Павленко Д.Г., Семенюк Ю.В., Лисецький Ю.М.

ВИКЛИКИ ГІБРИДНОЇ ВІЙНИ ТА НАЦІОНАЛЬНА БЕЗПЕКА

Монографія

лам&к
издательство

Київ–2021

УДК 327:355
ББК 66.4+68
Л63

Рекомендовано до друку Вченою радою
Воєнно-дипломатичної академії імені Євгенія Березняка
(протокол № 7 від 25.08.2021 р.)

Автори:
Павленко Д.Г. – кандидат педагогічних наук;
Семенюк Ю.В. – кандидат політичних наук;
Лисецький Ю.М. – доктор технічних наук.

Рецензенти:
Мокляк С.П. – доктор політичних наук, професор;
Семенченко А.І. – доктор наук із державного управління, професор.

За загальною редакцією Ю.М. Лисецького

Виклики гібридної війни та національна безпека: монографія / Павленко Д.Г., Семенюк Ю.В., Лисецький Ю.М.; за заг. ред. Ю. М. Лисецького. – Київ : ЛАТ&К, 2021. 136 с.

ISBN 978-617-7824-41-0

Монографія присвячена проблемі підвищення ефективності системи національної безпеки. Обраний напрямок дослідження включає в себе ретроспективний аналіз еволюції гібридних війн, їх компонентів та особливостей, визначення поняття, структури та складових системи національної безпеки й розроблення необхідних моделей і механізмів.

Запропоновано модель гібридної війни, концептуальну модель системи національної кібербезпеки, модель взаємодії центрів протидії кіберзагрозам, а також концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки. Обґрунтовано сутність комплексного механізму протидії гібридним загрозам національній безпеці та визначено напрями його вдосконалення і розвитку.

Матеріали монографії будуть корисні для аспірантів, викладачів вищих навчальних закладів, наукових співробітників і фахівців, діяльність яких пов'язана з безпекознавством.

ISBN 978-617-7824-41-0

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ

АЕС – атомні електростанції
ВРУ – Верховна Рада України
ДМСУ – Державна міграційна служба України
ДСНС – Державна служба України з надзвичайних ситуацій
ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації України
ЖЦ – життєвий цикл
ЗМІ – засоби масової інформації
ЗСУ – Збройні Сили України
ІТ – інформаційні технології
КМУ – Кабінет міністрів України
КДБ – Комітет державної безпеки
МГВ – модель гібридної війни
МВС – Міністерство внутрішніх справ
МОУ – Міністерство оборони України
НАТО – Організації Північноатлантичного договору
НБУ – Національний банк України
ОПК – оборонно-промисловий комплекс
РНБО – Рада національної безпеки та оборони
РФ – Російська Федерація
СБУ – Служба безпеки України
СРСР – Союз радянських соціалістичних республік
СЗНБ – Система забезпечення національної безпеки
СНБ – Система національної безпеки
США – Сполучені Штати Америки
ЦОВВ – центральні органи виконавчої влади

ПЕРЕДМОВА

Вибір Україною європейського та демократичного шляху розвитку став взірцем для сусідів. Російський авторитаризм сприйняв це як історичний виклик і загрозу для свого існування. За задумом російського керівництва, анексія Автономної Республіки Крим, війна та окупація частини території Донецької і Луганської областей, терористичні акти, торговельна блокада та енергетичний шантаж, кібератаки й масована пропаганда мали підірвати життєві сили та єдність українського народу, нав'язати Україні статус неоколоніальної «буферної зони», розколоти її на маріонеткові «народні республіки». Після провалу цих спроб Росія перейшла до політики постійного воєнного, дипломатичного та інформаційного тиску на Україну, виснаження наших економічних ресурсів і розмивання суспільної довіри.

Гібридна війна не є винаходом Російської Федерації (РФ). Вона лише вдосконалила її інструменти та збільшила масштаби їх застосування. Випробувавши цілий арсенал методів ведення гібридної війни, Росія фактично демонструє формат війни майбутнього, де інформаційні та кібертехнології, розвідка та політичний вплив «тихої війни», загроза силою та використання бойовиків можуть відігравати більше значення, ніж пряме військове втручання.

Боротьба за нову країну має багато складників, і серед них – рішення, які потрібно прийняти у військовій, дипломатичній, суспільно-політичній, соціально-економічній та гуманітарній сферах, що мають зміцнити внутрішнє та зовнішнє становище України. Необхідно доводити до кінця розпочаті реформи, знімати штучні бюрократичні та політичні бар'єри, що стримують використання значних внутрішніх ресурсів. На це мають бути спрямовані зусилля Верховної Ради України (ВРУ), Президента України, Кабінету Міністрів України (КМУ), державних адміністрацій та органів місцевого самоврядування. Тому головним завданням української влади є проведення реформ, які не дозволять агресору втілити в життя свої плани – примусити Україну згорнути демократичний, економічний та соціальний поступ. Більшість українців вірить у здатність України подолати труднощі.

Тематика цього дослідження є актуальною як у науково-теоретичному, так і в прикладному аспектах. Анексія РФ суверенної території України та збройне вторгнення для збереження й розширення територій терористичних квазідержавних утворень «Донецька народна республіка» та «Луганська народна республіка» не тільки переконливо показали неефективність функціонування попередньої моделі системи забезпечення національної безпеки (СЗНБ) країни, але й вимагають адекватного врахування в сучасних реаліях продовження реалізації Росією стратегії гібридної війни в нових інституційно-процедурних формах. У

цьому контексті особливої уваги потребують ризики національної безпеки нашої держави у військовій, політичній, економічній, соціальній, гуманітарній та інших сферах. Ефективність реагування на порушення національних інтересів значним чином залежить від вибору відповідного теоретико-методологічного й організаційно-технічного інструментарію та його ефективного застосування для протидії загрозам національній безпеці в умовах гібридної війни.

Значну кількість результатів, поданих у монографії, отримано вперше. Побудовано модель гібридної війни (МГВ). Наведено організаційно-правові основи протидії загрозам національній безпеці країни. Запропоновано концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки. Розроблено концептуальні основи побудови системи національної кібербезпеки. Визначено напрями вдосконалення й розвитку механізму протидії гібридним загрозам національній безпеці.

Структура і послідовність інформаційного подання результатів дослідження сприяють інтересу до монографії як теоретиків, так і практиків.

Автори висловлюють подяку рецензентам: докторам наук, професорам Мокляку С. П., Семенченко А. І. за зауваження та рекомендації; кандидату наук Старовойтенку О. О. за допомогу в підготовці монографії до друку та оформленні графічного матеріалу.

ВСТУП

Питання гібридних загроз національній безпеці України досліджувалися в наукових працях таких авторів: В. Горбуліна, Є. Магди, А. Слюсаренка, В. Ткаченка, Н. Дорошенка, М. Мальського, В. Мартинюка, В. Предборського, І. Руснака та інших [1–8].

Відомими є наукові розробки Ф. Хофмана, Т. Хубера, В. Немеца, М. Ішервуда, Р. Волкера, П. Мансура [9–14], що розкривають погляди західних фахівців стосовно гібридних війн. Безсумнівний інтерес також становлять роботи російських дослідників, присвячені гібридним війнам та національній безпеці: А. Баротоша, В. Тиханичева, А. Манойло, В. Карякина, А. Гильова, В. Слипченка [15–20].

Однак на сьогодні питання трансформації системи національної безпеки (СНБ) перед викликами гібридної війни та розроблення ефективних механізмів протидії загрозам національній безпеці залишаються недостатньо дослідженими. Тому ця монографія присвячена проблемі підвищення ефективності СНБ і передбачає вирішення таких наукових завдань:

- виконати аналіз еволюції гібридних війн, їх компонентів та особливостей;
- побудувати МГВ;
- визначити поняття, структуру та складові національної безпеки;
- сформувати науково-обґрунтовані погляди на організаційно-правові основи протидії загрозам національній безпеці країни;
- запропонувати концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки;
- розробити концептуальні основи побудови системи національної кібербезпеки;
- обґрунтувати сутність комплексного механізму протидії гібридним загрозам національній безпеці та визначити напрями його вдосконалення і розвитку.

Ураховуючи особливості предметної галузі та сформульованих завдань, під час проведення аналізу гібридних воєн використовувалися такі загальні та спеціальні методи і прийоми пізнання, як порівняння, узагальнення, аналогія. Під час дослідження СНБ, теоретико-методологічних та організаційних основ протидії гібридним загрозам національній безпеці, існуючих загроз національним інтересам країни, як методологічна основа використовувався системний підхід, а також основні положення й методи системного аналізу та теорії прийняття рішень.

ГЛАВА 1
ГІБРИДНІ ВІЙНИ: ЕВОЛЮЦІЯ, ОСОБЛИВОСТІ ТА КОМПОНЕНТИ

Для початку будь-якого дослідження існує потреба чітко визначитися з його категорійним апаратом. Це необхідно для того, щоб і автор, і читачі однаково розуміли його зміст. Тому розглянемо загальноприйняті, найбільш часто використовувані визначення та терміни.

Методологія – вчення про способи, методи і стратегії дослідження предмета.

Концепція – сукупність поглядів на що-небудь і зв'язків між ними, способів розуміння і трактування явища, предмета або процесу.

Концептуальні засади – сукупність теоретичних побудов, що визначають логіку, структуру і принцип функціонування системи.

Принцип – правило, яким керуються при виборі своєї поведінки і при виборі оцінки навколишньої дійсності.

Метод – сукупність дій, необхідних для вирішення певного завдання або досягнення певної мети.

Технологія – сукупність методів та інструментів для досягнення бажаного результату.

Алгоритм – сукупність послідовних кроків, які приводять до бажаного результату.

Засіб – прийом, спосіб дії для досягнення чого-небудь.

Спосіб – можливість, дія для здійснення, досягнення чого-небудь.

Модель – абстрактне уявлення реальності будь-якої форми (математичної, фізичної, символічної, графічної або дескриптивної), що дозволяє отримати відповіді на досліджувані питання.

Система – це сукупність взаємодіючих і взаємопов'язаних елементів, яка володіє похідними властивостями.

Структура – це впорядкована сукупність внутрішніх зв'язків деякого об'єкта, що забезпечують відтворюваність за змінюваних умов, основна характеристика системи, її інваріантний аспект.

Управління – це цілеспрямований і постійний процес впливу суб'єкта управління на об'єкт управління, спрямований на зміну станів об'єктів і (або) суб'єктів заздалегідь продуманим планом дій.

1.1. Гібридні війни: історична ретроспектива

Сама ідея про те, що війна – це не лише прямі бойові дії, не нова. Вона висловлювалася ще в китайському трактаті Сунь-цзи «Мистецтво

війни», написаному в VI ст. до н. е. [21]. У ньому говориться: «Війна – це шлях обману… Найкраща війна – розбити задуми противника. На наступному місці – розбити його союзи. Потім розбити його війська. І найгірше – осаджувати міста». Тобто можна вважати, що перші риси «гібридних» дій були описані ще в VI ст. до н. е.

Утім, аналіз існуючих визначень «гібридних війн» і поглядів фахівців на їх структуру показує, що основна їх складова – це приховане залучення сторонніх збройних угруповань і організацій для вирішення завдань міждержавного протиборства при супроводі озброєних дій, всебічними відволікаючими маневрами [14]. Мета цього – приховати свою участь у конфлікті для однієї зі сторін і не допустити переростання конфлікту в повномасштабну війну. Огляд історії військового мистецтва показує, що подібний принцип використовувався достатньо давно [22]. І цьому сприяло широке розповсюдження найманства в той історичний період, пов'язане з тим, що утримувати постійну боєготовність армії було дорого, дешевше було найняти професіоналів для вирішення конкретних завдань конфлікту. Тому принцип ведення війни чужими руками, силами найманців використовувався з давніх часів [23]. Ще в «Анабасисі» Ксенофонта (Ἀνάβασις – «сходження»), складеному в першій половині IV ст. до н. е., описана історія грецьких найманців [24]. Греки з одних і тих же полюсів воювали і у війську Дарія III, і у воюючому з ним війську Олександра Македонського. Але в ті часи, до появи елементарних основ міжнародного права, найманство не вважалося злочином і велося відкрито, будучи приватною справою самих найманців та їх роботодавців. Саме слово «солдат», що визначає в багатьох мовах військовослужбовця, з'явилося від слова «плата» (лат. Soldus, Solidus). І не важливо, це була плата своїм громадянам-військовослужбовцям, чи найманим представникам чужого народу. У Середньовіччі одними з перших найманцями стали вікінги, які наймалися в особисту гвардію візантійських імператорів. В історіографії Італії пізнього Середньовіччя кондотьєри (італ. Condotta – договір про наймання на військову службу), вожаки загонів найманців, стали невід'ємними фігурами безперервної низки внутрішніх війн між містами-комунами.

У XV-XVII ст. значну роль в європейських війнах відігравали ландскнехти – самостійні загони найманців із різних європейських країн. Не менш відомі швейцарські найманці того часу. У військовій історії XVII ст. можна зустріти численні згадки про ірландських найманців, відомих також як «дикі гуси» (wild geese), звідки й пішов сучасний жаргонний вислів. Широке поширення найманства в цю епоху пов'язане з економічними причинами, а також із тим, що воно було досить легальним. І лише із встановленням перших, ще не надто формалізованих систем міждержавних відносин, дії найманих військових формувань довелося якимось чином приховувати. Принаймні в цивілізованій Європі. Хоча поза її межами найманство, як і раніше, вважалося нормою. Наприклад, в 1830 році для

боротьби проти Аргентини Бразилія найняла німецьких і ірландських найманців, а в 1853 році Мексика набрала німецьких найманців, щоб запобігти спробі державного перевороту. А в його рамках довелося приховувати джерела фінансування й замовника раніше нехитрих найманих формувань.

З точки зору сучасних поглядів, такі наймані формування вже можна вважати підрозділами для ведення гібридних війн та прихованих дій. Яскравий приклад таких прихованих дій – пірати, що нападали на іспанські судна для блокування перевезень в Америку, прийняті в підпорядкування Британією. Дії кораблів сера Френсіса Дрейка (Francis Drake) проти іспанського флоту та узбережжя в період 1572-1596 рр. є типовим прикладом гібридних війн, хоча тоді подібного терміна ще не існувало. Утім, подібні дії можна приписати багатьом, наприклад, відомому османському пірату XV ст. – Хайреддіну Барбароссі (Хизир Рейс).

Проте в гібридній війні використовуються не тільки найманці, а й повстанці, партизани і т. д. Про це докладно пише у своїй статті Джеймс К. Уізер [25]. Військовий історик Петер Р. Мансур, наприклад, визначає гібридну війну як «конфлікт, що має на увазі поєднання конвенціональних військових сил і нерегулярних сил (партизанів, повстанців і терористів), які можуть бути державними або недержавними акторами, що діють в ім'я досягнення спільної політичної мети» [14].

Із цієї точки зору гібридна війна вочевидь не є чимось новим. Існує безліч прикладів гібридної техніки і гібридного підходу на тактичному, оперативному і стратегічному рівнях, що відходять у далеке минуле до часів Пелопоннеської війни і праць уже згадуваного китайського філософа Сунь-дзи. Нерегулярні бійці довели, що можуть стати прокляттям для численних конвенціональних збройних сил. Такі величезні армії, як Велика армія Наполеона та Вермахт Гітлера, з великими зусиллями боролися з нерегулярними бійцями, які розуміли і використовували місцевий людський і географічний ландшафт та нападали на вразливі бази постачання та лінії комунікацій. Згодом партизанські операції почали істотно і стійко впливати на більш широкі конвенційні військові кампанії, частиною яких вони були. Нещодавні антиповстанські кампанії в Іраку та Афганістані ще раз показали, наскільки важко перемогти переконаних нерегулярних бійців, без порушення людських прав місцевого населення, тим самим підриваючи внутрішню і міжнародну суспільну підтримку кампанії.

У 2000-х використання терміна «гібридна» стало звичним способом опису сучасної війни, зокрема, і через зростаючу витонченість та смертоносність недержавних акторів, які використовують насильство, і зростаючий потенціал кібервійни. Хоча не було спільної згоди про те, що це обов'язково є новою формою війни, у визначеннях гібридної війни підкреслювалося злиття конвенціональних і нерегулярних підходів у всьому спектрі конфліктів. Наприклад, у 2007 році Френк Г. Хоффман, провідний ідеолог цієї концепції, дефінував гібридну війну як «загрози, які включають

повний спектр різних способів ведення військових дій, у тому числі використання конвенціональних здібностей, використання тактики нерегулярних сил, терористичні дії із застосуванням недискримінуючого насилля і примусу, заворушення, ініційовані злочинними елементами, які застосовуються обома сторонами і різними недержавними гравцями» [9].

Під час війни з Грузією в 2008 році Росія використовувала поєднання регулярних збройних сил, південноосетинських й абхазьких поліцій і російських сил особливого призначення, що діяли під прикриттям образу сил «місцевої оборони». Вважається, що такі гібридні війни відрізняються від їх форм у минулому, комбінування конвенціональних і нерегулярних методів війни. Тоді конвенційні і нерегулярні операції проводилися паралельно, але окремо одна від одної, а не інтегрованим чином, як зараз. Крім того, операції, що проводилися нерегулярними бійцями, зазвичай були допоміжними для кампаній конвенціональних збройних сил.

До 2014 року найчастіше наведеним прикладом військових дій, що відповідають сучасним дефініціям гібридної війни, був конфлікт між Ізраїлем і «Хезболла». «Хезболла», яка отримувала підготовку й обладнання від Ірану, стала несподіванкою для Ізраїлю у витонченому поєднанні партизанської і конвенційної військових тактик та використанням озброєння і комунікаційних систем, що асоціювалися з озброєними силами розвинених країн. На стратегічному рівні «Хезболла» ефективно використовує Інтернет та інші медіа для інформації і пропаганди. Її інформаційний менеджмент із самого початку конфлікту виявився найбільш успішним та впливовим на світову думку, ніж менеджмент Ізраїлю. Як показують наведені вище приклади, гібридне поєднання конвенціональних і нерегулярних методів війни застосовувалося протягом усієї людської історії. Але приклад «Хезболла» та інші приклади, у тому числі партизани в Чечні, і в останній час Ісламська держава демонструють, що сучасні збройні системи істотно підвищили смертоносність недержавних акторів.

Дії Росії проти України у 2014 році підвищили інтерес до концепції гібридної війни, оскільки слово «гібридна» виявилося найбільш вдалим для опису різноманітності та поєднання інструментів і методів, застосованих РФ під час анексії Криму, підтримки сепаратистських груп на Східній Україні та ведення бойових дій у Донецькій і Луганській областях України.

Результати ретроспективного аналізу виникнення та еволюції гібридних війн систематизовано та наведено в таблиці 1.1.

Таблиця 1.1. Гібридні війни в історичній ретроспективі

№	Назва	Період (рік)	Переможці	Переможені
1	Пелопоннеська війна	431 до н. е. – 405 до н.е.	Делоський союз	Пелопоннеський союз

Продовження таблиці 1.1. Гібридні війни в історичній ретроспективі

2	Завоювання Германії римлянами	12 до н. е. – 12 н. е.	Римська імперія	Германські племена
3	Дев'ятирічна війна	1596 – 1603	Королівство Англія	Ірландські королівства
4	Війна французів і індіанців у Північній Америці	1754 – 1763	Британська імперія, індіанські племена	Королівство Франція, індіанські племена
5	Американська революція	1765 – 1783	Британські колонії в Північній Америці	Британська імперія
6	Піренейська війна	1808 – 1814	Британська імперія, Іспанська імперія, Королівство Португалія	Французька імперія, Королівство Іспанія, Королівство Італія, Неаполітанське королівство, Рейнський союз
7	Експедиція Гарібальді в Південну Італію	1860 – 1861	Гарібальдійці, Сардинське королівство, Британська імперія	Королівство обох Сицилій, Французька імперія, Королівство Іспанія
8	Протипарти-занські дії в ході громадянської війни в США	1861 – 1865	Сполучені штати Америки	Конфедеративні штати Америки
9	Франко-прусська війна	1870 – 1871	Північнонімецький союз, германські королівства і герцогства, Германська імперія	Французька імперія, Французька республіка, гарібальдійці

Продовження таблиці 1.1. Гібридні війни в історичній ретроспективі

10	«Велика гра» (суперництво за панування в Південній і Центральній Азії)	Середина XIX ст. – початок XX ст.	Британська імперія	Російська імперія
11	Британська компанія проти Османської імперії	1916 – 1918	Арабські племена, Британська імперія	Османська імперія
12	Громадянська війна в Китаї	1927 – 1950	Китайська народна республіка Комуністична партія Китаю, Червона армія Китаю, СРСР	Республіка Китай, Гоміндан, США, Німеччина
13	Громадянська війна в Іспанії	1936 – 1939	Іспанія, Німеччина, Італія, Португалія	Іспанія, СРСР, добровольці з країн Європи і США
14	Радянсько-фінляндська війна	1939 – 1940	СРСР	Фінляндія, Німеччина, Фінляндія, добровольці із Швеції та інших країн Європи
15	Японсько-китайська війна	1937 – 1945	Республіка Китай, Гоміндан, США, Великобританія, СРСР	Японська імперія, тимчасовий уряд Республіки Китай (режим Ван Цзинвея)
16	Індокитайська війна	1945 – 1954	В'єтнам, КНР, СРСР	Франція, В'єтнам, Камбоджа, Лаос, Великобританія, США
17	Війна в Кореї	1950 – 1953	КНДР, СРСР, КНР	Республіка Корея, США, Великобританія і союзники

Закінчення таблиці 1.1. Гібридні війни в історичній ретроспективі

18	Війна у В'єтнамі	1965 – 1975	СРВ, СРСР, КНР	Південний В'єтнам, США і їх союзники
19	Війна за незалежність в Еритреї	1961 – 1991	Еритрея, КНР, Судан, Сирія, Ірак, Туніс, Саудівська Аравія, Сомалі, США	Ефіопія, Куба, СРСР, НДР, Ємен, Ізраїль
20	Війна в Анголі	1975 – 2002	Ангола, Куба, СРСР, Португалія, КНДР	Ангола, ЮАР, КНР, Заїр, США
21	Холодна війна	1948 – 1991	США і союзники	СРСР і союзники
22	Війна в Лівії	2011	НАТО, Швеція, Катар, Швеція, Катар, Перехідний національний конгрес Лівії, Єгипет	Лівійська Арабська Джамахірія
23	Війна в Сирії	2011 – т/ч	Сирія, РФ, Туреччина, США і союзники	Сирійська опозиція, Курдські ополченці ІДІЛ
24	Війна в Україні	2013 – т/ч	?	?

Таким чином, аналізуючи історію, можна зробити висновок, що сучасні гібридні війни є не чимось абсолютно новим, а продовженням використовуваних раніше різноманітних форм міждержавного протистояння, що відрізняються комплексним застосуванням різних форм військового і невійськового протиборства, істотним зростанням технологічних можливостей щодо реалізації тих чи інших форм дій, а також масштабами, обумовленими глобалізацією сучасного світу.

1.2. Компоненти гібридних війн та їх особливості

Сутність та зміст війн у сучасних умовах значно змінюються, усе частіше вони носять гібридний характер, хоча даний феномен не можна

вважати абсолютно новим. Так, ще видатний китайський стратег і мислитель Сунь-цзи, що жив у VI–V ст. до н. е., у своєму знаменитому трактаті про військову стратегію «Мистецтво війни» писав: «Здобути сто перемог у ста битвах – це не вершина військового мистецтва. Повалити ворога без бою – ось вершина» [21]. А наприкінці XVII ст. французький вчений Габріель Ноде у своїй праці «Політичні роздуми про високу політику і майстерність державних переворотів» так описував стратегію конфліктів, які сьогодні називають гібридною війною: «Грім падає з небес, перш ніж його можна почути; молитви вимовляють, перш ніж на них скликає дзвін; хтось піддається удару, думаючи, що він сам його завдає; страждають ті, хто ніколи цього не очікував, і вмирають ті, хто думав, що знаходиться в цілковитій безпеці; і все це робиться під покровом ночі і темряви, серед штормів і замішання» [26].

Як бачимо, гібридна війна містить певний набір компонентів та особливостей, за допомогою яких водночас здійснюється вплив на супротивника за різними напрямами. Тому завдання їх більш глибокого дослідження є досить актуальним.

Протягом тривалого історичного періоду можна простежити використання інформаційної складової «гібридних» дій. Так, вправним майстром розроблення та реалізації технологій гібридної війни був ще засновник найбільшої у світовій історії континентальної імперії – Чингісхан (1162–1227). Його баскаки (збирачі податків) виконували роботу сучасних ЗМІ, поширюючи провокаційні і дезінформуючі чутки серед населення, перед походом татар на чужі землі, а мандрівники-агрономи із запасами коренів аїру йшли, розвідуючи шляхи (комунікації) висування кінноти [27]. Корінь аїру проростає лише в чистій воді, яку можуть пити коні. Саме тому в історії немає інформації про випадки загибелі монгольських коней.

Згодом подібні дії ставали все дедалі масштабнішими та різноманітнішими. Так, на думку російського вченого О. Тіханичева, це період від видання книги «Записки про Московію» Сигізмунда Герберштейна, «методички» про Росію для наполеонівської армії до агітаційних листівок часів Першої світової війни [28]. А наполеонівські «методички» й агітаційні листівки послужили прототипом такої складової інформаційної компетентності сучасної гібридної війни, як її медійний супровід [16]. У формі, наближеній до сучасної, цей процес уперше запустила Великобританія, порушивши в 1915 році негласну заборону на публікацію фотографій вбитих солдатів противника. У роки війни у В'єтнамі, з появою телебачення, війна буквально «зробила крок з екранів у кожен будинок». Зараз, в еру всезагальної інформатизації, війна ведеться практично у прямому ефірі. І для «гібридних» дій дуже важливо, хто буде формувати картинку цього ефіру. З урахуванням цього, наразі обсяг і завдання інформаційного протиборства істотно розширюються, створюються спеціалізовані формування інформаційно-психологічної боротьби та навіть кіберсили, здатні координовано проводити інформаційні

операції та кампанії. Як приклад можна навести російські ЗМІ, які виступають виключно за «методичками» Кремля, відому Петербурзьку «фабрику тролів» Пригожина, організовані групи російських хакерів під безпосереднім управлінням ГРУ ГШ РФ і ФСБ, що становлять серйозну загрозу світовому кіберпростору.

З настанням постіндустріальної епохи інформаційне протиборство доповнилося діями в кіберпросторі [29] та застосуванням деструктивних соціально-політичних технологій. Останні зараз використовуються настільки інтенсивно, що їх можна виділити як ще одну складову гібридної війни. Більше того, їх різноманітність навіть дозволяє проводити внутрішню класифікацію таких дій: від простої фінансової та інформаційної підтримки опозиційних течій і створення всередині держави-супротивника «п'ятої колони» до впровадження агентів впливу, які забезпечують так звану м'яку окупацію (soft occupation) країни і перехід її під зовнішнє управління.

Практика показує, що такі дії не лише ефективніші, але й істотно дешевші від прямого військового втручання. Наприклад, на підтримку керованого військового режиму у Венесуелі в 60–70-ті роки минулого століття США витрачали близько 200 мільйонів доларів щорічно. У XXI ст. спроба встановити в цій країні свій уряд коштувала США близько 10–15 мільйонів на рік, що витрачаються на фінансування «опозиції» [30]. Різниця в ціні питання – у рази. Але справа навіть не в економії коштів: для протидії багатьом країнам пряме військове протиборство просто небезпечне, а «розхитування» їх державної системи «зсередини» відносно безпечніше.

Одним з аспектів практичного застосування інформаційного протиборства можна вважати використання як обґрунтування «гібридних» дій національного питання. Здавна фактор національного складу територій міг слугувати підставою для їх анексії сусідніми державами, як це сталося в 1938 році із Судетською та Тешинською областями Чехословаччини, зайнятими під приводом захисту співвітчизників Німеччини та Польщі відповідно. Інший варіант «гібридних» дій – відділення етнічно відмінних регіонів і створення на їх основі окремих «держав» під зовнішнім протекторатом, як це відбулося за «допомогою» РФ із Придністров'ям у 1992 році, Абхазією в 1992–1993 роках, Південною Осетією, де протистояння з Грузією тричі переростало в збройні конфлікти 1991–1992, 2004 і 2008 роки. У новітній історії зі зростанням мобільності населення, подібні «передгібридні» дії можуть реалізовуватися шляхом присвоєння громадянства на території чужої держави, легітимізації громадян, придбання землі або нерухомості, міграції.

Найважливіший аспект гібридних війн – їх економічна складова. В історичній ретроспективі її використання розпочалося після переходу від натурального господарювання і відокремлених національних економік до світової системи господарювання, пов'язаної з міждержавним розподілом праці та міжнародною торгівлею. Історія демонструє безліч методів, що

використовувалися в рамках цієї складової протиборства. Франція в період наполеонівських війн підробляла англійські, австрійські та російські грошові знаки [31]. У наш час, з настанням епохи глобалізації, фінансова складова гібридних війн істотно посилилася як за масштабами застосування, так і за різноманітністю використовуваних методів. Останні змінюються від прямого блокування фінансових рахунків окремих осіб і навіть урядів держав-супротивників до непрямих методів на основі заборон. Прикладом першого типу дій може слугувати блокування закордонних рахунків Іраку в 2012 році і Венесуели в 2019-му. Непрямі методи чітко простежуються в забороні на проходження коштів через «треті країни» і компанії або блокуванні доступу іранських банків до системи SWIFT у 2018 році.

Одним із перших прикладів економічної війни можна назвати «континентальну блокаду»: комплекс заходів із блокування торгівлі Великобританії, що проводилися Францією в 1806–1814 рр. У період XIX–XX ст. найбільш поширеним видом економічної війни була саме морська блокада. До початку Першої світової війни блокаді піддавалися: Туреччина, Португалія, Нідерланди, Колумбія, Панама, Мексика, Аргентина і Сальвадор. Ініціаторами блокад були: Великобританія (12 разів), Франція (11 разів), Італія, Німеччина (3 рази), Австрія і Росія (2 рази) та Чилі [32]. Після Другої світової війни економічні санкції продовжували залишатися активним інструментом міжнародної політики. У період з 1971 року до кінця XX ст. можна зазначити близько 120 випадків санкцій, у першу чергу в рамках економічної війни заходу проти СРСР.

Вказаний інструмент використовується і в XXI ст.: від загороджувального мита до американських законів «Про контроль над експортом», яким у 1949 році був створений Координаційний комітет з експортного контролю, та «Про протидію противникам Америки за допомогою санкцій» (Countering America's Adversaries Through Sanctions Act, CAATSA) 2017 року. Цей тип санкцій фахівцями іноді виділяється в окрему форму дій – технологічне протиборство [33]. Ще одна складова економічного протиборства, що знаходиться на межі гуманітарно-допустимого – ресурсне. Його різновиди застосовувалися з давніх часів у формі блокування фортець при облозі, перекриття доступу провіанту і води. На сьогодні зі зростанням технічних можливостей і різноманітністю економічних зв’язків у сучасному світі з'являються нові форми ресурсного протиборства у формі транспортної, енергетичної та навіть водної блокади, що своїми масштабами призводять до екоциду цілих територій. Типові приклади таких дій – спроба відвести води річки Йордан від Ізраїлю, яка послужила однією з причин «шестиденної війни» 1967 року або кібердиверсії, здійснюваних для руйнування електроенергетики Венесуели в 2019 році [34], а також кібератаки російських хакерів, направлені на державні відомства й об'єкти критичної інфраструктури США, Канади, Великобританії, Німеччини, Франції, Італії та України.

У сучасній історії найбільш раннім із класичних прикладів «гібридних» дій, який реалізує всі компоненти з їх складу, може слугувати громадянська війна в Іспанії 1936–1939 рр. Аналіз цього конфлікту, з точки зору сучасної термінології, показує, що в ньому велося типове «гібридне» протиборство між фашизмом в особі Італії та Німеччини за підтримки Португалії та комунізмом в особі СРСР. Боротьба не просто чужими руками, але і на території чужої країни, при дотриманні угоди про «невтручання», підписаної іншими європейськими державами [35–37]. Надалі прикладів гібридних війн ставало все більше: як у «жорсткому» варіанті, наприклад, силова та інформаційна підтримка дій збройних формувань опозиції і приватних військових компаній у Сирії та Лівії, так і більш м'які варіанти у формі таємної підтримки лідерів різних «революцій» і «національно-визвольних» рухів.

Широке використання інформаційних технологій у сучасних конфліктах прискорює трансформацію війни та надає їй нову якість за рахунок появи військових операцій принципово нового типу, метою яких є інформаційне руйнування соціально вагомих сфер держави та інформаційно-психологічний тиск на супротивника, щоб зламати його волю, без застосування зброї [38].

Російський дослідник В. Карякін зазначає, що в умовах глобалізації та інформаційно-технологічної революції арсенал впливу противника доповнюється технологіями його символічного знищення, направленими на духовні і ціннісно-мотиваційні сфери діяльності людей [18]. Для розуміння й осмислення характеру сучасної війни почесної ролі набуває фактор, що обумовлює вторинність завдань окупації території противника і захоплення ресурсів, на противагу завданням установлення стратегічного, всеосяжного контролю над свідомістю населення країни-мішені та отримання повної влади над завойованою державою.

Однією з найважливіших галузей гібридних операцій є культура, культурно-цивілізаційні цінності і сенсовність населення країни впливу.

При цьому робиться ставка не на зміст, а на мінливість форм, а зміст як такий відходить на другий план та втрачає цінність, і з ним можна виконувати будь-які маніпуляції. Водночас сучасна масова культура передбачає зниження культурної, інтелектуальної планки подання матеріалу для аудиторії. З метою доступності інформація для широкої аудиторії не повинна вимагати великих інтелектуальних зусиль у глядача і слухача, впливаючи виключно на емоції споживача контенту. У результаті не з'явилося жодної принципово нової ідеології або системи цілісних поглядів, які могли б претендувати на цивілізаційну значущість. Замість ідеології пропонується яскравий «піар» із розмитими, нечіткими та доволі широкими інтерпретаціями ідей та сенсів, які хибно трактують як історичну картину, так і сучасне розуміння навколишнього світу. За відсутності ідеології, покликаної спонукати народ до дії, ідеологи гібридних технологій

провокують людей і підбурюють протестні рухи для організації заворушень і різного роду протистоянь.

Тут масова культура, її інформаційно-семантичне поле найчастіше використовується як гібридна зброя війни нового типу. З одного боку, це консцієнтальна зброя, спрямована на злам історичного коду пам'яті народу та знищення об'єктивного трактування світової історії. З іншого – взаємопов’язана з першою морально-правова зброя, коли відверта брехня стає правовою підставою для збройної агресії, арешту іноземних громадян й економічного тиску на державу [15].

Мабуть, саме тому «російсько-українська смислова війна реалізувалася в постійній реінтерпретації подій, коли з двох альтернативних джерел для опису обирається те, яке найбільше відповідає запланованим цілям війни» [2]. На підтвердження цього Євген Магда наводить ряд прикладів даного феномена:

- знищення військової приналежності: «зелені чоловічки», «ввічливі люди»;
- знищення незаконності: «народний мер», «народний губернатор», «народна самооборона», «возз'єднання Криму»;
- посилення негативних характеристик противника: «бойовики», «каратели», «карательна операція», «хунта», «самопроголошена київська влада», «самопроголошений прем'єр»;
- завищення свого позитиву аж до сакралізації: «Крим наш», «місто російських моряків», «місто російської слави»;
- опис дій і підбір відповідної мотивації з метою їх легітимації: захоплення адміністративних будівель пояснюється словами: «Це ж наше, народне, а ми народ».

