/rubric-polytics/3709436-nato-na-samiti-u-vilnusi-mae-nadati-ukraini-garantii-bezpeki-rasmussen.html.

87. Негодченко В. О. Адміністративно-правове забезпечення державної інформаційної політики органами Національної поліції України : автореф. дис. ... д-ра юрид. наук : 12.00.07 / МВС України, Харк. нац. ун-т внутр. справ. Харків, 2017. 40 с.

88. Новіков В.О. Аналіз сучасної концепції інформаційно-гібридної війни // Державне управління: удосконалення та розвиток: електронний журнал. 2023. № 9. URL: https://www.nayka.com.ua/index.php/dy/article/view/2133.

89. Новіков В.О. Дисфукнціоналізація інституційної системи та механізмів публічного управління в умовах інформаційно-гібридних війн // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2020. Вип. 2 (13). С. 345–354. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18688/1/vdu13.pdf.

90. Новіков В.О. Ризик-орієнтований підхід до формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн: досвід Франції, Казахстану й України // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2020. Вип. 1 (12). С. 300–308.

91. Новіков В.О. Information and hybrid wars in the current environment: public-administrative aspect // Public administration and state security aspects. 2023. Vol. 2. P. 43–51.

92. Новіков В.О. Theoretical and institutional features of the modern definition of the concept of hybrid war // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2023. Вип. 2 (19). С. 207–212.

93. Олещук П. М. Новітні політичні технології інформаційного впливу : монографія. Київ : Видавець Вадим Карпенко, 2018. 288 с.

94. Олійник О.В. Структура суб’єктів забезпечення інформаційної безпеки в Україні // Актуальні проблеми держави і права. Вип. 68. 2016. С. 485-491.

95. Ортіна Г.В. Складові антикризового управління підприємницької діяльності з системних позицій // Ефективна економіка. 2017. Вип. 1. URL: http://www.economy.nayka.com.ua/?op=1&z=5466.

96. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

97. Офіційний веб-сайт Державної служби статистики України. URL: https://www.ukrstat.gov.ua/.

98. Перцефф Д.Ж. Нарковойни XXI століття. Зброя масового ураження. URL: https://libking.com/books/nonf-/nonf-publicism/201704-24-den-pertseff-narkovoyny-xxi-veka-oruzhie-massovogo-porazheniya.html#book.

99. Петренко О.С. Інтернет як субпростір суспільства: структури та процеси: дис. ... канд. соціол. наук. Старобільськ, 2017. URL: http://dissertations.

100. Пилипчук В.Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми: матеріали наук.-практ. конф. / 06 жовт. 2016 р. / Упоряд.: В.М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка». 2016. С. 24-28.

101. Повний текст резолюції ПАРЄ, ухваленої державами-членами для спільної протидії гібридним загрозам і війні. URL: https://www.ukrinform.ua/rubric-polytics/2452506-ci-e-pravila-dla-gibridnoi-vijni-rezolucia-pare.html.

102. Помаза-Пономаренко А.Л. 53 Munich Security Report: нові акценти у формуванні соціальної безпеки // Вісник Національного університету цивільного захисту України. Серія: Державне управління». 2017. № 1 (6). С. 42–48.

103. Помаза-Пономаренко А.Л., Новіков В.О. Шляхи трансформації інституційних механізмів публічного управління в Україні: від інформаційних загроз до гібридних війн // Державне будівництво. 2023. № 2. URL: https://periodicals.karazin.ua/db/issue/archive.

104. Попович К.В. Гібридна війна як сучасний спосіб ведення війни: історичний та сучасний виміри // Науковий вісник Ужгородського університету. Сер. Історія. 2016. Вип. 2 (35). URL: http://dspace.uzhnu.edu.ua.

105. Почепцов Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ: ВД «Києво-Могилянська академія», 2017. 260 с.

106. Почепцов Г.Г. Смислові та інформаційні війни // Інформаційне суспільство. 2013. Вип. 18. С. 21–27.

107. Почепцов Г. Смислові та інформаційні війни: пошук відмінностей. Media Sapiens. URL: http://osvita.mediasapiens.ua/ ethics/manipulation/smislovi_ta_informats iyni_viyni_poshuk_vidminnostey/.

108. Почепцов Г. Сучасні інформаційні війни. Вид. 2-е, допов. Київ : Києво-Могилянська академія, 2016. 504 с.

109. Прав Р.Ю. Діяльність суб'єктів формування і реалізації політики державної безпеки в інформаційній сфері України. URL: http://www.dy.nayka.com.ua/pdf/9_2018/103.pdf.

