ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.Н. КАРАЗІНА
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ІНСТИТУТ ДЕРЖАВНОГО УПРАВЛІННЯ»

Завідувач кафедри права, національної
безпеки та європейської інтеграції
д.ю.н., професор
_____ Л.Ю. Величко

ІНТЕЛЕКТУАЛЬНІ РЕСУРСИ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦБЕЗПЕКИ УКРАЇНИ

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»
281 Публічне управління та адміністрування
28 Публічне управління та адміністрування

Виконав слухач 2-ого курсу
групи ППГЗ-2-23 В.Ф. Карачун

Керівник
д.ю.н., професор Л.Ю. Величко

Харків – 2024

ЗМІСТ

ВСТУП

Актуальність теми. В умовах зростання глобальних і регіональних викликів та загроз національній безпеці України, посилення гібридних впливів та інформаційної агресії з боку Російської Федерації ключового значення набуває ефективність функціонування системи державного управління у безпековій сфері. Від спроможності державних інститутів своєчасно ідентифікувати ризики, адекватно на них реагувати та забезпечувати стійкість держави і суспільства перед загрозами залежить не лише добробут, а часто і саме виживання української нації. Особливо яскраво це продемонстрували події 2014 року, коли неготовність системи національної безпеки протистояти «гібридній» агресії призвела до втрати контролю над частиною території та численних людських жертв. Натомість досвід останніх 8 років засвідчив, що надійна національна безпека є результатом не стільки кількісних параметрів сектору безпеки і оборони (чисельність особового складу, озброєнь і військової техніки тощо), скільки його інтелектуального потенціалу – здатності генерувати асиметричні рішення, передбачати розвиток безпекової ситуації, ефективно протидіяти як традиційним, так і новітнім загрозам.

За оцінками експертів, на сьогодні понад 80% безпекових функцій держави мають інформаційно-аналітичний та управлінський характер і вимагають відповідного інтелектуального забезпечення. Водночас, існуюча система формування та використання інтелектуальних ресурсів у секторі безпеки і оборони України все ще не повною мірою відповідає критеріям інноваційності, гнучкості та адаптивності. Про це свідчать результати комплексного огляду сектору безпеки і оборони (2019 р.), згідно з якими частка працівників з вищою освітою у силових структурах становить лише 46%, а питома вага інноваційної продукції – менше 2%.

Крім того, за даними соціологічних опитувань, майже 60% громадян України не довіряють державним органам у сфері безпеки і оборони, що суттєво

знижує їх легітимність та ускладнює реалізацію державної безпекової політики. Відтак, проблема удосконалення механізмів формування, розподілу та ефективного використання інтелектуальних ресурсів у системі державного управління національною безпекою набуває особливої актуальності та потребує ґрунтовного наукового дослідження.

Проблематика інтелектуальних ресурсів системи державного управління національною безпекою перебуває у фокусі уваги багатьох вітчизняних дослідників. Значний внесок у розробку теоретичних та прикладних аспектів цієї проблеми зробили такі вчені, як В. Абрамов, С. Борисович, О. Власюк, В. Горбулін, А. Дацюк, О. Кондратенко, В. Мандрагеля, Р. Марутян, І. Руснак, Г. Ситник, М. Шевченко та ін. Водночас аналіз публікацій за останні 5-6 років дозволяє виокремити кілька провідних підходів до розуміння сутності та специфіки інтелектуальних ресурсів у безпековій сфері.

Так, представники першого підходу (С. Борисович, О. Кондратенко, І. Дунаєв, Н. Колісніченко) розглядають інтелектуальні ресурси переважно крізь призму людського капіталу – сукупності знань, навичок, кваліфікацій та мотивацій працівників сектору безпеки і оборони. На їхню думку, саме високоосвічений, професійно підготовлений та патріотично налаштований персонал є головним чинником ефективності функціонування системи забезпечення національної безпеки. Натомість прихильники другого підходу (В. Дзюндзюк, Ю. Орел, В., Котковський, І. Дегтярьова, Р. Марутян, М. Шевченко, М. Майстро) акцентують увагу на інформаційно-аналітичній складовій інтелектуальних ресурсів, підкреслюючи вирішальне значення технологій збору, обробки та використання інформації для прийняття адекватних безпекових рішень в умовах невизначеності та «інформаційного хаосу».

Своєю чергою, В. Горбулін та А. Дацюк наголошують на необхідності системного та синергетичного підходу до формування інтелектуального потенціалу сектору безпеки і оборони, що передбачає узгоджений розвиток усіх його складових – людського капіталу, інформаційно-аналітичного забезпечення,

організаційної культури та мотиваційних механізмів. Схожої думки дотримується й І. Руснак, додаючи до цього переліку також інституційну пам’ять та мережеві комунікації між суб’єктами безпекової політики.

Попри певні розбіжності у трактуванні змісту та структури інтелектуальних ресурсів, більшість науковців сходяться на думці щодо їх вирішального значення для забезпечення стійкості та адаптивності системи державного управління національною безпекою в умовах сучасних викликів. Зокрема, О. Власюк підкреслює, що саме завдяки розвиненому інтелектуальному потенціалу сектор безпеки і оборони здатний ефективно протидіяти гібридним загрозам, забезпечувати аналітичний супровід прийняття державно-управлінських рішень, формувати позитивний імідж силових структур у суспільстві. Г. Ситник акцентує увагу на ролі інтелектуальних ресурсів у розробці інноваційних безпекових стратегій та доктрин, обґрунтуванні оптимальних шляхів реформування сектору безпеки і оборони відповідно до євроатлантичних стандартів.

Метою роботи є розробка пропозицій щодо вдосконалення механізмів формування та використання інтелектуальних ресурсів у системі державного управління національною безпекою України. Поставлена мета зумовила виконання низки *завдань:*

– уточнити сутність, структуру та особливості інтелектуальних ресурсів у системі державного управління національною безпекою;

– проаналізувати іноземний досвід використання інтелектуальних ресурсів у системах забезпечення національної безпеки;

– оцінити кадровий потенціал та інтелектуальний капітал системи державного управління національною безпекою України;

– виявити ключові проблеми та виклики у сфері використання інтелектуальних ресурсів;

– визначити стратегічні напрями розвитку інтелектуального потенціалу;

– розробити пропозиції щодо вдосконалення мережевої взаємодії та

інституційних механізмів використання інтелектуальних ресурсів у сфері національної безпеки.

Об'єктом дослідження є система державного управління національною безпекою України як середовище формування та використання інтелектуальних ресурсів.

Предметом дослідження є інструменти нарощування й ефективної реалізації інтелектуального потенціалу системи державного управління національною безпекою України.