Мета інформаційної та психологічної війни, за великим рахунком, одна – зламати моральний дух противника, ввести його в оману і в кінцевому підсумку перемогти малими жертвами з мінімальними витратами матеріальних ресурсів. Важливий нюанс – інформаційна та психологічна війна значно дешевше від класичної війни в плані використання матеріальних ресурсів. З іншого боку, у контексті додавання інтелектуальних ресурсів такий вид протиборства є набагато витратніший, оскільки вимагає більш ретельної роботи над проєктуванням стратегії і тактики, обчисленням слабких сторін противника і комплексу заходів впливу, які здатні надати максимальний ефект [39].

Ще як окрему компоненту гібридної війни українські дослідники В. Горбулін і Є. Магда виділяють «енергетичну», хоча зазвичай аналітики енергетичне вимірювання гібридної війни обходять стороною [1, 2]. Воно трохи губиться на тлі недружніх економічних кроків, проявів пропаганди і власне збройного протистояння.

Використання енергетичної зброї для досягнення політичних, стратегічних цілей аж ніяк не є ноу-хау Росії. Достатньо згадати нафтову кризу 1973 року, викликану введенням ембарго ОПЕК на постачання нафти

країнам Заходу, які підтримали Ізраїль у війні Йом-Кіпур. Вуглеводні ніколи не були звичайним товаром, їх ринок традиційно був чутливими до політичних коливань. За часів існування біполярного світу політична складова енергетичних взаємовідносин була радше винятком, ніж правилом, в умовах багатополярного світу енергетичний базис практично не обходиться без політичної надбудови. Спокуса використовувати енергетичні важелі в політичних цілях виглядає прямо пропорційно до реального впливу держави на події у світі.

В умовах якісної зміни сучасних конфліктів, розширення їх географії, по-новому проявляються принципово важливі для дослідження особливості війни. До таких особливостей російський дослідник А. Бартош відносить тертя та зношення війни [40]. Якщо перший термін був уперше введений ще К. Клаузевіцем, то у другого, на його думку, немає належної оцінки в роботах вітчизняних та зарубіжних фахівців.

Для традиційної війни К. Клаузевіц виділяє сім джерел спільного тертя [41]:

- небезпека;
- фізичне напруження;
- невизначеність і недостовірність інформації, на основі якої приймаються рішення;
- випадкові події, які неможливо передбачити;
- фізичні та політичні обмеження у використанні сили;
- непередбачуваність, що є наслідком взаємодії з противником;
- розриви між причинами і наслідками війни.

Появі нових або підвищенню загрозливої актуальності існуючих джерел тертя сприяють головним чином такі особливості конфліктів [42].

Перша – у гібридній війні атакуюча сторона одночасно й адаптивно використовує поєднання широкого спектру звичайних озброєнь, нерегулярної тактики, тероризму та злочинної поведінки в зоні бойових дій для досягнення політичних цілей війни, що значною мірою підвищує дію фактора непередбачуваності.

Друга – відмінність архітектури систем політичного та військового управління об’єкта і суб’єкта гібридної війни. Динаміка розвитку положення приходить у гостре протиріччя з дисбалансом системи державного управління, чому сприятиме порушення каналів узгодження дій між побудованими за ієрархічним принципом державними структурами, що здійснюють керівництво в адміністративно-політичній, військовій, соціально-економічній, фінансовій та культурно-світоглядній сферах.

Третя – зміна природи конфліктів, які виникають у зв’язку з протиріччями серед провідних держав, збільшенням кількості та жорстокості терористичних актів, тривалим збереженням нестабільності в слабких державах і поширенням руйнівних технологій.

Четверта – міжнародний тероризм, який набуває транскордонного розмаху та ігнорує всі правові норми.

П’ята – міграція, яка в країнах Європи зберігає високі темпи. Більшість мігрантів – молоді чоловіки з низьким рівнем освіти, без спеціальності, що перебувають під впливом псевдорелігійних сект або кримінальних організацій.

Говорячи про особливості гібридної війни, не можна не згадати доповідь начальника Генерального штабу ЗС Росії В. Герасимова на засіданні Академії військових наук у лютому 2013 року. Фактично, ще за рік до операції в Криму і подальших подій на Південному Сході України, головний російський воєначальник практично анонсував те, що через рік сталося в Україні [43]: «Війни вже не оголошуються, а розпочавшись – йдуть не за звичним шаблоном. Цілком благополучна держава за лічені місяці та навіть дні може перетворитися на арену запеклої збройної боротьби, стати жертвою іноземної інтервенції, зануритися в пучину хаосу, гуманітарної катастрофи і громадянської війни». Власне, уся суть виступу генерала Герасимова зводилася до тих особливостей збройних конфліктів, які безпосередньо перегукуються з подальшими подіями у Криму і на Південному Сході України: «Акцент використовуваних методів протиборств зміщується в бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів, реалізованих із залученням протестного потенціалу населення. Усе це доповнюється військовими заходами прихованого характеру, у тому числі реалізацією заходів інформаційного протиборства і діями сил спеціальних операцій. До відкритого застосування сили, найчастіше під виглядом миротворчої діяльності та кризового реагування, переходять лише на якомусь етапі, в основному для досягнення остаточного успіху в конфлікті» [43].

На його думку, трансформація сучасних конфліктів спричиняє зміну співвідношення вкладів військових і невійськових видів боротьби в загальний політичний результат війни. За даними російського Генштабу, сьогодні таке співвідношення становить 1:4 на користь невійськових видів боротьби.

Що особливо хотілося б підкреслити в даному ряді форм протиборства, так це те, що широкого поширення набули асиметричні дії, що дозволяють нівелювати перевагу противника в збройній боротьбі. До них відноситься використання сил спеціальних операцій і внутрішньої опозиції, для створення постійно діючого фронту на всій території протидіючої держави, а також інформаційний вплив, форми та способи якого постійно вдосконалюються.

На думку українського дослідника А. Слюсаренка, «асиметричним» війнам і конфліктам притаманні такі властивості [3]:

- завдання декількох зосереджених за часом і місцем невійськових ударів із неочікуваним для противника результатом і

неприйнятним для жертви збитком;

- нав’язування ворогу протиборства в принципово новій системі координат;
- відсутність звичної лінії фронту;
- приховування політичних цілей;
- застосування нових, неочікуваних засобів і форм насильства.

Він також уважає, що найбільш усталеними в науково-практичних міркуваннях сучасних дослідників є такі особливості гібридних війн:

- вона виступає різновидом асиметричних дій;
- інтегрує військові та невійськові інструменти протистояння та охоплює театр прямого конфлікту, тилову зону, простір міждержавних взаємовідносин;
- для неї притаманні інноваційні технології та засоби мобілізації (кібервійна, інформаційно-комунікаційні технології), хоча і не є обов’язковим розроблення нових видів летальної зброї;
- важливими суб’єктами протиборства виступають мережеві та поліцентричні форми (структури);
- вона включає комплекс дій дипломатичного, воєнного, інформаційного, економічного, екологічного характеру тощо;
- надзвичайно широким є комплекс «гібридних» загроз: традиційні воєнні, партизансько-терористичні, інформаційно-психологічні та інші високо-технологічні (наприклад, дії в енергетичній сфері, кібератаки, «кліматична зброя» тощо);
- у гібридних війнах зростає роль сил спеціальних операцій, партизансько-повстанських, терористичних, інших недержавних формувань, включаючи транснаціональну злочинність.

Безперечний інтерес становлять висновки, до яких дійшли деякі російські аналітики. На запитання: як же виглядає сьогодні багатовимірна або гібридна війна, вони звертають увагу на таке [19].

По-перше, це війна всеосяжна, з використанням усіх засобів одночасно, коли і військові, і невійськові форми впливу доповнюють одна одну. Різноманітність задіяних коштів створює в об’єкта атаки відчуття втрати контролю над ситуацією, коли необхідне одночасне планування і координація в реальному часі акцій, у яких в один і той самий момент задіяні спецслужби, фінансові органи, дипломатія, глобальні інформаційні джерела, неурядові організації, а також регулярні і наймані збройні формування.

По-друге, це перманентна війна, розрахована на досягнення мети змором, підривом зсередини, з використанням слабких місць противника. Вона може відбуватися фазами – через загострення і «перемир’я», чим і відрізняється нинішня ситуація в українсько-російських відносинах. Ми повинні твердо усвідомити, що тисячі дрібних ударів мають на меті знесилити, задушити, знекровити, одночасно ведучи переговори і

пропонуючи альтернативи, схиляючи на свій бік, завойовуючи симпатії невдоволених і фрондерів усередині країни.

І, нарешті, по-третє, що особливо важливо в нашому випадку, гібридна війна – це війна ідеологічна. Вона ведеться насамперед за людей, за їх погляди і переконання, а лише потім за територію: для її ведення необхідна мобілізація в багатьох галузях – від морпіхів до хакерів, від банкірів до журналістів. А це неможливо без ідеологічної обробки населення. Необхідною умовою є формування картини світу, поділеного на «хороших» і «поганих». Оскільки будь-яка операція покликана впливати на людей, то пропагандистська складова чи не найголовніша. Особливого значення набуває залучення на свою сторону ЗМІ – як їх керівництва, так і рядових репортерів – для перетворення органів інформації в інформаційно-психологічну зброю.

Ураховуючи особливості гібридних війн, а також їх компоненти, держава повинна мати власну стратегію протидії гібридній агресії. Для протидії гібридній агресії американським ученим Дж. Розенау запропонована класифікація політичної адаптації, що дозволяє на основі системного підходу встановити зв'язки між зовнішньою політикою держави та системою міжнародних відносин [44]. З урахуванням його ідей всю сукупність адаптивних стратегій гібридних війн можна звести до трьох основних типів:

- поступлива – стратегія пасивно пристосовується до викликів, що формуються зовнішнім середовищем, намагається максимально враховувати вимоги міжнародних організацій та окремих центрів сили;
- непоступлива – стратегія намагається відкинути виклики, які надходять із зовнішнього середовища, і базується на пріоритеті національних інтересів;
- запобіжна – стратегія дотримується певного балансу інтересів і запитів із зовнішнього середовища, який виявляється достатньо гнучким та дає можливість для перерозподілу системних ресурсів із запитів зовнішнього середовища на внутрішньосистемні вимоги і навпаки.

У цілому дії, що вважають рисами гібридної війни, багато в чому є традиційними (стандартними) рисами, елементами збройного конфлікту або протистояння держав.

Серед них – економічний тиск і санкції, інформаційна підготовка, політичне оформлення протиборчих сторін, методи таємної війни та робота спецслужб тощо.

Отже, в основі сутності гібридних війн – широкий спектр конфронтаційних дій, до яких вдаються в рамках гнучкої стратегії з довгостроковими цілями, основаної на комплексному застосуванні інформаційних, дипломатичних, воєнних, економічних, військових, ресурсних та інших компонентів для дестабілізації противника.

1.3. Гібридна війна як багатовимірне протистояння

У розроблених у США і НАТО прогнозах розвитку міжнародних процесів на майбутні кілька десятиліть є багато передбачень щодо зростання глобальної нестабільності, одним із чинників якої стане посилення ролі державних і недержавних суб'єктів за умови їх доступу до військових та інформаційних технологій, зброї масового ураження [9]. Як вважають дослідники, відповідно зросте загроза гібридних (асиметричних) війн і конфліктів [10].

Реалізуючи стратегію глобального домінування, військові експерти США зіткнулися з конфліктами більш низького рівня, ніж глобальна війна, висунули концепцію військових конфліктів різної інтенсивності. Інтерес становлять так звані конфлікти малої інтенсивності, які, за визначенням воєнно-політичних експертів, кваліфікуються як «політико-військова конфронтація між ворогуючими державами або групами, що не доходить до рівня звичайної війни, але вища за рівень простого мирного протистояння, охоплює весь спектр дій від підривної діяльності до використання військової сили, ведеться з використанням комбінованих політичних, економічних, інформаційних і воєнних інструментів» [12].

В. Горбулін у монографії «Світова гібридна війна: український фронт» стверджує, що вперше термін «гібридна війна» виник у військовому середовищі США – у Корпусі морської піхоти [1]. З відкритих джерел, цей термін можна зустріти ще до 1998 року, коли Р. Волкер визначив його як поєднання звичайної війни зі спеціальними операціями і дослідив ознаки гібридної війни на прикладі війни США за незалежність [13]. Він вважав, що структурна організація морської піхоти є гібридною за природою, і порушував питання про те, що інші роди військ у нових умовах мають застосовувати цей досвід. В. Немец [11] спробував довести, що поширення «гібридних спільнот» (*hybrid societies*) актуалізує «гібридне ведення війни» (*hybrid warfare*) і потребує створення «гібридних сил» (*hybrid forces*).

Окремі дослідники вважають, що автором концепції «гібридних війн» є Ф. Хоффман, колишній офіцер морської піхоти, а нині – науковий співробітник міністерства оборони США, яку він виклав у монографії «Конфлікт у XXI столітті. Поява гібридної війни» (2007 р.) Він вважається відомим теоретиком у сфері збройних конфліктів та воєнно-політичної стратегії, думку якого беруть до уваги в керівних колах країн НАТО [9]. Хоффман запропонував таке визначення: «Гібридні війни поєднують у собі цілу низку різних режимів ведення війни, включаючи звичайні можливості, іррегулярну тактику і формування, терористичні акти, зокрема, невибіркове насильство і примушення, кримінальний безлад» [45].

У 2009 році поняття «гібридні війни», або «гібридні сценарії військових дій» уточнив колишній міністр оборони США Гейтс. За його твердженням, у таких війнах продукція «Майкрософт» співіснує з мачете, а

технологія «Стелс» – з камікадзе [46].

У своєму звіті за 2017 рік Генеральний секретар НАТО Єнс Столтенберг навів таке визначення: гібридні війни – це «комбінація військових і невійськових, таємних і відкритих дій, що включають дезінформацію, пропаганду, розгортання іррегулярних збройних формувань аж до використання регулярних сил» [9].

Для концептуалізації поняття гібридної війни важливе значення мало формування у США уявлень про багатокомпонентну війну. У 1996 році Т. Гюбер сформулював компактне і зрозуміле визначення основного методу цієї війни: «Багатокомпонентна війна – це одночасне використання проти противника регулярних, або основних, військ та іррегулярних, або повстанських, сил» [10].

Синтез форм і способів збройної боротьби спричиняє появу нових ознак конфліктів, пов'язаних зі зміною співвідношення внеску того чи іншого виду боротьби в загальний політичний успіх війни [40]. У результаті відбувається трансформація сучасних конфліктів від лінійної до нелінійної парадигми війни. Така трансформація найбільш повно описується терміном некласичної філософії «трансгресія» [47]. Трансгресія є не що інше, як зміщення і стирання кордонів між речами та цінностями. Вона передбачає вихід предмета за власні межі.

Генерал М. Ішервуд у монографії «Повітряна міць для гібридної війни», виданій Інститутом Мітчелла Асоціації ВВС США у 2009 році, дає дуже близьке до наведеного академічного визначення трактування гібридної війни: «Вона стирає відмінність між суто конвенційною і типовою нерегулярною війною» [12].

Важливо зауважити, що проблеми сутності й ведення гібридної війни та протистояння її загрозам розглядаються в низці офіційних документів армії США, зокрема в «Білій книзі» командування спеціальних операцій сухопутних військ у розділі «Протидія нетрадиційній війні» та в оперативній концепції армії «перемогти у складному світі». Визначення «гібридні загрози» згадується в останніх американських офіційних оглядах з проблем оборони – 2006, 2010, 2014 і 2018 років. Водночас базове поняття «гібридні загрози» включає такі несприятливі чинники і ворожі наміри, як: кібервійна, імовірність асиметричних конфліктів низької інтенсивності, глобальний тероризм, піратство, незаконна міграція, корупція, етнічні і релігійні конфлікти, безпека ресурсів, демографічні виклики, транснаціональна організована злочинність, проблеми глобалізації та поширення зброї масового знищення.

Те саме знаходимо в колективних документах Північноатлантичного альянсу, концепції – «NATO's Bi-Strategic Command Capstone Concept» (2010 р.), у яких гібридні загрози визначено як такі, що створює противник, здатний одночасно інтегровано використовувати традиційні та нетрадиційні засоби для досягнення власних цілей. У підсумковій декларації саміту (Шотландія, вересень 2014 р.) уперше на високому рівні йшлося про

необхідність готувати збройні сили НАТО до участі у війнах нового типу – гібридних війнах. Під такими війнами треба розуміти широкий спектр прямих бойових дій і таємних операцій, які проводять за єдиним планом збройні сили, партизанські та інші іррегулярні формування за участю різноманітних цивільних компонентів.

В одному з найбільш поширених на Заході тлумачень явища гібридної війни вказується, що цей тип протиборства є комбінацією відкритих і таємних воєнних дій, провокацій і диверсій у поєднанні із запереченням власної причетності до них, що ускладнює повноцінну відповідь на них. У довіднику «Military Balance» за 2015 рік наводиться таке тлумачення гібридної війни: «використання воєнних і невоєнних інструментів в інтегрованій кампанії, спрямованій на досягнення неочікуваності, захоплення ініціативи та отримання психологічних переваг, що використовують дипломатичні можливості; масштабні й блискавичні інформаційні, електронні і кібероперації; прикриття і приховування військових і розвідувальних дій, у поєднанні з економічним тиском» [48].

Деякі російські дослідники та експерти дотримуються погляду, що гібридна війна – це «якісно нове поняття, більш широке, ніж просто сукупність сучасних форм і методів збройної боротьби» [17]. Головною перевагою цього виду міждержавного протистояння порівняно з традиційними є, на думку начальника Генерального штабу Збройних Сил РФ В. Герасимова, саме те, що застосування непрямих асиметричних дій і способів ведення гібридних війн дає можливість позбавити супротивну сторону фактичного суверенітету без захоплення території держави військовою силою [43].

О. Бартош у своїй монографії «Конфлікти XXI століття. Гібридна війна і кольорова революція» стверджує, що гібридизація методів війни нового типу характеризується поєднанням «жорсткої» військової сили зі стратегією «м'якої» сили як системи дипломатичних, економічних, юридичних, політичних і культурологічних інструментів несилового впливу на обстановку в державах відповідно до інтересів національної безпеки [15].

Ф. Хоффман, аналізуючи війни XXI ст., справедливо зауважує, що війна – це не лише воєнні дії, ведення боїв, а також необхідно брати до уваги соціально-культурні, техноекономічні і геополітичні виміри війни. Війна є динамічною реальністю, і наше розуміння та лексикон також мають змінюватися, щоб бути на вістрі часу. Нові умови потребують нових типів зброї для максимально ефективного реагування і нових творчих методів і концепцій [49].

З проведеного аналізу можна зробити висновок, що, незважаючи на деякі відмінності поглядів вітчизняних і зарубіжних дослідників на сутність гібридної війни, у них є багато спільного [50].

На нашу думку, основною відмінністю гібридної війни є те, що протистояння між державами відбувається одночасно в декількох різних вимірах: військовому, політичному, економічному, дипломатичному,

інформаційному, ідеологічному, екологічному, юридичному, соціально-культурному та інших (рис. 1.1).

Рисунок 1.1. Виміри гібридної війни

Отже, гібридна війна є за своєю сутністю багатовимірним міждержавним протистоянням, тому можемо дати визначення гібридної війни як нового рівня геостратегічного протистояння між державами, що відбувається в декількох різних вимірах із використанням мілітарних і немілітарних засобів, за допомогою збройних сил та іррегулярних збройних формувань, які ведуть прями бойові дії і приховані (таємні) операції, що стирає звичні межі між станами війни і миру [51].

Слід також зазначити, що для ефективної протидії агресору недостатньо ввести термін «гібридна війна» тільки в політичний, науковий і військовий дискурс, а необхідно також визначити його дефініцію в правовому полі й відобразити в нормативних та законодавчих актах України.

1.4. Модель гібридної війни

На сьогодні дуже швидко змінюються та розвиваються нові способи ведення гібридної війни, що, у свою чергу, потребує перегляду класичних воєнних методів прогнозування і планування, як наступальних, так і оборонних стратегій. Як і будь-яка інша війна, гібридна війна містить елементи недостовірності та невизначеності [52]. Так, наприклад, недостовірність розвідувальної інформації та постійне втручання випадковостей призводять до того, що сторони конфлікту в дійсності зіштовхуються із цілковито протилежним станом речей, ніж очікували, і це не може не позначатися на плануванні або принаймні на тих уявленнях про положення, які лягли в основу планів.

Одним із способів зменшення невизначеності при прогнозуванні, оцінці ресурсів, розробленні стратегії та контрстратегії є застосування моделювання і сучасних інструментальних засобів підтримки прийняття рішень. Моделювання дозволяє відображати вплив просторових і часових параметрів конфлікту, сприяти проведенню якісного аналізу воєнно-політичних ситуацій у сфері національної і міжнародної безпеки, запобігати впливу фактору спонтанності та забезпечувати обґрунтованість вжитих заходів із протидії противнику [53].

Використання МГВ допоможе оцінювати характер і небезпеку ситуацій, що виникають, визначати ступінь політичного ризику, напрямок політичного процесу, засоби розв’язання кризи, погоджувати застосовуваний комплекс гібридних загроз у рамках єдиного задуму, відображати процеси прогнозування, використання ресурсів і стратегічного планування. Вона являє собою інструмент для символічного відображення структури і стратегії управління процесами підготовки та ведення (або організації відсічі) гібридної війни, шляхом приведення їх у відповідність із задумом та цілями протиборства.

Для побудови МГВ необхідно насамперед сформулювати її призначення та вимоги до неї. МГВ повинна відображати багатовимірний характер гібридної війни, операції якої охоплюють адміністративно-політичну, фінансово-економічну і культурно-світоглядну сфери держави-жертви, проводяться в інформаційному та кіберпросторах.

Розглянуті процеси та етапи створення МГВ як складної системи повинні базуватися на таких методологічних елементах, як: системний підхід, системний аналіз, моделі супроводу її на етапах життєвого циклу (ЖЦ), математичне та імітаційне моделювання.

Системний підхід, як відомо, – універсальна методологія, яка має три складові: цілеорієнтація, систематизація і формалізація. Будь-яка складна система орієнтована на задоволення певних потреб людини, а метою процесу побудови є створення такої системи. Глобальна мета

декомпозується на цілі нижчих рівнів, які досягаються шляхом вирішення сукупності завдань [54].

Загалом модель – це абстрактне уявлення реальності в будь-якій формі (математичній, фізичній, символічній, графічній або дескриптивній), що дозволяє отримати відповіді на досліджувані питання. У нашому дослідженні МГВ являтиме собою графічно-математичний опис, який визначає її цілі, завдання, методи і засоби.

На першому рівні, згідно із задумом, розробляються та аналізуються можливі сценарії розвитку обстановки, кожен з яких може включати опис ймовірного початку, розвитку, завершення та наслідків реалізації комплексу гібридних загроз, дій щодо забезпечення міжнародної безпеки.

Джерелами інформації для вибору сценарію, здійснення контролю за ходом його реалізації, про конкретні політичні ситуації, що сприяють або перешкоджають розвитку обстановки в рамках обраного сценарію, можуть бути дипломатичні органи, всі види розвідки, міжнародні, державні та приватні інформаційно-аналітичні структури, ЗМІ. Ці ж самі структури, на основі первинного аналізу даних про стан ситуацій, і формулюють пропозиції щодо коригування стратегії гібридної війни у необхідному напрямку.

Оброблені, перевірені та узагальнені відомості про стан розвитку у сфері безпеки у вигляді інформаційних доносів, довідок та аналітичних звітів і слугують основою для аналізу та прийняття рішень щодо впливу на ситуацію та (або) коригування сценарію.

На другому рівні, відповідно до обраного сценарію, здійснюється розподіл та постановка завдань виконавцям та планування операцій для досягнення поставлених цілей. На основі аналізу інформації про розвиток обстановки та її відповідність до сценарію, розробляються вказівки щодо практичних дій на виконавчому рівні, а також готуються пропозиції для прийняття рішень на першому рівні.

На третьому рівні здійснюється вибір оптимальних методів вирішення конкретних задач, а на четвертому – засобів їх реалізації.

Під час дослідження МГВ її представляють як об’єкт, що має просторові та часові обмеження. На першому етапі, дотримуючись системного аналізу як прикладної наукової методології [55, 56], необхідно виділити МГВ за певними ознаками із зовнішнього середовища, установивши водночас саме ті відносини, які її з нею пов’язують. Далі, виходячи з мети створення МГВ, формують її елементарний базис, структуру, визначають функції. Ураховуючи, що будь-який аналіз базується на декомпозиції, необхідно звертати увагу на явище емерджентності, вплив зовнішнього середовища. У результаті виконання системного аналізу отримуємо системну МГВ [57] (рис. 1.2.).

Сукупність цілей визнається у вигляді певної системи E_z. Тоді будь-який елемент $e \in E_z$ можна представити у вигляді:

$$e =< R_e, Q_e, P_e, V_e, T_e >, \quad (1.1)$$

де R_e – результат, досягнення якого необхідне, відповідно до заданої цілі;

Q_e – вектор параметрів, що характеризують необхідну кількість R_e;

P_e – вектор параметрів вимог, що висуваються до процесу отримання результату R_e;

V_e – вектор параметрів, що характеризують витрати ресурсів на отримання R_e;

T_e – час отримання результату R_e.

Безліч задач, вирішення яких необхідне для досягнення цілі e_0, позначається E_s. Для множин E_z і E_s справедливе наступне співвідношення [58]. Задача $s \in E_s$ стає ціллю $s \in E_z$, якщо задані величини Q, V, T, де Q – вектор якості результатів вирішення задачі s, V – вектор, що характеризує витрати ресурсів на розв'язання задачі, T – час завершення рішення. Метод визначається як система (E_a, S_a), де E_a – безліч операцій (кінцеве), S_a – структура на множині операцій.

Система E_c, що реалізує рівень засобів, являє собою сімку елементів:

$$E_c =< M_e, M_a, L, O, I, P, T > \quad (1.2)$$

із заданою структурою S_c, де складові елементи – види забезпечень: M_e – методичне, M_a – математичне, L – лінгвістичне, O – організаційне, I – інформаційне, P – програмне, T – технічне.

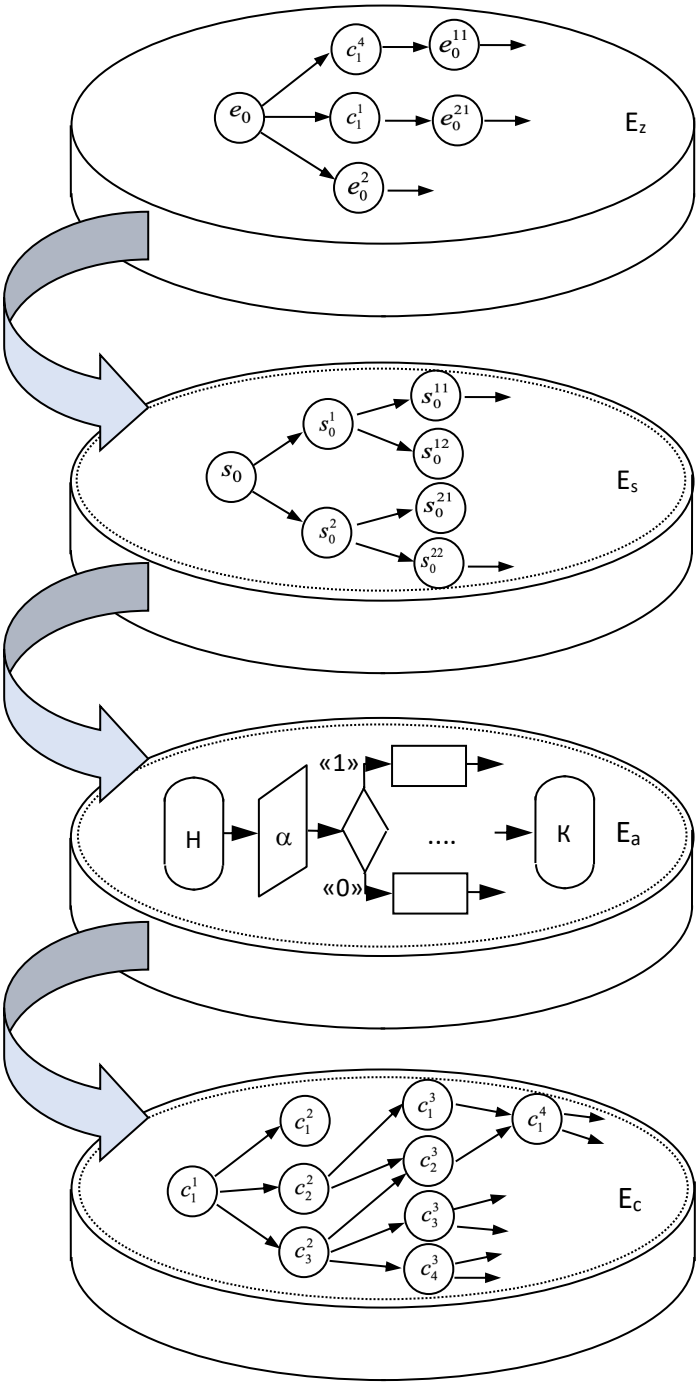

Рисунок 1.2. Системна МГВ

Особливість процесу системного дослідження – його ітераційний характер, що реалізується через ланцюг відображень:

$$E_z \to E_s \to E_a \to E_c, \tag{1.3}$$

де E_z – непорожня множина цілей, E_s – кінцева множина задач, E_a – кінцева множина методів, E_c – непорожня множина засобів.

Для трансформації <цілі>→<засоби> основним атрибутом служить категорія ймовірного, для зворотної трансформації <засоби>→<цілі> – категорія бажаного (рис. 1.3).

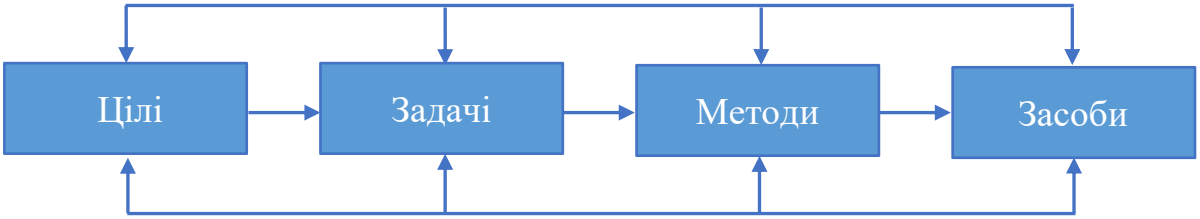

Рисунок 1.3. Ітераційний процес формування системної МГВ

Наступною складовою процесу створення МГВ є її прогнозуючий супровід на всіх етапах ЖЦ [59]. МГВ у процесі ЖЦ динамічна на етапах функціонування та модернізації. Функціонування разом із модернізацією є певним логіко-динамічним процесом. Моделюючи гібридну війну, здійснюємо тим самим прогнозування за рахунок вирішення завдань ідентифікації невідомих залежностей та їх оптимізації на основі статистичної та експертної інформації (рис. 1.4).

Рисунок 1.4. Моделювання гібридної війни

Ураховуючи вищенаведені складові, очевидно, що побудова МГВ супроводжується необхідністю вибору оптимальних варіантів з альтернативних. Для вирішення цього завдання необхідно використовувати сценарний аналіз, прогнозування, теорію і методи прийняття рішень.

Ефективні технології підтримки прийняття рішень при побудові МГВ не можуть бути реалізовані без СППР, у якій базовими елементами є завдання ідентифікації, класифікації, оптимізації, експертного оцінювання та вибору, які можуть бути вирішені за допомогою технологій, наведених на рис.1.5.

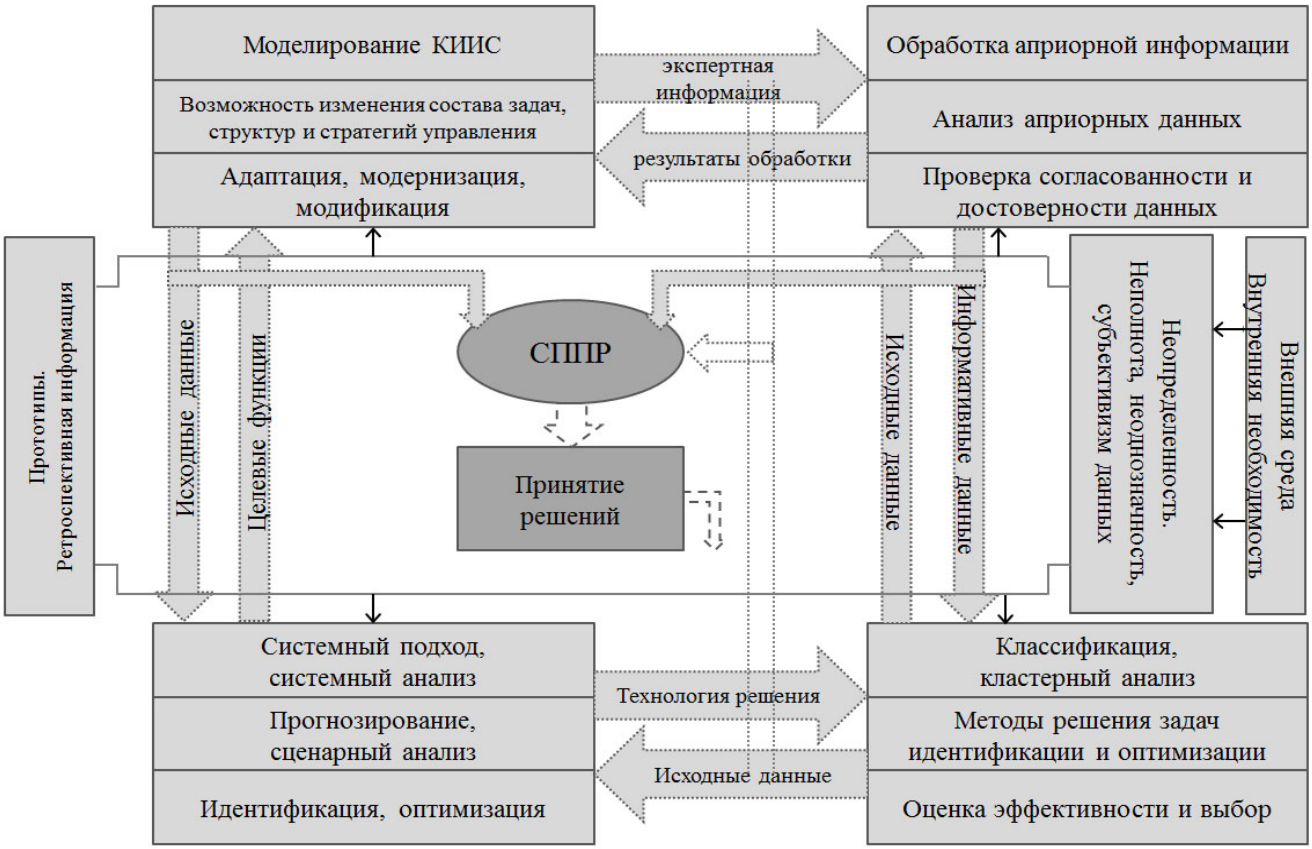

Рис. 1.5. Інтеграція технологій для побудови МГВ

Застосування МГВ дозволить досліджувати та аналізувати ідеї, концепції, принципи, методи та інструментальні засоби, які мають практичне застосування. Виявлення особливостей вказаних елементів, предметних областей їх застосування дозволить оцінити переваги МГВ, що є умовою для її успішної побудови та ефективного використання.