110. Прийнято закон «Про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції)». URL: https://www.rada.gov.ua/print/220177.html.

111. Про біологічну безпеку : рішення РНБО України 2009 р. URL: https://zakon.rada.gov.ua/laws/show/n0003525-09#Text.

112. Про затвердження Методичних рекомендацій щодо оцінки впливу нормативно-правових актів та проектів актів на конкуренцію // Антимонопольний комітет України. URL: https://zakon.rada.gov.ua/rada/show/v0117226-17#Text.

113. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Указ Президента України 47/2017, поточна редакція від 25.02.2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017/.

114. Проект закону України «Про державне стратегічне планування» // Міністерство економіки України. URL:

https://me.gov.ua/Documents/Detail?lang=uk-UA&id=e7b8af7a-7c03-4d5b-aaa5-e1c0d7e84388&title=ProektZakonuUkrainiproDerzhavneStrategichnePlanuvannia.

115. Проект закону України «Про державне стратегічне планування» // Міністерство економіки України. URL: https://me.gov.ua/Documents/Detail?lang=uk-UA&id=e7b8af7a-7c03-4d5b-aaa5-e1c0d7e84388&title=ProektZakonuUkrainiproDerzhavneStrategichnePlanuvannia.

116. Проект Концепції інформаційної безпеки України. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf.

117. Психотип «геніальності» та медіапростір мета модерну // Українська школа архетипіки. URL: https://usarch.org/%D0%BF%D1%80%D0%BE-%D1%81%D0%B0%D0%BC%D0%BE%D0%B4%D0%BE%D1%81%D1%82%D0%B0%D1%82%D0%BE%D1%87%D0%BD%D1%8B%D1%85-%D1%83%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%86%D0%B5%D0%B2-%D0%BF%D1%81%D0%B8%D1%85%D0%BE/#/.

118. Пулим О.В. Антиправова, антигуманна сутність гібридної війни Росії проти України та її соціальні наслідки // Науковий вісник Львівського державного університету внутрішніх справ. Сер. Юридичні науки. 2016. Вип. 2. URL: http://journal.lvduvs.edu.ua.

119. Рада національної безпеки і оборони України. URL: https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D0%B0_%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D1%96_%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8.

120. Ремез О. Астротурфінг – інструмент віртуальної маніпуляції та реальна загроза цивільній безпеці України. URL: http://www.jurnaluljuridic.in.ua/archive/2020/2/3.pdf.

121. Романюк О. Посткомуністичні революції // Політичний менеджмент. 2005. № 4. С. 16–28.

122. Рущенко І.П. Підривні соціальні технології у структурі гібридної війни // Право і безпека. 2015. № 2. URL: http://oaji.net/articles.

123. Рущенко І.П. Російсько-українська гібридна війна: погляд соціолога: монографія. Харків: ФОП Павленко О. Г., 2015. 268 с.

124. Рущенко І.П., Рущенко Ю.І. Гібридна агресія та громадянський спротив у Харкові 2014 р.: уроки першої фази російсько-української війни // Український соціум. 2016. № 3(58). URL: http://www.ukr-socium.org.ua.

125. Саприкін О. В. Інтернет-ресурси як інструмент інформаційної війни й інформаційна безпека України // Бібліотекознавство. Документознавство. Інформологія. 2015. № 2. С. 72–77.

126. Сасин Г. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір) // Грані. 2015. № 3. С. 18–23. URL: http://nbuv.gov.ua/j-pdf/Grani_2015_3_5.pdf.

127. Світова гібридна війна: український фронт / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.

128. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с.

129. Семен Н. Ф. Поняття «інформаційна війна» в контексті соціальних комунікацій // Держава та регіони: Серія: Соціальні комунікації. 2016. № 1 (25). С. 22–25.

130. Семен Н.Ф. Засоби протидії інформаційній агресії в українському інтернет-просторі // Перспективні напрямки дослідження українського медійного контенту: фундаментальні та прикладні аспекти : матеріали Всеукр. наук.-практ.конф. (м. Київ, 7 квіт. 2016 р.). Київ:Інститут журналістики. 2016. С. 231–234.

131. Ситник Г.П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади) : підручник. Київ: НАДУ, 2012. 544 с.

