МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

УКРАЇНА ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ 2014-2023 рр.:

ҐЕНЕЗА НАЦІОНАЛЬНОЇ СТІЙКОСТІ КРІЗЬ ПРИЗМУ НАУКОВИХ ДОСЛІДЖЕНЬ

Монографія

За загальною редакцією
кандидата військових наук, старшого наукового співробітника
заступника начальника Військового інституту
Бориса ПОПКОВА

доктора юридичних наук, професора
Сергія ПІСТКОВА

Київ
Видавництво Ліра-К
2023

УДК 94(477)"2014/2023":[355.48:316.64(=161.2)](02)
У45

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка (протокол № 12 від 15 червня 2023 року).

Рецензенти:

Ярослав ЖУРАВЕЛЬ доктор юридичних наук, професор, декан юридичного факультету Академії праці, соціальних відносин і туризму;

Володимир МІЛЬЧЕВ доктор історичних наук, професор, професор кафедри джерелознавства, історіографії та спеціальних історичних дисциплін факультету історії та міжнародних відносин Запорізького національного університету;

Ольга ЧЕРВЯКОВА доктор наук з державного управління, професор, проректор з науково-навчальної роботи ТОВ «Заклад вищої освіти Східно-європейський слов'янський університет».

Автори:

Вановська І.М., Джус О.А., Іляшко О.О., Колотун І.М., Коропатнік І.М., Первак І.О., Петков С. В, Попков Б.О., Скрябін О.Л., Стецюк С. П., Скриньковський Р.М., Сопільник Л.І., Трубчанінов М.А., Хан Є.В., Шемчук В.В.

У45 **Україна під час російсько-української війни 2014-2023 рр.**: генеза національної стійкості крізь призму наукових досліджень : монографія. // За заг. ред. Б. Попкова, С. Петкова. Київ : Видавництво Ліра-К. 2023. 272 с.
ISBN 978-617-520-545-7

В Україні протягом останніх десятиліть сформовані потужні наукові школи історії, права, соціології, психології, філології, педагогіки. Хто як не вчені, які присвятили роки свого життя вивченню проблематики становлення та реформування держав, державних інститутів, механізмів правового впливу на процеси, що відбуваються у суспільстві, мають дати відповідь на головне питання, яке стоїть нині перед українським і світовим суспільством: Як стабілізувати суспільно-політичну ситуацію яка склалась в північно-східній частині Євразійського континенту? Бо Світу потрібно вирішити глобальну проблему приведення в адекватний стан Російську Федерацію, її політичних лідерів і громадян, які вважають себе вправі нищити інших на догоду своїм ідеологічним штампам.

Колективна монографія містить творчий доробок вчених різних галузей науки, стане в нагоді всім хто вивчає проблематику рашизму, гібридних війн, протидію зовнішній військовій агресії та тероризму.

УДК 94(477)"2014/2023":[355.48:316.64(=161.2)](02)

ISBN 978-617-520-545-7

Це видання присвячене воїнам Збройних Сил України, які виконують священну місію – героїчно боронять Вітчизну від рашистських загарбників. Під час російсько-української війни відважні військові захищають європейську цивілізацію від хвилі варварства і жорстокості, демонструючи світові непохитну стійкість та самопожертву в обороні, неймовірну доблесть і відвагу під час наступу, вражаючі своєю професійністю та умінням в користуванні сучасною зброєю і технікою.

Складний і звитяжний історичний шлях, яким пройшли українці, гідний великого європейського народу. Війна не повинна залишитись у спадок прийдешнім поколінням. Подвиги героїв, які є взірцем виконання військового та громадянського обов'язку, вписані кров'ю в літопис боротьби українського народу за незалежність, завжди будуть нагадувати нащадкам, якою ціною дістається свобода, як здобувається право бути вільною, самодостатньою нацією.

Слава Україні! Героям слава!

Авторський колектив

ЗМІСТ

§ 4.1. Інформаційна безпека держави та інформаційна війна

Поширеним є підхід щодо розкриття сутності інформаційної безпеки через більш широке поняття – національна безпека. Зокрема, він застосовується в енциклопедичній та довідковій літературі.