Отже, у зв'язку зі зростаючими труднощами здобуття нових знань, моделювання набуває все більшої значущості в дослідженні проблем гібридних війн. При цьому моделі виступають як ефективний інструмент вивчення конфліктів XXI ст. і використовуються для вирішення завдань управління, створюючи основу для трансформації об'єкта вивчення в інтересах забезпечення національної безпеки.

Висновки до першої глави

Проведений ретроспективний аналіз виникнення й еволюції гібридних війн показав, що сучасні гібридні війни є не чимось абсолютно новим, а продовженням використовуваних раніше різноманітних форм міждержавного протистояння, що відрізняються комплексним застосуванням різних форм військового і невійськового протиборства, істотним зростанням технологічних можливостей щодо реалізації тих чи інших форм дій, а також масштабами, обумовленими глобалізацією сучасного світу. У цілому дії, що вважають рисами гібридної війни, багато в чому є традиційними рисами, елементами збройного конфлікту або протистояння держав. Серед них – економічний тиск і санкції, інформаційна підготовка, політичне оформлення протиборчих сторін, методи таємної війни та робота спецслужб тощо. В основі сутності гібридних війн – широкий спектр конфронтаційних дій, до яких вдаються в рамках гнучкої стратегії з довгостроковими цілями, заснованої на комплексному застосуванні інформаційних, дипломатичних, воєнних, економічних, військових, ресурсних та інших компонентів для дестабілізації противника.

Отже, гібридна війна за своєю сутністю є новим рівнем геостратегічного протистояння між державами, що відбувається в декількох різних вимірах, з використанням мілітарних і немілітарних засобів, за допомогою збройних сил та іррегулярних збройних формувань, які ведуть прями бойові дії і таємні операції, що стирає звичні межі між станами війни і миру. Ураховуючи особливості гібридних війн, а також їх компоненти, держава повинна мати власну стратегію протидії гібридній агресії.

У зв’язку зі зростаючими труднощами здобуття нових знань моделювання набуває все більшої значущості в дослідженні проблем гібридних війн. При цьому моделі виступають як ефективний інструмент вивчення конфліктів XXI ст. і використовуються для вирішення завдань управління, створюючи основу для трансформації об’єкта вивчення в інтересах забезпечення національної безпеки. Застосування запропонованої МГВ дозволить досліджувати та аналізувати ідеї, концепції, принципи, методи та інструментальні засоби, які мають практичне застосування при протидії гібридній агресії.

ГЛАВА 2
СИСТЕМА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

2.1. Національна безпека: поняття, складові, чинники впливу

Поняття «національна безпека» вживається стосовно широкого кола соціальних систем для характеристики їх захисту від різних негативних впливів природного і соціального характеру. Це поняття характеризує ступінь захищеності життєво важливих інтересів, прав і свобод особи, суспільства та держави від зовнішніх і внутрішніх загроз, або ступінь відсутності загроз правам та свободам людини, базовим інтересам і цінностям суспільства та держави. Її можна розглядати як специфічну властивість динамічних систем, комплексний критерій оцінки їх якості та ефективності [60].

Під соціальною системою зазвичай розуміють сукупність соціальних явищ та процесів, основним елементом яких є люди, їх взаємодія, відносини та зв'язки [61].

Динамічні системи – це системи, які під дією зовнішніх і внутрішніх сил змінюють свій стан у часі [62]. Найважливішою властивістю динамічних систем є їх стійкість: збереження системою своєї базової структури і основних виконуваних функцій протягом певного часу за зовнішніх впливів і внутрішніх збурень. Розвиток цих систем передбачає такі зміни їх структурної організації, які ведуть до більш ефективного виконання системою своїх основних функцій.

Поняття – «якість» – це сукупність характеристик об’єкта, які відносяться до його здатності задовольняти встановлені або передбачені вимоги, які дозволяють ефективно його використовувати за призначенням [63]. Цими об’єктами можуть бути як товари і послуги, так і будь-які процеси та суспільні відносини, зокрема соціально-економічні і політичні. У нашому дослідженні – це весь комплекс суспільних процесів і відносин, які охоплюються системою національної безпеки.

Найбільш відповідне в нашому випадку визначення поняття «ефективність» – це показник досягнення системою встановлених цілей у процесі її функціонування [64].

Національна безпека є кількісно-якісною характеристикою розвитку соціальної системи, тобто є не тільки оцінкою певної захищеності цієї системи від потенційних і реальних загроз. Вона відображає результати впливу тенденцій розвитку та умов життєдіяльності соціуму, його інститутів, за яких забезпечується збереження якісної визначеності соціальної системи і вільне функціонування, яке відповідає її природі.

На сьогодні існує велике розмаїття визначень національної безпеки, та їх автори мають власні думки і підходи з приводу трактування даного поняття.

Глазов О. В. зазначає, що національна безпека – це захищеність життєво важливих інтересів особистості, суспільства і держави в різних сферах життєдіяльності від зовнішніх та внутрішніх загроз, що забезпечує стійкий розвиток країни [65].

Ліпкан В. А. тлумачить його з іншого ракурсу як сукупність офіційно прийнятих поглядів на цілі і державну стратегію в частині забезпечення безпеки особистості, суспільства та держави від зовнішніх і внутрішніх загроз політичного, економічного, соціального, військового, техногенного, екологічного, інформаційного та іншого характеру з урахуванням наявних ресурсів і можливостей [66].

Національну безпеку також розуміють як здатність нації задовольняти потреби, необхідні для її самозбереження, самовідтворення і самовдосконалення з мінімальним ризиком збитку для базових цінностей її нинішнього стану [67].

Російський політолог Н. А. Косолапов пропонує таке тлумачення поняття «національна безпека», як стабільність, яка може підтримуватися протягом тривалого часу, стан досить розумної динамічної захищеності від найбільш істотних із реально існуючих загроз і небезпек, а також здатність розпізнавати такі виклики та своєчасно вживати необхідних заходів для їх нейтралізації [68].

Деякі дослідники визначають безпеку як стан, за якого відсутні загрози. Так, А. Возженніков зазначає: «Під національною безпекою розуміється стан країни, за якого відсутні або усунені реальні зовнішні та внутрішні загрози її національним інтересам і національному характеру життя» [69].

Виходячи з об’єктно-суб’єктної парадигми національної безпеки, Циганов В. В. її характеризує як міру реального рівня прав і свобод членів людського співтовариства (громадян) держави, що відповідає цьому співтовариству [70].

У Законі України «Про основи національної безпеки України» № 964-IV від 19 червня 2003 р. так розгорнуто тлумачиться це поняття: національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, охорони дитинства, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, кібербезпеки і кіберзахисту, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових

послуг, захисту прав власності, фондових ринків й обігу цінних паперів, податково-бюджетної та митної політики, торгівлі і підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості і сільського господарства, транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам».

Закон України «Про національну безпеку України» № 2469-VIII від 21 червня 2018 р. значно лаконічніше сформулював це поняття без переліку національних інтересів: «національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз».

Сьогодні виокремлюються принаймні три основних теоретичних підходи в розумінні сутності національної безпеки.

У межах першого підходу, представниками якого є А. Волферс, Д. Гадді, Г. Даєм, Дж. Джонсон, Д. Кауфман, Р. Коен, М. Міхалка та ін., увага акцентується на захисті цінностей суспільства. Серед базових цінностей виокремлюють політичну незалежність, економічний добробут, розвиток, справедливість тощо. При цьому безпека визначається не лише як захищеність національних цінностей, але і як їх безперешкодне поширення. Ці положення закріплені і в Стратегії національної безпеки США, у якій інші держави розглядаються в контексті їх відношення до демократичних цінностей. У ній стверджується, що «з метою захисту нашої нації та поваги до наших цінностей Сполучені Штати прагнуть поширити свободу у всьому світі, очолюючи міжнародні зусилля зі знищення тиранії і підтримки ефективної демократії» [71]. Пояснити цей погляд на безпеку і її забезпечення можна, проаналізувавши думки, висловлені Ф. Фукуямою в праці «Кінець історії та остання людина» і С. Хантінгтоном у роботі «Зіткнення цивілізацій». Ф. Фукуяма стверджує про те, що ліберальні демократії не становлять загрозу одна одній, а тому війна між справді демократичними державами фактично неможлива [72]. Що ж до С. Хантінгтона, то він вважає, що лінії розлому між цивілізаціями (культурами, системами цінностей) і є лініями фронтів у майбутніх війнах [73]. Проте такий підхід до забезпечення національної безпеки шляхом поширення власних цінностей навіть за допомогою збройних сил містить у собі деструктивний потенціал конфліктності. Український науковець у сфері національної безпеки та антитерористичної діяльності О. Бодрук із цього приводу цілком слушно зазначає, що дані положення ґрунтуються на усталених процесах розвитку західного суспільства, ринковій економіці,

індивідуалізмі, розвинутій демократії, а тому не завжди відповідають реаліям сьогодення [74].

Представники другого напрямку наголошують на взаємозв'язку національних цінностей та інтересів, необхідності врахування їх взаємообумовленості в дослідженні проблем національної безпеки. Серед них можна назвати А. Величка, І. Волощука, В. Горбуліна, Б. Демидова, А. Качинського, В. Ліпкана, Г. Ситника та ін.

Третій напрям наукових розробок полягає в дослідженні національної безпеки в контексті захисту національних інтересів. Представниками цього напряму є ряд українських, російських та західних науковців: А. Бетлер, В. Богданович, О. Бодрук, С. Браун, О. Данільян, О. Дзьобань, М. Каплан, Г. Моргентау, М. Панов, С. Хоффман та ін. Слід також звернути увагу на розширення змісту поняття «національна безпека»: якщо раніше забезпечення національної безпеки розглядалось у контексті захисту інтересів насамперед держави, то в сучасних дослідженнях концентрується увага на захисті інтересів особи (громадянина) та суспільства [75]. Зокрема, це положення відображене у вже не чинному Законі України «Про основи національної безпеки України». Такий підхід, на нашу думку, не зовсім відповідає сучасним вимогам, оскільки зосереджує увагу виключно на інтересах держави, розвитку її економічного та військового потенціалу і підпорядкування цим цілям інтересів окремих особистостей, виникненню внутрішньодержавних конфліктів, у кінцевому результаті призводить до дезінтеграційних процесів. Проблема співвідношення інтересів особи, суспільства і держави в політиці національної безпеки остаточно не вирішена на користь інтересів людини. Справа в тому, що в системі забезпечення національної безпеки провідну, системоутворюючу роль відіграє держава. Саме державні органи і посадові особи формують нормативно-правову базу у сфері забезпечення національної безпеки, приймають рішення щодо запобігання і нейтралізації загроз, виконання яких має обов'язковий характер. Важливою також є монополія держави на застосування державної воєнної організації та здійснення інших передбачених законами заходів примусового характеру щодо забезпечення національної безпеки.

На сучасному етапі розвитку науки безпекознавства виділяють такі основні складові національної безпеки (рис. 2.1): безпека особистості; державна безпека – поняття, що характеризує рівень захищеності держави від зовнішніх і внутрішніх загроз; громадська безпека – поняття, виражене рівнем захищеності особистості і суспільства, переважно, від внутрішніх загроз; техногенна безпека – рівень захищеності від загроз техногенного характеру; екологічна безпека і захист від загроз стихійних лих; економічна безпека; енергетична безпека (як складова економічної безпеки); інформаційна безпека; кібербезпека.

Рисунок 2.1. Основні складові національної безпеки

Головними об’єктами національної безпеки виступають громадяни (їх права і свободи), суспільство (його духовні та матеріальні цінності), держава (її конституційний устрій, суверенітет і територіальна цілісність). На цій підставі основними чинниками впливу на національну безпеку можна визначити [76]:

- національну незалежність і суверенітет, територіальну цілісність держави;
- розвиненість громадянського суспільства, рівень демократизму, сформованість та дієвість законодавчої бази правової держави, захищеність особи;
- економічні можливості держави;
- стан збройних сил, їхню боєздатність та боєготовність;
- національне визначення та самобутність;
- розвиток національної самосвідомості та культури;
- наявність загальної стратегії національного розвитку, «національної ідеї», загальновизнаної мети;
- національну згоду і єдність;
- внутрішньополітичну стабільність;
- готовність та здатність політичних сил реалізувати загальновизначені цілі.

А основними завданнями забезпечення національної безпеки є: захист державного ладу; захист суспільного ладу; забезпечення територіальної недоторканності і суверенітету; забезпечення політичної та економічної незалежності нації; забезпечення здоров'я нації; охорона громадського порядку; боротьба зі злочинністю; забезпечення техногенної безпеки; захист від загроз стихійних лих.

Отже, розглянувши поняття сутності національної безпеки, її основні складові та чинники впливу на національну безпеку України в умовах сучасних гібридних загроз, стає зрозумілим, що забезпечення національної безпеки являє собою комплекс політичних, економічних, соціальних, правових і військових заходів, спрямованих на гарантування нормальної життєдіяльності нації та усунення можливих загроз. Тому національну безпеку в цілому та її складові можна розглядати як стан, коли відсутня небезпека. А бажаний рівень національної безпеки як мету, спосіб або необхідну умову життєдіяльності людини, соціальної групи, суспільства і держави.

2.3. Основні суб'єкти протидії загрозам національній безпеці

Розглянемо більш детально основних суб'єктів протидії загрозам національній безпеці та окреслимо їх функції.

Президент України як глава держави забезпечує державну незалежність, національну безпеку і правонаступництво держави і безперервність функціонування державної влади, є Верховним Головнокомандувачем ЗСУ, призначає на посади та звільняє з посад вище командування ЗСУ, інших утворених відповідно до законів військових формувань, здійснює керівництво у сферах національної безпеки та оборони держави, очолює Раду національної безпеки і оборони України, здійснює інші повноваження, визначені Конституцією України у сфері забезпечення національної безпеки і оборони. Він визначатиме стратегічні цілі та основні завдання державної політики у сфері національної безпеки і оборони України, завдання складових сектору безпеки і оборони в мирний час, у кризових ситуаціях, що загрожують національній безпеці, і в особливий період, цілі та пріоритетні напрями розвитку складових сектору безпеки і оборони, мету, завдання, строки затвердження документів планування розвитку сектору безпеки і оборони та його складових.

Рада національної безпеки і оборони України та Апарат Ради національної безпеки і оборони України відповідно до Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України [77]. Функціями Ради національної безпеки і оборони України є:

- внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони;

- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в мирний час;
- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та в разі виникнення кризових ситуацій, що загрожують національній безпеці України.

Пріоритетами діяльності Апарату Ради національної безпеки і оборони України визначаються:

- інформаційно-аналітичне та організаційне забезпечення діяльності Ради національної безпеки і оборони України як координаційного органу з питань національної безпеки і оборони при Президентові України;
- забезпечення здійснення Радою національної безпеки і оборони України координації та контролю за діяльністю органів виконавчої влади, інших державних органів у сфері національної безпеки і оборони;
- підготовка пропозицій щодо вдосконалення законодавства з питань національної безпеки і оборони, уточнення Стратегії національної безпеки України, Воєнної доктрини України, інших актів з питань національної безпеки і оборони;
- вивчення та аналіз ситуації у сфері національної безпеки і оборони, функціонування сектору безпеки і оборони України та діяльності його складових, діяльності інших державних органів у цій сфері, підготовка та внесення Президентові України, Раді національної безпеки і оборони України та за їх дорученням органам виконавчої влади та іншим державним органам відповідних пропозицій;
- забезпечення роботи Головного ситуаційного центру України, забезпечення з використанням можливостей Головного ситуаційного центру України ефективної діяльності єдиної системи ситуаційних центрів державних органів, що входять до сектору безпеки і оборони;
- організація функціонування робочих та консультативних органів Ради національної безпеки і оборони України.

Міністерство оборони України є головним органом у системі центральних органів виконавчої влади, який забезпечує формування та реалізує державну політику з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва в мирний час та особливий період, а також центральним органом виконавчої влади та військового управління, у підпорядкуванні якого перебувають ЗСУ та Держспецтрансслужба. Міноборони є уповноваженим центральним органом виконавчої влади в галузі державної авіації. Його основними завданнями є [78]:

- забезпечення формування та реалізація державної політики з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва в мирний час та особливий період щодо:

- організації в силах оборони заходів оборонного планування;
- визначення засад воєнної, військової кадрової та військово-технічної політики у сфері оборони;

➢ здійснення військово-політичного та адміністративного керівництва ЗСУ;

➢ здійснення в установленому порядку координації діяльності державних органів та органів місцевого самоврядування щодо підготовки держави до оборони;

➢ забезпечення в межах повноважень, передбачених законом, реалізації державної політики з оборонних питань, що пов'язані з використанням повітряного простору України та захистом суверенітету держави;

➢ координація діяльності Держспецтрансслужби для забезпечення стійкого функціонування транспорту в мирний час та в особливий період.

ЗСУ – це військове формування, на яке відповідно до Конституції України покладаються оборона України, захист її суверенітету, територіальної цілісності і недоторканності. ЗСУ забезпечують стримування збройної агресії проти України та відсіч їй, охорону повітряного простору держави та підводного простору в межах територіального моря України у випадках, визначених законом, беруть участь у заходах, спрямованих на боротьбу з тероризмом [79].

Органи військового управління розвідки та військові частини розвідки ЗСУ, Сили спеціальних операцій ЗСУ відповідно до закону можуть залучатися до заходів добування розвідувальної інформації з метою підготовки держави до оборони, підготовки та проведення спеціальних операцій та/або спеціальних дій, забезпечення готовності ЗСУ до оборони держави. Сили спеціальних операцій ЗСУ здійснюють спеціальну розвідку та не можуть бути використані для обмеження прав і свобод громадян або з метою повалення конституційного ладу, усунення органів державної влади чи перешкоджання їх діяльності.

Ніякі надзвичайні обставини, накази чи розпорядження командирів і начальників не можуть бути підставою для будь-яких незаконних дій по відношенню до цивільного населення, його майна та навколишнього середовища.

Міністерство внутрішніх справ України (МВС) є центральним органом виконавчої влади, діяльність якого спрямовується і координується КМУ, що забезпечує формування державної політики у сферах [80]:

- забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку, а також надання поліцейських послуг;
- захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні;

- цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;
- міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Основними завданнями МВС є забезпечення формування державної політики у сферах:

- охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, забезпечення публічної безпеки і порядку, а також надання поліцейських послуг;
- захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні;
- цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;
- міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Національна гвардія України є військовим формуванням із правоохоронними функціями, що входить до системи Міністерства внутрішніх справ України і призначена для виконання завдань із захисту та охорони життя, прав, свобод і законних інтересів громадян, суспільства і держави від злочинних та інших протиправних посягань, охорони громадського порядку та забезпечення громадської безпеки, а також у взаємодії з правоохоронними органами – із забезпечення державної безпеки і захисту державного кордону, припинення терористичної діяльності, діяльності незаконних воєнізованих або збройних формувань (груп), терористичних організацій, організованих груп та злочинних організацій [81]. Вона бере участь відповідно до закону у взаємодії із ЗСУ у відсічі збройній агресії проти України та ліквідації збройного конфлікту шляхом ведення воєнних (бойових) дій, а також у виконанні завдань територіальної оборони.

Основними функціями Національної гвардії України є:

- захист конституційного ладу України, цілісності її території від спроб зміни їх насильницьким шляхом;
- охорона громадського порядку, забезпечення захисту та охорони життя, здоров’я, прав, свобод і законних інтересів громадян;
- участь у забезпеченні громадської безпеки та охорони громадського порядку під час проведення зборів, мітингів, походів,

демонстрацій та інших масових заходів, що створюють небезпеку для життя та здоров'я громадян;

- забезпечення охорони органів державної влади, перелік яких визначається КМУ, участь у здійсненні заходів державної охорони органів державної влади та посадових осіб;
- охорона ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, важливих державних об'єктів, перелік яких визначається КМУ;
- охорона спеціальних вантажів, перелік яких визначається КМУ;
- охорона дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних організацій в Україні;
- охорона центральних баз матеріально-технічного забезпечення МВС;
- участь у здійсненні заходів, пов'язаних із припиненням збройних конфліктів та інших провокацій на державному кордоні, а також заходів щодо недопущення масового переходу державного кордону з території суміжних держав;
- участь у спеціальних операціях із знешкодження озброєних злочинців, припиненні діяльності не передбачених законом воєнізованих або збройних формувань (груп), організованих груп та злочинних організацій на території України, а також у заходах, пов'язаних із припиненням терористичної діяльності;
- участь у припиненні масових заворушень;
- участь у відновленні правопорядку в разі виникнення міжнаціональних і міжконфесійних конфліктів, розблокуванні або припиненні протиправних дій у разі захоплення важливих державних об'єктів або місцевостей, що загрожує безпеці громадян і порушує нормальну діяльність органів державної влади та органів місцевого самоврядування;
- участь у підтриманні або відновленні правопорядку в районах виникнення особливо тяжких надзвичайних ситуацій техногенного чи природного характеру (стихійного лиха, катастроф, особливо великих пожеж, застосування засобів ураження, пандемій, панзоотій тощо), що створюють загрозу життю та здоров'ю населення;
- участь у відновленні конституційного правопорядку в разі здійснення спроб захоплення державної влади чи зміни конституційного ладу шляхом насильства, у відновленні діяльності органів державної влади, органів місцевого самоврядування;
- участь у ліквідації наслідків надзвичайних або кризових ситуацій на об'єктах, що нею охороняються;
- участь у здійсненні заходів правового режиму воєнного стану;
- участь у виконанні завдань територіальної оборони;

- оборона важливих державних об’єктів, спеціальних вантажів, переліки яких визначаються Президентом України, КМУ, центральних баз матеріально-технічного забезпечення МВС;
- участь у припиненні групових протиправних дій осіб, узятих під варту, засуджених, а також ліквідації наслідків таких дій в установах попереднього ув’язнення, виконання покарань;
- забезпечення внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та підтримання таких відомостей в актуальному стані в межах, визначених законодавством.

Національна поліція є центральним органом виконавчої влади, діяльність якого спрямовується та координується КМУ через МВС і який реалізує державну політику у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку [82]. Основними завданнями Національної поліції є:

- реалізація державної політики у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку;
- внесення на розгляд МВС пропозицій щодо забезпечення формування державної політики в зазначених сферах;
- надання в межах, визначених законом, послуг із допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

На *Державну прикордонну службу* України покладаються завдання щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні [83]. Основні функції Державної прикордонної служби України. Її основними функціями є:

- охорона державного кордону України на суші, морі, річках, озерах та інших водоймах із метою недопущення незаконної зміни проходження його лінії, забезпечення дотримання режиму державного кордону та прикордонного режиму;
- здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України та до тимчасово окупованої території і з неї осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення;
- охорона суверенних прав України в її виключній (морській) економічній зоні та контроль за реалізацією прав і виконанням зобов’язань у цій зоні інших держав, українських та іноземних юридичних і фізичних осіб, міжнародних організацій;
- ведення розвідувальної, інформаційно-аналітичної та оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону України згідно із законами України «Про розвідувальні органи України» та «Про оперативно-розшукову діяльність»;

- участь у боротьбі з організованою злочинністю та протидія незаконній міграції на державному кордоні України та в межах контрольованих прикордонних районів;
- участь у заходах, спрямованих на боротьбу з тероризмом, а також припинення діяльності незаконних воєнізованих або збройних формувань (груп), організованих груп та злочинних організацій, що порушили порядок перетину державного кордону України;
- участь у здійсненні державної охорони місць постійного і тимчасового перебування Президента України та посадових осіб, визначених у Законі України «Про державну охорону органів державної влади України та посадових осіб»;
- охорона закордонних дипломатичних установ України;
- координація діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України та пропуску до тимчасово окупованої території і з неї, а також діяльності державних органів, що здійснюють різні види контролю під час перетину державного кордону України та пропуску до тимчасово окупованої території і з неї або беруть участь у забезпеченні режиму державного кордону, прикордонного режиму і режиму в пунктах пропуску через державний кордон України та в контрольних пунктах в'їзду – виїзду.

Державна міграційна служба України (ДМСУ) є центральним органом виконавчої влади, діяльність якого спрямовується та координується КМУ через Міністра внутрішніх справ і який реалізує державну політику у сферах міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів [84]. Основними завданнями ДМСУ є:

- реалізація державної політики у сферах міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів;
- внесення на розгляд МВС пропозицій щодо забезпечення формування державної політики у сферах міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Державна служба України з надзвичайних ситуацій (ДСНС) є центральним органом виконавчої влади, діяльність якого спрямовується і координується КМУ через Міністра внутрішніх справ і який реалізує державну політику у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних

служб, а також гідрометеорологічної діяльності [85]. Основними завданнями ДСНС є:

- реалізація державної політики у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій, запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;
- здійснення державного нагляду (контролю) за додержанням і виконанням вимог законодавства у сфері цивільного захисту, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб;
- внесення на розгляд МВС пропозицій щодо забезпечення формування державної політики в зазначених сферах;
- реалізація в межах повноважень, передбачених законом, державної політики у сфері волонтерської діяльності.

Служба безпеки України (СБУ) – державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України [86]. Для організації і проведення антитерористичних операцій та координації діяльності суб'єктів, які ведуть боротьбу з тероризмом чи залучаються до антитерористичних операцій, при СБУ функціонує Антитерористичний центр. На СБУ покладається в межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань СБУ входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Державна охорона органів державної влади України та посадових осіб – це система організаційно-правових, режимних, оперативно-розшукових, інженерно-технічних та інших заходів, які здійснюються спеціально уповноваженими державними органами з метою забезпечення нормального функціонування органів державної влади України, безпеки посадових осіб та об’єктів [87]. Її функції не поширюються на заходи охоронного характеру, які здійснюються державними органами з метою забезпечення безпеки учасників кримінального судочинства. Вона здійснює охорону ВРУ; КМУ; Конституційного Суду України; Верховного Суду. Забезпечує охорону і безпеку Президента України в місцях його постійного і тимчасового перебування. Протягом строку повноважень Президента України також забезпечується безпека членів сім’ї, які проживають разом із ним або супроводжують його. Після припинення повноважень Президент

України забезпечується державною охороною довічно, якщо тільки він не був усунений з поста в порядку імпічменту. Також забезпечується охорона Голови ВРУ; Прем'єр-міністра України; Голови Конституційного Суду України; Голови Верховного Суду; Першого заступника Голови ВРУ; Першого віцепрем'єр-міністра України; Міністра закордонних справ України; Генерального прокурора. Протягом строку повноважень цих осіб забезпечується безпека членів їхніх сімей, які проживають разом із ними або супроводжують їх. Після припинення повноважень зазначені посадові особи забезпечуються державною охороною протягом року, крім випадків набрання законної сили обвинувального вироку щодо них.

Державна охорона здійснюється щодо глав іноземних держав, парламентів та урядів і членів їхніх сімей, міністрів закордонних справ, керівників міжнародних організацій (інших посадових осіб міжнародних організацій), які прибувають в Україну чи перебувають на її території у складі офіційних делегацій або відвідують Україну на запрошення органів державної влади. Перелік посадових осіб міжнародних організацій, стосовно яких здійснюється державна охорона, визначає Президент України.

Державна охорона в разі наявності загрози життю чи здоров'ю може здійснюватися щодо народних депутатів України, членів КМУ, керівників центральних органів виконавчої влади, які не є членами КМУ, суддів Конституційного Суду України та Верховного Суду, Голови Національного банку України, Голови Верховної Ради Автономної Республіки Крим, Голови Ради міністрів Автономної Республіки Крим.

Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку тощо [88]. Вона є складовою сектору безпеки і оборони України. Її основними завданнями є:

- формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів у частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;

- участь у формуванні та реалізації державної політики у сферах електронного документообігу (у частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), електронних довірчих послуг;
- забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

Державна спеціальна служба транспорту є спеціалізованим військовим формуванням, що входить до системи Міністерства оборони України, призначеним для забезпечення стійкого функціонування транспорту в мирний час та в особливий період [89]. Її основними завданнями є:

- технічне прикриття, відбудова, встановлення загороджень на об'єктах національної транспортної системи України з метою забезпечення діяльності ЗСУ та інших військових формувань;
- будівництво та ремонт у мирний час і в умовах воєнного стану нових та підвищення строку експлуатації і пропускної спроможності діючих об'єктів національної транспортної системи;
- відбудова транспортних комунікацій, порушених унаслідок надзвичайних ситуацій техногенного та природного характеру, аварій і катастроф;
- охорона об'єктів національної транспортної системи України в мирний час і в особливий період;
- виконання інших завдань, пов'язаних з участю в обороні держави та забезпеченням ефективного функціонування національної транспортної системи України.

Служба зовнішньої розвідки України є державним органом, який здійснює розвідувальну діяльність у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах та підконтрольна Президентові України і ВРУ [90]. На неї покладається:

- добування, аналітичне оброблення та надання розвідувальної інформації Президентові України, Голові ВРУ, Прем'єр-міністрові України та іншим визначеним Президентом України споживачам;
- здійснення спеціальних заходів впливу, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного і науково-технічного розвитку;
- участь у забезпеченні безпечного функціонування установ України за кордоном, безпеки співробітників цих установ та членів їх сімей у країні перебування, а також відряджених за кордон громадян України, які обізнані з відомостями, що становлять державну таємницю;

- участь у боротьбі з тероризмом, міжнародною організованою злочинністю, незаконним обігом наркотичних засобів, незаконною торгівлею зброєю і технологією її виготовлення, незаконною міграцією;
- вжиття заходів протидії зовнішнім загрозам національній безпеці України, зокрема в кіберпросторі, життю, здоров'ю її громадян та об'єктам державної власності за межами України.

Крім Служби зовнішньої розвідки України до розвідувальних органів належать [91]:

- розвідувальний орган МОУ, який поширює свою компетенцію на воєнну, воєнно-політичну, воєнно-технічну, воєнно-економічну, інформаційну та екологічну сферу національної безпеки, який може залучати органи військового управління розвідки та військові частини розвідки ЗСУ щодо добування розвідувальної інформації з метою підготовки і застосування ЗСУ для оборони держави та боротьби з тероризмом, шляхом застосування технічних засобів розвідки, а в особливий період і під час залучення до боротьби з тероризмом – спеціальні технічні засоби з непоширенням на них норм Закону України «Про оперативно-розшукову діяльність»;
- розвідувальний орган спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону, який поширює свою компетенцію на прикордонну та еміграційну політику, а також й щодо інших сфер, що стосуються питань захисту державного кордону України та її суверенних прав у виключній (морській) економічній зоні України.

Координацію діяльності розвідувальних органів України здійснює Президент України через очолювану ним Раду національної безпеки і оборони України.

До суб’єктів протидії загрозам національної безпеки в умовах гібридної війни належить центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику. На сьогодні до нього належить Міністерство економічного розвитку і торгівлі України. У Концепції розвитку сектору безпеки і оборони України зазначається, що його основною метою є розвиток оборонно-промислового комплексу, створення умов для виведення оборонно-промислового комплексу України на якісно новий рівень виробництва озброєння і військової техніки для забезпечення потреб ЗСУ та інших військових формувань і правоохоронних органів, який дасть змогу створити цілісну систему, здатну до відтворення та функціонування на принципі збалансованості.

Отже, суб’єкти протидії загрозам національної безпеки в умовах гібридної війни як комплексна система відображаються в чинному законодавстві України у змістовній формі складу сектору безпеки і оборони України з відповідними функціональними обов’язками. Ця система динамічна як за формою, так і функціональним змістом, адже залежно від

соціально-економічних та воєнно-політичних змін, які трансформують зовнішні і внутрішні загрози національній безпеці України, буде змінюватися склад сектору безпеки і оборони України, його стратегічні та тактичні цілі, а відповідно й функціональні обов'язки його складових.

2.3. Система забезпечення національної безпеки

Національна безпека будь-якої держави потребує наявності системи її забезпечення для виконання певних дій, спрямованих на захист національних цінностей і реалізацію національних інтересів. І це є СЗНБ [92].

СЗНБ являє собою організаційну систему державних і недержавних інституцій, інших суб'єктів, які покликані вирішувати завдання забезпечення національної безпеки у визначений законодавством спосіб.

Основним завданням функціонування СЗНБ є організація процесу управління загрозами і ризиками, за якого державними і недержавними інституціями та окремими особами гарантується збереження і зміцнення національних цінностей, захист і прогресивний розвиток національних інтересів шляхом своєчасного виявлення, упередження, локалізації, нейтралізації, подолання внутрішніх і зовнішніх загроз, а також забезпечення ефективного функціонування самої системи забезпечення національної безпеки та її складових.

СЗНБ є цілісною системою, елементи якої тісно пов'язані між собою. Розрив цих зв'язків може призвести до руйнації всієї системи. Основними елементами СЗНБ є її суб'єкти і об'єкти. Для забезпечення цілісності СЗНБ важливе значення мають також прямі та зворотні зв'язки між ними, взаємодія з владно-політичною організацією держави в цілому, вплив внутрішнього і зовнішнього середовища.

Як основні об'єкти СЗНБ слід розглядати національні цінності і національні інтереси. Розглядаючи національні цінності і національні інтереси через призму їх носіїв, можна розглядати також таку класифікацію об'єктів СЗНБ:

- держава (конституційний лад, суверенітет і територіальну цілісність України, політичну, економічну та соціальну стабільність, законність і правопорядок, розвиток рівноправної взаємовигідної міжнародної співпраці тощо);
- суспільство (розвиток демократії, збереження культури і духовно-історичної спадщини, досягнення й розвиток суспільної злагоди, політична стабільність, віротерпимість тощо);
- людина і громадянин (життя, здоров'я, культура, традиції тощо).

Суб'єктами системи забезпечення національної безпеки виступають: держава (у т. ч. її інститути, посадові особи), суспільство (соціальні верстви та групи, громадські організації), а також окремі громадяни. При цьому

головним суб’єктом забезпечення національної безпеки виступає держава, яка здійснює свої функції через органи законодавчої, виконавчої та судової гілок влади. Держава визначає пріоритетні цілі у сфері забезпечення національної безпеки, а також шляхи, сили, засоби, форми й методи, необхідні задля їхнього досягнення. Саме вона організовує взаємодію державних і недержавних інституцій, безпосередньо приймає рішення щодо застосування сил та засобів системи забезпечення національної безпеки.

У взаємодії об'єктів і суб'єктів системи забезпечення національної безпеки виникають деякі функціональні особливості. Так, завдання щодо забезпечення національних інтересів покладаються, передусім, на державу та її інститути, а суспільство і громадяни беруть меншу участь у відповідних процесах. Таким чином, суб'єкти СЗНБ тісно взаємодіють між собою, але кожен із них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції. У результаті такої взаємодії суб'єкти СЗНБ доповнюють один одного, утворюючи єдину організаційно-функціональну систему.

За своєю організаційно-функціональною та ресурсною спроможністю СЗНБ повинна, передусім, гарантувати суверенітет, територіальну цілісність, сталий розвиток, добробут та фізичну безпеку громадян.

Ключовим елементом системи забезпечення національної безпеки є сектор безпеки і оборони. Він являє собою охоплену єдиним керівництвом сукупність органів державної влади, правоохоронних та спеціальних органів і служб, діяльність яких спрямована на захист національних інтересів від зовнішніх і внутрішніх загроз шляхом проведення спеціальних заходів, правового примусу або застосування зброї в межах наданих їм повноважень.