132. Сіньцзян-Уйгурський автономний район. URL: https://uk.wikipedia.org/wiki/%D0%A1%D1%96%D0%BD%D1%8C%D1%86%D0%B7%D1%8F%D0%BD-%D0%A3%D0%B9%D0%B3%D1%83%D1%80%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_%D0%B0%D0%B2%D1%82%D0%BE%D0%BD%D0%BE%D0%BC%D0%BD%D0%B8%D0%B9_%D1%80%D0%B0%D0%B9%D0%BE%D0%BD.

133. Слюсаренко А.В. Новітні форми міждержавного протистояння як предмет дослідження сучасної воєнно-наукової думки // Військово-науковий вісник. 2015. Вип. 24. С. 173–186.

134. Смола Л.Є. Аспекти ведення інформаційної та гібридної війни в контексті застосування комунікаційних технологій. S.P.A.C.E. 2016. № 1. С. 48–53.

135. Смольц С.П. Інформаційна війна як чинник формування суспільного бутя // Вісник Національного технічного університету України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка. 2011. № 3. С. 70–74.

136. Стоєцький О. Суб’єкти забезпечення інформаційної безпеки України: адміністративно-правові засади. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/15824/39-Stoyetsky.pdf?sequence=1#:~:text96.

137. Стратегія інформаційної безпеки : рішення Ради національної безпеки і оборони України від 15.10.2021 р. URL: https://zakon.rada.gov.ua/laws/show/685/2021?find=1&text=%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD#w1_1.

138. Стрельбіцька Н. Уніфікований міжнародний стандарт ризик-

менеджменту як відповідь на виклики глобалізації // Соціально-економічні проблеми і держава. 2011. Вип. 2 (5). URL: http://sepd.tntu.edu.ua/images/stories/pdf/2011/11snynvh.pdf.

139. Сунь-дзи. Мистецтво війни / під ред. Т. Клірі. Софія, 2018. 224 с.

140. Ткаченко В.М., Дорошенко Н.С. «Гібридна війна»: політичні наслідки // Наукові записки Інституту політичних й етнонаціональних досліджень ім. І.Ф. Кураса НАН України. 2015. Вип. № 1. С. 58–69.

141. Тоффлер Е. Нова парадигма влади. Знання, багатство й сила. Харків: Акта. 2003.

142. Тоффлер Елвін. Третя хвиля / пер. А. Євса ; за ред. В. Шовкуна. Київ : Вид. дім «Всесвіт», 2000. 480 с.

143. Требін М.П. Феномен «гібридної» війни // Гілея: наук. вісн. 2014. Вип. 87. С. 366-371. URL: http://irbis-nbuv.gov.ua.

144. Требін М.П. Феномен інформаційної війни у світі, що глобалізується. Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. Серія: Філософія, філософія права, політологія, соціологія // Право. 2013. № 2 (16). С. 188–198.

145. Требін М.П. Феномен інформаційної війни у світі, що глобалізується // Вісник Національної юридичної академії України імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. 2013. № 2. С. 188–198.

146. Троцюк М. М. Політичні режими України та Грузії після «кольорових революцій» // Студентські наукові записки. Серія «Соціально-політичні науки». 2011. Вип. 3. URL: http://eprints.oa.edu.ua/id/eprint/868.

147. Угода між Російською Федерацією та Україною про параметри поділу Чорноморського флоту від 28 травня 1997 р. URL: http://docs.cntd.ru/document/1902222.

148. Україна очолила рейтинг країн, що піддаються кібератакам з

боку інших держав. URL: https://weukraine.tv/novyny/ukrayina-ocholyla-rejtyng-krayin-shho-piddayutsya-kiberatakam-z-boku-inshyh-derzhav/.

149. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукр. наук.-практ. конф. (м. Маріуполь, 9 черв. 2017 р.). Маріуполь: ДонДУУ, 2017. 311 с. URL: https://www.google.com.ua.

150. Федченко Д. І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності // Молодий вчений. Вип. 5 (57). 2017. с. 653-658.

151. Феськов І.В. Прояви гібридної агресії на масовокомунікаційному рівні Вісник Книжкової палати. 2016. № 11. URL: https://www.irbis-nbuv.gov.ua.

152. Феськов І.В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві // Актуальні проблеми політики. 2016. Вип. 58. С. 66–76.

153. Фісенко Т. Прояви гібридної агресії на массово-комунікаційному рівні // Вісник Книжкової палати. 2016. № 11. URL: https://www.irbis-nbuv. gov.ua.

154. Хакерську атаку на сайти українських відомств здійснили з Росії – урядові експерти. URL: https://www.epravda.com.ua/news/2022/01/14/681443/.

155. Чекаленко Л. Про поняття «гібридна війна» // Віче. 2015. № 5. С. 41-42. URL: http://www.irbis-nbuv.gov.ua.