Методи дослідження. Для досягнення мети та виконання завдань дослідження використано комплекс загальнонаукових та спеціальних методів:

– *методологічний аналіз* для визначення сутності та структури інтелектуальних ресурсів (підрозділ 1.1);

– *нормативно-правовий та порівняльно-правовий методи* при дослідженні іноземного досвіду та законодавчої бази (підрозділ 1.3);

– *структурно-функціональний аналіз* для оцінки кадрового потенціалу (підрозділ 2.1);

– *методи статистичного аналізу* при виявленні проблем та викликів (підрозділ 2.2);

– *проблемно-орієнтований підхід* для розробки напрямів удосконалення механізмів (розділ 3);

– *методи синтезу та дедукції* для формування стратегічних напрямів розвитку (підрозділ 3.1);

– *табличні методи* для наочного представлення результатів;

– *мережевий підхід* при розробці пропозицій щодо вдосконалення взаємодії (підрозділ 3.2).

Таким чином, методологія дослідження поєднує фундаментальні засади теорії публічного управління з сучасними міждисциплінарними підходами у сфері безпекових студій, а також орієнтована на вироблення практичних рекомендацій для вдосконалення взаємодії правоохоронних органів і сил оборони в умовах воєнного стану.

Практичне значення отриманих результатів полягає в тому, що **в**исновки та рекомендації дослідження можуть бути використані:

– *у науково-дослідній сфері* – для подальшого наукового дослідження в означеній сфері;

– *у правотворчій діяльності* – з метою удосконалення чинних і розроблення нових нормативно-правових актів з питань забезпечення нацбезпеки України;

– *у правозастосовній діяльності* для удосконалення процесів формування та використання інтелектуальних ресурсів у системі забезпечення національної безпеки України на різних рівнях:

1) *на законодавчому рівні* – Верховною Радою України для модернізації нормативно-правової бази у сфері забезпечення національної безпеки з урахуванням потреб нарощування інтелектуального потенціалу сектору безпеки і оборони;

2) *на рівні центральних органів виконавчої влади* – Кабінетом Міністрів України, Міністерством оборони України, Міністерством внутрішніх справ України та іншими органами для обґрунтування та реалізації цільових програм і проєктів розвитку інтелектуальних ресурсів відповідних складових сектору безпеки і оборони;

3) *на рівні державних органів спеціального призначення* – Службою безпеки України, Службою зовнішньої розвідки України, Управлінням державної охорони України для розробки та впровадження відомчих систем управління інтелектуальним капіталом, механізмів стимулювання інноваційної активності працівників;

– *у навчальному процесі* – для викладання та вивчення навчальних дисциплін «Глобалізація та політика національної безпеки», «Реагування та протидія гібридним загрозам», при написанні підручників, монографій, науково-практичних посібників, розробці методичних рекомендацій, а також для удосконалення освітніх програм підготовки фахівців з публічного управління у безпековій сфері, розвитку наукових досліджень проблем інтелектуального

забезпечення національної безпеки.

Інформаційну базу дослідження становитимуть: Конституція та закони України, укази Президента України, постанови Кабінету Міністрів України, відомчі нормативно-правові акти, що регулюють питання функціонування та розвитку системи забезпечення національної безпеки України; Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегічний оборонний бюлетень України, Концепція розвитку сектору безпеки і оборони України та інші документи стратегічного планування у безпековій сфері; дані офіційної статистики щодо кількісних та якісних параметрів кадрового потенціалу сектору безпеки і оборони України, показників ефективності його функціонування; аналітичні звіти та доповіді міжнародних організацій (ООН, ОБСЄ, НАТО), державних органів (РНБО, Міноборони, МТОТ та ін.), неурядових дослідницьких установ та експертних центрів (НІСД, Центр Разумкова, Український інститут майбутнього тощо); результати національних та міжнародних соціологічних досліджень громадської думки щодо оцінки ефективності функціонування системи забезпечення національної безпеки України та довіри до силових структур; монографічна література, наукові статті, матеріали дисертаційних досліджень вітчизняних та зарубіжних авторів за тематикою інтелектуального та кадрового забезпечення національної безпеки; публікації в друкованих та електронних засобах масової інформації, матеріали аналітичних інтернет-ресурсів, присвячені проблемам розвитку інтелектуального потенціалу сектору безпеки і оборони України.

Апробація результатів роботи. Магістерська кваліфікаційна робота самостійно виконана шляхом наукового дослідження та узагальнення. Усі результати отримані за допомогою самостійного опрацювання та аналізу і синтезу наданих даних.

Отримані в результаті проведеної роботи теоретичні висновки і практичні результати обговорювалися на засіданні кафедри права, національної безпеки та європейської інтеграції Навчально-наукового інституту «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна та

можуть бути використані в науково-дослідній роботі кафедри за темою: *«Організаційно-правовий механізм модернізації публічного управління відповідно до стандартів «Good Governance».*

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ РЕСУРСІВ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ УКРАЇНИ

1.1 Сутність та структура інтелектуальних ресурсів системи державного управління національною безпекою

Розвиток інтелектуального потенціалу системи державного управління національною безпекою є одним із ключових пріоритетів реформування сектору безпеки і оборони України відповідно до сучасних викликів та стандартів євроатлантичної спільноти. В умовах глобалізації безпекового середовища, появи нових загроз гібридного характеру, зростання ролі інформаційних та когнітивних факторів у протиборстві саме спроможність державних інститутів продукувати ефективні асиметричні рішення, швидко адаптуватися до мінливого контексту, забезпечувати дієву протидію деструктивним впливам визначає загальний рівень національної стійкості та обороноздатності країни.

Інтелектуальні ресурси є тим фундаментом, на якому вибудовується вся архітектура системи національної безпеки, її здатність надійно захищати суверенітет, територіальну цілісність та конституційний лад держави, життєво важливі інтереси особи, суспільства і держави від зовнішніх і внутрішніх загроз. Як зазначає С. Бєлай, «на відміну від традиційних ресурсів сектору безпеки і оборони (особового складу, озброєння та військової техніки тощо), які є важливими, але не визначальними, інтелектуальні ресурси у вигляді знань, навичок, мотивацій, організаційних спроможностей виступають системоутворюючими чинниками, що значною мірою детермінують якісні параметри всієї системи національної безпеки» [9, с. 24].

Водночас аналіз наукових публікацій засвідчує неоднозначність та

багатоаспектність розуміння сутності інтелектуальних ресурсів як економічної та управлінської категорії. У широкому сенсі під інтелектуальними ресурсами розуміють «сукупність явних і неявних знань та інформації, які можуть бути конвертовані у вартість через комерціалізацію та впровадження» [30, с. 132]. У більш вузькому трактуванні до інтелектуальних ресурсів зараховують «нематеріальні активи організації, що включають компетенції працівників, організаційні процеси та процедури, бази даних, програмне забезпечення, патенти, товарні знаки тощо» [26, с. 78].