До основних функцій СЗНБ належать:

- стратегічне прогнозування і планування у сфері забезпечення національної безпеки;
- виявлення, відстеження динаміки та визначення граничних значень загроз національній безпеці;
- розроблення і здійснення комплексу заходів щодо запобігання, нейтралізації загроз та відновленню нормального функціонування об’єктів національної безпеки;
- підтримання високого стану надійності функціонування системи забезпечення національної безпеки, забезпечення оперативного переходу в режим функціонування в кризовій ситуації, розвитку СЗНБ;
- участь у створенні ефективної системи регіональної та глобальної системи безпеки.

СЗНБ має всі ознаки складних системних утворень, зокрема, такі:

- елементи СЗНБ поєднані певною структурою, мають внутрішні системоутворюючі зв’язки і взаємовпливи;

- СЗНБ має таку стрижневу якість системи, як єдність і цілісність. При цьому єдність забезпечується її загальними цілями, засадами, принципами, організаційними нормами, безперервністю, а також охопленням усього спектру суб'єктів і об’єктів. Цілісність СЗНБ полягає в тому, що всі її структурні елементи є об’єктивно обумовленими і необхідними;
- СЗНБ є керованою системою. Вона передбачає наявність відповідних структур, а також чітко регламентованого процесу прийняття і реалізації управлінських рішень;
- структурні елементи СЗНБ, як і сама система в цілому, у певних межах можуть адаптуватися, зберігати відносну стійкість та самостійність. Вони не залишаються незмінними, а постійно розвиваються відповідно до суспільних змін та державної політики у сфері національної безпеки;
- СЗНБ має власні цілі, завдання, функції, принципи функціонування та розвитку, а також методи забезпечення поставлених завдань, взаємодія яких і забезпечує ефективне функціонування самої системи;
- СЗНБ має власні ексклюзивні функції, які покликані розв'язувати існуючі протиріччя та приводити об’єкт безпеки у відповідність до існуючих реалій у сфері національної безпеки.

Побудована за роки незалежності СЗНБ країни під час загострення відносин із РФ виявила свою слабкість. Непідготовленими до російської агресії виявились як суб’єкти забезпечення національної безпеки, так і законодавча основа їх діяльності. Серед головних причин, які призвели до низької ефективності системи забезпечення національної безпеки України, можна виділити такі:

- СЗНБ будувалася на основі застарілої радянської системи, з використанням її складових (радянської армії, міліції, КДБ, прикордонних військ, які залишились Україні у спадок від СРСР), радянського законодавства і досвіду її функціонування в минулому столітті в умовах двополярного світу;
- формування СЗНБ відбувалося під тиском світових та регіональних лідерів, які виходили з власних національних інтересів, а не інтересів України, як приклад, це вимоги до України стосовно відмови від ядерної зброї без надання їй дієвих гарантій безпеки;
- політичне керівництво України протягом усього періоду незалежності нашої держави формально ставилося до захисту національних інтересів, не докладало необхідних зусиль для формування і розвитку СЗНБ (хронічне недофінансування програм розвитку складових сектору безпеки з кожним роком погіршувало їх стан і вело до поширення корупції та повного занепаду);
- багатовекторна зовнішня політика в умовах цілеспрямованого поглиблення розбіжностей у політичних орієнтаціях населення за

регіональним принципом і налаштованість представників політичного керівництва держави на реалізацію власних, корпоративних, а не національних інтересів сприяли відцентровим тенденціям і неготовності СЗНБ до протидії загрозі сепаратизму;

- незавершеність формування і, як наслідок, неспроможність самої СЗНБ України до аналізу безпекового середовища та своєчасного виявлення загроз, а також значний вплив на керівництво суб'єктів забезпечення національної безпеки України з боку іноземних спецслужб приводило до вироблення помилкових управлінських рішень із питань забезпечення національної безпеки.

Саме ці причини спонукали ініціювання питання про докорінне реформування СЗНБ починаючи від створення моделі її функціонування та формування цілісної системи законодавчих актів у сфері національної безпеки і оборони України.

Висновки до другої глави

Розглянувши поняття сутності національної безпеки, її основні складові та чинники впливу на національну безпеку України в умовах сучасних гібридних загроз, стає зрозумілим, що забезпечення національної безпеки являє собою комплекс політичних, економічних, соціальних, правових і військових заходів, спрямованих на гарантування нормальної життєдіяльності нації та усунення можливих загроз. Тому національну безпеку в цілому та її складові можна розглядати як стан, коли відсутня небезпека, а бажаний рівень національної безпеки як мету, або необхідну умову життєдіяльності людини, соціальної групи, суспільства і держави.

СЗНБ являє собою організаційну систему державних і недержавних інституцій, інших суб'єктів, які покликані вирішувати завдання забезпечення національної безпеки у визначений законодавством спосіб. Основним завданням функціонування СЗНБ є організація процесу управління загрозами і ризиками, за якого державними і недержавними інституціями та окремими особами гарантується збереження і зміцнення національних цінностей, захист і прогресивний розвиток національних інтересів шляхом своєчасного виявлення, упередження, локалізації, нейтралізації, подолання внутрішніх і зовнішніх загроз, а також забезпечення ефективного функціонування самої системи забезпечення національної безпеки та її складових.

До суб'єктів протидії загрозам національній безпеці в умовах гібридної війни належать центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику. На сьогодні до нього належить Міністерство економічного розвитку і торгівлі України. У Концепції розвитку сектору безпеки і оборони України зазначається, що його основною метою є розвиток оборонно-промислового комплексу, створення умов для виведення

оборонно-промислового комплексу України на якісно новий рівень виробництва озброєння і військової техніки для забезпечення потреб ЗСУ та інших військових формувань і правоохоронних органів, який дасть змогу створити цілісну систему, здатну до відтворення та функціонування на принципі збалансованості.

Отже, суб'єкти протидії загрозам національній безпеці в умовах гібридної війни як комплексна система відображається в чинному законодавстві України у змістовній формі складу сектору безпеки і оборони України з відповідними функціональними обов'язками. Ця система динамічна як за формою, так і функціональним змістом, адже залежно від соціально-економічних та воєнно-політичних змін, які трансформують зовнішні і внутрішні загрози національній безпеці України, буде змінюватися склад сектору безпеки і оборони України, його стратегічні та тактичні цілі, а відповідно й функціональні обов'язки його складових.

ГЛАВА 3
ТЕОРЕТИКО-МЕТОДИЧНІ ТА ОРГАНІЗАЦІЙНІ ОСНОВИ ПРОТИДІЇ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

3.1. Організаційно-правові основи протидії гібридним загрозам національній безпеці

В умовах сучасних гібридних загроз систему національної безпеки України необхідно постійно вдосконалювати та динамічно змінювати, зокрема, і її організаційно-правові основи. Тому завдання дослідження організаційно-правових аспектів протидії загрозам національній безпеці держави є актуальним [93].

Указом Президента України № 92/2016 було затверджене рішення Ради національної безпеки і оборони України від 04.03.2016 р. «Про Концепцію розвитку сектору безпеки і оборони України», яка визначає систему поглядів на розвиток безпекових та оборонних спроможностей України в середньостроковій перспективі, сформованих на основі оцінки безпекового середовища та фінансово-економічних можливостей держави, здійснених у рамках комплексного огляду сектору безпеки і оборони України [94]. Правовою основою Концепції є Конституція та закони України. У Концепції визначена цілісна система управління сектором безпеки і оборони для забезпечення своєчасного й адекватного реагування на кризові ситуації, які загрожують національній безпеці, удосконалення системи планування в секторі безпеки та оборони, забезпечення раціонального використання державних ресурсів. У ній також визначена організаційна структура сектору безпеки і оборони України (рис. 3.1).

Концепцією ця організаційна структура значно розширена шляхом створення умов для широкого залучення недержавних організацій до виконання завдань в інтересах національної безпеки і оборони держави. Найбільш перспективними напрямами їх діяльності мають бути: надання послуг в інтересах виконання миротворчих завдань ЗСУ; функціонування мережі недержавних дослідних інституцій, що фахово опікуються проблемами безпеки та оборони тощо.

Рисунок 3.1. Організаційна структура сектору безпеки і оборони України

Основними завданнями сектору безпеки і оборони є: оборона України, захист її державного суверенітету, територіальної цілісності і недоторканності; захист державного кордону України; захист

конституційного ладу, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувальної і підривної діяльності іноземних спеціальних служб, посягань із боку окремих організацій, груп та осіб, а також забезпечення громадської безпеки та охорони державної таємниці, іншої інформації з обмеженим доступом; попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України, боротьба з тероризмом, корупцією та організованою злочинністю у сфері управління та економіки; забезпечення інформаційної та кібербезпеки; надання допомоги органам виконавчої влади та органам місцевого самоврядування в запобіганні та ліквідації наслідків надзвичайних ситуацій природного та техногенного характеру, а також воєнного характеру, розвиток міжнародної співпраці в цій сфері; участь у забезпеченні міжнародної стабільності та безпеки.

Указ Президента України № 287/2015 від 26.05.2015 р. про рішення Ради національної безпеки і оборони України від 06.05.2015 р. «Про Стратегію національної безпеки України», із змінами і доповненнями, внесеними Указом Президента України від 14.09.2020 р. № 392/2020 (із змінами, внесеними згідно з Указом Президента № 392/2020 від 14.09. 2020 р.) [95]. Стратегія національної безпеки України визначає: пріоритети національних інтересів України та забезпечення національної безпеки, цілі та основні напрями державної політики у сфері національної безпеки; поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов; основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки; напрями та завдання реформування й розвитку сектору безпеки і оборони; ресурси, необхідні для реалізації Стратегії.

Стратегія є основою для розроблення таких документів щодо планування у сферах національної безпеки і оборони, які визначатимуть шляхи та інструменти її реалізації: Стратегія людського розвитку; Стратегія воєнної безпеки України; Стратегія громадської безпеки та цивільного захисту України; Стратегія розвитку оборонно-промислового комплексу України; Стратегія економічної безпеки; Стратегія енергетичної безпеки; Стратегія екологічної безпеки та адаптації до зміни клімату; Стратегія біобезпеки та біологічного захисту; Стратегія інформаційної безпеки; Стратегія кібербезпеки України; Стратегія зовнішньополітичної діяльності; Стратегія забезпечення державної безпеки; Стратегія інтегрованого управління кордонами; Стратегія продовольчої безпеки; Національна розвідувальна програма.

Законом України «Про національну безпеку України» № 2469-VIII (2469-19) від 21.06.2018 р., із змінами і доповненнями, внесеними Законами України № 522-IX від 04.03.2020 р., № 808-IX від 17.07.2020 р.,

№ 912-IX від 17.09.2020 р., відповідно до ст. 1, 2, 17, 18 і 92 Конституції України, визначаються основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз [96]. Цим Законом також визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи в такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони.

Законом України від 01.07.2010 р. № 2411-VI «Про засади внутрішньої і зовнішньої політики» (зі змінами та доповненнями, внесеними згідно із Законами № 1170-VII від 27.03.2014 р., ВВР, 2014, № 22, ст. 816; № 35-VIII від 23.12.2014 р., ВВР, 2015, № 4, ст. 13; № 2091-VIII від 08.06.2017 р., ВВР, 2017, № 30, ст. 329; № 2180-VIII від 07.11.2017 р., ВВР, 2017, № 51-52, ст. 445; № 2469-VIII від 21.06.2018 р., ВВР, 2018, № 31, ст. 241) визначаються засади внутрішньої політики України у сферах розбудови державності, розвитку місцевого самоврядування та стимулювання розвитку регіонів, формування інститутів громадянського суспільства, національної безпеки і оборони, в економічній, соціальній та гуманітарній сферах, в екологічній сфері і сфері техногенної безпеки, а також засади зовнішньої політики України. Цим Законом визначається організаційно-функціональна структура СНБ, зокрема й в сучасних умовах гібридної війни на теренах Сходу України [97].

Воєнна доктрина України затверджена Указом Президента України від 24.09.2015 р. № 555/2015 про рішення Ради національної безпеки і оборони України від 02.09.2015 р. «Про нову редакцію Воєнної доктрини України» [98]. Нова редакція Воєнної доктрини України є системою поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів, яка базується на Стратегії національної безпеки України і Закону України «Про оборону України» та відредагована відповідно до сучасного внутрішнього і зовнішнього соціально-економічного та воєнно-політичного становища України.

Указ Президента України № 73/2017 від 22.03.2017 р. «Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Державну програму розвитку Збройних Сил України на період до 2020 року», у якому на підстави розглянутого проєкта Державної програми розвитку ЗСУ на період до 2020 року, розробленої МОУ на основі положень

Стратегічного оборонного бюлетеня України, рекомендується Президентові України затвердити Державну програму розвитку ЗСУ на період до 2020 року, а КМУ – забезпечити виконання Державної програми розвитку ЗСУ на період до 2020 року та інформувати щороку до 31 березня про підсумки виконання Державної програми розвитку ЗСУ на період до 2020 року за попередній рік [99].

Указом Президента України № 691/2014 від 27.09.2014 р. «Про рішення Ради національної безпеки і оборони України від 27.09.2014 р. «Про заходи щодо удосконалення державної військово-технічної політики» запроваджувалася низка секретних заходів щодо припинення експорту до РФ товарів військового призначення та подвійного використання з метою їх військового кінцевого використання РФ, за винятком космічної техніки, яка застосовується для досліджень та використання космосу в мирних цілях у рамках міжнародних космічних проєктів [100].

Указ Президента України від 03.11.2014 р. № 842/2014 «Про рішення Ради національної безпеки і оборони України від 12.09.2014 р. «Про комплекс заходів щодо зміцнення обороноздатності держави та пропозиції до проєкту Закону України «Про Державний бюджет України на 2015 рік» по статтях, пов'язаних із забезпеченням національної безпеки і оборони України» вводив у дію такий комплекс заходів [101]: перегляд порядку комплектування ЗСУ та інших утворених відповідно до законів України військових формувань особовим складом, сформованим на добровільній основі, передбачивши, зокрема, укладання короткострокових контрактів на проходження військової служби; впровадження заходів щодо відновлення початкової військової підготовки в загальноосвітніх навчальних закладах; опрацювання питання формування оптимальної моделі забезпечення безпеки України, зокрема щодо укладання багатостороннього міжнародного договору або двосторонніх міжнародних договорів України з іншими державами про надання Україні дієвих гарантій безпеки для захисту її суверенітету і територіальної цілісності; розроблення пропозиції щодо вдосконалення системи мобілізаційної підготовки та мобілізації; забезпечення вирішення питання щодо збільшення у військових формуваннях та правоохоронних органах України кількості посад, що заміщуються цивільними працівниками; розроблення і внесення на розгляд ВРУ законопроєкту про систему державного прогнозування та стратегічного планування; розроблення проєкту концепції розвитку сектору безпеки і оборони України; впровадження заходів щодо позбавлення в установленому порядку МОУ невластивих йому функцій з управління об'єктами державної власності, з реалізації надлишкового військового майна, майна, що набуло непридатного стану для подальшого використання ЗСУ; встановлення винагороди особовому складу ЗСУ, інших військових формувань та правоохоронних органів України за безпосередню участь у воєнних операціях залежно від складності виконуваних бойових завдань; невідкладне опрацювання питання розширення виробництва товарів

військового призначення та подвійного використання, для чого організувати інвентаризацію основних засобів виробництва підприємств ОПК; впровадження заходів щодо вдосконалення національної системи стандартизації і кодифікації товарів військового призначення та подвійного використання, модернізації ОПК, впровадження науково-технічних (експериментальних) розробок у виробництво товарів військового призначення та подвійного використання; забезпечення спрощеного порядку прийняття на озброєння ЗСУ зразків озброєння, військової та спеціальної техніки; розроблення разом із ДСНС плану розмінування територій Донецької та Луганської областей, а також пропозиції щодо актуалізації Положення про територіальну оборону України.

Указ Президента України № 831/2019 від 08.11.2019 р. «Про Рішення Ради національної безпеки і оборони України від 02.11.2019 р. «Про Міжвідомчу комісію з питань оборонно-промислового комплексу» затвердив положення щодо функціонування цієї комісії, яка є робочим органом Ради національної безпеки і оборони України з такими функціями [102]: концептуальних засад, пріоритетних напрямів та рішень із питань державної військово-технічної і військово-промислової політики та функціонування оборонно-промислового комплексу; реалізації науково-технічної, інвестиційної та інноваційної політики у сфері розроблення, виробництва, модернізації та ремонту озброєння і військової техніки, реформування та розвитку оборонно-промислового комплексу, збереження і розвитку виробничих потужностей та кадрового потенціалу підприємств оборонно-промислового комплексу; удосконалення координації та контролю діяльності органів виконавчої влади у сфері реалізації державної військово-технічної і військово-промислової політики; проєктів нормативно-правових актів, концепцій, державних програм, міжнародних договорів України з питань реалізації державної військово-технічної і військово-промислової політики та функціонування оборонно-промислового комплексу; проєкту Закону України про Державний бюджет України за статтями, пов'язаними із забезпеченням національної безпеки і оборони України, зокрема фінансуванням потреб оборонно-промислового комплексу та його розвитку, розробленням, виробництвом, модернізацією та ремонтом озброєння і військової техніки; вирішення проблемних питань реалізації військово-технічної і військово-промислової політики та функціонування оборонно-промислового комплексу.

Закон України «Про оборонні закупівлі» № 808-IX від 17.07.2020 р. визначає загальні правові засади планування, порядок формування обсягів та особливостей здійснення закупівель товарів, робіт і послуг оборонного призначення для забезпечення потреб сектору безпеки і оборони, а також інших товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони, а також порядок здійснення державного і демократичного цивільного контролю у сфері оборонних закупівель [103]. Метою цього Закону є визначення правових засад для забезпечення

матеріально-технічних і наукових потреб сектору безпеки і оборони держави шляхом ефективного та прозорого здійснення оборонних закупівель із дотриманням заходів захисту національних інтересів, створення конкурентного середовища, запобігання корупції у сфері оборонних закупівель, розвитку добросовісної конкуренції, а також ефективного та прозорого планування, реалізації і контролю за здійсненням оборонних закупівель. Цей Закон також передбачає гармонізацію законодавства України у сфері оборонних закупівель із положеннями Директиви № 2009/81/ЄС відповідно до Угоди про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з другої сторони.

Закон України «Про оборону України» № 1932-XII від 06.12.1991 р., із змінами, встановлює засади оборони України, а також повноваження органів державної влади, основні функції та завдання органів військового управління, місцевих державних адміністрацій, органів місцевого самоврядування, обов'язки підприємств, установ, організацій, посадових осіб, права та обов'язки громадян України у сфері оборони [104].

Закон України «Про Збройні Сили України» № 1934-XII від 06.12.1991 р., із змінами, який визначає функції, склад ЗСУ Сил України, правові засади їх організації, діяльності, дислокації, керівництва та управління ними [105].

Розпорядження КМ України «Про схвалення Концепції Державної цільової програми реформування та розвитку оборонно-промислового комплексу України на період до 2020 року» від 20.01.2016 р. № 19-р, у якій визначалося, що вітчизняний оборонно-промисловий комплекс не має змоги задовольнити потреби ЗСУ, інших утворених відповідно до законів військових формувань у сучасному озброєнні та військовій техніці в умовах проведення антитерористичної операції, в особливий період, а також для забезпечення обороноздатності країни в мирний час, що загрожує національній безпеці. У ній перелічувалися причини появи цієї проблеми в діяльності оборонно-промислового комплексу. Концепцією визначалася програма, метою якої є створення умов для підвищення рівня функціонування оборонно-промислового комплексу, що дасть змогу задовольнити потреби ЗСУ, інших утворених відповідно до законів військових формувань у сучасному озброєнні та військовій техніці, а також сприятиме створенню та розвитку цілісної системи оборонно-промислового комплексу на принципах збалансованості відповідно до потреб внутрішнього та зовнішнього ринку і визначенню ресурсної бази розв’язання її завдань [106].

Розпорядження КМУ «Про схвалення Стратегії розвитку оборонно-промислового комплексу України на період до 2028 року», яка розроблена на виконання Концепції розвитку сектору безпеки і оборони України, затвердженої Указом Президента України від 14.03.2016 р. № 92/2016 [107].

Ця стратегія є основою для розроблення нових та перегляду існуючих нормативно-правових актів (у тому числі державних цільових програм) у сфері розвитку та функціонування оборонно-промислового комплексу. Розроблення Стратегії зумовлене необхідністю перегляду державними інституціями України ролі оборонно-промислового комплексу в контексті нейтралізації внутрішніх та зовнішніх загроз національній безпеці, а також інтенсифікації економічного зростання держави. Стратегія визначає довгострокові пріоритети державної військово-промислової політики, а також напрями реалізації державних цільових програм реформування та розвитку оборонно-промислового комплексу в середньостроковій перспективі. Координація виконання та контроль за реалізацією Стратегії здійснюються Мінекономрозвитку. Мінекономрозвитку для забезпечення ефективності реалізації державної військово-промислової політики проводить раз на рік моніторинг виконання Стратегії та реалізації реформи оборонно-промислового комплексу. Щорічні результати такого моніторингу є основою для перегляду основних напрямів реалізації Стратегії у 2023 році. Для забезпечення прозорості, відкритості та неупередженості до проведення оцінювання ефективності реалізації Стратегії можуть бути залучені міжнародні експерти, наукові установи тощо. У разі істотної зміни умов функціонування економіки та/або зміни стратегічних пріоритетів загальнодержавної політики, зокрема з урахуванням міжнародної практики, підходи до інституційної моделі формування та реалізації державної військово-промислової політики можуть бути переглянуті.

Перелічені нормативно-правові акти України на сьогодні є правовою основою протидії загрозам національної безпеки в умовах гібридної війни, які в умовах сучасних гібридних загроз необхідно змінювати та вдосконалювати залежно від змін зовнішньої і внутрішньої соціально-економічної та воєнно-політичної обстановки.

3.2. Концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки

У системі формування та зміцнення національної безпеки України, безумовно, визначальну роль відіграє ефективне державне регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки та кібербезпеки. Тому ця науково-прикладна тематика є предметом дослідження таких науковців, як Політанський В.С. [108], Сопілко І.М. [109], Кузьмінчук Н., Клепікова С. та ін. [110], Рета М., Другова О. та ін. [111], Грохольський В.Л. [112], Аванесова Н.Е., Мордовцев О.С. [113], Ткачук Т.Ю. [114, 116], Золотар О.О. [115], Геворкян А.Ю. [117], Дєгтяр О.А., Лелеченко А.П., Орлова Н.С. та ін. [118, 119], Непомнящий О., Марушева О. та ін. [120, 121], Биркович Т.І. [122], Довгань О.Д. [123],

Заярний О.А. [124], Швець С.В., Швець У.С. [125], Нашинець-Наумова А.Ю. [126], Дзьобань О.П., Мануйлов Є.М. [127] та інші. Цими вченими якісно та обґрунтовано проаналізовано окремі складові цієї проблематики, але концептуальні засади державного регулювання сфери інформаційно-комунікаційних технологій та їх вплив на формування і зміцнення національної безпеки залишається ще недостатньо дослідженими.

У сучасних мінливих умовах усе частіше виникають проблеми соціально-економічної, технологічної і правової взаємодії суб'єктів інформаційно-комунікаційних технологій із виділенням особливої ролі інформаційного суспільства, стратегія розвитку якого в Україні підкреслюється особливою значущістю державного регулювання для впровадження заходів щодо формування національної безпеки країни.

Обов'язковими умовами сталого функціонування незалежної правової держави з демократичною та ефективною системою управління національною безпекою, а також підвищення рівня соціально-економічного розвитку на державному, регіональному та місцевому рівнях є інформаційний потенціал суспільства, що відповідає найвищим вимогам науково-технічного прогресу. Інформаційно-комунікаційні технології активно впливають на розвиток людства. Рівень правової захищеності людини знаходиться в прямій залежності від належного стану інформаційної і кібербезпеки країни, тому що використання інформаційно-комунікаційних технологій розширює прямі і зворотні зв'язки між державою і громадянським суспільством.

Також слід відзначити, що важливими умовами формування потужного інформаційного суспільства є розширення участі громадян в управлінні державою, підвищенні контролю за діяльністю всіх гілок влади, включенні громадян у процес прийняття важливих державних рішень. Визначальною умовою такого моніторингу діяльності з боку суспільства виступає відкритість органів влади, оскільки інформація про їх діяльність служить предметом аналізу та оцінки громадськості.

Таким чином, проблема пошуку дієвих механізмів державного регулювання у сфері інформаційно-комунікаційних технологій є одним з основних факторів підвищення ефективності діяльності держави на всіх рівнях, зокрема: загальнодержавному, регіональному та місцевому. Такий стан справ обумовлюється тим, що без застосування новітніх інформаційно-комунікаційних технологій неможливо ефективно здійснювати державне управління у сфері формування та зміцнення національної безпеки [128].

Одне з основних завдань сучасного курсу соціально-економічних перетворень в Україні, а також формування механізмів зростання національної безпеки полягає в модернізації регулівних функцій держави у сфері застосування всіма суб’єктами в процесі свого функціонування та життєдіяльності інформаційно-комунікаційних технологій.

Розвиток та постійне поширення сфер використання інформаційно-комунікаційних технологій є глобальною тенденцією науково-технічного

прогресу останніх десятиліть, що призводить до значущих змін у багатьох сферах людської діяльності [129]. Використання інформаційно-комунікаційних технологій має вирішальне значення для підвищення конкурентоспроможності економіки, розширення можливостей її інтеграції у світову систему господарства, збільшення ефективності державного управління та місцевого самоврядування та, що головне, є ключовим фактором формування та зміцнення національної безпеки країни.

Перехід до інформаційного суспільства зумовило якісні перетворення механізмів державного управління у сфері інформаційно-комунікаційних технологій [130]. Саме тому тенденції останніх років у світі загалом та в Україні зокрема стали часом активної трансформації системи державного регулювання, вектор розвитку якої почав спрямовуватися на підвищення її ефективності та результативності. У більшості розвинених країн і багатьох країнах із перехідною економікою впроваджується та реалізується комплекс програм, пов'язаних з адміністративно-правовою реформою і реформою державної служби.

Основна мета цих реформ полягає в підвищенні ефективності та безпечності державного управління на базі використання нових інформаційно-комунікаційних технологій, без яких сучасний ступінь соціально-економічної ефективності розвинених держав не може бути досягнутий. У нашому дослідженні, на основі узагальнення наукових джерел [109–111] пропонуються такі основні напрямки проведення перетворень (рис. 3.2).

Виходячи з сучасних соціально-економічних, техніко-технологічних та загальнонаукових реалій України, можна виділити проблеми реалізації запропонованих напрямків перетворень засад державного регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки та кібербезпеки, зокрема:

- невиправдано високі витрати та тривалий термін виконання, що призводить до неможливості отримання позитивного ефекту в короткостроковому періоді, а також до ситуації, коли ці заходи перестануть фінансуватися та впроваджуватися в довгостроковому періоді;
- низька ефективність використання бюджетних коштів у результаті відсутності кваліфікованого керівництва з боку державних управлінців та корупційної складової, що може призвести до загроз і небезпек інформаційній, кібербезпеці та національній безпеці країни;
- високий ступінь проєктних ризиків та відсутність розуміння у громадськості щодо заходів державного регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки і кібербезпеки;
- низький ступінь масштабованості та інтеграції систем державного регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки і кібербезпеки з нагальними потребами соціально-економічного розвитку та формування механізмів зміцнення національної безпеки країни;

- низький рівень розвитку державно-приватного партнерства у сфері інформаційного захисту та кіберзахисту.

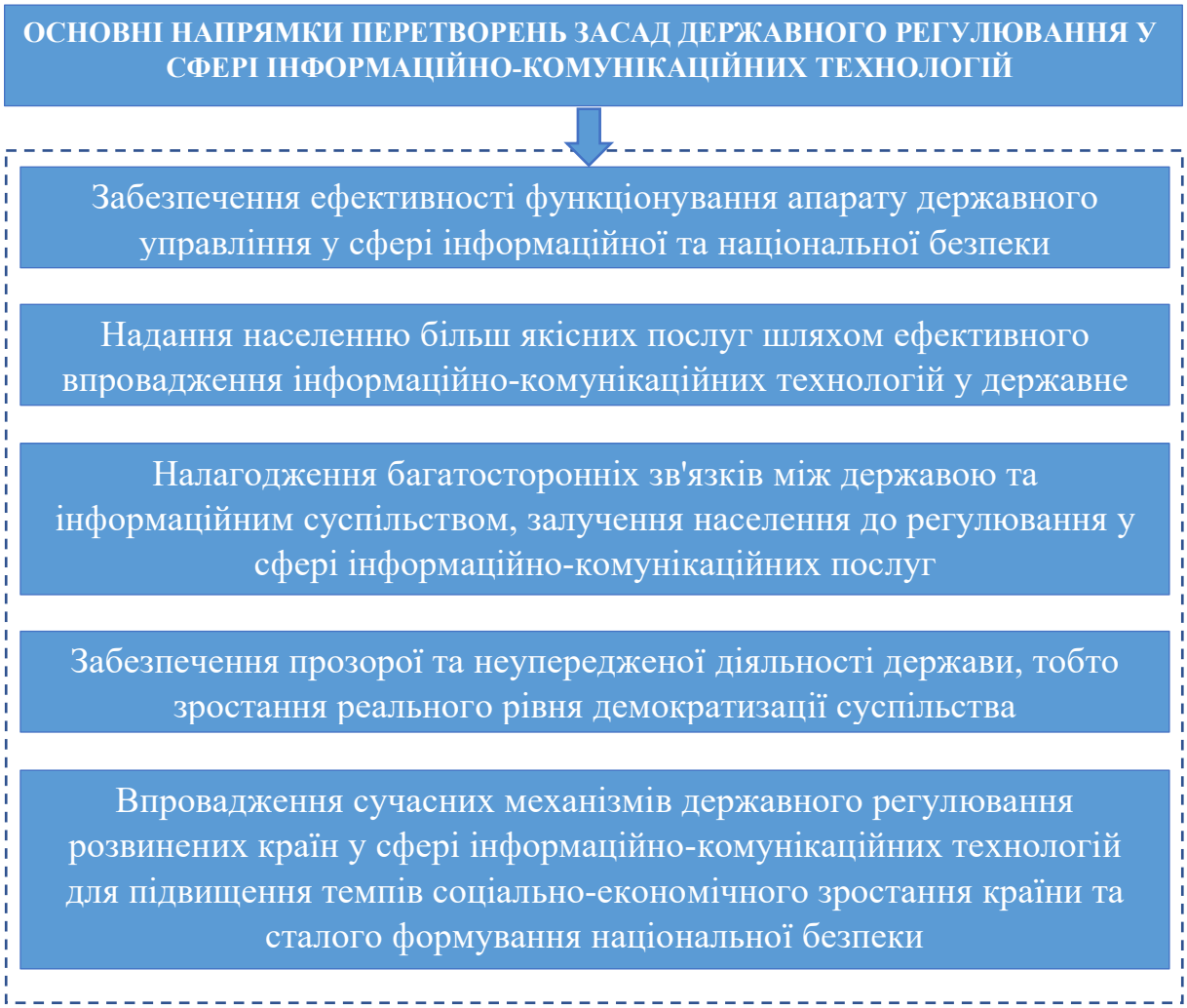

Рисунок 3.2. Основні напрямки перетворень засад державного регулювання у сфері інформаційно-комунікаційних технологій

Треба зазначити, що успішне подолання вищенаведених проблем можливе тільки за рахунок ефективного й сталого функціонування системи органів державної влади, що здійснюють державне регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки та кібербезпеки. Усі гілки влади беруть участь у державному регулюванні інформаційної сфери [7]. При цьому регулювання в загальних рисах повинне здійснюватися Президентом України, ВРУ, Урядом України, Національним банком України, а також судами всіх рівнів, до повноважень яких можна віднести, зокрема: розроблення і прийняття стратегії впровадження в державну діяльність інформаційно-комунікаційних технологій та захист їх від неправомірного використання; удосконалення державних програм розвитку та захисту в інформаційно-комунікаційний

сфері; реалізацію інформаційних прав фізичних і юридичних осіб; державний контроль і нагляд в інформаційній сфері як ключовий фактор формування та зміцнення національної безпеки країни.

Зазначимо, що інформаційна безпека та кібербезпека країни, регіону та/або муніципального утворення, будучи ключовим фактором формування й зміцнення національної безпеки, є одним з істотних напрямів державного регулювання в інформаційно-комунікаційний сфері, що забезпечує сталий соціально-економічний розвиток відповідних територій.

Узагальнивши наукові праці [113–116], під «інформаційною безпекою» у нашому дослідженні будемо розуміти стан захищеності життєво важливих інтересів особистості, інформаційного суспільства і держави від зовнішніх і внутрішніх загроз та небезпек в умовах широкого використання інформаційно-комунікаційних технологій у всіх сферах їх життєдіяльності. При цьому реалізація заходів інформаційної безпеки дозволяє належним чином забезпечити права суб'єктів на достовірну інформацію, одержувану законним способом, захищати різного роду конфіденційну інформацію, зберігати і примножувати культурні та духовно-моральні цінності, історичні традиції й норми суспільного життя країни.

А під «кібербезпекою» розуміємо забезпечення захисту цифрових даних, інформаційних систем та інформаційно-технологічної інфраструктури від загроз і атак, з використанням інформаційно-телекомунікаційних систем. Слід також зазначити, що система інформаційної безпеки і кібербезпеки в державному секторі сформована для інформації, яка є власністю держави, а не всієї існуючої інформації громадян і бізнесу. Виходячи з вищесказаного і на основі узагальнення наукових джерел [117–120], можна сформулювати основні напрямки державного регулювання щодо реалізації заходів інформаційної і кібербезпеки країни, регіону та/або муніципального утворення (рис. 3.3).

Як видно, усі п’ять напрямів взаємопов’язані та мають на меті не тільки забезпечення інформаційної і кібербезпеки, а й є основною для формування та зміцнення національної безпеки країни. Отже, набуває нагальної необхідності розроблення механізмів щодо координації дій у сфері забезпечення інформаційної і кібербезпеки у зв'язку зі складністю виникаючих проблем і взаємопов'язаності напрямків діяльності. Забезпечити таку координацію тільки органами влади на рівні держави практично неможливо, тому доцільно, щоб система, яка координує дії у сфері інформаційно-комунікаційної безпеки, була розподілена за трьома рівнями – державному, регіональному та місцевому, а також відображала структуру науково-технічних та соціально-економічних проблем.

При цьому основними координованими проблемами на регіональному та місцевому рівнях утворень будуть такі:

1. Розроблення моделей загроз інформаційній і кібербезпеці та прогноз реалізації їх наслідків для регіону або місцевого утворення.

2. Забезпечення ефективної законодавчої бази щодо захисту інформаційного ресурсу суб’єктів державного регулювання у сфері інформаційно-комунікаційних технологій, включаючи інформацію обмеженого доступу.

3. Систематизація, облік і забезпечення доступу до державного і недержавного інформаційних ресурсів суб’єктів державного регулювання на основі єдиних правових норм.

4. Забезпечення загальнодоступності інформаційно-комунікаційних мереж типу Інтернет та здійснення контролю за його користуванням згідно із чинним законодавством для запобігання загрозам інформаційній, кібер- та національній безпеці.

5. Виявлення і припинення поширення тенденційних і неправдивих відомостей, маніпулювання суспільною й особистою свідомістю населення та органів влади.

6. Запобігання злому інформаційних систем і копіювання інформації шляхом створення інформаційних систем захисту в регіоні.

7. Запобігання загрозам тероризму по відношенню до об'єктів інформаційно-комунікаційної інфраструктури територій.

8. Забезпечення державних і місцевих структур висококваліфікованими фахівцями з інформаційної, кібер- та національної безпеки [121–123].