156. Чиж І. Теорія масових комунікацій Герберта Маршалла Маклюена: Проекція на сучасні тенденції суспільного розвитку // Слова Просвіти. 07.11.2018. URL: http://slovoprosvity.org/2018/11/07/teoriya-masovyh-komunikatsij-herberta-marshalla-maklyuena-proektsiya-na-suchasni-tendentsiji-suspilnoho-rozvytku/.

157. Чистоклетов Л. Г., Шишко В. Й. Інформаційно-психологічні

впливи як невід'ємна складова парадигми інформаційної безпеки // Науковий вісник Львівського державного університету внутрішніх справ. 2012. С. 183–192.

158. Чухліб Т. Батько «психологічних війн». Газета "День". 2004. URL: http://day.kyiv.ua/uk/article/ ukrayina-incognita/batko-psihologichnih-viyn.

159. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення // Вип. 2 (28). 2012. С. 299-309.

160. Шпига П., Рудник Р. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. № 8. С. 326–339.

161. Щепанський Е.В. Public Management of Socio-Economic Risks: A Paradigm of Essential Organizational Aspects in the Conditions of Digitalization. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/28224/1/011-044-047.pdf.

162. Яровий Т.С. Концептуальні засади лобіювання як інструмент реалізації цілей державної безпеки // Інвестиції: практика та досвід. 2020. № 2. С. 99–103.

163. 4internationalmedia&newspapers. 2019 Newspaper web rankings. Top 200 Newspapers in the World // 4internationalmedia&newspapers. URL: https://www.4imn.com/top200/.

164. Aménagement du territoire et gestion des risques. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000023459558.

165. Brahm H. The desintegration Soviet Union and Europe// Aussenpolitik.- Hamburg, 1992. Vol. 43. № 1. P. 43-44.

166. Brehmer B., N.E. Sahlin Future Risks and Risk Management (Risk, Governance and Society, 9). 1994. Springer. 270 p.

167. Brzezinski Z. Ideology and Power in Soviet Politics. New-York, 1962. P. 161

168. Caryl C. If You Want to See Russian Information Warfare at its Worst, Visit These Countries. URL: https://www. washingtonpost.com/news/democracy-post/wp/2017/04/05/if-you-want-to-see-russian-information-warfare-at-its-worst-visit-these-countries/?noredirect=on&utm_term=.4b778df7877f.

169. Clarke A., Knake R. Cyber War. 2010. New York: Harper Collins Publishers.

170. Cyberwar. The Economist. URL: http://www.economist.com/node/16481504?story_id=16481504 &source= features_box1.

171. Daily movement news and resources. US Spent $4.2M in 2015 to De-stabilize Venezuelan Government. April 9, 2017. URL: https://popularresistance.org/us-spent-4-2m-in-2015-to-destabilize-venezuelan-government.

172. Denning D. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Nautilus Institute for security and sustainability. 1999. URL: http://nautilus.org/global-problem-solving/ activism-hacktivism-and-cyberterrorism-the-internet-as-a-toolfor-influencing-foreign-policy-2/.

173. Edelstein A. Total propaganda. From mass culture to popular culture. 1997. New York: Lawrence Erlbaum Associates.

174. European Centre of Excellence for Countering Hybrid Threats. URL: hybridcoe.fi.

175. Expertology. «10 most reading countries in the world» // Expertology. URL: https://expertology/10-samykhchitayushchikh-stran-mira/.

176. Federal Register Executive order 13925 of May 28, 2020. Preventing online sponsorship // Federal Register. URL: https://www.federalregister.gov/documents/2020/06/02/2020-12030/preventing-online-censorship.

177. FM 3-05.130. Army Special Operations Forces Unconventional Warfare, Washington, Department of the Army. URL: https://fas.org/irp/doddir/army/fm3-05-130.pdf.

178. Forest, J.J.F., ed. Influence Warfare. How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas. Westport, Conn: Praeger Security International, 2009. 236 p.

179. GiegerichBastian.Hybrid Warfare and the Changing Character of Conflict. Connections, Vol. 15, No. 2 (Spring 2016), pp. 65–72. URL: https://www.jstor.org/stable/26326440.

180. Gray C. Geopolitics of the Nuclear Era: Hartland, Rimland and the Technological Revolutiorn. New-York, 1977. P. 5.

181. Hoffman F. Conflict in the 21th Century: the Rise of Hybrid Wars. URL: http://www.projectwhitehorse.com/pdfs/ HybridWar_0108.pdf.