У контексті державного управління національною безпекою найбільш повним і обґрунтованим видається визначення В. Мандрагелі, який під інтелектуальними ресурсами розуміє «систему знань, інформації, технологій, а також відповідних людських, організаційних і технічних носіїв, які забезпечують розвідувальну, інформаційно-аналітичну, контррозвідувальну, кібербезпекову та інші види інтелектуальномісткої діяльності в інтересах забезпечення національної безпеки і оборони держави» [29, с. 112]. Важливо підкреслити, що у структурі інтелектуальних ресурсів системи державного управління нацбезпекою поєднуються три взаємопов’язані компоненти:

1) Людський капітал як сукупність знань, навичок, умінь, здібностей та мотивацій працівників сектору безпеки і оборони, що використовуються ними для вирішення службово-бойових завдань. Саме від професійно-інтелектуальних якостей особового складу, його аналітичних і креативних спроможностей значною мірою залежать результати інформаційно-аналітичної, оперативно-розшукової, контррозвідувальної та інших видів спеціальної діяльності у безпековій сфері.

2) Організаційний (структурний) капітал як нематеріальні активи системи забезпечення національної безпеки, що сприяють реалізації людського капіталу та включають інформаційні системи й мережі, бази даних, програмне забезпечення, організаційні процеси і процедури, управлінські технології, репутаційні активи тощо. Саме завдяки їм забезпечується необхідна якість та ефективність внутрішньоорганізаційних комунікацій, управління знаннями та

прийняття рішень у секторі безпеки і оборони.

3) Соціальний капітал як потенціал взаємодії та співробітництва органів сектору безпеки і оборони з іншими державними і недержавними інституціями та громадянським суспільством на основі спільних інтересів і цінностей, взаємної довіри і готовності до колективних дій в інтересах зміцнення національної безпеки. Розвинені соціальні зв'язки та партнерські відносини дозволяють ефективно мобілізувати наявні інтелектуальні ресурси суспільства для комплексної протидії загрозам.

Таблиця 1.1 – Структура інтелектуальних ресурсів системи державного управління національною безпекою

Структурні компоненти	**Зміст**	**Індикатори**
Людський капітал	Знання, навички, досвід, мотивація працівників	Рівень освіти, професійна підготовка, інноваційна активність
Організаційний капітал	Інформаційні системи, бази даних, процеси, технології	Якість управлінських рішень, ефективність бізнес-процесів
Соціальний капітал	Мережа соціальних зв'язків, довіра, готовність до співпраці	Рівень довіри до органів безпеки, залученість громадськості

Слід зазначити, що в умовах розвитку інформаційного суспільства та економіки знань роль інтелектуальних ресурсів у забезпеченні національної безпеки невпинно зростає. Як справедливо підкреслює О. Власюк, «якщо головними викликами індустріальної епохи були переважно воєнні загрози, то в постіндустріальну епоху на перший план виходять інформаційні, кібернетичні, когнітивні, репутаційні впливи метою яких є не стільки фізичне знищення супротивника, скільки дестабілізація та хаотизація його державно-управлінських механізмів, дезорієнтація населення та підрив довіри до влади» [10, с. 18]. За таких умов перемога у безпековому протиборстві дедалі більше залежить не від кількості танків і гармат, а від інтелекту нації, її здатності швидше за супротивника здобувати й обробляти критично важливу інформацію, продукувати ефективні асиметричні стратегії, гнучко реагувати на

гібридні загрози.

Разом з тим, системна оцінка реального стану інтелектуальних ресурсів сектору безпеки і оборони України виявляє низку проблем, що негативно позначаються на спроможності держави адекватно реагувати на актуальні виклики національній безпеці. Зокрема, за даними кадрового аудиту Міноборони України (2019 р.), в органах управління відомства лише 54% службовців мають вищу освіту, а частка працівників з науковими ступенями не перевищує 0,8%. При нормативній потребі у фахівцях з вищою освітою понад 70% реальна їх наявність становить лише 44%, що свідчить про недостатній рівень професійної підготовки особового складу [1, с. 23].

Ще гіршою є ситуація із впровадженням сучасних інформаційно-аналітичних технологій у процеси забезпечення національної безпеки. Зокрема, більшість вітчизняних силових відомств досі не мають повноцінних систем накопичення та обробки даних, центрів ситуаційного аналізу, програмних комплексів моделювання та прогнозування розвитку безпекової ситуації.Обмін інформацією між різними суб’єктами сектору безпеки і оборони відбувається безсистемно та епізодично, в ручному режимі, що суттєво знижує оперативність прийняття та якість управлінських рішень в умовах кризових ситуацій [20; 19, с. 147].

Таблиця 1.2 – Проблемні аспекти формування та використання інтелектуальних ресурсів системи державного управління національною безпекою України

Проблемні аспекти	**Зміст**	**Негативні наслідки**
Низька якість людського капіталу	Недостатній рівень професійної підготовки та інноваційної активності працівників	Низька ефективність виконання завдань, схильність до прийняття шаблонних рішень
Технологічна відсталість	Брак сучасних інформаційно-аналітичних систем, баз даних, спеціального програмного забезпечення	Запізніле реагування на загрози, необґрунтованість управлінських рішень

Продовження таблиці 1.2.

Проблемні аспекти	**Зміст**	**Негативні наслідки**
Інституційна фрагментація	Відомча відокремленість суб'єктів сектору безпеки, низький рівень довіри та співпраці між ними	Неузгодженість і суперечливість дій, неефективне використання наявних ресурсів

*Джерело: розробка автора.

Причини такого стану справ криються у відсутності в Україні цілісної та науково обґрунтованої державної політики щодо розвитку інтелектуального потенціалу системи забезпечення національної безпеки. Як зазначають В. Горбулін та А. Качинський, «…попри визнання на політико-декларативному рівні важливості зміцнення інтелектуальної складової сектору безпеки і оборони, на практиці державні програми та проєкти у цій сфері реалізуються безсистемно та непослідовно, без належного врахування реальних потреб і викликів» [16, с. 37]. Бракує ефективних механізмів та дієвих стимулів нарощування інтелектуального капіталу силових структур, їх інноваційного розвитку та технологічної модернізації.

Відтак на сучасному етапі державотворення постає нагальна необхідність концептуального переосмислення ролі та місця інтелектуальних ресурсів у системі забезпечення національної безпеки, формування та реалізації цілеспрямованої державної стратегії розвитку інтелектуального потенціалу сектору безпеки і оборони України. Така стратегія має передбачати комплекс правових, інституційних, організаційних, фінансово-економічних та інформаційних механізмів й інструментів активізації інтелектуальної діяльності у безпековій сфері – від створення необхідних умов для залучення та закріплення висококваліфікованих фахівців до впровадження сучасних систем управління знаннями та винагороди інновацій.