Рисунок 3.3. Напрями державного регулювання щодо реалізації заходів інформаційної, кібер- та національної безпеки

Для реалізації загальної координації щодо вирішення вищенаведених проблем повинна ефективно функціонувати відповідна повноважна державна структура з проблем інформаційної і кібербезпеки, яка визначала б специфічні підходи й методи їх розв'язання та подолання. Водночас пропонується впровадити мережу координаційних рад, яка буде функціонувати при найбільш компетентних державних і приватних підприємствах, установах та організаціях. Основним завданням цієї мережі координаційних рад стане забезпечення вирішення конкретних організаційно-технічних питань щодо формування інформаційної і кібербезпеки окремих галузей та сфер життєдіяльності суб'єктів інформаційно-комунікаційних технологій для зміцнення загального рівня національної безпеки (рис. 3.4).

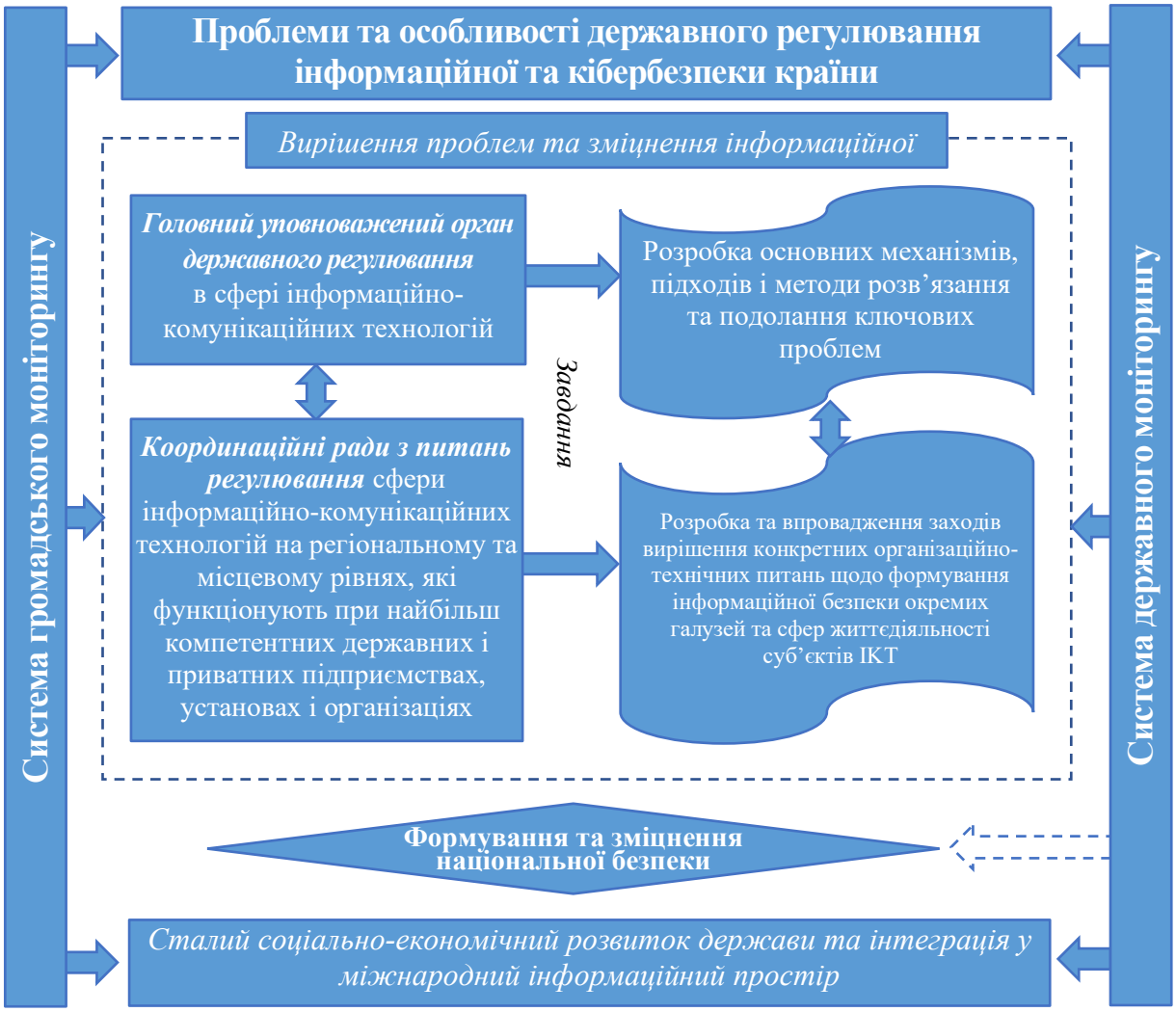

Рисунок 3.4. Механізм вирішення проблем державного регулювання у сфері інформаційно-комунікаційних технологій

Як ми бачимо, важливе місце в запропонованому механізмі вирішення проблем державного регулювання у сфері інформаційно-комунікаційних технологій посідає система громадського та державного моніторингу [124–127].

Мета створення такої системи моніторингу полягає в здійсненні постійного контролю з боку громадськості та уповноважених державних органів за ефективним впровадженням та реалізацією нормативно-правових інститутів державного регулювання сфери інформаційно-комунікаційних технологій.

Крім того, специфіка сучасного соціально-економічного розвитку України диктує необхідність створення самостійної системи моніторингу корупційної діяльності, який визначить найбільш важливі напрямки антикорупційних програм, дозволить оцінити їх ефективність і своєчасно їх скорегувати. Зазначимо, що саме корупційна складова часто породжує найбільш значні порушення у сфері користування та застосування інформаційно-комунікаційних технологій та є ключовою загрозою національній безпеці крайні. Виходячи із цього, для вирішення завдання моніторингу корупційної діяльності можна запропонувати такі заходи:

- дослідити загальноприйняті корупційні практики та впроваджувати їх у нормативно-правовій практиці України;
- відстежити механізми корупційних угод та розробити механізми щодо їх запобігання;
- визначити рівень та структуру корупційної діяльності та розробити стратегічні положення щодо зниження цього рівня;
- проаналізувати фактори, що сприяють корупційній діяльності, та вдосконалити механізми виявлення та усунення цих факторів;
- здійснювати комплексний контроль за ефективністю реалізації антикорупційних програм.

Для успішного виконання зазначених заходів необхідно проаналізувати законодавство як України, так і розвинених країн, дослідити з наукового та юридичного боку конкретні кримінальні справи та розробити дієві механізми боротьби з корупцією на державному, регіональному та місцевому рівнях.

Таким чином, розроблення системи моніторингу результативності державного регулювання сфери інформаційно-комунікаційних технологій дозволить оцінити хід впровадження нормативно-правових інститутів, визначити, наскільки досягнуто поставлені цілі та отримано заплановані показники результативності. Основні результати успішно вибудованої системи громадського та державного моніторингу будуть такими.

1. Своєчасна і достовірна оцінка та загальне сприйняття інформаційним суспільством заходів щодо державного регулювання сфери інформаційно-комунікаційних технологій шляхом організації публічних обговорень основних напрямів цього регулювання, що, у свою чергу, забезпечить інформаційну та експертно-методологічну підтримку його успішної реалізації.

2. Здійснення ефективних та комплексних реформ у сфері інформаційної та кібербезпеки суб’єктів інформаційно-комунікаційних технологій.

3. Підвищення відкритості діяльності органів державного управління та місцевого самоврядування в цілому за рахунок використання сучасних інформаційно-комунікаційних технологій.

4. Розроблення та впровадження об'єднаної бази даних щодо регулювання сфери та суб’єктів інформаційно-комунікаційних технологій.

5. Створення механізмів, за допомогою яких можна оцінити ефективність державного регулювання інформаційно-комунікаційної сфери окремими органами регіональної та місцевої влади для забезпечення мотивації та фінансової підтримки впровадження цих заходів.

6. Формування та зміцнення національної безпеки країни як в інформаційній сфері, так і в інших галузях шляхом впровадження дієвих механізмів захисту інформації та комунікацій.

Отже, комплексна та дієва система державного регулювання сфери інформаційно-комунікаційних технологій є ключовим напрямом функціонування влади на всіх рівнях – від державного до місцевого та включає в себе ряд заходів нормативно-правового, технологічного, технічного, програмного, соціально-економічного і політичного характеру, успішне впровадження яких розкриє широкі горизонти реалізації ідей демократичного інформаційного суспільства і правової держави, а також дозволить зміцнити всі напрями національної безпеки країни.

3.3. Концептуальні основи системи національної кібербезпеки

В умовах сучасних кіберзагроз, зважаючи на те, що Росія активно впроваджує нові форми гібридної війни, зокрема, у кіберпросторі необхідно постійно вдосконалювати систему національної кібербезпеки [131–133]. Від рівня безпеки інформаційних систем державних і силових відомств, об'єктів критичної інфраструктури залежать не лише стабільність та надійність їх функціонування, але часто й життя багатьох людей [134]. Тому проблема вдосконалення, підвищення надійності та ефективності системи національної кібербезпеки є актуальною як у теоретично-методологічному, так і в організаційно-технічному аспектах.

У червні 2015 року Україна зазнала кібератаки від вірусу-здирника Petya.A, яку було спрямовано на об'єкти критичної інфраструктури: Чорнобильську атомну станцію, міжнародні аеропорти «Бориспіль» та «Київ», Укрзалізницю, Київський метрополітен, Укрпошту, Ощадбанк та Укргазбанк.

Хоча кібератака Petya.A і не завдала непоправної шкоди, але саме тоді стало зрозуміло, наскільки ця зброя ефективна, що за її допомогою можна паралізувати практично всю країну. Стало також очевидним, що наступна масштабна кібератака може призвести і до людських жертв, оскільки за допомогою комп'ютера, перебуваючи за тисячі кілометрів від об'єкта атаки, можливо відключити електропостачання для цілого регіону,

відкрити шлюзи на водосховищі, паралізувати рух авіаційного, залізничного та автомобільного транспорту [135]. Висновок беззаперечний – в Україні необхідно створювати надійну та ефективну систему кіберзахисту [136].

Першим документом, що визначає стратегію нашої держави у сфері кібербезпеки, став Указ Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України» від 27.01.2016 р. № 96/2016 «Про Стратегію кібербезпеки України», у якому було визначено такі основні завдання:

- розвиток безпечного, стабільного та надійного кіберпростору;
- кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для оброблення інформації;
- кіберзахист критичної інфраструктури;
- розвиток потенціалу сектора безпеки та оборони у сфері забезпечення кібербезпеки;
- боротьба з кіберзлочинністю.

Згідно з Указами Президента України № 8/2017, № 32/2017 та № 254/2017 введено в дію рішення Ради національної безпеки і оборони України «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», «Про заходи забезпечення захисту об'єктів критичної інфраструктури та заходи щодо нейтралізації кіберзагроз», «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

5 жовтня 2017 року було прийнято Закон «Про основні засади забезпечення кібербезпеки України», який набув чинності 09.05.2018 р.. Цей закон є основоположним нормативно-правовим актом у сфері забезпечення кібербезпеки держави, який:

- визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України в кіберпросторі;
- структурує положення про національну систему кібербезпеки;
- вводить механізми застосування сучасних європейських практик і стандартів;
- розподіляє функції між правоохоронними органами та спецслужбами щодо забезпечення кібербезпеки.

Закон також визначає основних суб'єктів забезпечення кібербезпеки України: Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), СБУ, МВС, МОУ, розвідувальні органи України, Національний банк України (НБУ).

За стратегічне управління та координацію роботи відомств, що забезпечують кібербезпеку, відповідає Рада національної безпеки та оборони (РНБО). Їй підпорядкована ДССЗЗІ, що розробляє комплексну систему кіберзахисту стратегічних об'єктів та опікує компанії, які проводять аудит стратегічних об'єктів. ДССЗЗІ підпорядкований Державний центр

кіберзахисту та протидії кіберзагрозам, підрозділ якого – Оперативний центр реагування на кіберінциденти здійснює моніторинг і виявляє потенційні кіберзагрози (рис. 3.5).

Кіберзахистом також займається МВС України, яке відповідає за запобігання кіберзлочинам та їх розслідування; МОУ і Генеральний штаб ЗСУ, забезпечують охорону військових об'єктів та об'єктів критичної інфраструктури під час війни та в період надзвичайного стану; СБУ має запобігати терористичним атакам у кіберпросторі, її наділено правом перевіряти об'єкти критичної інфраструктури, перелік яких визначає КМУ, а кібербезпека в банківській сфері – зона відповідальності НБУ.

Власники об'єктів критичної інфраструктури вважаються виконавцями державної політики кібербезпеки, тобто зобов'язані впроваджувати її на своєму підприємстві. Якщо державні установи, включаючи міністерства, стануть об'єктом кіберзлочинців, відповідальність буде нести керівництво цих установ. Чиновники нарешті усвідомили, що різні галузі економіки та сфери життєдіяльності України стають дедалі більш вразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Слід зауважити, що зловмисники прямо чи опосередковано пов'язані з РФ.

Рисунок 3.5. Державний центр кіберзахисту
та протидії кіберзагрозам

Як бачимо, повноваження органів, що відповідають за кібербезпеку, частково перетинаються, тому спробуємо точніше визначити, який орган і за що саме відповідає.

ДССЗЗІ відповідає за технічний захист інформації та криптозахист даних, що є власністю держави, та захист персональних даних. Ця служба ліцензує компанії, які мають право надавати послуги криптозахисту та технічного захисту інформації, видає атестати відповідності на засоби та комплексні системи захисту інформації. При ДССЗЗІ є Центр реагування на кіберзагрози для ресурсів держави – CERT.UA (підрозділ, який структурно належить до Державного центру кіберзахисту та протидії кіберзагрозам). На нього покладено функції попередження кібератак та ліквідації їх наслідків. При ДССЗЗІ також працює Центр антивірусного захисту інформації, який відповідає за захист інформаційних ресурсів держави.

СБУ відповідає за захист інтересів держави та прав громадян в інформаційному середовищі. В СБУ створено Ситуаційний центр забезпечення кібернетичної безпеки на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки цього відомства. Завдання Центру – запобігання хакерському втручанню в роботу об'єктів критичної інфраструктури та державних служб. Центр має власну лабораторію комп'ютерної криміналістики та реагування на кіберінциденти. Підрозділом МВС України є кіберполіція, яка веде розслідування у сфері розміщення протиправного контенту в Інтернеті, злому платіжних систем і майданчиків e-commerce. Цей підрозділ також зобов'язаний інформувати громадян про нові загрози та протидіяти їх поширенню.

У МОУ теж є підрозділи, що відповідають за інформаційну безпеку. Спеціальні заходи щодо забезпечення національних інтересів в інформаційній сфері організовує і проводить Головне управління розвідки МОУ, а також Служба зовнішньої розвідки України.

Створено Центр кіберзахисту при НБУ для реагування на кіберінциденти в банківській системі України та аналогічний центр при Міністерстві інфраструктури – Галузевий центр цифровізації та кібербезпеки (ГЦЦК).

Отже, основою системи національної кібербезпеки є центри виявлення, управління та реакції на кіберзагрози [135]. У світовій практиці існує декілька термінів на позначення таких центрів: CERT (Computer Emergency Response Team), CSIRT (Computer Security Incident Response Team), SOC (Security Operation Center). Так, національні центри протидії кіберзагрозам майже завжди називають CERT. Ці центри створено державними структурами для боротьби з кіберзагрозами, спрямованими на державні органи управління та інші критично важливі об'єкти, або з кіберзагрозами державного масштабу. В Україні таких центрів два: CERT-UA в ДССЗЗІ, а також центр рівня CERT в СБУ. Такі центри є ядром системи кібербезпеки держави, вони взаємодіють у системі міжнародного обміну інформацією про кіберзагрози, шкідливі активності та тренди атак.

Крім центрів національного масштабу, система кібербезпеки держави включає галузеві команди реагування на комп'ютерні надзвичайні

події (CSIRT). Такі команди рекомендовано створювати в кожній галузі, особливо якщо галузь має велику кількість об'єктів критичної інфраструктури. Саме на ці центри покладено завдання реагувати на кіберінциденти на підприємствах критичної інфраструктури галузі, відповідно до постанови КМУ № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Цей документ визначає організаційно-методологічні, технічні й технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесено до об'єктів критичної інфраструктури.

Загалом такі галузеві центри кібербезпеки покликані виявляти кіберзагрози на підприємствах галузі, реагувати на них та взаємодіяти з національними CERT.

Наступним рівнем системи кібербезпеки є центри управління кібербезпекою окремих організацій, державних чи комерційних підприємств, зокрема інфраструктурних та фінансових установ, різноманітних об'єднань, підприємств та ін. Такі центри управління кібербезпекою називають SOC, вони покликані виявляти, локалізувати загрози та реагувати на кіберінциденти на окремому підприємстві, в організації, корпорації чи холдингу. Перевагами SOC є максимальна заглибленість в IT-інфраструктуру конкретного підприємства, тобто можливість швидко розібратися в сутності інциденту й локалізувати його наслідки, тому такі центри є найбільш ефективними для боротьби з кіберзагрозами для підприємств, у яких кількість користувачів перевищує 500, а також для тих, які зберігають чи обробляють інформацію, втрата або виток якої буде критичним для підприємств і організацій або держави.

Ще одним компонентом системи кібербезпеки є комерційні SOC, що надають послуги з виявлення кіберзагроз та кіберінцидентів і, по можливості, реагування на них для підприємств, які розуміють важливість забезпечення кібербезпеки, але з якихось причин не створюють свій SOC, а отримують ці послуги із хмари оператора. Такі оператори називаються MSSP (Managed Security Service Provider) або MDR (Managed detection and response), і таки комерційні центри можуть взаємодіяти із CERT національного рівня після перевірки щодо виконання вимог та умов взаємодії з точки зору забезпечення національної безпеки.

Використовуючи системний підхід [137], який полягає в застосуванні сукупності методологічних принципів і теоретичних положень, що дають змогу розглядати кожний елемент системи в його зв'язку і взаємодії з іншими елементами; простежувати зміни, що відбуваються в системі в результаті зміни окремих її ланок; вивчати специфічні системні (емерджентні) властивості; робити обґрунтовані висновки про закономірності розвитку системи; визначати оптимальний режим її функціонування [138], можна побудувати модель системи національної кібербезпеки у вигляді трирівневої піраміди (рис. 3.6).

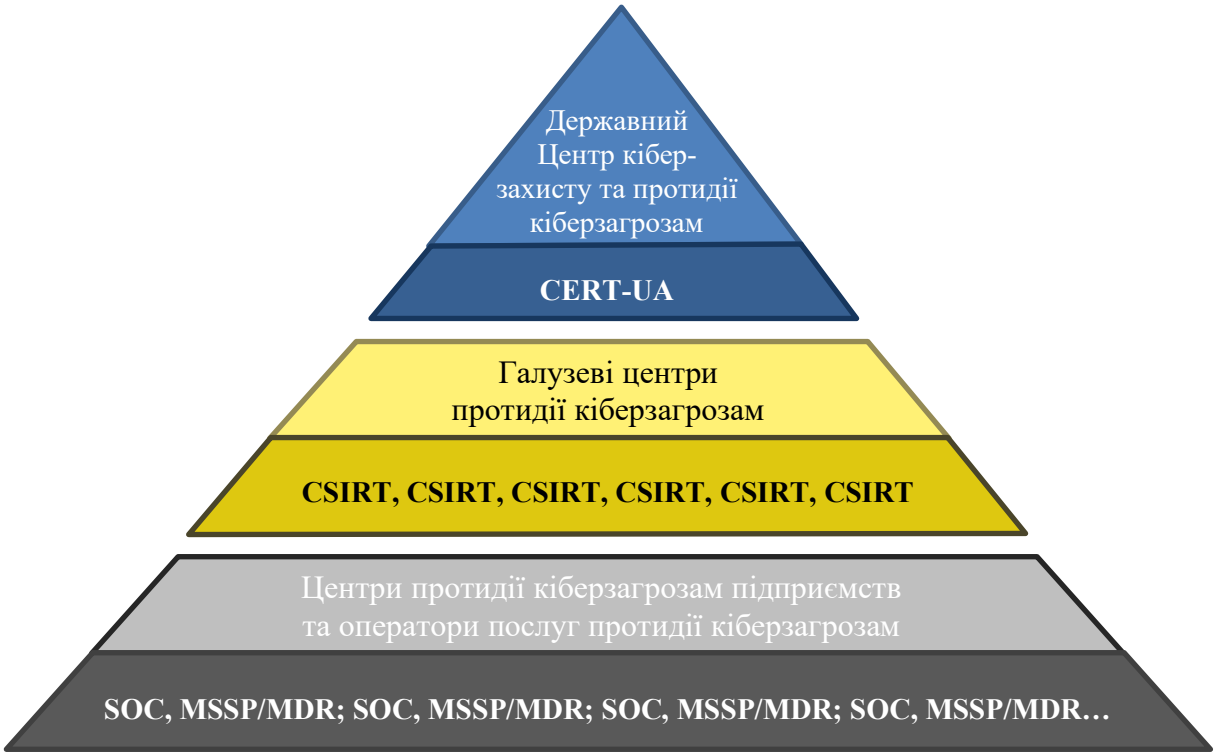

Рисунок 3.6. Модель системи національної кібербезпеки

В основу моделі покладено концепцію єдиного інформаційного простору для обміну даними про кіберінциденти як усередині країни, так і за її межами, та такі принципи [139]:

- принцип цілісності – розгляд водночас системи як єдиного цілого і як підсистеми для вищих рівнів;
- принцип ієрархічності – наявність безлічі елементів, розташованих на основі підпорядкування елементів нижчого рівня елементам вищого рівня;
- принцип структуризації – аналіз елементів системи та їх взаємозв'язку в рамках конкретної організаційної структури;
- принцип множинності – використання безлічі кібернетичних, економічних і математичних моделей для опису окремих елементів і системи в цілому;
- принцип системності – володіння об'єктом усіх ознак системи.

Для підвищення ефективності боротьби з кіберзагрозами на рівні країни організовано взаємодію центрів та обмін інформацією про виявлені кіберінциденти, особливо якщо вони викликані невідомими раніше кіберзагрозами. У цих випадках якнайшвидше поширення такої інформації та внесення до бази індикаторів компрометації (indicators of compromise, IoC) правил кореляції та реакції кожного центру боротьби з кіберзагрозами є принципово важливим для запобігання масовим атакам і порушенням у

роботі інформаційно-технологічної інфраструктури державних установ та відомств.

Модель взаємодії центрів протидії кіберзагрозам подано на рис. 3.7. Ядром цієї моделі є центри національного рівня CERT, які здійснюють обмін інформацією про загрози (IoC) з подібними національними та міжнародними центрами. CERT національного рівня є центром збирання, аналізу, опрацювання, зберігання та обміну інформацією про загрози в країні. CERT також узгоджує протокол взаємодії й обміну інформацією в національній мережі та вимоги для підключення центрів до цієї мережі.

CSIRT галузевого рівня здійснюють обмін інформацією безпосередньо із центрами національного рівня. Підприємства галузі, які мають власний SOC, є третім рівнем системи національної кібербезпеки. Вони підключаються до національної мережі обміну інформацією з кібербезпеки через CSIRT відповідної галузі, якщо такий є, і безпосередньо із центром національного рівня CERT, якщо CSIRT галузі не функціонує.

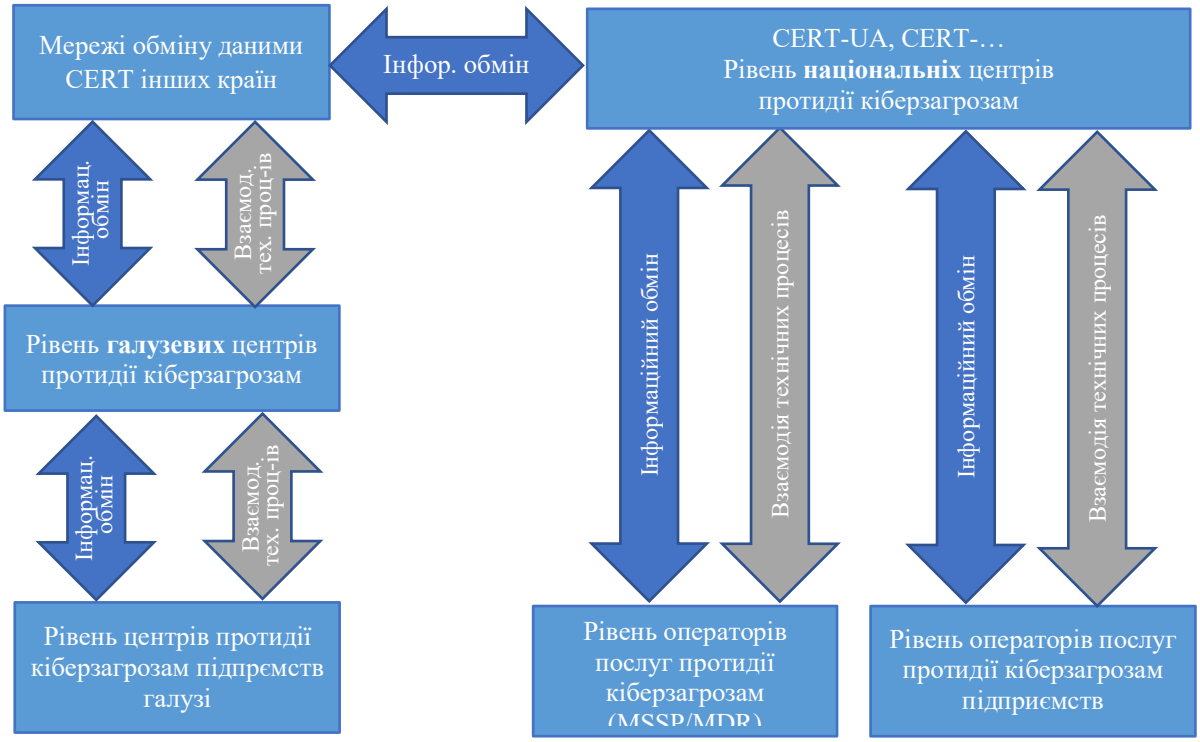

Рисунок 3.7. Модель взаємодії центрів протидії кіберзагрозам

SOC окремих підприємств, корпорацій та холдингів також взаємодіє безпосередньо із центром національного рівня CERT, підключається до мережі згідно із затвердженими протоколами взаємодії після виконання відповідних вимог.

Підключення до національної мережі для обміну інформацією щодо кібербезпеки операторів, які надають послуги SOC, здійснюється за тими ж принципами, що й підключення SOC підприємств, але перед тим потрібно

провести аналіз і контроль усіх замовників їх послуг, оскільки такі оператори можуть надавати послуги організаціям і установам різних країн.

Зважаючи на те, що останнім часом розвідувально-підривна діяльність іноземних спецслужб у кіберпросторі посилюється, систему кіберзахисту в Україні необхідно розвивати та вдосконалювати, з урахуванням рівня сучасних загроз. Державним організаціям, що відповідають за кіберзахист, треба постійно актуалізувати вимоги щодо кіберзахисту, яких мають дотримуватися всі об'єкти критичної інфраструктури, визначити повний список таких об'єктів й уточнювати його в разі потреби. Керівникам цих об'єктів необхідно впроваджувати досить надійну систему кіберзахисту з урахуванням всіх вимог. Не можна забувати про захист і керівникам підприємств та організацій, які не входять до переліку об'єктів критичної інфраструктури. Слід пам’ятати, що захист від кіберзагроз тепер стосується кожного, отже, варто подбати про нього і пересічним громадянам.

Висновки до третьої глави

Організаційно-правові основи протидії загрозам національної безпеки в умовах гібридної війни є динамічними як за формою, так і функціональним змістом. Залежно від соціально-економічних та воєнно-політичних змін, які трансформують зовнішні і внутрішні загрози національній безпеці України, буде змінюватися склад сектору безпеки і оборони України, його стратегічні та тактичні цілі, а відповідно, і функціональні обов’язки його складових.

Проаналізовані нормативно-правові акти України, які на сьогодні є правовою основою протидії загрозам національній безпеці в умовах сучасних гібридних загроз, також необхідно змінювати та вдосконалювати залежно від змін зовнішньої і внутрішньої соціально-економічної та воєнно-політичної обстановки.

Проведено теоретико-методологічні та практично-прикладні дослідження концептуальних засад державного регулювання у сфері інформаційно-комунікаційних технологій та їх впливу на ефективне функціонування СНБ країни.

Визначено основні напрямки перетворень засад державного регулювання у сфері інформаційно-комунікаційних технологій та виокремлено проблеми їх реалізації.

Доведено, що реалізація заходів інформаційної та кібербезпеки дозволяє належним чином забезпечити права суб'єктів на достовірну інформацію, одержувану законним шляхом, захищати різного роду конфіденційну інформацію, зберігати і примножувати культурні та духовно-моральні цінності, історичні традиції й норми суспільного життя

країни.

Сформовано механізм вирішення проблем координації дій у сфері державного регулювання інформаційно-комунікаційних технологій.

Проведено аналіз основних аспектів функціонування системи громадського та державного моніторингу, який є ключовим елементом запропонованого механізму вирішення проблем державного регулювання у сфері інформаційно-комунікаційних технологій.

Розроблено концептуальні основи побудови системи національної кібербезпеки, запропоновано модель системи національної кібербезпеки і модель взаємодії центрів протидії кіберзагрозам.

ГЛАВА 4
НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

4.1. Сучасні загрози національній безпеці України

Будь-яка суспільна система постійно стикається з проблемою збалансованості в досягненні соціальних цілей та ресурсними можливостями їх забезпечення. У соціальної спрямованості їх розвитку виникають протиріччя з економічними обмеженнями або, за наявності економічних ресурсів, із пріоритетністю їх використання, яка часто визначається не на користь соціальним пріоритетам.

Економічна безпека створює переваги для соціального розвитку людини, суспільства і держави. Це не відбувається автоматично, а лише через пріоритетність економічного забезпечення досягнення соціальних цілей завдяки важелям державного регулювання цих процесів. У багатьох країнах результати економічного зростання спрямовуються на подальший економічний розвиток, а вирішення соціальних проблем консервується та стримується. В Україні в цьому сенсі простежуються значні коливання. Соціальні витрати з бюджету не збалансовуються з економічними можливостями. Вони можуть бути або надмірними через політичні важелі, або використовуються на подальші економічні пріоритети без урахування соціальних цілей. За Конституцією України, держава визначається як правова та соціальна з подальшим розкриттям цінності людини, її життя та здоров'я, пріоритетності захисту її прав та свобод тощо, чим зобов'язує підпорядковувати державне управління збалансованості досягнення економічних та соціальних процесів. Але ненаціленість на одночасне досягнення економічних та соціальних пріоритетів не приводить до очікуваних наслідків через цільову кінцеву різноспрямованість вкладень та результатів. Напрями досягнення безпечного стану в соціальній та економічній сферах між собою не корелюють, не скоординовані, не відрегульовані, що викликає протиріччя між досягненням економічних та соціальних цілей.

Отже, сучасний стан соціальної орієнтації економіки України на сьогодні є низьким, що свідчить про наявність загроз національній безпеці в економічній та соціальній сферах і потребує проведення виваженої, ефективної економічної політики та державного регулювання соціально-економічних процесів [141, 142].

На сьогодні можливо виділити такі загрози національній безпеці, зумовлені гібридною війною в Україні [143]: воєнні, економічні,

енергетичні, соціогуманітарні, загрози державній безпеці, інформаційні та кіберзагрози (рис. 4.1). Далі розглянемо їх детальніше.

Рисунок 4.1. Загрози національній безпеці України в умовах гібридної війни

Воєнні загрози:

- продовження на Донбасі керованого РФ «млявого», з періодичними загостреннями, виснажливого для України збройного конфлікту;
- цілеспрямовані провокації російсько-терористичних військ;
- обстріли противником мирних населених пунктів;
- мінування ділянок місцевості, які створюють небезпеку передусім цивільному населенню;
- несанкціонований вивіз зброї, боєприпасів, вибухових та інших небезпечних речовин із району ведення операції та встановлення особливого порядку в'їзду/виїзду з нього;
- особливо небезпечні дії снайперських та диверсійно-розвідувальних груп супротивника;
- посилення угруповання збройних формувань РФ на Донбасі шляхом збільшення в його складі бронетехніки, артилерії, засобів розвідки, радіоелектронної боротьби, зв'язку та управління;
- загострення ситуації в акваторії Азовського моря, пов'язане з нарощуванням військово-морської та військово-повітряної присутності РФ, яка вдається до військово-морської та економічної блокади України в Азовському морі, з прагненням «пробиття» Росією сухопутного коридору через Маріуполь та Бердянськ до Криму й перетворення Азовського моря у внутрішнє російське море;

- подальшими цілями російської агресії можуть стати чорноморські порти України, що завдасть серйозного удару нашій економіці, суттєво обмеживши експорт українських товарів та транзитний потенціал країни;
- півострів Крим, перетворений на єдину воєнно-морську базу як плацдарм для зміцнення воєнних позицій РФ у Чорноморському регіоні та Середземному морі;
- загроза проведення російськими військами псевдомиротворчої операції з примушення до миру України, а також так званих ДНР і ЛНР із метою розширення окупованих територій на Донбасі до адміністративних кордонів Донецької та Луганської областей;
- можливість широкомасштабної збройної агресії Росії проти України.

Економічні загрози:

- призупинення дії угоди про зони вільної торгівлі з РФ, яка поширила на Україну заборону на ввезення сільгосппродукції та продовольства, а також запровадила значні обмеження на інші українські товари; застосування низки антидемпінгових заходів щодо української металургійної продукції на п'ятирічний період;
- транзитні обмеження через територію РФ до країн Середньої і Південної Азії та Китаю;
- позови до Світової організації торгівлі зі звинуваченнями в порушенні Україною своїх зобов'язань;
- ескалацією напруження з боку РФ стали системні дії з підриву конкурентоспроможності української економіки у сфері портової галузі (системні недобросовісні та антиконкурентні дії РФ в акваторії Азовського та Чорного морів поєднуються з вагомим потенціалом силових механізмів втручання або шантажу з їх застосування).

Гібридна агресія істотно звузила можливості опанування стабільного економічного зростання в нових міжнародних економічних реаліях, зумовлюючи:

- низьку економічну продуктивність, яка компенсується збільшенням боргу як зовнішнього, так і внутрішнього;
- інтенсивну трудову міграцію;
- зростання інфляційного тиску;
- гальмування виконання Угоди про Асоціацію України з ЄС;
- низьку інвестиційну привабливість країни.

Загрози державній безпеці:

- посягання на державний суверенітет, територіальну цілісність України російських окупаційних військ та незаконних збройних формувань;
- високий рівень терористичної та диверсійної діяльності;
- інспірування і спроби поширення сепаратистських настроїв у районах компактного проживання національних меншин, формування

сепаратистських рухів у країні, створення умов для автономізації певних територій;

- поширення подвійного громадянства перетворилося на фактор негативного впливу на національну безпеку України;
- розвідувально-підривна діяльність російських спеціальних служб, спрямована на: організацію масових заворушень із використанням агентурних мереж та підконтрольних проросійських громадсько-політичних структур; розпалювання сепаратистських і автономістських настроїв; дестабілізацію політичної ситуації; створення позицій впливу в органах державної й місцевої влади в Україні тощо;
- загрози у сфері безпеки державного кордону (мілітаризація Росією суміжних з Україною областей) та перешкоджання РФ заходам української сторони з охорони державного кордону і незаконне здійснення промислової діяльності в акваторіях Азовського й Чорного морів та у виключній (морській) економічній зоні України.