182. Hoffman Frank G. Future Thoughts on Hybrid Threats. Small Wars Journal. 2009. URL: https://www.smallwarsjournal.com.

183. Human Rights Watch. URL: https://www.hrw.org/.

184. Hybrid warfare resistance Bureau. URL: https://www.facebook.com/hwrbureau/photos/?paipv=0&eav=AfZ1luyEvu_kAvZNXIWp1PahZpxzfJCll_Jy8t7nv9-hKs69ShFNRci8qMwETE6MV-o&_rdr.

185. Hybrid Warfare. Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities. Committeeon Armed Services, Houseof Representatives. September 10, 2010. URL: https://www.gao.gov/assets/100/97053.pdf.

186. Irregular Warfare. Joint Operating Concept. Washington, Department of Defense, 2007. URL: https://www.globalsecurity.org/military/library/policy/dod/iw-joc_v1_2007.pdf.

187. Islamic State Hacking Division. URL: https://en.wikipedia.org/wiki/Islamic_State_Hacking_Division/

188. Kahn Herman. The Coming Boom: Economic, Political, and

Social.Hutchinson : Simon&Schuster, 1983. 268 p.

189. Lawrence T. Greenberg, Seymur E. Goodman, Kevin J. Soo Hoo. Information Warfare and International Law. National Defense University Press, 1998. 476 p.

190. Luttwak E.N. Coup d'État: A Practical Handbook. Harvard University Press, Cambridge, Massachusetts, London, England, 1979. 728 p.

191. MacKinder H. J. Demokratic Ideas and Reality. New-York, 1962. 150 p.

192. Mediascope: Instagram audience in Russia decreased by 16%, Facebook audience by more than 40% // Esquire. URL: https://esquire/news/business-news/20-03-2022/671443-mediascope-auditoriya-instagram-vrossii-snizilas-na-16-auditoriya-facebook-bolee-chem-na-40/.

193. Miles F. Asymmetric warfare: an historical perspective. Carlisle Barraks, U. S. Army War Colledge, 1999. 47 p.

194. National Intelligence Council. URL: odni.gov/index.php/who-we-are/organizations/mission-integration/nic/nic-who-we-are.

195. Nazarbayev N.A. Kazakhstan 2030 "Prosperity, security and improvement of the well-being of all Kazakhstanis / Message of the President of the country to the people of Kazakhstan 1997 // http://adilet.zan.kz/rus/docs/K970002030_#z0/

196. Novikov V. Approaches to improvement of the institutional system and mechanisms of public administration in the conditions of information-hybrid wars // Eurasian Academic Research Journal. 2020. Vol. 37. Pp. 75-80.

197. OSINT. URL: https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B0_%D0%BF%D0%BE_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B0%D0%BC.

198. Pomaza-Ponomarenko A., Hren M., Durman O., Bondarchuk N.,

Vorobets V. Management mechanisms in the context of digitalization of all spheres of society // Revista San Gregorio. SPECIAL EDITION-2020. Núm. 42. URL: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/issue/view/RSAN42/showToc.

199. Porat M., Rubin M. The Information Economy: Development and Measurement. Wash., 1978. 274 p.

200. Public administration // RINA Services. URL: http://www.rina.org/EN/SETTORI/Pubblica_amministrazione/Pubblica_amministrazione.aspx#More.

201. Quadrennial Defense Review Report. Washington, Department of Defense, 2010. URL: https://comw.org/qdr/ fulltext/1002QDR2010.pdf.

202. Radchenko, O., Kriukov, Kovach, V. ext of “Civilizations Clash” as the Main Object of Infovation War in Ukraine. In: Radchenko, O., Kovach, V., Semenets-Orlova, I., Zaporozhets, A. (eds) National Security Drivers of Ukraine. (2023) Contributions to Political Science. Springer, Cham. https://doi.org/10.1007/978-3-031-33724-6_18. pp. 301-316.

203. RAND Corporation. URL: https://ru.wikipedia.org/wiki/RAND_(%D0%BA%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%86%D0%B8%D1%8F).

204. Repressionahead // The Economist. URL: https://www.economist.com/europe/2013/06/01/repression-ahead.

205. Riesman David. The Lonely Crowd. 13th edition. Yale University, 1968.

206. Rose R., Mishler W.T., Haerpfer C.W. Democracy and its Alternatives: Understanding Post-communist Societies. Baltimore, MD: Johns Hopkins University Press. 1998.