Так, у багатотомній юридичній енциклопедії *інформаційна безпека України* визначається як один із видів національної безпеки, важлива функція держави. Інформаційна безпека України передбачає: законодавче формування державної інформаційної політики; створення можливостей досягнення інформаційної достатності для ухвалення рішень суб'єктами права; гарантування свободи інформаційної діяльності та права доступу до інформації; всебічний розвиток інформаційної структури; підтримку розвитку національних інформаційних ресурсів; створення і впровадження безпечних інформаційних технологій; захист права власності держави на стратегічні об'єкти інформаційної інфраструктури України; охорону державної таємниці; створення загальної системи охорони інформації; захист національного інформаційного простору України; встановлення законодавством режиму доступу іноземних держав до національних інформаційних ресурсів; законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [680].

У контексті національної безпеки інформаційну безпеку розглядають М. Желіховський, В. Ліпкан, Є. Максименко, О. Степко, Л. Ткачук та інші вчені. Водночас дискусійним залишається питання самостійності інформаційної безпеки як елемента в системі національної безпеки.

Так, В. Ліпкан, Є. Максименко, М. Желіховський зазначають, що національна безпека являє собою цілісний екзистенціальний феномен, відтак не може бути репрезентована сукупністю корелятивно пов'язаних складових (економічна, інформаційна, політична безпека тощо). Національну безпеку слід аналізувати крізь призму її системних властивостей, отже, доцільно стверджувати про національну безпеку в інформаційній сфері, екологічній сфері тощо. Адже з появою інших «складових», національна безпека як така не змінить своєї сутності. Водночас, коли йтиметься про прояви національної

безпеки в різних сферах життєдіяльності, то поява чи то нових суспільних відносин чи сфер життєдіяльності жодним чином не вплине на зміст національної безпеки, лише змінить її [361].

На думку Б. Кормича, інформаційний аспект національної безпеки є її невід'ємним компонентом, і так само, як інформаційна безпека не може існувати поза межами загальної національної безпеки, національна безпека не буде всеохоплюючою в разі позбавлення своїх інформаційних векторів [324].

Н. Нижник, Г. Ситник, В. Білоус, аналізуючи загрози національній безпеці України в життєво важливих сферах діяльності, виокремлюють ряд основних функціональних складових (сфер) національної безпеки України: економічну, політичну, соціальну, воєнну, екологічну, епідемічну, технологічну та інформаційну безпеку. Відповідно, під інформаційною безпекою зазначені автори розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень на захист інформаційних ресурсів країни [410].

Дещо іншу позицію щодо співвідношення понять національної та інформаційної безпеки відстоюють вчені Ф. Медвідь, О. Младьонова, І. Проноза, О. Соснін, О. Степко, Л. Ткачук, М. Форос та інші. Зокрема, вони розглядають інформаційну безпеку як складову, підсистему чи елемент національної безпеки.

Наприклад, Ф. Медвідь зазначає, що інформаційна безпека України як важлива складова національної безпеки передбачає системну превентивну діяльність органів державної влади щодо надання гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому і спрямована на досягнення достатнього для розвитку державності та соціального прогресу рівня духовного та інтелектуального потенціалу країни [386].

Наступна позиція, що використовується при з'ясуванні змісту поняття «інформаційна безпека», засновується на визначенні характеру (статичного чи динамічного) цього суспільного явища.

Так, Д. Дубов, А. Корсунський та деякі інші вчені під інформаційною безпекою України розуміють стан захищеності її національних інтересів в

інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства й держави [217, с. 19–30].

В. Гасеський, В. Авраменко визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації [110, с. 17–18].

В. Богуш вказує, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави [145].

На переконання О. Сорокіна, інформаційна безпека розкривається як стан захищеності особистості, суспільства, держави від інформації, що носить шкідливий або протиправний характер, від інформації, що надає негативно впливає на свідомість особистості, перешкоджає сталому розвитку особистості, суспільства і держави. Інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючи також комп'ютери та інформаційно-телекомунікаційну інфраструктуру й інформацію, що в них знаходиться, який також забезпечує сталий розвиток особистості, суспільства й держави [580, 18-22].

Близькою за змістом видається позиція О. Дзьобаня і В. Пилипчука, які визначають інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства та держави в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, що забезпечує їх сталий розвиток.

В. Ярочкін визначає безпеку як стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек і загроз, який ґрунтується на діяльності людей, суспільства, держави, світового співтовариства з виявлення (вивчення), запобігання, послаблення, ліквідації та відбиття небезпек і загроз, здатних загубити їх, лишити фундаментальних матеріальних і духовних

цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку [684, с. 7].