При цьому вкрай важливо забезпечити системність та узгодженість розвитку всіх компонентів інтелектуальних ресурсів – людського, організаційного та соціального капіталу, їх органічне включення в єдиний

управлінський цикл. Адже, як показує досвід провідних країн світу, саме синергія висококомпетентного персоналу, розвиненої інформаційно-аналітичної інфраструктури та тісних партнерських зв'язків у форматі «держава-наука-бізнес-громадськість» здатна забезпечити якісний прорив у нарощуванні інтелектуального потенціалу системи національної безпеки [41, с. 215].

Не менш важливим є врахування специфічних особливостей інтелектуальної діяльності у безпековій сфері, які відрізняють її від інших галузей державного управління. Йдеться, зокрема, про:

– превалювання закритих (таємних) форм і методів роботи, що ускладнює зовнішню оцінку та контроль ефективності;

– високий ступінь невизначеності та ризикованості більшості аналітичних процедур і прогностичних суджень;

– необхідність одночасного й узгодженого застосування різнопрофільних знань і компетентностей – управлінських, правничих, військових, технічних, соціогуманітарних тощо;

– підвищені вимоги щодо політико-ідеологічної благонадійності та морально-психологічних якостей інтелектуальних працівників тощо.

Усе це диктує потребу в розробці та впровадженні спеціальних управлінських підходів, процедур і технологій, адаптованих до предметної специфіки інтелектуальної праці у секторі безпеки і оборони. Зокрема, вкрай важливо забезпечити ретельний професійно-психологічний відбір та спеціальну поліфункціональну підготовку аналітиків і експертів, налагодити дієві канали циркуляції знань та обміну досвідом між різними відомствами, впровадити ефективні методики верифікації інформації в умовах «гібридних» загроз, мінімізувати ризики витоку чутливих даних тощо.

Протягом останнього століття погляди на сутність та роль інтелектуальних ресурсів у системі державного управління національною безпекою зазнали суттєвої еволюції під впливом геополітичних, технологічних та соціокультурних трансформацій. У першій половині XX ст. в умовах домінування силових чинників та реалістичної парадигми міжнародних відносин інтелектуальний

потенціал держав розглядався переважно крізь призму їх воєнно-промислових можливостей та здатності мобілізувати науково-технічні здобутки для забезпечення перемоги у збройному протиборстві. Так, у Британській імперії ключову роль відігравали аналітичні центри при Форин-офісі та Адміралтействі, які забезпечували стратегічне планування і координацію дій колоніальної адміністрації, прогнозування розвитку ситуації в різних регіонах світу [82, с. 78]. Подібним чином в Німецькій імперії значна увага приділялася розвитку військових наукових установ та конструкторських бюро, які працювали над створенням новітніх систем озброєнь [75, с. 115].

У період між світовими війнами акценти поступово зміщуються в бік врахування невійськових чинників забезпечення національної могутності – економічних, дипломатичних, інформаційно-пропагандистських. Зокрема, в США під впливом ідей В. Вільсона та Ф. Рузвельта формується концепція «розумної сили» (smart power), яка передбачає комплексне використання всіх ресурсів держави для посилення її глобального впливу та лідерства [69, с. 241]. В її межах особлива роль відводилася аналітично-прогностичному забезпеченню зовнішньополітичних рішень та інформаційно-психологічному супроводу дій США на міжнародній арені. Подібна тенденція простежувалася і в інших провідних державах того часу, що знайшло відображення у створенні спеціалізованих аналітичних структур на кшталт Королівського інституту міжнародних відносин (Chatham House) у Великій Британії чи Ради зовнішніх зносин (Council on Foreign Relations) у США.

Після Другої світової війни в умовах ідеологічного протистояння двох наддержав і гонки озброєнь інтелектуальні ресурси почали розглядатися як ключовий фактор забезпечення стратегічної переваги в біполярному світі. У СРСР було розгорнуто масштабну мережу науково-дослідних інститутів і конструкторських бюро оборонного профілю, які працювали на потреби військово-промислового комплексу. Паралельно розвивалася система закритих аналітичних центрів у структурі ЦК КПРС, КДБ, Міноборони та МЗС, що забезпечували інформаційно-аналітичну підтримку вищого партійного

керівництва з широкого спектру проблем – від оцінки воєнно-політичної обстановки до прогнозування соціально-економічного і науково-технічного розвитку [27, с. 93].

Своєю чергою, у США в цей період активно розбудовувалася розгалужена мережа «фабрик думок» (think tanks), тісно пов'язаних з військово-промисловими корпораціями та спецслужбами. Такі структури, як RAND Corporation, Гудзонівський інститут, Інститут Брукінгса та інші, стали потужними центрами військово-стратегічних досліджень, розробки інноваційних концепцій і технологій у сфері безпеки [58, с. 174]. Саме в їх надрах було розроблено теорію ядерного стримування, концепцію «м'якої сили», доктрину інформаційної війни та низку інших парадигмальних ідей, що заклали підґрунтя американського лідерства.

У 1970-1980-х рр. з розвитком інформаційного суспільства та процесів глобалізації відбувається концептуальний зсув у розумінні інтелектуальних ресурсів безпеки в бік їх «демілітаризації» та розширення предметного поля безпекових досліджень. Дедалі більше уваги починає приділятися не стільки воєнним, скільки невійськовим аспектам забезпечення національної стійкості – економічній, технологічній, енергетичній, екологічній, інформаційній безпеці. Поширення набувають концепції «м'якої» та «розумної» сили, які акцентують на ролі знання, інновацій, культурно-ціннісної привабливості як ключових чинників глобального впливу держав [78, с. 312; 87]. Все це зумовлює зміну пріоритетів у розвитку інтелектуальної інфраструктури безпеки, орієнтацію на міждисциплінарні дослідження на стику різних галузей науки та більш тісну взаємодію державних, приватних і громадських інституцій.

З кінця XX ст. і дотепер домінуючим трендом стає становлення постіндустріальної парадигми безпеки, в рамках якої інтелектуальні ресурси розглядаються як самостійний і найбільш затребуваний компонент сукупного стратегічного потенціалу держави і суспільства. Їх головним змістом стає продукування проривних ідей та рішень щодо протидії комплексним загрозам в умовах глобальної турбулентності, мережевих конфліктів і гібридних війн [14, с.

428; 67; 87]. Важливого значення набуває розвиток горизонтальних форм інтелектуальної співпраці та краудсорсингу у сфері безпеки, залучення потенціалу широких експертно-аналітичних мереж, використання технологій штучного інтелекту та великих даних для моделювання безпекової ситуації.