207. Rosenau J. The study of political adaptation. L.: N.Y., 1981. P. 61.

208. Scharpf, F.W. Ideological Conflict on the Public-Private Frontier: Some Exploratory Notes. Working paper. Wissenschftszentrum. Berlin, 1985.

209. Schnaufer TadA. II. Redefining Hybrid Warfare: Russia's Non-linear War against the West. Journal of Strategic Security, Vol. 10, No. 1 (Spring 2017), pp. 17–31. URL: https://www.jstor.org/stable/26466892.

210. Shepsle, K.A., Weingast B.R. Legislative, Politics and Budget Outcomes in Federal Budget Policy in the 1980's // Washington, D.C.: Urban Institute Press. 1984. Pp. 343-367.

211. Simon G. The Ukraine and the end of the Soviet Union // Aussenpolitik. Hamburg, 1992.-Vol. 43. № 1. P. 68.

212. Statement on the Results of Meeting on the Highest Level in Warsaw, 9 July 2016, statement 72. URL: https://www.nato.int/cps/en/ natohq/official_texts_133169.htm?selectedLocale=.

213. Stomer T. Information and the Internal. Structure of the Universe.London :Springer, 1990.

214. Strategic Communications Centre of Excellence. URL: https://stratcomcoe.org/.

215. Stratégie nationale de gestion des risques d'inondation (2014). URL: https://www.ecologie.gouv.fr/sites/default/files/2014_Strategie_nationale_gestion_ risques_inondations.pdf.

216. Tapscott Don. The Digital Economy: Promise and Peril in the Age of Networked Intelligence. McGraw-Hill, 1997.

217. Thomas P. Rona. Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976.

218. Trojan Footprint 18. URL: https://www.flickr.com/photos/us_soceur/albums/72157698152715825/.

219. Vacca W., Davidson M. The Regularity of Irregular Warfare. Parameters, 2011, vol. 41, no. 1, pp. 18-34.

220. Whitney Webb: “Lights Out!”. Did Trump and His Neocons Recycle Bush-Era Plan to Knock Out Venezuela’s Power Grid?, Even as the Venezuelan government blamed the recent power outage on U.S.-led “sabotage”, the U.S. has long had a plan on the books for targeting the civilian power grid of adversarial nations, Mint Press News (MPN), 11 March 2019. URL: https://www.mintpressnews.com/did-the-us-recycle-a-bush-eraplan-to-take-outvenezuelas-power-grid/256113/.

221. William J. Aceves.Virtual Hatred: How Russia Tried to Start a Race War in the United States // Michigan Journal of Race and Law Volume 24. URL: https://repository.law.umich.edu/mjrl/vol24/iss2/2/.

222. Wither James K. Making Sense of Hybrid Warfare. Connections. (Spring 2016). Vol. 15, No. 2.P. 73–87. URL:https://www.jstor.org/stable/26326441.

223. Wu J., Yang Y. Does public servants’ trust in citizen raters really matter? Evidence from mainland China. International Public Management Review. 2011. № 12 (1). Pp. 1–21.

224. Yang K. Public administrators’ trust in citizens: A missing link in citizen involvement efforts. Public Administration Review. 2005. № 65 (3). Pp. 273–285.

225. Yurcik W. Information Warfare: Legal & Ethical Challenges of the Next Global Battleground. The Proceedings of The Second Annual Ethics and Technology Conference (Ethics’97), Loyola University Chicago, Chicago, IL. USA. (June 6-7), pp. 1–20. https://doi.org/10.1.1.15.2 345&rep=rep1&type=pdf.

ДОДАТКИ

Додаток А

Кількість органів державної влади та місцевого самоврядування, що надають можливість використання інструментів електронної демократії, за угрупуваннями установ[1] у 2019 р.

	Усього	З них			
		органи державної влади	органи судової системи	органи місцевого самоврядування	державні організації (установи, заклади)
Кількість установ, які мали доступ до мережі Інтернет, од	17678	5102	695	10584	1297
Частка установ, які мали доступ до мережі Інтернет, у загальній кількості установ, які взяли участь в обстеженні, %	94,7	92,5	87,9	96,6	92,8
Кількість установ, які надавали можливість використання інструментів електронної демократії "Е-звернення", "Е-петиція", "Е-консультація", "Бюджет участі (громадський бюджет)" та інших інструментів електронної демократії, од	3853	1326	568	1818	141
з них					
"Е-звернення"	3365	1253	565	1417	130
"Е-петиція"	678	к	х	659	к
"Е-консультація"	358	145	–	210	3
"Бюджет участі (громадський бюджет)"	416	31	х	385	х

[1] Угрупування установ здійснено відповідно до Державного класифікатора "Класифікація організаційно-правових форм господарювання" (ДК 002:2004): орган державної влади (410), судова система (415), орган місцевого самоврядування (420), державна організація (установа, заклад) (425).