Інформаційна безпека – це стан захищеності систем оброблення і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення. Інформаційну безпеку, залежно від суб'єкта захисту інформації, прийнято поділяти на інформаційну безпеку держави, організації та особи [344].

Так, інформаційна безпека організації – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів щодо досягнення стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток. Часто здійснюється службами інформаційної безпеки.

Інформаційна безпека держави, як зазначає О. Князєв, характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо) інформаційних впливів, причому як до впровадження, так і до вилучення інформації [295].

Інформаційна безпека особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору, а також зазіхань на її майно та інтелектуальну власність.

Не можна не погодитися з В. Горлинським, який переконує, що реалії інформаційної діяльності людини з позиції феномена безпеки як об'єкта аксіологічної рефлексії свідчать про необхідність вироблення нової аксіологічної парадигми, яка відповідає новій організації публічного управління на підставі використання інформаційних технологій [187, с. 1–2].

Якщо ж розглядати інформаційну безпеку в динаміці, то її можна визначити як процес, певну діяльність, забезпечення нормального стану інформаційної сфери чи застосування заходів протидії інформаційній агресії та методів захисту інформаційного простору.

Наприклад, О. Логінов стверджує, що не слід обмежуватись поняттям «стан» при визначенні категорії «інформаційна безпека», і стверджує, що вона є процесом. Зокрема, на його думку, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності органів виконавчої влади [364, с. 153–161].

На думку А. Шумки, П. Черника, інформаційна безпека являє собою діяльність органів державного управління. Звідси витікає важливий висновок, що слід діяти активно, здійснюючи вплив на джерела інформаційної небезпеки [677, с. 10 –16].

Л. Харченко, В. Ліпкан, О. Логінов визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками, державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [634].

Л. Наливайко пропонує розуміти інформаційну безпеку як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [400, с. 60–65].

О. Литвиненко, розкриваючи поняття «інформаційна безпека», трактує її як єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [357, с. 18].

Слід звернути увагу на ще один підхід до визначення поняття «інформаційна безпека», згідно з яким воно розглядається крізь призму

суспільних відносин. У науковій літературі такий підхід визнається неординарним та інноваційним, але, на наш погляд, він дає змогу розкрити правову природу інформаційної безпеки, детально вивчити її структуру.

Зазначений підхід у своїх дослідженнях використовує В. Гуровський, який пропонує розуміти національну інформаційну безпеку України як суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [198].

О. Литвиненко також визначає інформаційну безпеку як одну із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [356, с. 47-49].

П. Ткачук, Р. Гула, О. Сивак, О. Щурко та інші дослідники відзначають, що зміст поняття «інформаційна безпека» визначається через політико-інструментальний, технологічний та комплексний підходи. По-перше, політико-інструментальний підхід розкриває сутність інформаційної безпеки держави через стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдають істотної шкоди національним інтересам і забезпечують прогресивний розвиток усіх сфер життя суспільства [262, с.160].

За визначенням Б. Кормича, це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, суспільства та держави [324, с. 92].

По-друге, технологічний підхід наголошує на захищеності насамперед інформаційної системи від випадкового або навмисного втручання, що завдає збитку власникам або користувачам інформації.

По-третє, комплексний підхід визначає інформаційну безпеку як стан захищеності інформаційного простору, його формування і розвиток в інтересах громадянина, організацій і держави в цілому, захист від неправомірного зовнішнього і внутрішнього втручання, стан інформаційної інфраструктури, в якому інформацію використовують у мирних цілях лише за призначенням, і вона нездатна негативно впливати на інформаційну чи інші системи як самої держави, так і інших країн [262, с. 160].

В одній із останніх публікацій з даної тематики, автором якої є Т. Ткачук, виявлено три концептуальні підходи до трактування інформаційної безпеки, а саме:

1) статичний (безпека як стан захищеності інформаційного середовища/ інформації, система гарантій тощо);

2) діяльнісний (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси і цінності);

3) комплексний (безпека як стан і процес).

Водночас згаданий дослідник обґрунтував авторську позицію, що найбільш прийнятним, зважаючи на сучасну практику забезпечення інформаційної безпеки держави, є останній. За такого підходу вбачається за доцільне інформаційну безпеку держави розглядати як перманентний процес діяльності компетентних органів, спрямований на запобігання і протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Цей підхід ґрунтується на принципі, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища [610].