Особливої актуальності ці тенденції набувають для тих держав, які постали перед викликами посткомуністичних і постколоніальних трансформацій, необхідністю переосмислення своєї ідентичності та вибудовування власних моделей безпеки в умовах обмежених ресурсів. Зокрема, в Україні потреба формування ефективної системи інтелектуального забезпечення національної безпеки особливо загострилася на тлі анексії Криму та розв'язаної Росією «гібридної» агресії. Це зумовлює актуальність вивчення передового світового досвіду розбудови інтелектуальної інфраструктури безпеки при одночасному врахуванні національної специфіки, розробки на цій основі власних інноваційних рішень.

Таблиця 1.3 – Еволюція підходів до розуміння інтелектуальних ресурсів державного управління національною безпекою у світі

Період	**Домінуюча парадигма**	**Зміст і роль інтелектуальних ресурсів**	**Ключові країни та інституції**
І пол. XX ст.	Реалістична (силова)	Забезпечення воєнно-промислового потенціалу, стратегічне планування	Велика Британія, Німеччина (аналітичні центри при силових відомствах)
1920-1940-ві рр.	Ідеалістична (економіко-дипломатична)	Аналітичне забезпечення зовнішньої політики, інформаційний вплив	США (Рада зовнішніх зносин), Велика Британія (Chatham House)
1950-1980-ті рр.	Неореалістична (ядерно-стратегічна)	Військово-стратегічні дослідження, розробка інноваційних концепцій і технологій безпеки	США (RAND Corp., Гудзонівський ін-т), СРСР (ВПК, закриті аналіт. центри)
з кін. XX ст.	Постіндустріальна (комплексна)	Продукування проривних рішень щодо протидії гібридним загрозам, розвиток мережевої аналітики та краудсорсингу	США, ЄС, Китай та ін. (мережі незалежних центрів, експертно-аналіт. спільноти)

*Джерело: розробка автора.

Підсумовуючи викладене, можна констатувати, що інтелектуальні ресурси є стратегічним активом системи державного управління національною безпекою, від якості та ефективності використання якого значною мірою залежить спроможність держави своєчасно ідентифікувати, попереджати та нейтралізувати існуючі й потенційні загрози в умовах високодинамічного безпекового середовища. Структурними компонентами інтелектуальних ресурсів є людський, організаційний та соціальний капітал, органічне поєднання яких генерує додану вартість у вигляді обґрунтованих управлінських рішень, асиметричних стратегій протидії, інноваційних організаційних форм і технологій спеціальної діяльності.

Водночас рівень розвитку інтелектуальних ресурсів вітчизняного сектору безпеки і оборони все ще не повною мірою відповідає вимогам часу, що актуалізує завдання розробки та реалізації цілеспрямованої державної стратегії нарощування інтелектуального потенціалу силових структур. Ключовими напрямами такої стратегії мають стати модернізація кадрової політики, технологічне переоснащення інформаційно-аналітичної інфраструктури, розбудова багаторівневої системи партнерської взаємодії суб'єктів сектору безпеки і оборони з науково-експертним середовищем і громадянським суспільством. Лише на цій основі можна досягти якісного прориву у зміцненні інтелектуального фундаменту національної безпеки України.

1.2 Особливості формування та використання інтелектуальних ресурсів у системі забезпечення національної безпеки

Формування та ефективне використання інтелектуальних ресурсів є однією з ключових передумов забезпечення національної безпеки держави в умовах глобальних трансформацій та зростання «гібридних» загроз. Як слушно зауважує В. Горбулін, «в епоху турбулентності та невизначеності, коли

традиційні схеми та методи забезпечення безпеки виявляються недостатньо ефективними, саме інтелект нації, її здатність продукувати нові знання, ідеї та рішення стає вирішальним фактором стійкості та конкурентоспроможності держави на міжнародній арені» [14, с. 12]. Дійсно, в умовах тотальної інформатизації та розмивання кордонів між воєнною та цивільною сферами, зовнішніми та внутрішніми аспектами безпеки інтелектуальний потенціал суспільства перетворюється на ключовий ресурс протидії широкому спектру загроз – від військової агресії та тероризму до кіберзлочинності, екстремізму й організованої злочинності.

Водночас аналіз світового досвіду засвідчує, що ефективність формування та використання інтелектуальних ресурсів у системі забезпечення національної безпеки визначається низкою специфічних чинників та особливостей, які відрізняють безпекову сферу від інших галузей державного управління. По-перше, це надзвичайно високий ступінь закритості та конфіденційності інтелектуальної діяльності, зумовлений потребою збереження державної таємниці, протидії розвідувально-підривним зусиллям супротивника, захисту чутливої інформації [68, с. 64]. На відміну від цивільних галузей (освіти, науки, медицини тощо), де пріоритетом є генерування відкритого знання, вільна циркуляція ідей та даних, у секторі безпеки домінує культура секретності, обмеження доступу та компартменталізації інформації. Це суттєво звужує можливості для широкої наукової дискусії, експертного обміну та громадського контролю, ускладнює залучення зовнішнього інтелектуального ресурсу.

По-друге, формування кадрового потенціалу системи забезпечення національної безпеки характеризується підвищеними вимогами щодо світоглядно-ціннісних орієнтацій, морально-вольових якостей та лояльності співробітників. На відміну від більшості цивільних сфер, де визначальними критеріями добору є насамперед професійні компетентності та досвід, у силових структурах не менш важливе значення має політико-ідеологічна благонадійність, відданість національним інтересам, готовність до самопожертви [53, с. 128; 65]. Особливо яскраво ця тенденція простежується в роботі спецслужб, де ретельна

перевірка та постійний моніторинг лояльності співробітників є обов'язковою умовою їх допуску до виконання завдань. Все це накладає суттєвий відбиток на систему відбору, підготовки та мотивації кадрів сектору безпеки, вимагає застосування специфічних методик і процедур роботи з персоналом.

По-третє, зміст та характер інтелектуальної діяльності у сфері національної безпеки вирізняється високим ступенем міждисциплінарності, необхідністю органічного поєднання методологій і підходів різних галузей знань – політичних, воєнних, технічних, правничих, соціогуманітарних тощо. Забезпечення ефективного захисту національних інтересів від широкого спектру загроз вимагає не просто вузькопрофільних спеціалістів, а фахівців з розвиненим стратегічним мисленням, здатних системно аналізувати комплексні проблеми на стику різних наукових дисциплін [49, с. 218]. При цьому тактико-технологічний рівень завдань (розробка систем озброєнь, організація захисту інформації, контррозвідувальна робота тощо) має органічно доповнюватися політико-стратегічним осмисленням викликів національній безпеці, виробленням цілісного бачення шляхів реагування на них з урахуванням усіх вимірів державної могутності. Все це диктує потребу в розвитку специфічних компетентностей та налагодженні тісної міжгалузевої співпраці між різнопрофільними структурами сектору безпеки.