Соціогуманітарні загрози:

- загострення проблеми становлення національної ідентичності українців;
- ускладнення соціально-економічної ситуації в країні, проблеми із зайнятістю населення, погіршення рівня життя населення, незадоволення ходом реформ;
- триваюче протистояння різних політичних сил, політизація й радикалізація певних суспільних відносин;
- загострення криміногенної ситуації в Україні, чому сприяє зростання незаконного обігу зброї, боєприпасів, вибухових речовин та засобів ураження, а також прошарку громадян, які готові при нагоді їх застосовувати, і незаконного обігу наркотиків;
- значну загрозу становить також створення та діяльність на території держави парамілітарних збройних формувань, які діють не тільки в зоні проведення ООС, а й в інших регіонах держави та спричиняють небезпеку силового вирішення соціальних протиріч;
- активізація протиправних дій, спрямованих на перерозподіл майнових прав;
- посилення міграційних процесів, що ускладнюються значною кількістю внутрішньо переміщених осіб, та проблеми, зумовлені належним облаштуванням та соціальною адаптацією переселенців з окупованих регіонів;
- загрози відтоку людського капіталу, підсилені війною на Сході України.

Енергетичні загрози:

- незавершеність створення енергетичних ринків, заснованих на принципах вільної конкуренції, належного захисту прав споживачів і безпеки постачань, а також здатних до інтеграції з ринками держав – членів

Енергетичного Співтовариства, що залишає енергетичну залежність від РФ;

- РФ здатна заблокувати дві третини постачання нафтопродуктів;
- унаслідок будівництва газопроводу «Північний потік – 2» виникла реальна загроза збереженню транзитних можливостей держави;
- велика залежність від постачання тепловиділяючих елементів, тобто ядерного палива для АЕС України.

Інформаційні та кіберзагрози:

- проблемою все ще лишаються стратегічні дезінформаційні кампанії, що реалізуються агресором із залученням усього доступного йому арсеналу прийомів та засобів ведення інформаційної війни для дискредитації української влади, сіяння розбрату між владою та громадянами як начебто антагоністичних суб'єктів, дискредитація України на міжнародній арені, легітимація анексії Криму та терористичних утворень на Сході України, інспірування внутрішньополітичного вибуху;
- використання РФ мережі агентів впливу із числа представників політичної еліти, медіасфери, церковних структур, псевдогромадських організацій та окремих публічних осіб, які активно задіяні у спробах протидіяти становленню України як єдиної, незалежної, суверенної держави;
- агресор продовжує активно використовувати мережеві інформаційні ресурси, фінансуючи чинні (шукаючи нові шляхи для цього) або створюючи нові;
- проблеми деструктивного використання інтернет-сервісів, пов'язані з невизначеністю юридичного статусу інтернет-ЗМІ в Україні та обмеженими можливостями України вплинути на тих інформаційних суб'єктів, що ведуть свою діяльність із території інших країн, враховуючи те, що українське законодавство в цій сфері є чи не найбільш ліберальним з усіх європейських держав, що подекуди ставить під загрозу суспільну злагоду та національну безпеку України;
- дедалі більше деструктивних інформаційних впливів в Україні здійснюються на регіональному рівні, причому це характерно не лише для територій, які традиційно є зонами пріоритетного інформаційного впливу російської пропаганди, а й для західних регіонів України, де, крім російського, посилюється інформаційний вплив і сусідніх держав;
- залишається інформаційне домінування держави-агресора на тимчасово окупованих територіях Криму та Донбасу, і, незважаючи на поступово відновлювану мережу теле- та радіомовлення для донесення українських новин на ці території, саме російські наративи все ще здебільшого формують світосприйняття мешканців окупованих територій України;
- значною мірою маніпулятивні впливи з боку агресора стають наслідком усе ще несистемних зусиль із впровадженням медіаграмотності в

Україні та слабкими освітніми програмами щодо виховання критичного мислення;

Однією з важливих арен інформаційного протиборства з агресором залишається кіберпростір, де агресор:

- атакує об'єкті критичної інфраструктури, перешкоджаючи роботі систем управління великих компаній, банківських установ, підприємств енергетичної та транспортної галузі для послаблення економіки країни;
- прагне добувати конфіденційну інформацію щодо діяльності органів державного управління, офісів міжнародних, зокрема правозахисних, організацій (у тому числі на тимчасово окупованих територіях Донецької та Луганської областей і в Криму), політичних партій, впливових ЗМІ;
- намагається здійснювати вплив на виборчий процес.

Таким чином, гібридна війна ускладнила й урізноманітнила загрози національній безпеці України в усіх сферах суспільного життя. Це значне ускладнення загроз і викликів інтересам та фізичному існуванню українського суспільства і держави дозволить, у разі успіху протидії їх впливу, сформувати ефективний та якісний механізм відстоювання і захисту національних інтересів.

4.2. Національні інтереси та їх реалізація в умовах гібридної війни

Переважна більшість підходів щодо забезпечення національної безпеки базується на усвідомленні та реалізації на державному і міжнародному рівнях концепції національних інтересів[144, 145]. Сферою, де знаходять прояв інтереси, є політика [146]. Вона визначається різними детермінантами. Серед них, зокрема: рівень та особливості культурного, соціально-економічного та суспільно-політичного розвитку; географічне положення країни; ресурсні можливості держави; національно-історичні традиції; потреби забезпечення суверенітету та територіальної цілісності. Саме вказані детермінанти і знаходять своє відображення в національних інтересах, а останні – у законах, концепціях, стратегіях, інших нормативних актах як об'єктивні потреби розвитку суспільства. Першоосновою національних інтересів є потреби розвитку та безпеки суспільства і держави [147]. Тому за своєю суттю та спрямованістю вони зорієнтовані на забезпечення виживання та прогресивного розвитку й тією чи іншою мірою лідерства особи, суспільства, держави. Тільки через призму їх реалізації та захисту можуть та повинні розглядатися всі проблеми, пов'язані із забезпеченням національної безпеки.

Зміст національних інтересів зумовлює, якою має бути політика та стратегія національної безпеки. Для визначення пріоритетних напрямків

політики національної безпеки, на яких мають бути зосереджені основні зусилля в конкретний історичний період розвитку країни та суспільства, важливою є побудова ієрархії національних інтересів, для чого визначають ступінь їх важливості, як правило, на основі оцінки збитку (шкоди) національній безпеці в разі неналежної реалізації того чи іншого інтересу. З огляду на сказане розрізняють інтереси виживання, життєво важливі, важливі та периферійні національні інтереси, особливо акцентуючи увагу на інтересах виживання та життєво важливих.

Ієрархія національних інтересів є ключовим чинником під час прийняття управлінських рішень суб'єктами державного управління національною безпекою. За її відсутності було б неможливим існування тієї чи іншої комбінації управлінських впливів, і внаслідок цього процес вибору оптимального управлінського рішення не мав би логічного завершення.

Життєво важливими національними інтересами України, зокрема, є:

- дотримання прав і свобод людини і громадянина;
- забезпечення суверенітету України, її територіальної цілісності, недоторканності державного кордону, демократичного конституційного ладу, верховенства права;
- забезпечення конкурентоспроможності держави та економічного добробуту населення шляхом всебічного розвитку людського, науково-технічного, інноваційного потенціалів країни;
- збереження і розвиток духовних і культурних цінностей суспільства;
- удосконалення механізмів реалізації конституційного принципу розподілу влади на законодавчу, виконавчу і судову;
- створення безпечних умов життєдіяльності, захисту навколишнього природного середовища;
- створення умов для сприйняття Української держави міжнародним співтовариством як повноцінного і рівноправного його члена.

Реалізація національних інтересів в умовах гібридної війни повинна здійснюватися за сімома основними напрямками.

1. Захист та дотримання прав і свобод людини і громадянина вимагає реалізації таких дій:

- розширення сфер суспільного виробництва для мінімізації безробіття і суттєвого підвищення заробітних плат у всіх сферах народного господарства для підняття матеріального рівня громадян України, а також поглиблення пенсійної реформи із запуском фондового ринку, які будуть спроможні дати належні джерела матеріальних надходжень для громадян непрацездатного віку;
- створення умов для повернення в Україну та реінтеграції в суспільство трудових мігрантів та членів їхніх сімей і визначення стратегії державної міграційної політики;

- законодавча і матеріальна реалізація забезпечення майнових і громадянських прав вимушених переселенців для їх успішної адаптації на нових місцях помешкання;
- реформування освітньої сфери відповідно до світових тенденцій розвитку соціально-економічної сфери, узгодження знань і навичок, які здобувають ті, хто навчається, з реальними життєвими потребами; прискорення процесів оновлення професійних знань і навичок, приведення у відповідність структури підготовки кадрів до потреб і запитів економіки з урахуванням вимог четвертої технічної та енергетичної революцій та того освітнього аспекту, що ключовими індикаторами ефективності освітньої системи будь-якої країни є доступність і якість освіти, а також синхронізацією освітньої трансформації з реформою місцевого самоврядування;
- реформа системи охорони здоров'я, яка має вирішити низку питань: а) винайдення суспільно-економічного балансу між бізнесом і соціальним аспектом щодо надання послуг у цій сфері; б) запуск кількарівневої системи медичного страхування; в) реформування системи підготовки та ліцензування лікарів та молодшого медичного персоналу; г) створення системи охорони здоров'я на основі раціоналізації та доступності медичних послуг у різних регіонах країни; д) запровадження системи профілактики стану здоров'я громадян;
- модернізація житлово-комунальної сфери в умовах реформи децентралізації, яка передбачає: а) переведення системи надання ЖКП на ринкові засади, тобто запровадження конкурентних засад щодо їх надання; б) подолання розриву між механізмами діяльності комунального та експлуатаційно-ремонтного господарства, що обслуговує житлову сферу, процесів на ринку будівництва, перепродажу та оренди житла, функціонування проєктно-планових архітектурних та містобудівних структур, дорожньо-транспортних структур, організацій із благоустрою та побутового обслуговування; в) налагодження дієвого контролю за дотриманням норм під час будівництва та експлуатації об'єктів, створюють високий ризик виникнення надзвичайних ситуацій зі спричиненням шкоди життю та здоров'ю населення країни; г) подолання опору щодо утворення ОСББ;
- реформа системи соціальних послуг для створення умов надання допомоги вразливим категоріям населення долати складні життєві обставин, попереджати їх виникнення та створювати умови для самостійного розв'язання їх життєвих проблем, чим посилюється захист їх конституційних прав та свобод, забезпечується повага до кожної людини та її гідності, яка ґрунтується на таких принципах: а) поглиблення адресності державної соціальної допомоги; б) заміна окремих пільг на соціальні послуги; в) перехід від бюджетного фінансування відповідних державних установ до програмного фінансування на конкурсних засадах громадських організацій, які надаватимуть такі послуги; г) посилення ролі місцевого

рівня влади в наданні соціальних послуг та передання їм повноважень щодо планування, фінансування та організації надання соціальних послуг.

2. Забезпечення суверенітету України, її територіальної цілісності, недоторканності державного кордону, демократичного конституційного ладу, верховенства права.

Передусім, джерелом такої загрози для України є РФ і російські окупаційні війська та незаконні збройні формування, що діють на тимчасово окупованих територіях. Крім підтримки РФ терористичної діяльності на тимчасово окупованих територіях України, високий рівень терористичної та диверсійної загрози з боку агресора залишається для стратегічних об'єктів державного значення та інших об'єктів критичної інфраструктури, розташованих як у районі проведення операції Об'єднаних сил, так і поза її межами. Після анексії РФ Криму та окупації окремих районів Донецької та Луганської областей питання подвійного громадянства перетворилися на фактор негативного впливу на національну безпеку України. Країна-агресор намагається надзвичайно активно маніпулювати інститутом громадянства, використовуючи його як елемент гібридної війни.

Незважаючи на вжиті нашою державою захисні обмежувальні заходи, зокрема, в інформаційній сфері, керівництво РФ не відмовилося від спроб посилення свого впливу на населення нашої держави. Передусім, у їх фокусі залишаються східні й південні області України, які мають велике значення в багатьох аспектах: політичному, військовому, економічному, науково-інтелектуальному, і, зокрема, з погляду можливості прокладання сухопутного коридору до Кримського півострову та Придністров'я, а також повного відрізання доступу України до Чорного моря. Продовжується й перешкоджання РФ заходам української сторони з охорони державного кордону та незаконне здійснення промислової діяльності в акваторіях Азовського й Чорного морів та у виключній (морській) економічній зоні України.

3. Створення безпечних умов життєдіяльності, захисту навколишнього природного середовища.

Загрози у сфері екологічної безпеки посилюються через високий рівень техногенного навантаження на земельні, водні, біотичні, мінерально-сировинні ресурси України. Незважаючи на певний спад виробництва в Україні, залишається стабільно високим забруднення атмосферного повітря великих міст і промислових населених пунктів у державі. Основними забруднювачами атмосферного повітря залишаються підприємства добувної й переробної промисловості, постачання електроенергії, газу, викиди забруднюючих речовин яких становлять понад 90 % від загального обсягу викидів в атмосферне повітря в Україні. Серед основних причин, що зумовлюють незадовільний стан якості атмосферного повітря в населених пунктах, можна виокремити недотримання підприємствами режиму експлуатації пилогазоочисного обладнання, невиконання заходів щодо скорочення обсягів викидів забруднюючих речовин в атмосферне повітря

стаціонарними джерелами забруднення з метою досягнення встановлених нормативів граничнодопустимих викидів, низькі темпи впровадження новітніх технологій і значне збільшення кількості індивідуального автомобільного транспорту.

4. Забезпечення конкурентоспроможності держави та економічного добробуту населення шляхом всебічного розвитку людського, науково-технічного, інноваційного потенціалів країни. Україна в порівнянні з багатьма іншими країнами має конкурентні переваги. До таких відносяться: вигідне географічне розташування країни та запаси природних ресурсів; потужна матеріально-технічна та наукова база, кваліфіковані трудові ресурси. Однак реалізація національних конкурентних переваг ускладнюється неефективністю їх використання. Адже головний показник конкурентоспроможності країни на світовому ринку – рівень ефективності використання всіх економічних ресурсів і насамперед праці.

М. Портер у своїй теорії виділив чотири складові, які формують конкурентні переваги галузей, фірм і економіки в цілому [148]:

1. Параметри факторів виробництва. Це праця, земля, капітал, підприємницька активність, інформаційна, наукова і технічна забезпеченість.

2. Стратегія фірми чи країни. Вона має відповідати галузі і стану ринку, у якому працює фірма, країна.

3. Параметри попиту. Він включає місткість ринку, динаміку та структурну зміну, рівень вимог покупців до якості товару.

4. Споріднені і підтримуючі галузі. Це взаємозалежні галузі для створення готового продукту, тобто забезпечують експортні галузі необхідними матеріалами та послугами.

Портер зазначає, що на світовому ринку конкурують фірми, а не держави. Уряд може лише сприяти успіху конкурентної боротьби вітчизняних виробників, запроваджуючи програми з підтримки виробників [148]. Для характеристики конкурентоспроможності національної економіки беруть до уваги модель ЖЦ факторів конкурентоспроможності національної економіки. Вона включає: стадію факторів виробництва (зручні транспортні маршрути, дешева робоча сила та сировина, місткий споживчий ринок); стадію інвестицій (інвестування в розвиток освіти та нових технологій, розвиток інформаційної інфраструктури); стадію нововведень (інновації в освіту; розвиток інформаційно-комп'ютерних технологій; розширення доступу компаній до венчурного капіталу; якість управління країною та компаніями; ефективну політику залучення прямих іноземних інвестицій та ін.); стадію нагромадження. Індекс глобальної конкурентоспроможності складається з більш ніж 100 змінних, що згруповані у 12 контрольних показників («Інституції», «Інфраструктура», «Макроекономічне середовище», «Охорона здоров'я та початкова освіта», «Вища освіта і професійна підготовка», «Ефективність ринку товарів», «Ефективність ринку праці», «Розвиток фінансового ринку», «Технологічна

готовність», «Розмір ринку», «Відповідність бізнесу сучасним вимогам» та «Інноваційний потенціал») за 3 основними групами субіндексів: «Основні вимоги», «Підсилювачі продуктивності» та «Інновації та фактори вдосконалення».

Підвищення конкурентоспроможності національної економіки України для участі у глобальному процесі без наукомісткої продукції підприємств на світовому ринку неможливе. Темпи розвитку науково-технічного прогресу держави, у свою чергу, залежить від державної політики у сфері науки та освіти. Загалом конкурентні переваги можна здобути шляхом отримання пільг, дотацій із державного бюджету, заниженого курсу національної валюти, прямого чи прихованого субсидування галузей, отримання тіньових прибутків, ефективної експлуатації вичерпних природних та екологічних ресурсів тощо. Україна та з небагатьох держав, що має всі можливості за певний час стати державою з високим показником конкурентоспроможності національної економіки та брати активну участь у процесі глобалізації [149].

Від рівня конкурентоспроможності національної економіки прямо пропорційно залежить рівень всебічного розвитку людського, науково-технічного, інноваційного потенціалів країни, які, у свою чергу, впливатимуть на рівень конкурентоспроможності країни.

5. Збереження та розвиток духовних і культурних цінностей суспільства.

До культурних цінностей належать об'єкти матеріальної і духовної культури, що мають художнє, історичне, етнографічне та наукове значення [146]. Унікальні цінності матеріальної та духовної культури, а також культурні цінності, що мають виключно історичне значення для формування національної самосвідомості українського народу, визнаються об'єктами національного культурного надбання і заносяться до Державного реєстру національного культурного надбання. Основою існування і розвитку будь-якого суспільства, національної спільноти, держави виступає відповідна система цінностей як своєрідний моральний орієнтир загальносуспільного поступу, завдяки якій і навколо якої зорганізується життя всього соціуму. Духовні цінності формують загальнонаціональний суспільний ідеал, єдину національну ідею, загальновизнану ідеологію державотворення, розвинену національну самосвідомість.

У національній свідомості українського суспільства поки що не сформована значуща для всіх громадян України узагальнена система цінностей, без якої важко сподіватися на можливість швидкої національної консолідації.

Вирішення цього завдання має здійснюватися засобами реалізації державної гуманітарної політики, шляхом суспільного діалогу, гармонійної та активної взаємодії органів державної влади, громадських організацій, наукових закладів із метою формування об’єднаного духовного простору української нації [150].

6. Удосконалення механізмів реалізації конституційного принципу розподілу влади на законодавчу, виконавчу і судову.

Світовий досвід підтверджує, що надійним засобом усунення негативних явищ, котрі виникають під час організації та функціонування державної влади, є система стримувань і противаг, за допомогою якої взаємодіють різні гілки влади у процесі вирішення ними загальнодержавних питань. Конституція України також закріпила найзагальніші теоретичні положення, на котрих ґрунтується механізм — стримувань і противаг. Водночас перманентне загострення парламентсько-урядової кризи впродовж років незалежності, що на сучасному етапі переросла в системну політичну кризу, засвідчує, що дієвий механізм функціонування згаданої системи не сформовано. Серед основних проблем взаємодії між виконавчою та законодавчою гілками влади в Україні виокремимо: незбалансований характер системи влади; зниження політичного впливу Верховної Ради як представницького органу; відсутність ефективних механізмів впливу парламенту на систему виконавчої влади та політичного зв'язку між ВР України (депутатською більшістю) і КМУ як передумови їх конструктивної взаємодії; недостатність і неефективність системи стримувань і противаг між Президентом та ВРУ, відсутність дієвих механізмів парламентського контролю [151].

7. Створення умов для сприйняття Української держави міжнародним співтовариством повноцінним і рівноправним членом.

У цьому контексті слід наголосити, що розширення і поглиблення міжнародних відносин України з іншими державами, а також поглиблення інтеграції України в міжнародну політику, економіку та інші сфери міждержавного інтеграційного співробітництва, зокрема, у рамках ЄС та в умовах зовнішньої агресії викликає нагальну необхідність вдосконалення організаційно-правового регулювання зовнішньополітичної діяльності України у сфері забезпечення національної безпеки держави, а саме: поглиблення конституційно-правового забезпечення зовнішньополітичної діяльності держави; удосконалення механізму координації зовнішньополітичної діяльності державних органів і посадових осіб, наділених повноваженнями у сфері зовнішньої політики і міжнародних відносин та забезпечення національної безпеки в зовнішньополітичній сфері; підвищення злагодженості функціонування всього механізму здійснення зовнішньої політики держави в умовах зовнішньої агресії; проведення комплексної інвентаризації чинних угод і домовленостей у сфері зовнішніх відносин із РФ [152].

4.3. Пріоритети протидії загрозам національній безпеці

Українське суспільство і держава постійно стикаються з проблемою збалансованості в досягненні соціальних цілей та ресурсними можливостями їх забезпечення. У соціальної спрямованості їх розвитку

виникають протиріччя з економічними обмеженнями або, за наявності економічних ресурсів, – із пріоритетністю їх використання не на користь соціальним пріоритетам.

Гібридна війна ускладнила й урізноманітнила загрози національній безпеці України в усіх сферах суспільного життя [153, 154]. Це значне ускладнення загроз і викликів інтересам та фізичному існуванню українського суспільства і держави дозволить, у разі успіху протидії їх впливу, сформувати потужний ефективний та якісний механізм відстоювання і захисту національних інтересів.

У сучасних історичних реаліях в Україні існує безліч зовнішніх, а особливо внутрішніх загроз та викликів щодо задоволення цілісного комплексу провідних національних інтересів. Для визначення пріоритетних напрямків політики національної безпеки, на яких мають бути зосереджені основні зусилля в конкретний історичний період розвитку країни та суспільства, важливою є побудова ієрархії національних інтересів [155]. Як правило, для цього визначають ступінь їх важливості. Він визначається на основі оцінки завданої шкоди національній безпеці в разі неналежної реалізації того чи іншого інтересу, особливо в умовах зовнішньої агресії та ослаблення суспільних зв'язків і якості та ефективності функціонування соціальних та державних інститутів.

Визначаючи національні інтереси України як життєво важливі інтереси людини, суспільства й держави, новий Закон України «Про національну безпеку України» наголошує, що саме від їх реалізації залежить державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності й добробут громадян [96]. Як фундаментальні національні інтереси Закон визначає: державний суверенітет і територіальну цілісність, демократичний конституційний лад, недопущення втручання у внутрішні справи України, сталий розвиток національної економіки, громадянського суспільства та держави для забезпечення зростання рівня і якості життя населення, інтеграцію України в європейський політичний, економічний, безпековий та правовий простір, набуття членства в ЄС і в НАТО, розвиток рівноправних взаємовигідних відносин з іншими державами.

Захист та забезпечення реалізації цих національних інтересів є основою життєздатності нашої держави та умовою її подальшого прогресивного розвитку. В умовах переходу збройного протистояння на Сході України в стан затяжного тривалого конфлікту основні зусилля керівництва РФ зосереджуються саме на підриві цих базових принципів української державності. Внутрішня дестабілізація та дискредитація України, поступове знесилення нашої держави та її військових ресурсів – є на сьогодні основними цілями антиукраїнської політики РФ.

Відповідно захист національних інтересів України вимагає розроблення системи протидії наявним загрозам, яка, серед іншого, має включати такі заходи системно-комплексної реалізації:

В аналітично-прогнозній сфері:

- проведення системного аналізу і прогнозування змін глобальної та регіональної рівноваги геополітичних сил; основних трендів розвитку міжнародної і воєнно-політичної обстановки навколо України та Росії; перспектив розвитку озброєння і військової техніки;
- виявлення загроз національній безпеці, а також їх оцінка і ідентифікація за ступенями рівня вірогідності появи небезпек (зокрема, гібридного характеру);
- визначення «точок» вразливості держави (суспільства) щодо «гібридних загроз» та вжиття заходів щодо нейтралізації факторів вразливості;
- розроблення адекватних превентивних заходів протидії «гібридним загрозам» (зокрема, асиметричним конфліктам низької інтенсивності).

У законодавчій сфері:

- удосконалення національного законодавства щодо ефективного реагування та запобігання «гібридним загрозам»;
- активна участь України в процесах удосконалення міжнародного права у сфері глобальної, регіональної безпеки з питань протидії «гібридним загрозам»;
- удосконалення, з урахуванням сучасних викликів та загроз національній безпеці, законодавства щодо забезпечення громадянських прав і свобод.

У безпековій сфері:

- розроблення і впровадження ефективних правових, інституційних механізмів, які забезпечуватимуть антикризову стійкість, безпеку державного і воєнного управління в кризові періоди;
- забезпечення безперебійного функціонування державного (публічного) управління, політичної системи в умовах можливих кризових ситуацій;
- активізація розвідувальної діяльності, спрямованої на викриття можливих планів, намірів та ходу підготовки потенційних супротивників до війни проти України із застосуванням нових форм її проведення;
- орієнтація обороноздатності і правоохоронних органів та інших сил сектору безпеки і оборони України на готовність протидіяти «гібридним загрозам», зокрема, в умовах асиметричної конфліктності низької інтенсивності;
- удосконалення систем територіальної оборони та захисту державних кордонів;
- підвищення рівня ефективної протидії загрозам щодо критичної інфраструктури України (зокрема, її захист від можливих терористичних нападів та кібератак, а також забезпечення достатнього рівня пожежної безпеки).

У зовнішньополітичній сфері:

- налагодження взаємодії та тісної співпраці зі світовою громадськістю, стратегічними партнерами України, міжнародними організаціями, громадськими рухами щодо протидії загрозам розв'язання нових форм війни;
- використання можливостей публічної дипломатії та інформаційних комунікацій для викриття форм і методів реалізації технологій управління «гібридними загрозами» та їх ініціаторів;
- забезпечення в зовнішньополітичній, економічній, торговельній, фінансовій та оборонно-безпековій сферах стратегічної стабільності, розвитку стратегічного партнерства, реалізації заходів щодо стратегічного стримування посягань на національні інтереси та безпеку України.

У внутрішньополітичній сфері:

- протидія спробам дестабілізації внутрішньополітичної ситуації, провокаціям та антидержавній діяльності;
- забезпечення гуманітарної безпеки, консолідація суспільства навколо спільних духовних та культурно-історичних цінностей;
- запобігання та профілактика злочинності в суспільстві;
- системна робота з нейтралізації радикально-екстремістських проявів у суспільстві, насамперед, на релігійному, міжетнічному, расовому підґрунті, а також вжиття системно-режимних заходів щодо протидії міжнародному тероризму;
- патріотичне виховання молоді;
- контроль за міграційними процесами, запобігання використанню національних меншин із метою дестабілізації суспільно-політичної ситуації в Україні.

В інформаційній сфері:

- забезпечення ефективної протидії російській пропаганді, зорієнтованій на руйнацію національних цінностей України та єдності української нації, що здійснюється через інформаційну експансію і застосування інформаційно-психологічних, ціннісно-світоглядних, історичних, релігійних та інших засобів деструктивного впливу на суспільну свідомість;
- моніторинг інформаційного простору держави для завчасного блокування механізмів зовнішнього дестабілізуючого впливу та мережевого кризового управління.

У фінансово-економічній сфері:

- забезпечення захисту від гібридних загроз фінансово-банківської і економічної системи України, національних інвестиційного, фондового, товарного ринків тощо.

У сфері екології:

- підвищення рівня техногенної, екологічної, епідеміологічної, ядерної та радіаційної безпеки тощо.

В енергетичній сфері:

- створення енергетичних ринків, заснованих на принципах вільної конкуренції, належного захисту прав споживачів і безпеки постачань, незалежних від РФ;
- блокування введення в експлуатацію газопроводу «Північний потік – 2»;
- суттєве зменшення залежності від постачання ядерного палива для АЕС України.

У сфері кібербезпеки:

- забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі;
- підвищення рівня захисту об'єктів критичної інфраструктури [156].

Отже, успішна боротьба Української держави та українського народу проти російської агресії вимагає, насамперед, досягнення єдності української нації, збереження внутрішньої стабільності і вдосконалення всіх форм та напрямів державної політики, спрямованої на протидію загрозам національній безпеці. Таким чином, перед Україною стоїть комплекс завдань у дев'яти пріоритетних сферах суспільного життя, які на сьогодні мають забезпечити міцність української держави зсередини, одночасно максимально можливу активність на зовнішньополітичній арені, а також розбудову та подальше зміцнення обороноздатності нашої країни.

Висновки до четвертої глави

Для визначення пріоритетних напрямків політики національної безпеки, на яких мають бути зосереджені основні зусилля в конкретний історичний період розвитку країни та суспільства, важливою є побудова ієрархії національних інтересів. Гібридна війна ускладнила й урізноманітнила загрози національній безпеці України в усіх сферах суспільного життя. На сьогодні існують: воєнні, економічні, енергетичні, соціогуманітарні, загрози державній безпеці, інформаційні та кіберзагрози. Це значне ускладнення загроз і викликів національним інтересам та фізичному існуванню українського суспільства і держави потребує протидії їх впливу, формування ефективного та якісного механізму відстоювання і захисту національних інтересів.

Отже, успішна боротьба української держави та українського народу проти російської агресії вимагає, насамперед, досягнення єдності української нації, збереження внутрішньої стабільності і вдосконалення всіх форм та напрямів державної політики, спрямованої на протидію загрозам

національній безпеці. Таким чином, перед Україною стоїть комплекс завдань у десяти пріоритетних сферах суспільного життя: аналітично-прогнозній; законодавчій; безпековій; зовнішньополітичній; внутрішньополітичній; інформаційній; фінансово-економічній; енергетичній; екологічній; кібербезпековій, які на сьогодні мають забезпечити міцність української держави зсередини, одночасно максимально можливу активність на зовнішньополітичній арені, а також розбудову та подальше зміцнення обороноздатності нашої країни.

ГЛАВА 5
РОЗВИТОК І ВДОСКОНАЛЕННЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

5.1. Механізм протидії загрозам національній безпеці

У публічній політиці, як формі політичного процесу, на підставі суспільних цінностей та інтересів формуються і реалізуються стратегічні цілі суспільства та держави. Їх втілення в життя здійснюється за допомогою специфічних механізмів та інструментів цілеспрямованого впливу суб'єктів політики, управління, протидії на об'єкти і відносини суспільного життя, який забезпечує узгодження та захист інтересів його учасників. В умовах гібридної війни, яка характеризується сукупністю заздалегідь підготовлених та реалізованих агресором дій військового, дипломатичного, економічного, інформаційного характеру, спрямованих на досягнення стратегічних цілей із метою підпорядкування інтересів однієї держави іншій в умовах формального збереження політичного устрою країни, завдання формування дієвого механізму протидії загрозам національній безпеці є дуже актуальним.

Словник української мови в 11 томах тлумачить поняття «протидія» як дію, що спрямована проти іншої дії, яка перешкоджає їй [157]. Отже, протидія загрозам – це комплекс дій, спрямованих проти загрозливих дій для унеможливлення завдання шкоди об'єкту, на який вони спрямовані. Поняття «загроза» розуміється як наявні, так і потенційно важливі чинники, які створюють небезпеку фізичному існуванню та реалізації життєво важливих інтересів людини, суспільства і держави. Отже, поняття «небезпека» є ключовим у визначенні поняття «загроза». Характеризуючи чинники, які впливають на національну та міжнародну безпеку, широко вживаються такі поняття, як «ризик» і «виклик». Деякі дослідники ототожнюють поняття «виклик» і «загроза», а також поняття «загроза» з поняттям «небезпека» [158]. Відсутність критерію, за допомогою якого можна було б класифікувати реальні і потенційні загрози, зумовлює суперечливість при вживанні в діяльності органів державної влади понять «небезпека», «загроза», «виклик», «ризик», що потребує більш детального розгляду цих понять.

У словникових виданнях із російської мови під поняттям «небезпека» розуміється можливість загрози, біди, катастрофи, тобто в них ці поняття семантично не розрізняються [159]. У словнику-довіднику «Геополітика, міжнародна і національна безпека» поняття «небезпека» тлумачиться як цілком усвідомлена, але не фатальна можливість завдання

шкоди, майнового, фізичного або морального збитку особистості, суспільства, держави і займає проміжне положення між викликом і загрозою [160]. У ньому пропонується поняття «загроза національній безпеці», яке трактується як сукупність умов і чинників, що перешкоджають реалізації національних інтересів, а також створюють безпосередню можливість заподіяння збитку національним цінностям і національному способу життя [162]. В іншому словнику подається більш ширше розуміння поняття «небезпека», як об'єктивно існуюча можливість негативного впливу на об'єкт чи процес, унаслідок чого їм може бути завдано збитку, ймовірність збільшення шкоди або зменшення вигоди; це стан, коли не забезпечена захищеність життєво важливих засобів суб'єктів від можливості зменшення користі чи завдання шкоди [162].

А. Костров і А. Ткачова визначають небезпеку як стан суб'єкта чи об'єкта, які психологічно сприймають міру об'єктивної ймовірності реалізації зовнішніх загроз і міру шкоди, яка може бути заподіяна внаслідок реалізації цих загроз, з урахуванням у суб'єкта наявного захисту [162]. В. Акімов, В. Новіков, М. Радаєв [163] вважають, що одним із напрямів державної політики у сфері безпеки має бути виявлення небезпек, оцінка ризиків і прогнозування надзвичайних ситуацій, а також мінімізація ризику та підвищення ефективності захисту населення і територій, тобто вони розуміють певну сукупність небезпек, що небезпека – це об'єктивна реальність будь-якого виду діяльності, а її міра характеризується ризиком. О. Бодрук вважає, що загроза – реальна ознака небезпеки, яка є базовою конструкцією, що поєднує між собою інші компоненти безпеки, із чим погоджується В. Манілов [74, 164]. А В. Мунтіян розуміє під поняттям «загроза» реальну, а не фатальну можливість завдання шкоди, різноманітних збитків особистості, суспільству та державі [165]. Український науковець А. Качинський переконаний, що загроза – це явище з прогнозованими, але не контрольованими небажаними подіями, які можуть у певний момент на конкретній території завдати шкоди здоров'ю людей та спричинити матеріальні збитки [166]. Він вважає, що загроза відображає можливість виникнення деяких умов технічного, природного, економічного або соціального характеру, за наявності яких можуть виникнути несприятливі події та процеси. У нього ключем до розуміння сутності поняття «загроза» є ймовірна певна можливість виникнення несприятливих умов, які можуть призвести до заподіяння певної шкоди.

У сучасній науці ретельно опрацьовано питання класифікації загроз. Їх існує декілька, зокрема:

- За джерелами походження: природного походження – це небезпечні геологічні, метеорологічні, гідрологічні явища, деградація ґрунтів чи надр, природні пожежі, масове руйнування (через природні катаклізми) каналів зв'язку, зміна стану водних ресурсів та біосфери тощо; техногенного походження – транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку,

аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів системи управління національною безпекою тощо; антропогенного походження – вчинення людиною різноманітних дій із руйнування інформаційних систем, ресурсів, програмного забезпечення тощо.