Правове регулювання інформаційної безпеки в Україні здійснюється на підставі Конституції України, Закону України «Про національну безпеку України» № 2469-VIII від 21.06.2018 р., Закону України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 р., Закону

України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» № 537-V від 09.01.2007 р., Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України», яке затверджене Указом Президента України № 47/2017 від 25.02.2017 р. тощо.

Прикметно, що законодавче визначення інформаційної безпеки міститься лише в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» № 537-V від 09.01.2007 р. Зокрема, згідно зі ст.13 цього закону інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [244].

У Законі України «Про національну безпеку України» № 2469-VIII від 21.06.2018 р. зміст інформаційної безпеки не розкривається, вона лише визнається одним із напрямів державної політики у сфері національної безпеки і оборони. Так само і в Законі України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 р. інформаційна безпека називається невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки, але саме поняття не деталізується.

Перехід держави до інформаційного суспільства потребує переосмислення в окремих випадках і розроблення нових механізмів регулювання відносин, що виникають між громадянами, їх об'єднаннями та державою. Усі суб'єкти інформаційних відносин повинні усвідомлювати і виконувати свою роль у цьому процесі, але саме держава покликана активно впливати на ці трансформаційні процеси, залучати до співпраці політиків, науковців, практиків, міжнародних експертів і громадськість.

Інформаційна безпека держави та інформаційна війна.

Події, які відбуваються в Україні в останні декілька років демонструють появу нових викликів і загроз у цій сфері. Зокрема, особливої уваги заслуговують різні форми впливу, протиборства тощо. З розвитком та впровадженням сучасних інформаційних технологій практично в усі сфери нашого життя, зростає рівень загроз несанкціонованого доступу в процес роботи систем та витоку важливої інформації. Технічний прогрес суттєво впливає на вирішення військових, торговельних, економічних конфліктів, внаслідок чого силові методи іноді поступаються інформаційним.

Тому очевидно, що змінилось традиційне чи класичне розуміння механізму забезпечення безпеки держави та суспільства, оскільки раніше, наприклад, не були поширені інформаційні атаки та інформаційні війни і фактично без участі держави, групи держав, а іноді й узгоджених дій світової спільноти неможливо убезпечитись від них.

Слід зазначити, що практично в усіх збройних конфліктах за останні десятиліття ефективно використовувалися методи та засоби інформаційної боротьби, які можуть призвести до таких трагічних наслідків як: зміна суспільного ладу та політичного устрою; розпад держави; втрата армії; занепад економічної системи в країні; втрата національної ідеї та духовних цінностей; загибель людей тощо [553, с. 18–23].

Проблематику *інформаційних впливів та протиборств, інформаційних воєн* неодноразово порушували і вивчали вітчизняні та зарубіжні дослідники. Тут варто назвати таких учених: Дж. Арквілли, Р. Гула, Г. Почепцов, Н. Камінська, Г. Карпенко, Я. Короход, І. Костюк, Д. Кюль, М. Лібікі, С. Любарський, Р. Моландер, Дж. Най, В. Остроухов, С. Расторгуєв, О. Саприкін, Г. Сасин, О. Сивак, П. Ткачук, П. Шевчук, О. Цуканова, В. Хорошко, Ю. Хохлачова, О. Щурко та ін. Разом з тим, неоднозначне розуміння згаданих категорій, іноді їх ототожнення, змушують і надалі привернути увагу, особливо стосовно з’ясування їх суті, а також правових основ запобігання їм і протидії.

Інформаційні війни як явище існували тією чи іншою мірою з давніх часів. Історичний розвиток людства свідчить про те, що поняття «інформаційна

війна» завжди супроводжувало та визначало разом зі зброєю хід, характер і результат воєн, битв, операцій.

Видатний китайський воєнний теоретик Сун-Цзи у VI–V ст. до н.е. вперше запропонував використовувати інформаційні заходи як альтернативу бойовим діям. Він сформулював дев'ять заповідей, дотримання яких забезпечувало такий потужний вплив на духовний світ армії противника, що вона просто «розкладалася» ще до початку битви. Сун-Цзи зазначав, що «у війні, як правило, найкраща політика зводиться до захоплення держави цілісною... Здобути сотню перемог у боях – це не вершина мистецтва. Підкорити суперника без бою – ось вінець мистецтва» [590, с. 40].