По-четверте, на відміну від більшості цивільних сфер суспільного життя, де пріоритетом інтелектуальної діяльності є продукування нового знання у вигляді теорій, концепцій, технологічних рішень, для системи забезпечення національної безпеки визначальне значення має розвідувальна інформація – цінні відомості про наміри, плани та потенціал реальних і потенційних супротивників, отримані з використанням специфічних методів і джерел [51, с. 92]. Саме на здобуванні розвідувальної інформації, її перевірці, аналізі та інтерпретації зосереджена левова частка інтелектуальних зусиль спецслужб, органів воєнної розвідки, зовнішньополітичного відомства. При цьому, на відміну від наукового знання, якість та цінність розвідувальної інформації визначається не стільки її достовірністю та обґрунтованістю, скільки

актуальністю, повнотою та придатністю для прийняття стратегічних рішень в умовах невизначеності й ризику.

По-п’яте, формування та розвиток інтелектуального потенціалу системи забезпечення національної безпеки об’єктивно вимагає тісної та скоординованої співпраці державних, наукових, освітніх та бізнес-структур. Як свідчить досвід провідних країн світу, саме ефективна взаємодія влади, академічної спільноти, індустрії та громадянського суспільства дозволяє сформувати потужну «екосистему» генерування та впровадження безпекових інновацій, забезпечити трансфер передових знань і технологій у практику державного управління. Зокрема, у США, Великій Британії, Ізраїлі давно та успішно функціонують різноманітні механізми державно-приватного партнерства у сфері досліджень і розробок для потреб оборони та безпеки, створення інноваційної інфраструктури, впровадження моделі «потрійної спіралі» (наука – бізнес – держава). Натомість у більшості пострадянських країн, у т.ч. в Україні, й досі домінують патерналістські підходи, які розглядають інтелектуальне забезпечення безпеки як виключну прерогативу держави.

У цьому контексті цікавим є досвід організації аналітичної та прогнозної роботи в колишньому СРСР, який демонструє як переваги, так і недоліки надмірно централізованої та ідеологізованої моделі інформаційно-аналітичної підтримки прийняття державно-управлінських рішень з питань національної безпеки. З одного боку, в Радянському Союзі була створена розгалужена мережа науково-дослідних установ та аналітичних підрозділів, підпорядкованих вищим органам компартійно-державного керівництва (ЦК КПРС, КДБ, міністерствам оборони, закордонних справ тощо). Ці структури забезпечували партійну еліту не лише оперативною інформацією про події в країні та світі, але й глибокими аналітичними розробками стратегічного характеру, довгостроковими прогнозами розвитку міжнародної обстановки, науково-технічного прогресу, соціальних та ідеологічних процесів [27, с. 32]. Багато в чому саме завдяки високому рівню аналітичного забезпечення вдалося реалізувати масштабні проекти розвитку ракетно-ядерного потенціалу, освоєння космосу, забезпечити

військово-стратегічний паритет із США.

Водночас монополізація державою інтелектуальної сфери, примат ідеології над об'єктивним науковим пошуком, культивування «кабінетної» аналітики в умовах закритості та цензури інформаційних потоків мали й чимало негативних наслідків. Як зазначають О. Власюк та С. Кононенко, «аналітичне забезпечення державної політики в СРСР було переважно ситуативним, кон'юнктурним і апологетичним стосовно рішень вищого політичного керівництва, базувалося на «підганянні» фактів та аргументів під наперед визначені ідеологічні постулати та схеми» [11, с. 41]. Система підготовки аналітичних матеріалів була вкрай забюрократизованою, не стимулювала ініціативу та критичне мислення виконавців, які змушені були орієнтуватися не стільки на об'єктивну істину, скільки на політичну доцільність та ієрархічне становище замовника. Як результат – катастрофічне відставання СРСР у розвитку інформаційних технологій, неадекватне сприйняття керівництвом глибинних причин системної кризи радянської моделі наприкінці 1980-х років.

Ще одним промовистим історичним прикладом є розвиток аналітичної думки в Німеччині 1930-х років у контексті становлення нацистської диктатури. Прихід до влади А. Гітлера та його оточення супроводжувався не лише фізичним знищенням інакодумців, але й тотальною «нацифікацією» інтелектуальної сфери, підпорядкуванням науки расистським та імперським постулатам нацистської ідеології. Особливо виразно ця тенденція проявилася в діяльності аналітичних центрів, покликаних забезпечувати інтелектуальну підтримку агресивних зовнішньополітичних амбіцій Третього Рейху. Зокрема, під егідою зовнішньополітичного відомства (Аусвертігес Амт) було створено низку псевдонаукових інституцій на кшталт Німецького інституту зовнішньополітичних досліджень, Інформаційного відділу з міжнародних відносин тощо [75, с. 127]. Попри позірну академічність, діяльність цих установ зводилася переважно до пропагандистського обґрунтування нацистської концепції «життєвого простору», расової вищості німецького народу, легітимізації загарбницьких планів гітлерівського керівництва.

Подібним чином і в мілітаристській Японії напередодні та під час Другої світової війни була розгорнута ціла мережа дослідницьких інституцій, спрямована на культивування ідей паназійського націонал-шовінізму, обґрунтування історичної місії Японії як лідера «східноазійської сфери спільного процвітання» [88, с. 364]. Під егідою армії та флоту активно розроблялися геополітичні концепції на кшталт «японського життєвого простору», «японської світової революції» тощо. Показово, що більшість японських аналітиків того часу щиро вірили у швидку та неминучу перемогу країни «вранішнього сонця» над США та іншими західними демократіями, недооцінюючи потенціал супротивника та ресурсні обмеження власної держави.

Іншу модель інтелектуального забезпечення безпеки представляли країни англо-саксонського світу, в яких протягом ХХ ст. склалася розгалужена та гнучка мережа аналітичних центрів («фабрик думок»), тісно пов’язаних з військово-промисловим комплексом, розвідувальним співтовариством та системою прийняття політичних рішень. Попри фінансову й організаційну залежність від держави, ці інституції все ж зберігали відносну автономію, можливість продукування альтернативних поглядів і концепцій, широкі контакти з академічним середовищем [86, с. 73; 63]. Типовим прикладом такої моделі є корпорація RAND, утворена в 1948 р. на замовлення Військово-повітряних сил США. За кілька десятиліть свого існування RAND перетворилася на визнаний у світі центр військово-стратегічних досліджень, кузню інноваційних концепцій і технологій у сфері безпеки (ядерне стримування, теорія ігор, системний аналіз, штучний інтелект тощо) [84, с. 191]. При цьому значна частина напрацювань корпорації мала відкритий характер, активно обговорювалася фаховою спільнотою та політичним істеблішментом США.