- За ступенем гіпотетичної шкоди: загроза – явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері і створюють небезпеку для системи управління національною безпекою, життєзабезпечення її системоутворюючих елементів; небезпека – безпосередня дестабілізація функціонування системи управління національною безпекою.
- За повторюваністю вчинення: повторювані – такі загрози, які мали місце раніше; продовжувані – неодноразове здійснення загроз, що складається з низки тотожних загроз, які мають спільну мету.
- За сферами походження: екзогенні – джерело дестабілізації системи лежить поза її межами; ендогенні – алгоритм дестабілізації системи перебуває в самій системі.
- За ймовірністю реалізації: вірогідні – які за певних умов обов'язково настануть; неможливі – які за певних умов ніколи не настануть (такі загрози зазвичай мають більш декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають характер залякування); випадкові – які за певних умов кожного разу реалізуються по-різному.
- За рівнем детермінізму: закономірні – які носять стійкий, повторюваний характер, зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки; випадкові – які можуть або трапитися, або не трапитися.
- За значенням: допустимі – які не можуть призвести до колапсу системи; неприпустимі – які можуть у разі їх реалізації призвести до колапсу і дестабілізації СНБ.
- За структурою впливу: системні – що впливають одразу на всі складові елементи системи управління національною безпекою; структурні – що впливають на окремі структури системи; елементні – що впливають на окремі елементи структури системи. Дані загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу.
- За характером реалізації: реальні – активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією; потенційні – активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління; здійснені – які втілені в життя; уявні – псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

- За ставленням до них: об'єктивні – які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище; суб'єктивні – така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою.
- За об’єктом впливу: особа; суспільство; держава.

Для розуміння сутності процесів управління та протидії загрозам і послідовності етапів їх реалізації необхідно виділити чотири типи інструментів: інформаційні; фінансові; владні; структурні. Інструменти політики, управління, протидії загрозам – це дії органів влади, за допомогою яких реалізуються політичні, військово-політичні, соціально-економічні цілі та завдання; це специфічні засоби реагування на суспільні проблеми внутрішнього і зовнішнього характеру [167]. А механізм протидії загрозам національної безпеки становить складну управлінську систему, яка має низку складових: цільову – сукупність усіх цілей, на реалізацію яких спрямована управлінська діяльність; функціональну – види управлінської діяльності необхідні для виконання основних функцій публічної системи; методологічну – методи, які застосовуються для виконання всіх видів управлінської діяльності, для забезпечення реалізації функціональної складової; принципову – сукупність норм чи правил, які необхідні для успішної реалізації управління; технологічну – технології (процедури) підготовки, прийняття і реалізації управлінських рішень; інструментальну – управлінські рішення, повноваження, інформаційно-матеріально-енергетичні засоби впливу на об’єкт управління. Виходячи із цього, зрозуміло, що інструменти політики, управління, протидії – це складові механізму, які уособлюють у собі політичні та військово-політичні рішення, низку політичних повноважень, інформаційні, макро- і мікроекономічні та енергетичні важелі і засоби впливу на зовнішні та внутрішні суспільні процеси.

Отже, механізм протидії загрозам національній безпеці в умовах гібридної війни – це сукупність правових, організаційних, економічних, дипломатичних, інформаційних, психологічних, військових та інших способів і методів цілеспрямованого впливу суб’єктів політики, управління, протидії на об’єкти і відносини суспільного життя, який забезпечує узгодження та захист інтересів його учасників для формування комплексу дій, спрямованих проти загрозливих процесів для унеможливлення завдання шкоди захищеності життєво важливих інтересів особистості, суспільства і держави в різних сферах життєдіяльності від зовнішніх та внутрішніх загроз, яка сприяє стійкому розвитку країни в умовах гібридної війни [168].

Розглянемо його структуру детальніше. Комплексний механізм протидії загрозам національній безпеці в умовах гібридної війни складається з певної сукупності механізмів (рис. 5.1):

Рисунок 5.1. Комплексний механізм протидії загрозам національній безпеці в умовах гібридної війни

Організаційний – це об'єкти, суб'єкти державного регулювання, їх цілі, завдання, функції, методи управління та організаційні структури і результати їх функціонування [169].

Економічний – це державні механізми з грошово-валютної, інвестиційної, кредитної, податкової, страхової діяльності тощо [165].

Мотиваційний – сукупність командно-адміністративних та соціально-економічних стимулів до якісної й ефективної діяльності у всіх сферах суспільного життя [170].

Політичний – формування економічної, соціальної, фінансової, промислової політики тощо [167].

Правовий – нормативно-правове забезпечення: комплекс чинних законів та підзаконних актів органів державної влади та управління [171].

Організаційний механізм включає в себе (рис. 5.2):

- об'єкти: національні інтереси; громадяни України; загрози національним інтересам; виклики національним інтересам;
- суб'єкти: Президент України; РНБО України; МОУ; ЗСУ; МВС; Національна гвардія України; Національна поліція України; Державна прикордонна служба України; ДМСУ; ДСНС; СБУ; Управління державної охорони України; ДССЗЗІ; Державна спеціальна служба транспорту; координаційний орган з питань розвідувальної діяльності при Президентові України та розвідувальні органи України; Апарат РНБО України; центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику;

- функції, цілі та завдання інвестиційної та інвестиційно-інноваційної проєктної діяльності:
  - забезпечення державної незалежності, національної безпеки, правонаступництво держави і безперервність функціонування державної влади;
  - визначення стратегічних цілей та основних завдань державної політики у сфері національної безпеки і оборони України, складових сектору безпеки і оборони в мирний час, у кризових ситуаціях, що загрожують національній безпеці, та в особливий період, цілі та пріоритетні напрями розвитку складових сектору безпеки і оборони;
  - координація та контроль за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в мирний час, в умовах воєнного або надзвичайного стану та в разі виникнення кризових ситуацій, що загрожують національній безпеці України;
  - вдосконалення законодавства з питань національної безпеки і оборони, уточнення Стратегії національної безпеки України, Воєнної доктрини України, інших актів із питань національної безпеки і оборони;
  - реалізація державної політики з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва в мирний час та особливий період;
  - військово-політичне та адміністративне керівництво ЗСУ;
  - захист суверенітету, територіальної цілісності і недоторканності кордонів, стримування збройної агресії проти України та відсіч їй, охорона повітряного простору держави і підводного простору в межах територіального моря України;
  - добування розвідувальної інформації з метою підготовки держави до оборони, підготовки і проведення спеціальних операцій та/або спеціальних дій, забезпечення готовності ЗСУ до оборони держави;
  - забезпечення охорони прав і свобод людини, інтересів суспільства та держави, протидії злочинності, підтримання публічної безпеки і порядку;
  - захист державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні, здійснення прикордонного контролю і пропуску через державний кордон України;
  - здійснення цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації надзвичайних ситуацій;
  - припинення діяльності незаконних воєнізованих або збройних формувань, терористичних організацій, організованих груп та злочинних організацій, відновлення правопорядку в разі виникнення міжнаціональних і міжконфесійних конфліктів, розблокування або припинення протиправних дій у разі захоплення важливих державних об’єктів або місцевостей;

- протидія нелегальній міграції, громадянству, реєстрації фізичних осіб, біженців;
- захист населення і територій від надзвичайних ситуацій, запобігання їх виникненню, ліквідація наслідків надзвичайних ситуацій, рятувальна справа;
- забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку;
- забезпечення стійкого функціонування транспорту в мирний час та в особливий період;

➢ методи управління: сіткове та календарне планування, логістика, програмні ІТ-продукти, стандартне, структурне і ресурсне планування, пофазна організація роботи, імітаційне моделювання, системний підхід, єдиноначальність, вертикальний характер взаємодії та розміщення конкретних керівників на чолі окремих підрозділів;

➢ організаційні структури: міністерства, ради, служби, управління, комітети, координаційні та виконавчі органи, збройні та воєнізовані підрозділи, побудовані за принципом ієрархічного підпорядкування тощо.

Рисунок 5.2. Організаційний механізм

Економічний механізм складається з державних механізмів управління грошово-валютною та бюджетною діяльністю (рис. 5.3):

- нормативно-правові (Бюджетний кодекс України, Закони України про щорічні державні бюджети, «Про Національний банк України», «Про банки і банківську діяльність», постанови і розпорядження КМУ, накази міністерств, служб та управлінь, постанови Правління НБУ та інструкції НБУ);

- організаційно-інституціональні (Президент України, КМУ, НБУ, міністерства, служби, управління і комітети сектору безпеки і оборони, Державна фіскальна служба України, Державний комітет зв'язку та інформатизації України, Міністерство фінансів України, Міністерство економічного розвитку і торгівлі України);
- методи управління і регулювання (сіткове та календарне планування, логістика, програмні ІТ-продукти, стандартне, структурне і ресурсне планування, пофазна організація роботи, імітаційне моделювання, системний підхід, єдиноначальність, вертикальний характер взаємодії та розміщення конкретних керівників на чолі окремих, тендерні закупівлі).

Рисунок 5.3. Економічний механізм

Мотиваційний механізм включає в себе (рис. 5.4):

- сукупність командно-адміністративних мотиваційних інструментів: відповідні Закони України, постанови КМУ, накази міністерств, служб, управлінь сектору безпеки і оборони України ЦОВВ, а також статути, стандарти, дозволи, ліміти, заборони, обмеження, нормативи;
- сукупність соціально-економічних мотиваційних інструментів: податки, бюджетні закупівлі, субсидії, дотації, державні кредити, кредитні гарантії, позички, ціни, державні плани та цільові програми, національні проєкти, державний і місцеві бюджети, державне замовлення та державний контракт, державно-приватні договори, прогнози;
- прямі мотиваційні інструменти регулювання: державні соціальні гарантії, кар'єрне зростання, законодавче регулювання умов наймання та використання фахівців і службовців, фундаментальні наукові дослідження;
- непрямі мотиваційні інструменти регулювання: державна фінансова, податкова, інвестиційна, освітньо-наукова політика тощо.

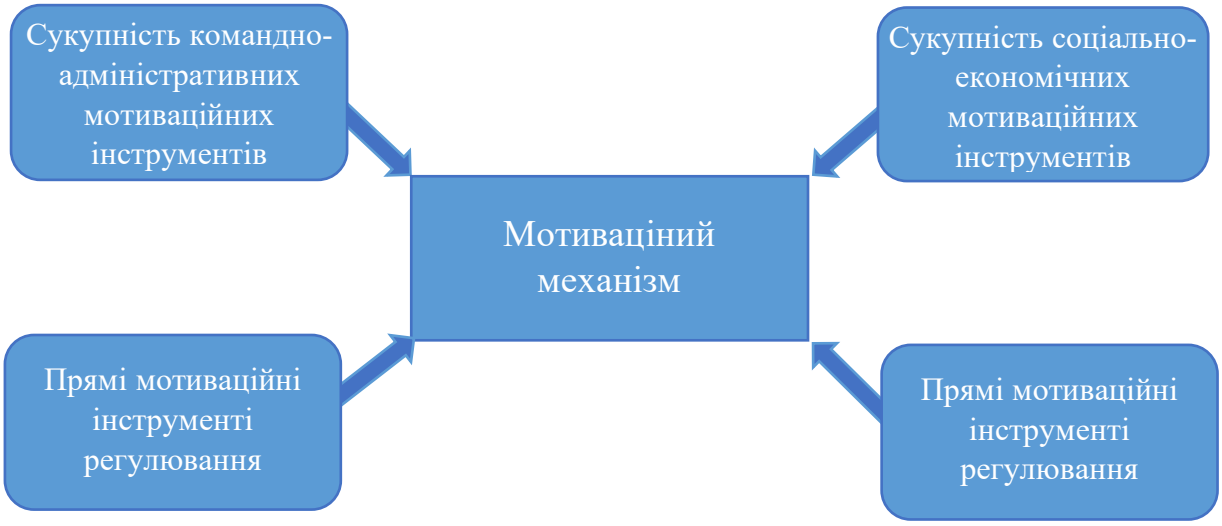

Рисунок 5.4. Мотиваційний механізм

Політичний механізм реалізації стратегічних завдань сектору безпеки і оборони України – це (рис. 5.5):

- організаційно-політичний механізм: ВРУ, Президент України, КМУ, усі центральні органи виконавчої влади, регіональні органи державної влади та органи місцевого самоврядування, органи судової влади;
- політико-правовий механізм: чинне законодавство України, де сформульоване і на підставі якого реалізується безпекова політика суспільства та держави в Україні, державні програми і національні проєкти.

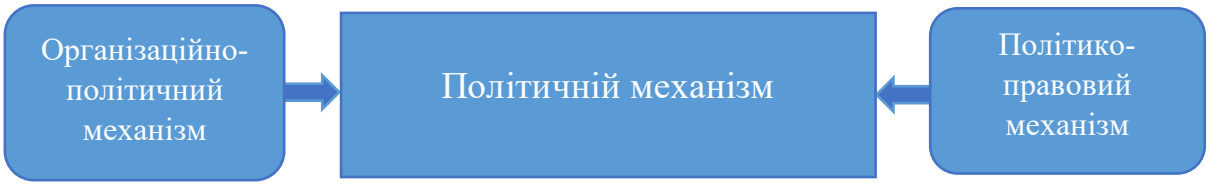

Рисунок 5.5. Політичний механізм

Правовий механізм – це сукупність нормативно-правових актів, що регулюють функції та ресурсне забезпечення їх виконання сектором безпеки та оборони України (рис. 5.6).

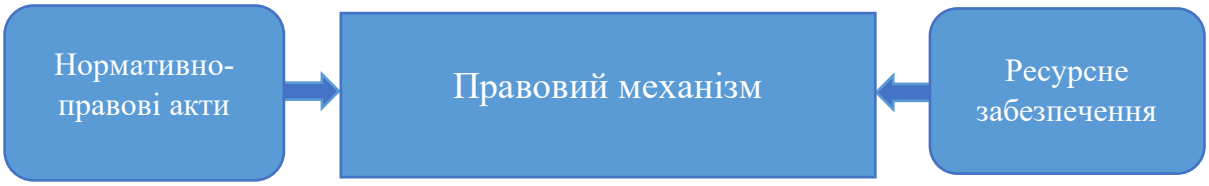

Рисунок 5.6. Правовий механізм

Розглянувши структуру комплексного механізму протидії загрозам національній безпеці в умовах гібридної війни, можна зробити висновок, що головною умовою його розвитку є збалансоване, гармонійне, якісне та ефективне функціонування організаційного, економічного, мотиваційного, політичного та правового механізмів. Також цей комплексний механізм має бути відкритою динамічної системою, яка чутливо та оперативно реагує на різноманітні загрози і виклики національним інтересам суспільства та держави.

5.2. Критерії оцінки функціонування механізму державного управління при протидії гібридним загрозам національній безпеці

Оцінка діяльності органу влади зосереджена в основному на наслідках його діяльності, оскільки кінцевою метою виробництва послуг у державному секторі є не послуги як такі, а їх спроможність задовольняти інтереси користувачів – платників податків. Найважливішими показниками є результати цього процесу та наслідки.

Державний апарат забезпечує реалізацію завдань та функцій держави і є інтегрованим суб'єктом державного управління. Зміст і характер цілей управління, способи та методи їх реалізації, сприйняття їх громадськістю і відповідність цілей потребам суспільного розвитку та особистості – це чинники, що безпосередньо впливають на ефективність і якість функціонування державного апарату [172].

Також важливою є й витратна складова оцінки функціонування державного апарату, оскільки досить великими є матеріальні, фінансові, інтелектуальні, кадрові, інформаційні та інші витрати на функціонування державного апарату. Значним є також обсяг управлінської діяльності, що виражається в реалізації нормативно-правових засад забезпечення життєдіяльності суспільства, у здійсненні організаційно-розпорядчих, консультативно-дорадчих і нормо-проєктних повноважень, у витратах робочого часу державних службовців. При цьому необхідно зазначити, що оцінка діяльності органів управління різними суб'єктами здійснюється з різних позицій. Так, громадянина цікавлять результати цієї діяльності; законодавця – досягнуті результати та характер виконаної роботи для виділення коштів із бюджету; керівника органу, державного службовця – досягнення цілей, що поставлені перед органом. Це обумовлює диференційований підхід до оцінки функціонування державного апарату, як із точки зору суб'єкта оцінки, так і з погляду об'єкта оцінки, а саме функціональної оцінки, тобто оцінки соціальних наслідків діяльності державного апарату та оцінки витратної складової. Функціональна оцінка в даному випадку є соціально-економічною категорією, що розкриває взаємозв'язок між результатами управлінської діяльності, вираженими соціальними ефектами і техніко-економічними показниками та затратами

управлінської праці (живої та матеріалізованої). Такою категорією може бути визнана категорія «результативності» (в іноземній спеціалізованій літературі – «efficiency») [173].

Проблема полягає в тому, що для державного апарату, як і для його складових органів державної влади (законодавчої, виконавчої, судової) та державної служби, розроблення критеріїв оцінки їх функціонування пов'язане із суттєвими труднощами, які обумовлені невизначеністю як отриманих соціальних результатів, так і витрат на їх досягнення (останнє пов'язане з тим, що об'єкт управління також несе певні витрати, які не завжди можна порахувати). При цьому необхідно враховувати таке:

- загальний соціальний ефект створюється не тільки суб'єктами управління, а й об'єктами управління;
- поряд із державним апаратом в управлінні суспільними процесами беруть участь й інші суб'єкти механізму управління держави, а саме: органи самоврядування, громадські об'єднання тощо.

Це підтверджує, що із загально-соціального ефекту необхідно виокремити соціальний ефект, отриманий за рахунок активності об'єктів господарювання (що для ринкових умов може становити визначальну частину), соціальний ефект, створений іншими суб'єктами управління, і тільки залишок можна співвідносити з діяльністю конкретного органу управління [174].

У науковому середовищі вважається, що соціальний ефект є інтегрованим критерієм. Це фактично є результат, що отримує суспільство, як в умовах споживання матеріальних, соціальних та духовних цінностей, так і в процесі їх виробництва. Соціальний ефект отримується протягом і внаслідок усього ЖЦ послуги, процесу, організаційної форми тощо, завдяки раціональній організації суб'єкта управління, оптимальному функціонуванню об'єктів управління, узгодженості їх активності та діяльності із закономірностями соціально-економічного стану суспільства, відповідності потребам, інтересам і спроможності громадян. Наведені ознаки раціональності, оптимальності, узгодженості та відповідності є характерними для прояву позитивного соціального ефекту [175].

Для того щоб оцінювати результат, він повинен бути сталим, прогресуючим, містити джерело і ресурси майбутнього розвитку.

Якщо визнавати, що соціальний ефект – це соціальний результат, то потрібно визнати, що не всі соціальні результати є позитивними. Існують і негативні соціальні результати. Саме тому слід розуміти, що лише той соціальний результат має вагоме значення для суспільства чи для певних його прошарків, якщо вони можуть ним послуговуватися з користю для себе в повсякденному житті. Такий результат є корисним, тобто таким, що задовольняє прагнення та інтереси членів суспільства. Виходячи із цього, потрібно підкреслити, що соціальний результат повинен бути також і якісним.

У сучасних умовах необхідно застосовувати механізм державного управління для протидії гібридним загрозам і забезпечення національній безпеці.

При цьому необхідно враховувати, що державний механізм управління являє собою складний комплекс взаємопов'язаних елементів і за своєю сутністю є складною системою. Така система характеризується цілісністю, протистоїть зовнішньому середовищу та забезпечує роботу всіх своїх компонентів над виконанням спільного призначення системи. Згідно з визначенням, міра виконання системою свого призначення називається ефективністю [176].

Формально ефективність *(E)* є функцією якості результату *(Q)*, часу його отримання *(T)*, витрачених на це ресурсів *(W)*:

$$E = F(Q, T, W).$$

Також цей механізм має бути відкритою динамічної системою, яка чутливо та оперативно реагує на різноманітні загрози і виклики національним інтересам суспільства та держави.

Отже, механізм державного управління при протидії загрозам національній безпеці в умовах гібридної війни та результати його функціонування може мати критерієм оцінки якісний та ефективний результат, у забезпеченні захисту життєво важливих національних інтересів українського суспільства, зокрема:

- дотриманні прав і свобод людини та громадянина;
- забезпеченні суверенітету України, її територіальної цілісності, недоторканності державного кордону, демократичного конституційного ладу, верховенства права;
- збереженні і розвитку духовних та культурних цінностей суспільства;
- удосконаленні механізмів реалізації конституційного принципу розподілу влади на законодавчу, виконавчу і судову;
- створенні безпечних умов життєдіяльності, захисту навколишнього природного середовища;
- забезпеченні конкурентоспроможності держави та економічного добробуту населення, шляхом всебічного розвитку людського, науково-технічного, інноваційного потенціалів країни;
- створенні умов для сприйняття української держави міжнародним співтовариством як повноцінного і рівноправного його члена.

5.3. Напрями розвитку і вдосконалення механізму протидії гібридним загрозам національній безпеці

В умовах переходу збройного протистояння на Південному Сході України і стану затяжного тривалого конфлікту основні зусилля РФ зосереджуються саме на підриві базових принципів української державності. Внутрішня дестабілізація та дискредитація України, поступове знесилення нашої держави та її військових ресурсів – є на сьогодні основними цілями антиукраїнської політики РФ. Ця політика складається з кількох напрямів: дезорганізації політичного, державного і воєнного управлінь у нашій державі, введення їх у кризові стани; загострення суперечностей серед національної та регіональних еліт України; розколу українського суспільства; дискредитації діючої української влади і ходу реалізації її євроінтеграційного курсу; підриву української економіки та знесилення державних і військових ресурсів; формування антиурядових настроїв в Україні, підготовки передумов до виникнення соціальної напруги та антиурядової протестної активності серед населення; руйнації єдності політики західних держав у питанні запровадження і розширення санкцій; введення в оману світової спільноти щодо природи та причин ситуації, породженої російською агресією; нав'язування країнам ЄС і США рішення щодо недоцільності співпраці з Україною без урахування зовнішньополітичної позиції Росії тощо.

При цьому РФ демонструється воєнна сила та готовність до повномасштабної війни з метою нагнітання воєнно-політичної обстановки, отримання дипломатичних зисків та поступового моделювання майбутніх домовленостей з Євроатлантичним співтовариством щодо розподілу сфер геополітичного впливу. Існує ймовірність того, що керівництво РФ може наважитися на реалізацію концепції силового «реваншу» стосовно України. Один зі сценаріїв може ґрунтуватися на застосуванні моделі дестабілізації суспільно-політичної ситуації в країні під час майбутніх виборів у поєднанні із прихованою силовою підтримкою, зорієнтованою на зміну влади в Україні.

Тому перед українським суспільством і державою стоїть стратегічно важливе завдання – зберегти єдність та усвідомлення пріоритету національних цінностей, інтересів і цілей, забезпечити внутрішньополітичну злагоду в країні та не допустити деструктивних проявів російського втручання у внутрішні справи України.

Захист національних інтересів України в умовах гібридної війни вимагає вдосконалення та розвитку механізму протидії наявним загрозам, якій повинен включати в себе заходи системно-комплексної реалізації, що потребує внесення відповідних змін в усі його складові [177, 178].

Зміни в організаційний механізм:

- аналітично-прогнозна складова:

- проведення системного аналізу і прогнозування змін глобальної та регіональної рівноваги геополітичних сил; основних трендів розвитку міжнародної і воєнно-політичної обстановки навколо України та Росії; перспектив розвитку озброєння і військової техніки;
- виявлення загроз національній безпеці, а також їх оцінка й ідентифікація за ступенями рівня вірогідності появи небезпек (у т. ч. гібридного характеру);
- визначення «точок» вразливості держави (суспільства) щодо «гібридних загроз» та вжиття заходів щодо нейтралізації факторів вразливості;
- розроблення адекватних превентивних заходів протидії «гібридним загрозам», зокрема, асиметричним конфліктам низької інтенсивності;

➢ функціональна складова:

- розроблення і впровадження ефективних правових, інституційних механізмів, які забезпечуватимуть антикризову стійкість, безпеку державного та воєнного управління в кризові періоди;
- забезпечення безперебійного функціонування державного (публічного) управління, політичної системи в умовах можливих кризових ситуацій;
- активізація розвідувальної діяльності, спрямованої на викриття можливих планів, намірів та ходу підготовки потенційних супротивників до війни проти України із застосуванням нових форм її проведення;
- орієнтація обороноздатності і правоохоронних органів та інших сил сектору безпеки і оборони України на готовність протидіяти «гібридним загрозам», зокрема, в умовах асиметричної конфліктності низької інтенсивності;
- удосконалення систем територіальної оборони та захисту державних кордонів;
- підвищення рівня ефективної протидії загрозам щодо критичної інфраструктури України. Зокрема, її захист від можливих терористичних нападів та кібератак, а також забезпечення достатнього рівня пожежної безпеки;

➢ інформаційна складова:

- забезпечення ефективної протидії російській пропаганді, зорієнтованій на руйнацію національних цінностей України та єдності української нації, що здійснюється через інформаційну експансію і застосування інформаційно-психологічних, ціннісно-світоглядних, історичних, релігійних та інших засобів деструктивного впливу на суспільну свідомість;

- моніторинг інформаційного простору держави для завчасного блокування механізмів зовнішнього дестабілізуючого впливу та мережевого кризового управління;

➢ екологічна та інфраструктурна складова:

- підвищення рівня техногенної, екологічної, епідеміологічної, ядерної та радіаційної безпеки тощо.

Зміни у правовий механізм:

- удосконалення національного законодавства щодо ефективного реагування та запобігання «гібридним загрозам»;
- активна участь України в процесах удосконалення міжнародного права у сфері глобальної, регіональної безпеки з питань протидії «гібридним загрозам»;
- вдосконалення, з урахуванням сучасних викликів та загроз національній безпеці, законодавства щодо забезпечення громадянських прав і свобод.

Зміни в політичний механізм:

➢ зовнішньополітична організаційно-політична складова:

- налагодження взаємодії та тісної співпраці зі світовою громадськістю, стратегічними партнерами України, міжнародними організаціями, громадськими рухами щодо протидії загрозам розв'язання нових форм війни;
- використання можливостей публічної дипломатії та інформаційних комунікацій для викриття форм і методів реалізації технологій управління «гібридними загрозами» та їх ініціаторів;
- забезпечення в зовнішньополітичній, економічній, торговій, фінансовій та обороннобезпековій сферах стратегічної стабільності, розвитку стратегічного партнерства, реалізації заходів щодо стратегічного стримування посягань на національні інтереси та безпеку України.

➢ внутрішньополітична організаційно-політична складова:

- протидія спробам дестабілізації внутрішньополітичної ситуації, провокаціям та антидержавній діяльності;
- забезпечення гуманітарної безпеки, консолідація суспільства навколо спільних духовних та культурно-історичних цінностей;
- запобігання та профілактика злочинності в суспільстві;
- системна робота з нейтралізації радикально-екстремістських проявів у суспільстві, насамперед на релігійному, міжетнічному, расовому підґрунті, а також вжиття системно-режимних заходів щодо протидії міжнародному тероризму;
- патріотичне виховання молоді;
- контроль за міграційними процесами, запобігання використанню національних меншин із метою дестабілізації суспільно-політичної ситуації в Україні.

Зміни в економічний механізм:

- забезпечення захисту від гібридних загроз фінансово-банківській і економічній системі України, національних інвестиційного, фондового та товарного ринків тощо.

Забезпечення гарантованого відбиття агресії РФ потребувало не лише проведення термінових масштабних заходів із підвищення боєздатності сил оборони держави. Постала також нагальна потреба в розробленні нової концепції захисту суверенітету, територіальної цілісності та недоторканності України в умовах сучасних воєнних конфліктів. Класична оборона, зорієнтована переважно на відбиття збройної агресії та протидію збройним силам інших держав, уже не відповідає сучасному характеру ведення збройної боротьби. Уже той факт, що інспірування збройного конфлікту всередині держави стає невід'ємною складовою агресії, порушує стереотипи минулого.

Тому виникає необхідність вийти за межі організації та ведення лише класичної оборони держави і розглядати більш широке поняття – забезпечення воєнної безпеки як захищеності національних інтересів України від воєнних загроз, як зовнішніх, так і внутрішніх. При цьому як інструменти забезпечення, поряд із військовими, значна роль має бути відведена невоєнним засобам (економічним, політичним, інформаційно-психологічним, кібернетичним тощо).

У затвердженій Президентом України 14.09.2020 р. «Стратегії національної безпеки України» формування та розвиток сектору безпеки і оборони визначено як пріоритет політики національної безпеки [94]. Так само Воєнна доктрина України визначає його як головний елемент системи забезпечення воєнної безпеки. Це функціональне об'єднання державних органів дає змогу поєднати спроможності військових формувань, правоохоронних та розвідувальних органів, спеціальних служб для забезпечення адекватного реагування на широкий спектр загроз і, передусім, воєнного характеру. В умовах, коли агресор проводить воєнні дії в комплексі з інструментами впливу на соціально-політичну обстановку, провокує сепаратистські рухи та створення їх збройних формувань, використовує у своїх цілях кримінальні елементи, посилює розвідувально-підривну діяльність спецслужб, саме поєднання безпекових та оборонних потенцій у рамках сектору безпеки і оборони дає змогу ефективно діяти у відповідь.

Таким чином, постає потреба в більш високому рівні поєднання зусиль усіх складових сектору безпеки і оборони, забезпечення керівництва ним як цілісної системи. Реалізація цього завдання вимагає [177, 178]:

1) Розроблення комплексу взаємоузгоджених планів діяльності (застосування) усіх складових сектору безпеки і оборони, які реалізують як військові (силові), так і невійськові інструменти при протидії воєнним загрозам. На сьогодні в Україні на особливий період розробляються два плани державного рівня – Мобілізаційний план України та Стратегічний

план застосування ЗСУ та інших складових сил оборони. Перший із них (як уже видно з його назви) визначає порядок мобілізаційного розгортання сил оборони, переведення національної економіки та життєдіяльності країни загалом на функціонування в умовах особливого періоду. Другий стосується використання (застосування) сил оборони під час відсічі збройної агресії. Питання ведення боротьби проти агресора в політичній, інформаційній та економічній сферах випадають із загальнодержавного стратегічного планування. У більшості випадків ведення зазначених видів боротьби має ситуативний характер або проводиться окремими державними органами в інтересах виконання визначених їм основних завдань. Політичний, інформаційний та економічний види боротьби мають свою специфіку, суттєво відмінну від збройної боротьби. Процеси, які відбуваються у відповідних сферах, особливо в політичній та інформаційній, більш динамічні і швидкоплинні. У багатьох випадках важко ідентифікувати час зміни загальної мети заходів, які проводить потенційний агресор у цих сферах: перехід від етапу конкуренції (перманентно присутня в міждержавних відносинах) до конфронтації.

У протистоянні з більш сильним у військовому вимірі противником політичні та інформаційні види боротьби, а за певних умов і економічна боротьба, можуть відігравати роль елементів асиметричної стратегії. На відміну від нинішніх стратегічних планів України стратегічний план забезпечення воєнної безпеки, що передбачає комплексне застосування воєнних і невоєнних інструментів, має реалізовувати принцип поступового нарощування потенціалу захисту.

2) Удосконалення системи керівництва та управління сектором безпеки і оборони, застосування його сил та засобів, а також процесу забезпечення воєнної безпеки України в кризовій ситуації і в особливий період. Оцінка різних варіантів структури і функціональних зв’язків системи керівництва та управління сектором безпеки і оборони та забезпеченням воєнної безпеки держави в особливий період показує, що найбільш оптимальною необхідно визнати систему, в основу якої покладено змішану ієрархічну структуру з вертикальними і горизонтальними зв’язками. Ідея такої структури вперше була запропонована академіком В. М. Глушковим [179].

Для успішного виконання РНБО цих завдань необхідно буде переглянути структуру Апарату Ради та укомплектувати його фахівцями відповідної спеціалізації.

На другому рівні ієрархічної вертикалі мають розміщуватися суб’єкти керівництва, які здійснюють безпосереднє управління підпорядкованими або передані їм силами за певними напрямами на підставі рішень Президента України. Серед таких суб’єктів, зокрема, є:

- Головнокомандувач ЗСУ і Генеральний штаб – забезпечують збройний захист держави;
- МЗС – організовує і проводить політико-дипломатичні заходи;

- МВС – забезпечує підтримання публічної безпеки, захист державного кордону, припинення діяльності незаконних збройних формувань, ліквідацію наслідків надзвичайних ситуацій;
- Міністерство економічного розвитку і торгівлі – забезпечує захист держави в економічній сфері;
- Міністерство інформаційної політики (спільно з іншими зацікавленими державними структурами) – забезпечує захист державних інтересів в інформаційному просторі.

Під час виконання завдань у кризовій ситуації суб'єкти другого рівня взаємодіють між собою, а в разі потреби за рішенням Президента України проводять заходи спільно з розвідувальними органами та спецслужбами.

3) Проведення спільних навчань і тренувань органів управління, військ, сил та підрозділів складових сектору безпеки і оборони.

4) Розроблення теорії та освоєння ефективних форм і способів спільного застосування (діяльності) структурами сектору безпеки і оборони інформаційної, політико-дипломатичної та економічної боротьби.

Отже, на сьогодні Україна накопичила достатньо досвіду, що дозволяє аналізувати і виявляти особливості гібридних дій противника, а також визначати форми і способи взаємодії всіх складових сектору безпеки і оборони для протидії наявним гібридним загрозам. Таким чином, розроблені пропозиції дозволять забезпечити захист національних інтересів України в умовах гібридної війни, а також удосконалення та розвиток комплексного механізму протидії сучасним загрозам національній безпеці.

Висновки до п'ятої глави

Механізм протидії загрозам національній безпеці в умовах гібридної війни – це сукупність правових, організаційних, економічних, дипломатичних, інформаційних, психологічних, військових та інших способів та методів цілеспрямованого впливу суб'єктів політики, управління, протидії на об'єкти і відносини суспільного життя, який забезпечує узгодження та захист інтересів його учасників для формування комплексу дій, спрямованих проти загрозливих процесів для унеможливлення нанесення шкоди захищеності життєво важливих інтересів особистості, суспільства і держави в різних сферах життєдіяльності від зовнішніх та внутрішніх загроз, який сприяє стійкому розвитку країни в умовах гібридної війни. Він складається з певної сукупності механізмів: організаційного, економічного, мотиваційного, політичного і правового, тому являє собою комплекс взаємопов'язаних елементів і за своєю сутністю є складною системою, яка характеризується цілісністю, протистоїть зовнішньому середовищу та забезпечує роботу всіх своїх компонентів над виконанням спільного призначення системи. Також цей механізм має бути відкритою динамічної системою, яка чутливо та оперативно реагує на

різноманітні загрози і виклики національним інтересам суспільства та держави.

Отже, механізм протидії загрозам національній безпеці в умовах гібридної війни та результати його функціонування повинні мати критерієм оцінки якісний та ефективний результат у забезпеченні захисту життєво важливих національних інтересів українського суспільства, а розроблені пропозиції дозволять забезпечити його вдосконалення і розвиток.

ВИСНОВКИ

У монографії досліджено трансформацію СНБ перед викликами гібридної війни і запропоновано механізм протидії загрозам національній безпеці, який підвищує ефективність СНБ в цілому. При цьому отримано нові теоретичні, методичні та практичні результати:

- виконано аналіз еволюції гібридних війн, їх компонентів та особливостей;
- побудовано МГВ;
- визначено поняття, структуру та складові національної безпеки;
- сформовано науково-обґрунтовані погляди на організаційно-правові основи протидії загрозам національній безпеці країни;
- запропоновано концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки;
- розроблено концептуальні основи побудови системи національної кібербезпеки;
- побудовано модель системи національної кібербезпеки і модель взаємодії центрів протидії кіберзагрозам;
- обґрунтовано сутність і структуру комплексного механізму протидії гібридним загрозам національній безпеці та визначено напрями його вдосконалення і розвитку.

У цілому отримані результати у вигляді концептуальних основ, моделей і механізмів створюють теоретико-методологічні та організаційні основи, які надають загальне бачення та розуміння можливостей трансформації СНБ для розвитку і вдосконалення протидії гібридним загрозам і захисту національних інтересів.