Джерело: складено на підставі [97]

Додаток Б

Використання інструментів електронної демократії органами державної влади та місцевого самоврядування за угрупуваннями установ[1] у 2019 р.

	Усього	З них			
		органами державної влади	органами судової системи	органами місцевого самоврядування	державними органі-заціями (установами, закладами)
	"Е-звернення"				
Кількість зареєстрованих "Е-звернень", од	873685	314018	77738	356634	125295
Кількість розглянутих "Е-звернень", од	858682	311359	76936	349779	120608
Частка розглянутих "Е-звернень" у загальній кількості зареєстрованих "Е-звернень", %	98,3	99,2	99,0	98,1	96,3
	"Е-петиції"				
Кількість оприлюднених "Е-петицій", од	10350	к	х	9607	к
Кількість підтриманих (які набрали необхідну кількість голосів на їх підтримку) "Е-петицій", од	1551	к	х	1533	к
Кількість "Е-петицій", підтриманих рішеннями органів, яким адресовані петиції, од	934	к	х	918	к
Частка "Е-петицій", підтриманих рішеннями органів, яким адресовані петиції, у загальній кількості підтриманих (які набрали необхідну кількість голосів на їх підтримку) "Е-петицій", %	60,2	84,6	х	59,9	100,0
	"Е-консультації"				
Кількість оприлюднених "Е-консультацій", од	11399	5639	–	5736	24
Кількість оприлюднених звітів за результатами "Е-консультацій", од	6603	4735	–	1844	24
	"Бюджет участі (громадський бюджет)"				
Кількість поданих громадськістю проєктів "Бюджет участі (громадський бюджет)", од	15347	1598	х	13749	х

Кількість винесених на голосування проєктів "Бюджет участі (громадський бюджет)", од	12757	1241	х	11516	х
Кількість підтриманих проєктів (проєктів-переможців) "Бюджет участі (громадський бюджет)", од	5443	429	х	5014	х
Кількість проєктів "Бюджет участі (громадський бюджет)", реалізованих за рахунок місцевого бюджету у звітному році, од	4143	353	х	3790	х
Частка проєктів "Бюджет участі (громадський бюджет)", реалізованих за рахунок місцевого бюджету у звітному році, у загальній кількості підтриманих проєктів (проєктів-переможців) "Бюджет участі (громадський бюджет)", %	76,1	82,3	х	75,6	х
[1] Угрупування установ здійснено відповідно до Державного класифікатора "Класифікація організаційно-правових форм господарювання" (ДК 002:2004): орган державної влади (410), судова система (415), орган місцевого самоврядування (420), державна організація (установа, заклад) (425).					

Джерело: складено на підставі [97]

Додаток В

СЛУЖБА БЕЗПЕКИ УКРАЇНИ
Управління Служби безпеки України в Харківській області
вул. Мироносицька, 2, м. Харків, 61002, факс:(057)700-14-22, тел.(057)700-16-61
www.ssu.gov.ua, e-mail: usbu_Khr@ssu.gov.ua Код ЄДРПОУ 20001711

14.11.2022 № 70/4-8859-1 на № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження Новікова В.О. на тему «Інституційні механізми публічного управління в умовах інформаційно-гібридних війн»

Представлене дослідження вивчає актуальну проблему, оскільки в ньому обґрунтовано напрямки розвитку організаційних механізмів публічного управління України в умовах військового конфлікту крізь призму підтримки її громадської (цивільної) безпеки. У науковому дослідженні систематизовані фактори та загрози такій безпеці, зокрема, інформаційні, які відзначаються значним дестабілізуючим характером. На цій підставі в науковій роботі Новікова В.О. визначено необхідність урахування зарубіжного досвіду публічного управління у сфері громадської (цивільної) безпеки крізь призму забезпечення інформаційної безпеки, що вимагає функціонування ефективної, стабільної та гнучкої адміністративної системи публічного управління. Вона передбачає оперативне реагування на зміну в потребах населення, дієву взаємодію міжнародних і вітчизняних структурних підрозділів у підтримці системи безпеки в Україні. У цьому контексті автором слушно обстоюється позиція щодо перспектив упровадження ризик-орієнтованих підходів до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, у т.ч. на регіональному рівні.