Загалом, досвід провідних країн світу переконливо доводить, що ефективність формування та використання інтелектуальних ресурсів у системі забезпечення національної безпеки визначається органічним поєднанням цілеспрямованих зусиль держави щодо нарощування кадрового та науково-технологічного потенціалу сектору безпеки з розвитком незалежних аналітичних

центрів, належних умов для вільної творчості та критичного мислення інтелектуалів. Як справедливо зазначає Г. Ситник, «лише за умов демократичного цивільного контролю, відкритості й залучення громадськості до обговорення проблем безпеки і оборони стає можливим уникнути загроз монополізації та деградації безпекової думки, забезпечити її адекватність і суспільну легітимність» [50, с. 85]. Водночас надмірна плюралізація експертного середовища, утвердження культури «піару» та «хайпу» в безпековій аналітиці, коли будь-яка екзотична концепція може набути розголосу й вплинути на прийняття рішень, також є небезпечною крайністю, здатною призвести до дезорієнтації та фрагментації інтелектуального простору.

З іншого боку, в умовах глобалізації та розмивання кордонів між внутрішньою та зовнішньою безпекою інтелектуальне забезпечення національної безпеки і стійкості дедалі більше залежить від здатності держави та суспільства налагоджувати продуктивний міжнародний діалог, гнучко реагувати на транснаціональні виклики, формувати спільне бачення перспектив розвитку безпекового середовища. На сучасному етапі світового розвитку жодна країна, навіть наддержава, не здатна самотужки протидіяти таким загрозам, як міжнародний тероризм, поширення зброї масового ураження, кіберзлочинність, нелегальна міграція, епідемії тощо [13, с. 248]. Відтак формування глобальних мереж безпекової експертизи, співпраця аналітичних центрів різних держав, гармонізація методологій оцінювання й прогнозування розвитку безпекової ситуації стають імперативом часу.

Особливої актуальності ці тенденції набувають для країн пострадянського простору, у т.ч. України, які все ще перебувають у процесі трансформації власних безпекових систем і форматів взаємодії з зовнішнім світом. Попри наявність потужних академічних шкіл та інституцій у галузі міжнародних відносин, воєнної стратегії, розвідувальної аналітики тощо, їх нинішній інтелектуальний продукт часто позначений рудиментами ментальності «холодної війни», схильністю до стереотипного сприйняття Заходу й Сходу, недооцінкою глобальних трендів безпекового розвитку. Як зазначає відомий

український безпекознавець В. Горбулін, «криза аналітичного мислення, зацикленість на ілюзіях і фантомах радянської епохи, брак стратегічного бачення та проактивності в умовах наростання гібридних загроз є однією з ключових вад вітчизняної системи аналітичного забезпечення національної безпеки» [45, с. 17].

Водночас в Україні поступово формується нова генерація безпекових експертів, які поєднують глибоке розуміння національної специфіки з інтегрованістю до глобальних мереж безпекової аналітики, володінням сучасною методологією стратегічного аналізу та прогнозування. Активно розвивається мережа незалежних аналітичних центрів, які спеціалізуються на комплексному вивченні проблем національної безпеки та оборони, здійснюють альтернативні урядовим оцінки та розробки (Центр Разумкова, Український центр економічних і політичних досліджень ім. О. Разумкова, Інститут світової політики, Центр досліджень армії, конверсії та роззброєння, Інститут євроатлантичного співробітництва та ін.) [56, с. 22].

Набуває поширення практика співпраці державних безпекових інституцій з академічним і експертним середовищем у форматі спільних дослідницьких проектів, науково-комунікативних заходів, підготовки аналітичних доповідей тощо.

Разом з тим, попри наявність окремих позитивних зрушень, формування цілісної та збалансованої системи інтелектуального забезпечення національної безпеки України все ще перебуває на початковій стадії та стикається з низкою викликів.

Зокрема, йдеться про збереження успадкованих з радянських часів елементів закритості та несприйняття альтернативних думок у роботі державних аналітичних структур, недостатній рівень інтегрованості відомчої та незалежної експертизи, брак усталених каналів трансляції напрацювань аналітичної спільноти на рівень вироблення політико-управлінських рішень, низький рівень аналітичної культури більшості представників політичної еліти, схильність до ухвалення волюнтаристських рішень в умовах гібридної агресії [54, с. 138].

Таблиця 1.4 – Порівняльна характеристика моделей інтелектуального забезпечення національної безпеки окремих держав у XX – на поч. XXI ст.

Країна / Період	**Модель взаємодії держави та інтелектуального середовища у сфері безпеки**	**Провідні «мозкові центри»**	**Переваги**	**Недоліки**
США (з сер. XX ст.)	Поліцентрична модель, плюралізм державних, приватних і незалежних аналітичних центрів	RAND Corporation, Brookings Institution, Heritage Foundation	Конкуренція ідей, залучення позаурядової експертизи, зв'язок з академічною наукою	Фрагментація аналітичного простору, непрозорість лобістських впливів
СРСР (1930-1980-ті рр.)	Моноцентрична модель з домінуванням партійно-державних дослідницьких установ, закритий характер аналітики	Інститути системи АН СРСР, аналітичні підрозділи ЦК КПРС, КДБ та ін.	Цілісність, системність і ресурсна забезпеченість державної аналітики	Ідеологізація та політизація експертизи, відірваність від потреб суспільства
Німеччина (1933-1945 рр.)	Моноцентрична модель з домінуванням державних аналітичних центрів, підпорядкованих нацистській ідеології	Німецький інститут зовнішньополітичних досліджень, Інформаційний відділ МЗС	-	Ідеологізація та догматизація аналітики, обґрунтування агресивної політики режиму
Японія (1930-1940-ві рр.)	Моноцентрична мілітаризована модель з домінуванням аналітичних структур армії та флоту	Інститут тотальної війни, Інститут політичних і економічних досліджень	-	Ідеологізація та мілітаризація аналітичного супроводу експансіоністської політики
Велика Британія (з поч. XX ст.)	Поліцентрична модель з провідною роллю незалежних аналітичних центрів і тісними зв'язками держави та академічної науки	Королівський інститут міжнародних відносин (Chatham House), Міжнародний інститут стратегічних досліджень	Залучення позаурядової експертизи, зв'язок з академічною наукою	Елітарність та відірваність частини аналітичних центрів від потреб держави та суспільства

Продовження таблиці 1.4.

Країна / Період	**Модель взаємодії держави та інтелектуального середовища у сфері безпеки**	**Провідні «мозкові центри»**	**Переваги**	**Недоліки**
Україна (з 1991 р.)	Трансформаційна модель переходу від державно-відомчої до поліцентричної системи аналітичного забезпечення безпеки	Національний інститут стратегічних досліджень, Центр Разумкова, Центр досліджень армії, конверсії та роззброєння	Поступовий розвиток незалежної аналітики, посилення співпраці держави та експертної спільноти	Фрагментація та різновекторність аналітичного простору, недостатній зв’язок аналітики та політики

*Джерело: розробка автора.

Таким чином, інтелектуальні ресурси є ключовим компонентом стратегічного потенціалу системи забезпечення національної безпеки в умовах глобальних трансформацій та «гібридних» викликів сучасності.