Основні ідеї Сунь-Цзи активно розвивали й інші китайські мислителі. Зокрема, Чжуге Лян (III ст. н.е.). вважав, що «у воєнних діях атака на психіку – головне завдання. Психологічна війна – це головне, бій – це другорядна справа». Не абсолютизував збройне насильство і відомий прусський воєнний теоретик К. Клаузевіц, автор класичного визначення поняття «війна»: «Доведеться хоч-не-хоч визнавати і такі війни, які полягають лише в погрозі супротивнику» [382, с. 231]. Вперше термін «інформаційна війна» використав у 1985 р. в Китаї Шень Вейгуаном.

Здійснення інформаційних впливів з використанням інформаційної зброї (приховування інформації; подача її частково, в певному ракурсі; перебільшення наслідків) було зафіксовано літописцями на теренах України ще за Київської Русі. Так, загальновідомим є факт поїздки княгині Ольги до Константинополя, проте ні візантійські, ні руські джерела не висвітлюють причини та мети подолання такого довгого шляху. Войовничий князь Святослав заздалегідь повідомляв противника про свій похід, проте залишалися таємницею напрям та сили, котрі планувалося задіяти. Це давало можливість навести паніку у стані військ та швидко розгромити противника [195].

В інформаційному просторі України тривалий час спостерігається боротьба за управління ресурсами, вплив і контроль на території нашої держави. Події з кінця 2013 – початку 2014 рр. стали драматичними для України. Внаслідок дестабілізації внутрішньої політичної ситуації, анексії

Криму та «гібридної війни» на сході України змінилася геополітична ситуація як у Європі, так і фактично в усьому світі.

Це, на нашу думку, потребує з'ясування природи і сутності таких споріднених категорій як інформаційна війна, інформаційний вплив, експансія, гібридна війна, електронна війна, хакерська війна, мережева війна, кібервійна, консцієнтальна війна, психологічна війна, інформаційне протиборство тощо.

Так, одним із перших у відкритому друці, хто написав про феномен інформаційних воєн, був М. Маклюєн у 1960 роках. Уже тоді було відомо, що «холодна війна» ведеться за допомогою інформаційних технологій, так як в усі часи війни велися за допомогою передових технологій. Дослідник відмітив, що якщо «гарячі» війни минулого використовували зброю, знищуючи ворогів одного за іншим, то інформаційна зброя за допомогою телебачення та кіно, навпаки, занурює все населення у певний світ уяви: «земна куля тепер – не більше, ніж село» [375, с. 5].

Інформаційна війна є тотальним явищем, де неможливо визначити його початок і кінець. Зокрема, на думку С. Расторгуєва, інформаційна війна – це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті та приховані цілеспрямовані інформаційні впливи систем (держав) одна на одну, з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи за допомогою таких засобів, використання яких дає змогу досягати задуманих цілей [530, с. 455 –456].

Можна погодитися з думкою О. Саприкіна, що інформаційна експансія є технологією набагато місткішою, ніж «інформаційна війна» або «інформаційна атака». Ці терміни можна вважати складовими інформаційної експансії. Інформаційна експансія – система, що склалася в засобах інформації розвинених держав, і методи, використані для пропагандистського забезпечення певних геополітичних цілей [552, с. 40–43].

У листопаді 1991 року аналізуючи досвід досягнення інформаційної переваги після операції «Буря у пустелі», генерал Гленн Отіс, колишній командувач Командування сухопутних військ США з навчання та доктрин, опублікував працю, в який стверджував, що «природа війни повністю

змінилася. Та сторона, яка виграє інформаційну війну, – переможе…інформація є ключем до сучасної війни – у стратегічному, оперативному, тактичному і технічному планах». Офіційно визначеним термін «інформаційна війна» як комплексне спільне застосування сил і засобів інформаційної боротьби та збройної боротьби (при домінуванні засобів інформаційної боротьби) вперше застосували у керівних документах США, зокрема в директиві МО США Т 3600.1 від 12 грудня 1992 року під назвою «Інформаційна війна» [3].

У сучасному науковому дискурсі проблемі вивчення надскладного соціально-політичного явища «інформаційна війна» надається достатньо уваги. Різноманітність підходів до визначення основного змісту, відсутність єдиної системи класифікації призвели до унеможливлення створення уніфікованої дефініції понять «інформаційна війна» та «інформаційно-політичний простір», відсутність методологічного осмислення співвідношення цих понять та ін.