Зважаючи на це, результати дисертаційного дослідження Новікова В.О. можуть бути враховані в практичній діяльності Управління Служби безпеки України в Харківській області, зокрема в інформаційно-аналітичній роботі, спрямованій на забезпечення системи безпеки шляхом управління інформаційною безпекою.

Сектор інформаційно-аналітичного відділу
Управління Служби безпеки України
в Харківській області,
капітан СБУ **Ірина ЧЕРЕДНИК**

Додаток Г

ЧЕРКАСЬКА РАЙОННА РАДА

✉ вул. В.Чорновола, 157, м. Черкаси, 18003, ☎/факс 64-34-76
E-mail: cherkaskarada@ukr.net Код ЄДРПОУ 25659510

06. 02. 2024 № 10 101-13
на №_____ від _____

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Новікова Владислава Олександровича
на тему «Інституційні механізми публічного управління
в умовах інформаційно-гібридних війн» на здобуття наукового ступеня
кандидат наук з державного управління
зі спеціальності 25.00.02 – механізми державного управління

Громадська безпека є складовою національної безпеки, інституційне забезпечення якої має відбуватися на всіх рівнях публічного управління. На місцевому рівні цей процес набуває особливої ролі, адже регіони є найбільш наближеними до інтересів населення, серед яких особливе місце займають безпекові. На них деструктивний вплив значною мірою чинять інформаційні загрози, що становлять базис для виникнення інформаційно-гібридної війни.

Представлене дослідження присвячено визначенню шляхів протистояння негативному впливу інформаційним загрозам із позиції реалізації інституційних механізмів публічного управління та необхідного для цього організаційного, аналітичного, методичного й інформаційного забезпечення. Автором обґрунтовано напрямки розвитку інституційних механізмів публічного управління України в умовах зовнішньої агресії крізь призму підтримки громадської безпеки, на зниження рівня якої впливають поширення недостовірної інформації з боку країни-агресора за допомогою новітніх технологій, друкованих ЗМІ тощо. На цій підставі в науковій роботі Новікова В.О. визначено необхідність урахування зарубіжного досвіду публічного управління у сфері громадської безпеки крізь призму забезпечення інформаційної безпеки, що вимагає функціонування ефективної, стабільної та гнучкої адміністративної системи публічного управління. Вона передбачає оперативне реагування на зміну в потребах населення, дієву взаємодію міжнародних і вітчизняних структурних підрозділів у підтримці системи безпеки в Україні. У цьому контексті автором слушно обстоюється позиція щодо перспектив упровадження ризик-

орієнтованих підходів до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, у т.ч. на регіональному рівні.

Зважаючи на актуальність наданих автором пропозицій, визнаємо за доцільне їх використання в практичній діяльності, зокрема, в організаційній, інформаційній, аналітичній, Черкаської районної ради Черкаської області. Довідка видана без фінансових зобов'язань.

Голова Олександр ВАСИЛЕНКО

Додаток Д

ЗАТВЕРДЖУЮ

Проректор з навчальної та методичної роботи Національного університету цивільного захисту України

_____ Юрій КЛЮЧКА

АКТ №22-20 від 28.11.2022 р.

Про впровадження результатів дисертаційного дослідження докторанта навчально-науково-виробничого центру Національного університету цивільного захисту України Новікова В.О. на тему «Інституційні механізми публічного управління в умовах інформаційно-гібридних війн» на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку.

Комісія в складі:

Голова – начальник навчально-науково-виробничого центру, держ.упр., проф. Домбровська С.М.

Члени комісії – завідувач кафедри публічного адміністрування у сфері цивільного захисту, держ.упр., проф. Майстро С.В.; професор кафедри публічного адміністрування у сфері цивільного захисту, держ.упр., проф. Крюков О.І.

Цим актом засвідчують, що результати дисертаційного дослідження Новікова В.О. на тему «Інституційні механізми публічного управління в умовах інформаційно-гібридних війн» (зокрема, поглиблення понятійно-категоріального апарату, методології формування інституційних механізмів публічного управління у сфері інформаційної безпеки) використовуються під час проведення лекцій і практичних занять із навчальних дисциплін «Інформаційна політика в Україні» і «Сучасні геополітичні процеси: світ і Україна» за програмою підготовки магістрів державного управління у Національному університеті цивільного захисту України.

Голова комісії:

д.держ.упр., професор Світлана ДОМБРОВСЬКА

Члени комісії:

д.держ.упр., проф. Сергій МАЙСТРО

д.держ.упр., проф. Олексій КРЮКОВ