ПІСЛЯМОВА

У монографії проаналізовано виникнення та еволюцію гібридних війн, їх компоненти та особливості, також наведено МГВ. Визначено поняття, структуру і складові національної безпеки, основні суб'єкти протидії загрозам національній безпеці і розглянуто СЗНБ. Основну увагу приділено теоретико-методологічним та організаційним основам протидії загрозам національній безпеці в умовах гібридної війни, реалізації національних інтересів країни та розвитку і вдосконаленню механізму протидії гібридним загрозам національній безпеці.

Методологічну основу дослідження становив комплексний міждисциплінарний підхід, що використовує методи різних наук, заснований на сполученні як загальнонаукових методів, таких як аналіз і синтез, історичний та діалектичний, так і спеціальних методів, тобто статистичний метод, аналіз нормативно-правових актів. Інформаційну базу становили нормативно-правові документи, наукові праці вітчизняних та зарубіжних фахівців, дані первинної відкритої інформації ЗМІ.

Для аналізу існуючих моделей функціонування механізму протидії загрозам національній безпеці в умовах гібридної війни як у вітчизняній, так і закордонній практиці, використано методи порівняння та узагальнення. Для вивчення можливостей використання ресурсів цього механізму застосовано системний, статистичний і порівняльний аналіз. Проведений аналіз теперішнього стану реалізації ресурсів недержавних суб'єктів національної безпеки України дозволив зробити практичні рекомендації щодо модернізації і вдосконалення механізму протидії загрозам національній безпеці в умовах гібридної війни. Крім цього, визначено напрями розвитку цього механізму, критерії якості й ефективності його функціонування та перспективи трансформації сектору безпеки і оборони країни.

Практичне значення одержаних результатів полягає в тому, що це дослідження може бути покладене в основу розроблення нової концепції захисту національного суверенітету, територіальної цілісності та недоторканності України в умовах сучасних гібридних конфліктів, а також нових форм та способів дій складових сектору безпеки і оборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с.

2. Магда Е.В. Гибридная война: выжить и победить. Харьков : Виват, 2015. 320 с.

3. Слюсаренко А.В. Новітні форми міждержавного протистояння як предмет дослідження сучасної воєнно-наукової думки. *Військово-науковий вісник*. 2015. Вип. 24. С. 173–186.

4. Ткаченко В., Дорошенко Н. «Гибридная война»: политические последствия. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України*. 2015. Вип. 1. С. 58–69.

5. Мальський М.З. Транскордонна безпека: політико-правовий, соціально-економічний, гуманітарний та екологічний вимір. *Зб. матеріалів Міжнар. наук.-практ. конф.* (Львів, 21 квітня 2017 р.) / уклад.: М. З. Мальський, О. С. Кучик, Р.В. Вовк. Львів : Факультет міжнародних відносин, 2017. 96 с.

6. Мартинюк В. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і східного партнерства. Київ, 2018. 106 с.

7. Предборський В.А. Гібридна війна як відбиття закономірностей розвитку суспільства незавершеної модернізації. *Формування ринкових відносин в Україні*. 2014. № 10. С. 13–18.

8. Руснак І.С. Воєнна безпека України у світлі реформування сектора безпеки і оборони. *Наука і оборона*. 2015. № 2. С. 9–14.

9. Hoffman F.G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA : Potomac Institute for Policy Studies, 2007. P. 14.

10. Huber T.M. Compound Warfare. That Fatal Knot. *US Army Command and General Staff College Press.* Fort Leavenworth, KS, 2002. P. 2. URL: https://apps.dtic.mil/sti/pdfs/ADA481548.pdf (date of access: 17.04.2021).

11. Nemeth W.K. USMC, Future War and Chechnya: A Case for Hybrid Warfare. Monterey, California : Naval Postgraduate School, 2002. URL:

https://core.ac.uk/download/pdf/36699567.pdf (date of access: 16.04.2021).

12. Michael W. Isherwood. Airpower for Hybrid Warfare. P. 33. A New Challenge, 2009. URL: https://www.airforcemag.com/article/1009hybrid (date of access: 18.04.2021).

13. Walker R.G. SPEC FI: the United States Marine Corps and Special Operations. Monterey, California : Naval Postgraduate School, 1998. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a359694.pdf (date of access: 15.04.2021).

14. Mansoor P.R., Murray W. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge, New York : Cambridge University Press, 2012. 334 p.

15. Бартош А.А. Конфликты XXI века. Гибридная война и цветная революция. Москва : Горячая линия-Телеком, 2018. 284 с.

16. Тиханичев О.В. Гібридні війни: нове слово в військовому мистецтві чи добре забуте минуле? *Питання безпеки*. 2020. № 1. С. 30–43.

17. Манойло А.В. Цветные революции и гибридные войны. *Стратегия России*. 2015. № 7. С. 19.

18. Карякин В.В. Геополитика постмодерна: восприятие гибридных войн и цветных революций в общественном сознании. *Гражданин. Выборы. Власть*. 2019. № 3(13). С. 68–78.

19. Гилёв А. Многомерная война и новая оборонная стратегия. *Россия в глобальной политике*. 2014. Т. 12, № 5. С. 47–58.

20. Слипченко В.И. Воины шестого поколения: оружие и военное искусство будущего. Москва : Вече, 2002. 384 с.

21. Сунь-цзи. Мистецтво війни / за ред. Т. Клірі. Київ : Софія, 2018. 224 с.

22. Лисецький Ю.М., Семенюк Ю.В. Гібридні війни. Ретроспективний аналіз. *Вісник воєнної розвідки*. 2021. № 68. С. ?–?.

23. Лисецький Ю.М., Старовойтенко О.О., Семенюк Ю.В., Павленко Д.Г. Виникнення і еволюція гібридних воєн. *Держава і право.* 2021. Вип. 90. С. ?–?.

24. Ксенофонт Анабасис. Санкт-Петербург : Азбука, Азбука-Аттикус, 2019. 320 с.

25. Уізер Д.К. Сенс гібридної війни. *Connections: The Quarterly Journal*. 2016. Vol. 15, N 2. P. 84–100.

26. Luttwak E.N. Coup d'État: A Practical Handbook. Harvard University Press, Cambridge, Massachusetts, London, England, 1979. 728 p.

27. Гостев А.Н. Гибридная война: практика, проблемы безопасности. *Инноватика и экспертиза*. 2019. Вып. 1 (26). С. 237–257.

28. Герберштейн С. Записки о Московии / пер. с нем. А.И. Малеина, А.В. Назаренко. Москва : Изд-во МГУ, 1988. 430 с.

29. Гахов В.Р. Кибер-угрозы автоматизированным системам управления. *Вестник Академии военных наук*. 2013. № 1 (42). С. 103–109.

30. Daily movement news and resources. US Spent $4.2M in 2015 to Destabilize Venezuelan Government. 2017. 9 April. URL: https://popularresistance.org/us-spent-4-2m-in-2015-to-destabilize-venezuelan-government (date of access: 23.07.2021).

31. Денежное обращение России: Исторические очерки. Каталог: в 2 т. / под ред. Г.И. Лунтовского, А.Н. Сахарова, А.В. Юрова. Москва : ИНТЕРКРИМ-ПРЕСС, 2010. Т. I: Исторические очерки: с древнейших времен до наших дней / сост. Ю.П. Бокарев (науч. рук.), В.А. Кучкин, В.Л. Степанов, М. Б. Маршак, С.В. Калмыков, В.В. Узденников, А.В. Бугров, Л.Е. Морозова, А.Г. Баранов, Е.Ю. Гончаров. 462 с.; Москва : ИНТЕРКРИМ-ПРЕСС, 2010. Т. II: Каталог. / сост. А. В. Юров, А. Г. Баранов, А. В. Бугров, В. М. Герасимов. 736 с.

32. Катасонов В. Экономические войны и экономические санкции. Сайт «Военное обозрение». URL: https ://topwar.ru/68238-ekonomicheskie-voyny-i-ekonomicheskie-sankcii.html (дата звернення: 24.07.2021).

33. Бокарев Ю.П. СССР и становление постиндустриального общества на Западе (1970–1980-е гг). Москва : Наука, 2007. 381 с.

34. 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)*. 2019. 11 March. URL: https://www.mintpressnews.com/did-the-us-recycle-a-bush-era-plan-to-take-outvenezuelas-power-grid/256113/ (дата звернення: 25.07.2021).

35. Интернациональные бригады в Испании. *Советская военная энциклопедия:* в 8 т. / под ред. Н.В. Огаркова. Т. 3. Москва : Воениздат, 1977. 567 с.

36. Дюпюи Р.Э., Тревор Н. Дюпюи Всемирная история войн: в 4 т. Кн. 4: 1925–1997. Санкт-Петербург ; Москва : Полигон-АСТ, 1998. С. 35–36.

37. Рыбалкин Ю. Операция «Х». Советская помощь республиканской Испании (1936–1939). Москва, 2000. С. 43–45.

38. Бартош А.А. Ускорители гибридной войны. *Военно-промышленный курьер*. 2018. № 4 (759). URL: https://vpk-news.ru/articles/46584 (дата звернення: 24.07.2021).

39. Манойло А.В. Основы теории современных информационных войн. *Геополитический журнал*. 2017. № 4 (19). С. 3–23.

40. Бартош А.А. «Трение» и «износ» гибридной войны. *Военная мысль*. 2018. № 1. С. 5–13.

41. Клаузевиц К. О войне: в 8 т. Москва : Госвоениздат, 1934. 692 с.

42. Лисецький Ю.М., Старовойтенко О.О., Семенюк Ю.В., Павленко Д.Г. Гібридні війни. Компоненти та особливості. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Державне управління.* 2021. Т. 32 (71), № 5. С. ?–?.

43. Герасимов В.В. Ценность науки в предвидении. *Военно-промышленный курьер.* 2013. № 8 (476). С. 17–24.

44. Rosenau J. The study of political adaptation. L.: N.Y., 1981. P. 61.

45. Галака О., Ільяшов О., Павлюк Ю. Основи тенденції розвитку та ймовірні форми воєн та збройних конфліктів майбутнього. *Наука і оборона*. 2007. № 4. С. 10–15.

46. Гейтс Р. Сбалансированная стратегия. *Россия в глобальной политике*. 2009. № 2. С. 26.

47. История философии. Энциклопедия. ТРАНСГРЕССИЯ. URL: http://velikanov.ru/philosophy/transgressija.asp (дата звернення: 18.04.2021).

48. Пухов Р. Миф о «гибридной войне». URL: http://nvo.ng.ru/realty/2015-05-29/1_war.html (дата звернення: 19.04.2021).

49. Hoffman F.G. Hybrid Warfare and Challenges. *Joint Force Quarterly (JFQ)*. 2009. Issue 52. Forth Quarter. P. 34–39.

50. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Міждержавні протистояння. Нові реалії. *Держава і право*: *зб. наук. праць. Політичні науки.* 2021. № 89. С. 249–257.

51. Лисецький Ю.М., Семенюк Ю.В., Старовойтенко О.О. Гібридна війна як багатовимірне протистояння. *Вісник воєнної розвідки*. 2021. № 67. С. ?–?.

52. Бартош А.А. Туман гибридной войны. Неопределенности и риски конфликтов современности. Москва : Горячая линия-Телеком, 2019. С. ???.

53. Бартош А.А. Модель гибридной войны. *Военная мысль.* 2019. № 5. С. 6–23.

54. Лисецкий Ю.М. Корпоративные интегрированные информационные системы. Концепция, технологии разработки и внедрения: монография. Киев : ЛАТ&К, 2019. 204 с.

55. Згуровский М.З., Доброногов А.В., Померанцева Т.Н. Исследование социальных процессов на основе методологии системного анализа. Киев : Наукова думка, 1997. 221 с.

56. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ. Москва : Высшая школа, 1989. 367 с.

57. Снитюк В.Е. Эволюционные технологии принятия решений в условиях неопределенности: монография. Киев : МП Леся, 2015. 347 с.

58. Тимченко А.А. Основы системного проектирования и системного анализа сложных объектов. Киев : Лыбидь, 2000. 272 с.

59. Карпунин М.Г., Любинецкий Я.Г., Майданчик Б.И. Жизненный цикл и эффективность машин. Москва : Машиностроение, 1989. 312 с.

60. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Національна безпека: поняття, складові, чинники впливу. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Державне управління.* 2021. Т. 32 (71), № 3. С. 102–107.

61. Луман Н. Социальные системы: очерк общей теории / пер. с нем. И.Д. Газиева; под ред. и со вступ. ст. Н.А. Головина. Санкт-Петербург : Наука, 2007. 641 с.

62. Биркгоф Дж. Динамические системы. Москва : ОГИЗ, 1999. 480 с.

63. Лисецкий Ю.М. Модели, методы и технологии количественной оценки качества систем: монография. Киев : ЛАТ&К, 2018. 102 с.

64. Рац О.М. Визначення сутності поняття «ефективність функціонування підприємства». *Економічний простір:* зб. наук. праць. Дніпропетровськ : ПДАБА, 2008. Вип. 15. С. 275–285.

65. Глазов О.В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Політологія. Наукові праці.* 2011. Вип. 143, Т. 155. С. 42–46.

66. Ліпкан В.А., Ліпкан О.С., Яковенко О.О. Національна і міжнародна безпека в визначеннях та поняттях. Київ : Текст, 2006. 256 с.

67. Алешенков М.С., Родионов Б.Н. Секьюритология: монография. Москва : МГУЛ, 2008. 104 с.

68. Косолапов Н. Национальная безопасность в меняющемся мире (К дискуссии о содержании понятия). *МЭ И МО*. 1992. № 10. С. 67–75.

69. Возженников А.В. Национальная безопасность: теория, политика. *Стратегия*. Москва : НПО «МОДУЛЬ», 2000. 240 с.

70. Циганов В.В. Національна безпека України : посіб. Київ, 2004. 100 с.

71. The National Security Strategy of the United States of America. Washington, 2006. 54 p.

72. Фукуяма Ф. Конец истории и последний человек. Санкт-Петербург, 2005. 592 с.

73. Huntington S.P. The Clash of Civilizations and the Remakink of World Order. N.Y. : Simon & Shuster, 1996. 368 p.

74. Бодрук О.С. Структури воєнної безпеки: національний та міжнародний аспекти. Київ, 2001. 300 с.

75. Богданович В.Ю., Семенченко А.І., Єгоров Ю.В., Бортник О.О. Теоретико-методологічні засади забезпечення національної безпеки держави у її визначальних сферах: монографія. Київ : Кий, 2007. 370 с.

76. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Аналіз чинників, що впливають на систему забезпечення національної безпеки України в умовах гібридної війни. *Вісник воєнної розвід*ки. 2020. № 60. С. 99–103.

77. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/_98-%D0%B2%D1%80 (дата звернення: 18.04.2021).

78. Про затвердження Положення про Міністерство оборони України: Постанова Кабінету Міністрів України від 26.11.2014 р. № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF (дата звернення: 18.04.2021).

79. Про Збройні сили України: Закон України від 06.12.1991 р. URL: https://zakon.rada.gov.ua/laws/show/1934-12 (дата звернення: 18.04.2021).

80. Про затвердження Положення про Міністерство внутрішніх справ України: Постанова Кабінету Міністрів України від 28.10.2015 р. URL: https://www.kmu.gov.ua/ua/npas/248608057 (дата звернення: 18.04.2021).

81. Про Національну гвардію України: Закон України від 13.03.2014 р. № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18 (дата звернення: 18.04.2021).

82. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28.10.2015 р. № 877. URL:

https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF (дата звернення: 18.04.2021).

83. Про Державну прикордонну службу України: Закон України від 03.04.2003 р. № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15 (дата звернення: 18.04.2021).

84. Про затвердження Положення про Державну міграційну службу України: Постанова Кабінету Міністрів України від 20.09.2014 р. № 360. URL: https://zakon.rada.gov.ua/laws/show/360-2014-%D0%BF (дата звернення: 18.04.2021).

85. Про затвердження Положення про Державну службу України з надзвичайних ситуацій: Постанова Кабінету Міністрів України від 16.12.2015 р. № 1052. URL: https://zakon.rada.gov.ua/laws/show/1052-2015-%D0%BF (дата звернення: 18.04.2021).

86. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 18.04.2021).

87. Про державну охорону органів державної влади України та посадових осіб: Закон України від 04.03.1998 р. № 160/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/160/98-%D0%B2%D1%80 (дата звернення: 18.04.2021).

88. Про державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3473-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення: 18.04.2021).

89. Про державну спеціальну службу транспорту: Закон України від 05.02.2004 р. № 1449-IV URL: https://zakon.rada.gov.ua/laws/show/1449-15 (дата звернення: 18.04.2021).

90. Про Службу зовнішньої розвідки України: Закон України від 01.12.2005 р. № 3160-IV. URL: https://zakon.rada.gov.ua/laws/show/3160-15 (дата звернення: 18.04.2021).

91. Про розвідувальні органи України: Закон України від 22.03.2001 р. № 2331-III. URL: https://zakon.rada.gov.ua/laws/show/ru/2331-14/ed20160728 (дата звернення: 18.04.2021).

92. Резнікова О.О., Цюкало В.Ю., Паливода В.О., Дрьомов С.В., Сьомін С.В. Концептуальні засади розвитку системи забезпечення національної безпеки України: аналіт. доп. Київ : НІСД, 2015. 58 с.

93. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Національна безпека України. Організаційно-правові аспекти. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Державне управління.* 2021. Т. 32 (71), № 4. С. ?–?.

94. Про рішення Ради національної безпеки і оборони України «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 04.03.2016 р. № 92/2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016#Text (дата звернення: 27.05.2021).

95. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/ laws/show/ 392/2020#Text (дата звернення: 28.05.2021).

96. Про національну безпеку України: Закон України, із змінами і доповненнями від 21.06.2018 р. № 2469-VIII (2469-19). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 28.05.2021).

97. Про засади внутрішньої і зовнішньої політики: Закон України від 01.07.2010 р. № 2411-VI. URL: https://zakon.rada.gov.ua/laws/show/ 2411-17#Text (дата звернення: 01.06.2021).

98. Про рішення Ради національної безпеки і оборони України «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24.09.2015 р. № 555/2015. URL: https://zakon. rada.gov.ua/laws/ show/555/2015#Text (дата звернення: 01.06.2021).

99. Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Державну програму розвитку Збройних Сил України на період до 2020 р.»: Указ Президента України від 22.03.2017 р. № 73/2017. URL: https://www.president.gov.ua/ documents/732017-21498 (дата звернення: 02.06.2021).

100. Про рішення Ради національної безпеки і оборони України від 27.09.2014 р. «Про заходи щодо удосконалення державної військово-технічної політики»: Указ Президента України від 27.09.2014 р.

№ 691/2014. URL: https://www.president.gov.ua/documents/6912014-17592 (дата звернення: 02.06.2021).

101. Про рішення Ради національної безпеки і оборони України від 12.09.2014 р. «Про комплекс заходів щодо зміцнення обороноздатності держави та пропозиції до проєкту Закону України «Про Державний бюджет України на 2015 р.»: Указ Президента України від 03.11.2014 р. № 842/2014. URL: https://president.gov.ua/documents/8422014-17959 (дата звернення: 02.06.2021).

102. Про Рішення Ради національної безпеки і оборони України від 02.11.2019 р. «Про Міжвідомчу комісію з питань оборонно-промислового комплексу»: Указ Президента України від 08.11.2019 р. № 831/2019. URL: https://www.president.gov.ua/documents/8312019-30377 (дата звернення: 02.06.2021).

103. Про оборонні закупівлі: Закон України від 17.07.2020 р. № 808-IX. URL: https://zakon.rada.gov.ua/laws/show/808-20#Text (дата звернення: 03.06.2021).

104. Про оборону України: Закон України від 06.12.1991 р. № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 03.06.2021).

105. Про Збройні Сили України: Закон України від 06.12.1991 р. № 1934-XII. URL: https://zakon.rada.gov.ua/laws/show/1934-12#Text (дата звернення: 03.06.2021).

106. Про схвалення Концепції Державної цільової програми реформування та розвитку оборонно-промислового комплексу України на період до 2020 р.: Розпорядження Кабінету Міністрів України від 20.01.2016 р. № 19-р. URL: https://zakon.rada.gov.ua/laws/show/19-2016-%D1%80#Text (дата звернення: 03.06.2021).

107. Про схвалення Стратегії розвитку оборонно-промислового комплексу України на період до 2028 р.: Розпорядження Кабінету Міністрів України від 20.06.2018 р. № 442-р. URL: https://zakon.rada.gov.ua/laws/show/442-2018-%D1%80#Text (дата звернення: 03.06.2021).

108. Політанський В.С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету. Право*. 2017. Вип. 42. С. 16–22.

109. Сопілко І.М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. *Юридичний вісник*. 2017. № 3 (44). С. 61–64.

110. Kuzmynchuk N., Kutsenko T., Strygul L., Terovanesova O., Klepikova S. Intellectual instrumental analysis in economic security management of the enterprises for countering raiding. F*inancial and credit activity: problems of theory and practice*. 2021. Vol. 2. N 37 (2021). P. 231–243. DOI: https://doi.org/10.18371/fcaptp.v2i37.230242.

111. Reta M., Druhova E., Lisnichuk O. Methods for diagnosing the effectiveness of the enterprise's financial strategy in the strategy controlling system. *Baltic Journal of Economic Studies*. 2018. Vol. 4 (3). P. 235–244.

112. Грохольський В.Л. Визначення сутності державного управління та його відмежування від суміжних понять. *Інтернаука. Юридичні науки.* 2017. № 1 (1). С. 28–32.

113. Аванесова Н.Е., Мордовцев О.С., Сергієнко Ю.І. Теоретико-методичні засади ідентифікації та взаємозв'язку впливу дестабілізуючих факторів на економічну безпеку промислового підприємства. *Бізнес Інформ*. 2020. № 9. С. 20–28. URL: https://doi.org/10.32983/2222-4459-2020-9-20-28 (дата звернення: 05.01.2021).

114. Ткачук Т.Ю. Інформаційна безпека: сучасні підходи до визначення категорії. *Актуальні питання публічного та приватного права.* 2017. № 2 (16). С. 45–54.

115. Золотар О.О. Досвід правового забезпечення інформаційної безпеки в країнах східного партнерства ЄС (Молдова, Грузія). *LEX PORTUS*. 2017. № 3 (5). С. 70–80.

116. Ткачук Т.Ю. Складники інформаційної безпеки: аналіз критеріїв. *Visegrad journal on human rights*. 2017. № 4. С. 153–158.

117. Геворкян А.Ю. Другова О.С., Клепікова С.В. Фактори, що впливають на визначення інвестиційної привабливості та вартості бізнесу. *Вісник Національного технічного університету «Харківський політехнічний інститут»*. 2018. № 19 (1295). С. 131–134.

118. Lelechenko A.P., Diegtiar O.A., Lebedinska O.Y., Derun T.M., Berdanova O.V. Mechanisms of inter-state communications for solving

sustainable development problems. Asia life sciences Supplement 29 (2). *The Asian International Journal of Life Sciences*. 2020. N 1–9. P. 1–14.

119. Diegtiar O.A., Orlova N.S., Kozureva O.V., Shapovalova A.M., Prykazka S.I. Financial capacity of territorial communities: european experience and ukrainian case. *Фінансово-кредитна діяльність: проблеми теорії та практики*: зб. наук. праць. 2019. Vol. 4, N 31. P. 516–526. URL: http://fkd.org.ua/issue/view/11616 (дата звернення: 25.09.2020).

120. Nepomnyashchyy O.M., Marusheva O.A., Prav Yu.H., Medvedchuk O.V., Lahunova I.A. Certain aspects of the system of public administration of universities: World practices and the Ukrainian dimension. *Journal of the National Academy of Legal Sciences of Ukraine*. 2021. N 28(1). P. 99–105.

121. Nepomnyashchyy O., Shevchenko I., Marusheva I., Medvedchuk O., Lahunova I. Marketing Communications Management in the Public Administration System. I*nternational Journal of Criminology and Sociology*. 2020. N 9. P. 2882–2890.

122. Биркович Т.І. Механізми публічного управління у сфері цифрових трансформацій. Державне управління: удосконалення та розвиток. URL: http://www.dy.nayka.com.ua/pdf/9_2019/4.pdf (дата звернення: 25.02.2021).

123. Довгань О.Д. Інформаційна безпека: стан, проблеми, тенденції. *Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: філософсько-правові та прикладні аспекти:* матеріали круглого столу (Вінниця, 12 травня 2017 р.). Київ : Видавничий дім «АртЕк», 2017. С. 31–39.

124. Заярний О.А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект: монографія. Київ : Видавничий дім «Гельветика», 2017. 700 с.

125. Швець С.В., Швець У.С. Основи системного аналізу: навчальний посібник. Суми : Сумський державний університет, 2017. 126 с.

126. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Київ : Видавничий дім «Гельветика», 2017. 168 с.

127. Дзьобань О.П., Мануйлов Є.М. Інформаційна безпека в контексті інформаційної культури. *Інформація і право.* 2017. № 1 (20). С. 74–81.

128. Лисецький Ю.М. Інформаційні технології в управлінні та обробці інформації: монографія. Київ : ЛАТ&К, 2018. 268 с.

129. Лисецкий Ю.М. Инновационные информационные технологии. Опыт интеграции и внедрения: монография. Киев: ЛАТ&К, 2020. 276 с.

130. Лисецький Ю.М. Концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки. *Вісник військової розвідки*. 2021. № 69. С. ?–?.

131. Шейн Х. Кибервойн@. Пятый театр военных действий. Москва : Альпина нон-фикшн, 2016. 392 с.

132. Богданов А.М., Мохор В.В. О кибербезопасности в широком смысле. *Information Technology and Security*. 2013. № 1 (3). С. 51–58.

133. Сейранова С.Н. Киберугрозы как серьезный вызов национальной безопасности КНР. *Актуальные проблемы современных международных отношений.* 2017. № 2. С. 131–134.

134. Лисецький Ю.М. Комплексная безопасность корпоративных информационных систем. *Управляющие системы и машины*. 2019. № 1. С. 145–148.

135. Лисецкий Ю.М., Бобров С.И. Новые угрозы информационной безопасности или оружие массового заражения. *Математичні машини і системи*. 2018. № 1. С. 41–50.

136. Лисецький Ю.М. Концептуальні основи системи національної кібербезпеки. *Вісник військової розвідки*. 2021. № 65. С. 145–148.

137. Блауберг И.В. Проблема целостности и системный подход. Москва: Эдиториал УРСС, 1997. 448 с.

138. Лисецький Ю.М., Бобров С.І. Деякі аспекти побудови системи національної кібербезпеки. *Математичні машини і системи*. 2021. № 2. С. 15–22.

139. Шрейдер Ю.А., Шаров А.А. Системы и модели. Москва : Радио и связь, 1982. 150 с.

140. Берталанфи Л. Общая теория систем – обзор проблем и результатов. *Системные исследования*. Москва: Наука, 1969. С. 34–35.

141. Дацюк А., Садовський В., Полтораков О., Марутян Р. Аналіз державної політики у сфері національної безпеки і оборони України. URL: https://rpr.org.ua/wp-content/uploads/2018/02/Analiz-polityky-NB-pravl-final.pdf (дата звернення: 27.06.2021)

142. Новікова О.Ф., Сидорчук О.Г., Панькова О.В. та ін. Стан та перспективи соціальної безпеки в Україні : експертні оцінки : монографія / Львівський регіональний інститут державного управління НАДУ; НАН України, Інститут економіки промисловості. Київ ; Львів: ЛРІДУ НАДУ, 2018. 184 с.

143. Мокляк С.П., Лисецький Ю.М. Загрози національний безпеці України в умовах гібридної війни. *Вісник військової розвідки*. 2021. № 67. С. ?–?.

144. Запорожець Т.В. Національні інтереси та безпека України в контексті геополітики. *Управління:* зб. наук. праць. 2011. № 3. С. 22–29.

145. Ковалюк Р.Т. Національні інтереси України в новій геополітичній ситуації. URL: http://www.kymu.edu.ua/vmv/v/06/ kovaluk.htm (дата звернення: 24.10.2021).

146. Воронянський О.В. «Національні інтереси» як категорія політичної науки. *Вісник Національної юридичної академії України ім. Ярослава Мудрого. Філософія, філософія права, політологія, соціологія:* зб. наук. пр. / Національна юридична академія України ім. Ярослава Мудрого. 2011. Вип. 10. С. 131–136.

147. Глембоцький Д. Осмислення поняття «національний інтерес» для подальшої реалізації в розвитку країни. URL: http://visnyk.academy.gov.ua/ wp-content/uploads/2013/11/2012-3-5.pdf (дата звернення: 14.10.2021).

148. Портер М. Международная конкуренция. Конкурентные преимущества стран. Москва : Альпина Паблишер, 2020. 948 с.

149. Побережець О.В., Макаревич Г.В. Забезпечення конкурентоспроможності національної економіки України в умовах глобалізації. URL: http://www.economy.nayka.com.ua/?op=1&z=5669 (дата звернення: 20.05.2021).

150. Карлова В.В. Духовні цінності в структурі національної свідомості: українські реалії. URL: http://academy.gov.ua/ej/ej11/txts/10kvvsur.pdf (дата звернення: 20.05.2021).

151. Сорока С. Аналіз механізмів взаємодії Верховної Ради України та Кабінету Міністрів України в контексті сучасного конституційного розвитку держави. URL: http://www.dbuapa.dp.ua/zbirnik/2011-02(6)/11ssvkrd.pdf (дата звернення: 20.05.2021).

152. Сіцинський Н.А. Концептуальні принципи зовнішньополітичної діяльності України та її нормативно-правове наповнення. URL: http://www.investplan.com.ua/pdf/5_2017/21.pdf (дата звернення: 20.05.2021).

153. Магда Є.М. Гібридна війна: сутність і структура феномену. *Міжнародні відносини. Політичні науки*. 2014. № 4. С. 14–22.

154. Мальський М.З. Транскордонна безпека: політико-правовий, соціально-економічний, гуманітарний та екологічний вимір. Зб. матеріалів Міжнар. наук.-практ. конф. (Львів, 21 квітня 2017 р.) / уклад.: М.З. Мальський, О.С. Кучик, Р.В. Вовк. Львів : Факультет міжнародних відносин, 2017. 96 с.

155. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Пріоритети протидії загрозам національній безпеці країни в умовах гібридної війни. *I Международная научно-практическая конференция «TOPICAL ISSUES OF MODERN SCIENCE, SOCIETY AND EDUCATION»* (Харьков, Украина, 8–10 августа 2021 г.). С. 795–800.

156. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show /2163-19#Text (дата звернення: 26.07.2021).

157. Словник української мови: в 11 т. / АН Української РСР, Ін-т мовознавства ім. О.О. Потебні; редкол.: І. К. Білодід (голова) та ін. Т. 8: Природа-Ряхтливий / за ред. В.О. Винника та ін. Київ : Наукова думка, 1977. 927 с.

158. Словарь русского языка / сост. С.И. Ожегов. 15-е изд. Москва : Русский язык, 1984. 816 с.

159. Словарь русского языка: в 4 т. / АН СССР, Ин-т русского языка. Москва : Русский язык, 1981. Т. 1. 698 с.; Москва : Русский язык, 1981. Т. 2. 736 с.;

Москва : Русский язык, 1981. Т. 3. 752 с.; Москва : Русский язык, 1981. Т. 4. 794 с.

160. Геополитика, международная и национальная безопасность: словарь. Москва : Пробел, 1999. 374 с.

161. Безопасность России. Правовые, социально-экономические и научно-технические аспекты: словарь терминов и определений. 2-е изд., доп. Москва : МГФ «Знание», 1999. 361 с.

162. Костров А.В., Ткачова А.А. Защита населения и территорий: семантический анализ, синтез и формализация ключевых терминов. *Проблемы безопасности.* 2000. № 6. С. 24–47.

163. Акимов В.А., Новиков В.Д., Радаев Н.Н. Природные и техногенные ситуации: опасности, угрозы, риски. Москва : Деловой экспресс, 2001. 344 с.

164. Манилов В.А. Безопасность в эпоху партнерства: монография. Москва : ТЕРРА, 1999. 368 с.

165. Мунтіян В.І. Економічна безпека України. Київ : КВІЦ, 1999. 462 с.

166. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи: монографія. Київ : ІПНБ, НА СБУ, 2004. 472 с.

167. Тертичка В.В. Державна політика: аналіз та здійснення в Україні: монографія. Київ : Вид-во С. Павличка «Основи», 2002. 750 с.

168. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Механізм протидії загрозам національній безпеці в умовах гібридної війни. *RESULTS OF MODERN SCIENTIFIC RESEARCH AND DEVELOPMEN*: VI Междунар. науч.-практ. конф. (Мадрид, Испания, 22–24 августа 2021 г.). С. 401–407.

169. Ситник Г.П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади): підручник. Київ : НАДУ, 2012. 544 с.

170. Мескон М., Альберт М., Хедоури Ф. Основы менеджмента. Москва : Дело, 1997. 704 с.

171. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення. Київ : Текст, 2003. 180 с.

172. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Критерії оцінки функціонування механізму державного управління при протидії гібридним загрозам національній безпеці. *Нові імпульси розвитку публічного управління та електронного урядування: питання наукових досліджень*: Міжнар. наук. конф. (Лодзь, Республіка Польща, 8–9 жовтня 2021 р.). С. ?–?.

173. Efficiency Definition & Meaning|Dictionary.com. URL: https://www.dictionary.com/browse/efficiency (date of access: 02.09.2021).

174. Журавський де Сас Т.Б. Питання ефективності механізмів державного управління. URL: http://www.investplan.com.ua/pdf/13_2013/29.pdf (дата звернення: 02.09.2021).

175. Социальный эффект. Что такое? Зачем и как считать? URL: http://zubr-consulting.kz/node/574 (дата звернення: 02.09.2021).

176. Снитюк В.Е. Эволюционные технологии принятия решений в условиях неопределенности: монография. Киев : МП «Леся», 2015. 347 с.

177. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Розвиток і вдосконалення механізму протидії загрозам національній безпеці в умовах гібридної війни. *EUROPEAN SCIENTIFIC DISCUSSIONS*: XI Междунар. науч.-практ. конф. (Рим, Италия, 12–14 сентября 2021 г.). С. ?–?.

178. Про внутрішнє і зовнішнє становище України в 2018 р.: Аналітична доповідь до щорічного послання Президента України до Верховної Ради України / Національний інститут стратегічних досліджень. *Стратегічні пріоритети*. 2019. № 1 (49). 1289 с.

179. Капитонова Ю.В., Летичевский А.А. Парадигмы и идеи академика В.М. Глушкова. Киев : Наукова думка, 2003. 456 с.

Наукове видання

Павленко Дмитро Григорович, Семенюк Юрій Володимирович,
Лисецький Юрій Михайлович

ВИКЛИКИ ГІБРИДНОЇ ВІЙНИ ТА НАЦІОНАЛЬНА БЕЗПЕКА

Монографія

За загальною редакцією Ю. М. Лисецького

Літературний редактор, коректор – А. В. Галушкіна
Комп'ютерна верстка, макетування – А. О. Брем, О. О. Старовойтенко
Дизайн обкладинки – О. О. Старовойтенко
Технічний редактор – В. Ю. Бихун

Підп. до друку ??.??.2021. Формат 64x90/16.
Папір офсетн. Друк офсетн.
Ум. друк. арк. 17,92. Наклад 1000 прим. Зам. № 27/11

Видавництво «ЛАТ & К»
01601, м. Київ, вул. Леонтовича, 9.
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції
ДК № 181 від 15.09.2000 р.
тел./факс: +38 044 235 00 09
моб.: +38 050 310 22 04
email: lk@ukr.net