Наприклад, А. Манойло зміст поняття «інформаційна війна розглядає на різних рівнях пізнання як соціальне явище; як поле політичних конфліктів; як особливу форму політичного конфлікту; як інструмент інформаційної політики [381]. А. Фісун до цього додає ще й форму психологічного впливу [624, с. 534–538].

Найбільш важливими, як відзначають В. Хорошко та Ю. Хохлачова, є електронна та психологічна війни. Електронна війна об’єктом свого впливу має засоби електронних комунікацій – радіозв’язку, телевізійних і комп’ютерних мереж. Психологічна війна здійснюється шляхом пропаганди, «промивання мозку» та іншими методами інформаційного оброблення населення. Далі згадані автори виділяють інформаційну війну, безліч визначень якої пов’язано складністю і багатогранністю такого явища, труднощами побудови аналогій з традиційними війнами. Якщо спробувати трансформувати визначення в поняття «інформаційна війна», то навряд чи вийде щось конструктивне. Це пов’язано з рядом особливостей інформаційної війни [635, 256].

Загалом залежно від основних аспектів дослідження об’єкта, які вирізняють науковці, та від гіпотез щодо сутності явища, виділяється вісім основних підходів до поняття «інформаційна війна».

Так, за *соціально-комунікативним підходом* трактують поняття інформаційна війна як сукупність окремих інформаційних заходів, інформаційних способів і засобів корпоративної конкуренції, що є продуктом еволюційного розвитку способів і засобів комунікації між людьми, суспільствами, державами та світом загалом. У межах цього підходу український дослідник Г. Почепцов визначає «інформаційну війну» як всеосяжну, цілісну стратегію, яка надає значущості та цінності інформації в процесах командування, управління і виконання наказів збройними силами й реалізації національної політики [462]. Особливостями соціально-комунікативного підходу:

– відображення сутності досліджуваного явища лише як закономірного розвитку людського суспільства в рамках біологічної еволюції з домінуванням принципів природного відбору, боротьби за існування й виживання найбільш пристосованих як визначальних факторів громадського життя;

– визначення природи соціального конфлікту як вічного та непереборного;

– трактування інформаційної агресії як нової трансформованої форми природної агресії людини.

Маніпулятивно-психологічний підхід визначає суть інформаційної війни як системи способів і засобів психологічного впливу на індивідуальну та масову свідомість з метою спрямування її у вигідному для суб'єкта впливу напрямі. Формами інформаційної війни є використання психотропної зброї, побудова віртуального світу, підміна реальності та ін. Представники цього підходу вважають, що інформаційно-психологічна війна – це вплив на суперника через засоби масового психологічного впливу для зміни світогляду чи ініціювання процесу самознищення, добровільної здачі території, ресурсів і т.п. [394].

Тобто специфічними особливостями цього підходу є:

– розкриття психологічного впливу феномена;

– комплексне розкриття психологічного аспекту і маніпулятивної природи інформаційної війни;

– ігнорування оборонного (захисного) характеру інформаційної війни;

– нівелювання технічного аспекту, матеріальних засобів інформаційного протиборства;

– недостатнє прогнозування наслідків впливу економічної складової.

Військово-прикладний підхід зараховує інформаційну агресію до сфери військового протиборства й розглядає її у комплексі спільного застосування сил і засобів інформаційної та збройної боротьби. При цьому представники військово-прикладного підходу не вважають інформаційну війну окремим методом ведення війни. На їх думку, існує множина форм інформаційної війни, кожна з яких претендує на різні концепції, зокрема: командно-контрольні, розвідувальні війни; радіоелектронна боротьба; психологічні операції; хакерська війна, програмні атаки на інформаційні системи; інформаційно-економічна війна; кібервійни [60]. Кібервійну розглядають як процес розвитку та поширення інформаційних технологій. У військовій сфері – як комплексне використання високоточної зброї, технологій «Стелс», бойових і розвідувальних засобів з урахуванням футуристичних розробок у галузі роботизації й автоматизації [294, с. 78–84]. Характерні особливості цього підходу:

– системність, що дає можливість охопити політичний, економічний, психологічний та інший аспекти;

– «агресивний характер», зорієнтований на швидке досягнення бажаного тактичного результату з одночасною втратою стратегічної перспективи;

– ігнорування прогнозування наслідків для іншої сторони конфлікту;

– нівелювання соціального аспекту при домінуванні політичної складової конфлікту.

Державно-інструментальний підхід називає інформаційну війну інструментом зовнішньої та внутрішньої політики, «можливістю для збирання, оброблення та поширення безперервного потоку інформації…у відповідь на дії противника» [106, с. 43]. Особливістю цього підходу є абсолютизація ролі політичних інститутів і організації держави у веденні інформаційної війни й нівелювання впливу соціальних, економічних і психологічних чинників.

Геополітичний підхід. Дослідники вважають інформаційну війну явищем латентним мирного періоду міждержавного протиборства, що дозволяє вирішувати зовнішньополітичні завдання несиловими методами. Інформаційна війна стосується сфери геополітичного протиборства, її трактують як особливий вид відносин між державами, при якому для вирішення існуючих протиріч використовують методи, засоби й технології впливу на інформаційну сферу функціонування цих держав. Під інформаційною війною дослідники цього напряму розуміють дії, які спрямовані на завдання противнику конкретного, відчутного збитку в окремих галузях його діяльності [382, с.481].

З-поміж характеристик цього підходу виокремимо такі:

– охоплення геополітичних суб'єктів інформаційно-політичного простору;

– трактування інформаційної війни як певного природного закону;

– ігнорування значимості особистості як окремого об'єкта для впливу;

– недостатнє вивчення причин інформаційної війни.

Віртуально-кібернетичний підхід. Інформаційна війна розглядається як сукупність технічних, програмних та інших засобів, які використовують у віртуальному просторі, з метою ураження інформаційних систем противника (комп'ютерні віруси та ін.). Кібервійна – елемент інформаційної війни, що здійснюється з використанням засобів всесвітньої мережі у формі кібератак. Сутність інформаційної війни полягає в застосуванні прихованих цілеспрямованих інформаційних впливів інформаційних систем одна на одну з метою одержання певного прибутку в матеріальній сфері [530, с. 51].

Наголошено на тому, що інформаційно-блогова або мережева війна – це внутрішньо-середовищна особливість Інтернету, яка виявляється у формах жорсткої дискусії, цілковитого свавілля із взаємними образами, атаками на ресурси противника, зламами особистої інформації та ресурсів. Блоги стають потужним інструментом формування громадської думки [230, с. 48]. «Інформаційна війна, на думку американських теоретиків Дж. Аркуїла та

Д. Ронфельдта, може бути частиною широкого та всеохоплюючого поняття ворожих дій – мережевої війни або кібервійни» [6].

Властивостями віртуально-кібернетичного підходу є:

– розкриття суті інформаційної війни крізь площину математичного виміру;

– виокремлення тенденцій сучасного інформаційного простору та розвитку інформаційних технологій (особливо в контексті інформаційно-блогових процесів);

– ігнорування психологічного аспекту явища;

– невизначеність ролі держави в цьому процесі;

– домінування теоретичного, а не практичного значення, відсутність рекомендацій та прийомів, які дали б змогу виявити інформаційну агресію і захиститися від неї.

Комплексний підхід. Український дослідник А. Фісун констатує, що жоден із зазначених підходів не розкриває сутності інформаційної війни комплексно ні як політичного конфлікту, ні як соціального явища, ні як соціокультурного феномена: «Інформаційна війна – це комплексний відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони чи взаємний вплив сторін одна на одну, який містить систему методів і засобів впливу на людей, їхню психіку та поведінку, на інформаційні ресурси та інформаційні системи, з метою досягнення інформаційної переваги (в забезпеченні національної стратегії), що обумовлює прийняття сприятливих для ініціатора впливу рішень або знищення інформаційної інфраструктури противника, з одночасним зміцненням і захистом власної інформації та інформаційних систем» [624, с. 534–538].

На нашу думку, до комплексного підходу слід зарахувати й дефініцію В. Ліпкана, Ю. Максименко, В. Желіховського: «Інформаційна війна – це

1) дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що ґрунтуються на інформації та інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації та інформаційних системах;

2) нефізична атака на інформацію, інформаційні процеси та інформаційну інфраструктуру;

3) найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї)» [361, с. 270].

В ідеологіях маргінальних політичних формувань екстремістського та окультистського напрямів став популярним так званий *конспірологічний підхід.* Найбільш послідовним апологетом цього напрямку можна вважати О. Дугіна. Інформаційну війну він розглядає як форму тотального впливу глобальних політичних, економічних, терористичних, сектантських мережевих структур (хасидсько-парамасонська група, Захід на чолі з США, країни «золотого мільярда») з метою контролювання політичної, соціальної, економічної ситуації та інтенсифікації трансформаційних тенденцій духовності світового суспільства через спрямування інформаційних процесів в інтересах США, які одночасно створюють систему захисту власного мережевого коду, який ці процеси дешифрує та структурує.

Сегментами глобальної мережі у цьому підході є:

– пряме проамериканське лобі експертів, політологів, аналітиків, технологів, які контролюють владу та претендують на роль інтелектуальної еліти суспільства;

– представники великого бізнесу та політичної еліти, які орієнтовані на фінансово-економічну діяльність за кордоном;

– ЗМІ та ЗМК, які виконують функцію масованого інформаційного впливу за допомогою потоків візуальної та смислової інформації.

Тобто «інформаційну війну ведуть ідейні кілери — найманці з числа політиків, духівництва, інтелектуалів, які зраджують інтереси народу, проституюючи совість і розум». Характерною рисою «мережевої війни», за О. Дугіним, є тотальний інформаційний вплив «мережевої п'ятої колони» «агентів

впливу» – рушійної сили світового заколоту з метою десуверенізації країни [219]. Особливості цього підходу:

– дослідження мережевого характеру сучасного світового бізнесу, політичних проектів, терористичних формувань і сектантських організацій;

– розкриття сутності діяльності «агентів впливу»;

– надмірна абсолютизація поняття «мережі», ігнорування психологічних особливостей людини як самостійного індивіда;

– містично-конспірологічний погляд на роль світових глобальних структур, демонізація західного світу, захоплення ідеєю «світового єврейського заколоту», окультизм і расовий фактор.

Інформаційна війна здійснюється у формі інформаційного протиборства як системи цілеспрямованих дій для створення інформаційної переваги, за допомогою руйнування інформації, інформаційних систем протилежної сторони, при цьому одночасно відбувається процес захисту власної інформації та інформаційних систем [609, 368, с. 31–39].

Отже, на нашу думку, *інформаційна війна* – це суспільно-політичне явище, яке у політичному аспекті є продовженням домінуючих ідеологічних засад державної політики, що здійснюється за допомогою комплексу засобів інформаційно-технологічної індустрії, механізмів інформаційно-психологічного впливу на суспільство всередині держави чи населення країн-конкурентів в умовах політичного (воєнно-політичного, економічного) конфлікту з метою формування в *соціальному аспекті* єдності суспільства, визначення його ідентичності та інформаційного захисту світоглядних цінностей, а також деморалізації та фрагментації населення, силової компоненти держав-противників у межах глобального інформаційного простору.

Інформаційна війна як явище деструктивно впливає на розвиток інформаційних суспільств, інформаційну безпеку людини, держави і суспільства та одночасно сприяє розвитку практично всіх пріоритетних сфер життєдіяльності, у т.ч., через вплив маніпулятивних технологій, що використовуються в інформаційних війнах, на світову політику тощо. Світові тенденції розвитку державно-правових явищ потребують не тільки

удосконалення форм і методів організації та здійснення влади, й нових стратегій забезпечення національної інформаційної безпеки. З огляду на це, важливо удосконалити правові основи протидії та запобігання інформаційним війнам, негативному інформаційно-психологічного впливу на національному рівні в Україні. Для цього важливо вивчати як зарубіжний досвід, так і відповідні доктринальні та нормативні джерела з метою пошуку оптимальних шляхів виходу з тих ситуацій, у яких опинилось українське суспільство останніми роками [667, с. 29 –35].

Таким чином, що існують різні підходи до таких багатогранних категорій, як «інформаційна безпека», «інформаційна війна». Водночас, враховуючи системне зростання загроз і протиправних намірів супротивників, інших держав, важливо їх виявляти, запобігати та своєчасно протидіяти, захищати національні інтереси й цінності, включаючи інформаційну безпеку, інформаційний суверенітет і т. д.

У зв’язку з цим, на наше переконання, пріоритетним має стати власне комплексне розуміння сутності та гарантій забезпечення інформаційної безпеки держави, враховуючи функціональні аспекти національної безпеки та специфіку інформаційної сфери, національного і світового інформаційного простору, можливі потенційні загрози інформаційних воєн та інших викликів.