Їх ефективне формування та використання потребує органічного поєднання цілеспрямованих зусиль держави щодо нарощування кадрового й інформаційно-аналітичного потенціалу сектору безпеки з розвитком мережі незалежних «мозкових центрів», забезпеченням умов для вільної творчості та критичного мислення експертів.

Світовий досвід переконливо свідчить, що продуктивність безпекової аналітики значною мірою визначається рівнем демократичності політичної системи, представленістю в інтелектуальному полі різних ідейних течій і методологічних підходів, здатністю влади до сприйняття альтернативних поглядів і рекомендацій.

Натомість надмірна централізація та політизація експертного середовища, обслуговування аналітикою волюнтаристських рішень правлячої еліти неминуче призводить до догматизації стратегічного мислення, втрати зв’язку з реальністю, прорахунків та невиправданих ризиків у сфері безпеки.

1.3 Сучасний іноземний досвід використання інтелектуальних ресурсів у системі державного управління національною безпекою для цілей посилення національної безпеки

Останнє десятиліття XXI ст. ознаменувалося кардинальними трансформаціями глобального безпекового ландшафту, обумовленими посиленням геополітичної конкуренції, технологічними зрушеннями, наростанням гібридних загроз та викликів сталому розвитку людства. В умовах «плинної модерності» (за влучним визначенням З. Баумана) та тотальної невизначеності традиційні підходи до забезпечення національної безпеки, засновані на нарощуванні військової потуги та ресурсному домінуванні, дедалі більше поступаються місцем стратегіям «розумної сили» (smart power). Їх суть полягає в ефективному поєднанні «жорстких» і «м'яких» інструментів впливу на безпекове середовище, досягненні цілей на основі комплексного застосування політико-дипломатичних, інформаційно-психологічних, соціально-економічних та інших невійськових механізмів [78, с. 178].

Ключовим компонентом «розумної сили» в арсеналі провідних держав світу стають саме інтелектуальні ресурси – сукупність наукових знань, аналітичних компетентностей, технологічних розробок та креативних рішень у сфері національної безпеки. Як відзначають О. Власюк та С. Кононенко, «в постіндустріальну епоху, коли центр протиборства зміщується з традиційного геополітичного та воєнного вимірів у бік інформаційно-психологічного та когнітивного впливу, саме якість людського капіталу, його інтелектуальне оснащення стає важливішою за кількісні параметри озброєнь і військ» [12, с. 92]. Недаремно в стратегічних документах США, Великої Британії, Франції, Німеччини та інших розвинених країн останніми роками дедалі більше уваги приділяється зміцненню кадрового потенціалу сектору безпеки, нарощуванню спроможностей аналітичних структур, розвитку перспективних досліджень і технологічних інновацій.

Так, у Стратегії національної безпеки США (2017 р.) серед ключових пріоритетів визначено «збереження миру силою», що передбачає посилення інтелектуальної переваги Америки через модернізацію збройних сил, розвиток ракетно-космічних та кібернетичних можливостей, залучення проривних технологій, вдосконалення розвідувально-аналітичного забезпечення [76]. Підкреслюється, що в епоху комплексних викликів перевага у воєнній силі, якою традиційно пишалися США, вже не гарантує автоматичного глобального домінування, а повинна доповнюватись економічним, інформаційним, інноваційним лідерством. Відтак державна політика у сфері національної безпеки та оборони спрямовується на розвиток інтелектуального капіталу в найширшому сенсі – від поглиблення технологічної співпраці з недержавним експертним середовищем до підвищення якості військової освіти та аналітики.

Знаковим прикладом практичної реалізації цих настанов стала реформа системи воєнної розвідки США, розпочата у 2011-2012 рр. за ініціативи міністра оборони Л. Панетти. Її ключовим завданням стало подолання фрагментованості та розпорошеності розвідувального співтовариства, приведення його у відповідність з вимогами мережевоцентричних війн та мультидоменних операцій майбутнього [5, с. 37]. Зокрема, зусилля реформаторів були спрямовані на подолання міжвідомчих бар’єрів, поглиблення інтеграції розвідувальних структур видів збройних сил, Агентства національної безпеки, ЦРУ, Національного управління військово-космічної розвідки, підвищення автоматизації процесу обміну даними. Окрема увага приділялась розширенню аналітичних спроможностей та впровадженню технологій роботи з великими даними, передових методів прогнозування розвитку безпекової ситуації.

У результаті навколо Розвідувального управління Міноборони США (РУМО) було побудовано інтегровану архітектуру органів, пов’язаних між собою високошвидкісними каналами зв’язку, уніфікованими базами даних, спільними алгоритмами аналізу розвідувальної інформації. Це суттєво підвищило оперативність та ефективність розвідувальної підтримки всього спектру воєнних місій – від протидії тероризму та контрповстанській боротьби

до забезпечення безпеки морських та повітряно-космічних рубежів. Завдяки зусиллям із розвитку автоматизованих систем збору та обробки даних лише протягом 2014-2018 рр. об'єм інформації, накопиченої в розвідувальних базах міністерства оборони, зріс у понад 4 рази і сягнув 17 петабайт [61, с. 116].

Іншим напрямом зміцнення інтелектуального потенціалу оборонної сфери США стало запровадження нових підходів до взаємодії військових структур з експертним середовищем – як урядовим, так і незалежним. Показовими в цьому контексті є два масштабні проекти. Перший передбачав вихід Агентства передових оборонних дослідницьких проектів (DARPA) за межі «традиційної» оборонної науки та різке розширення взаємодії із цивільними дослідницькими установами й університетами. Якщо раніше більшість проектів DARPA концентрувалась довкола проривних технологій у царині озброєнь та військової техніки, то з середини 2010-х років основний акцент змістився в бік фундаментальних розробок в галузі штучного інтелекту, робототехніки, нано- та біотехнологій, нових матеріалів і джерел енергії, які мають подвійне застосування [71, с. 49].

Другий проект стосувався створення при міністерстві оборони США Ради оборонних інновацій (Defense Innovation Board) як постійно діючого консультативного органу з широким представництвом «капітанів» Кремнієвої долини та інноваційних хабів. Основним завданням цієї структури стало залучення експертного потенціалу лідерів високотехнологічних індустрій для прогнозування напрямів військово-технологічного розвитку, своєчасного виявлення перспективних розробок подвійного призначення, вирішення проблем кібербезпеки [74, с. 113]. Переконливим свідченням високої ефективності Ради стало впровадження на її рекомендацію більш як 60 інноваційних систем та рішень у практику оборонного планування і закупівель США лише протягом 2017-2021 рр.

Не менш цілеспрямовано на зміцнення інтелектуального забезпечення національної безпеки працюють у цей період і європейські країни. Показовим прикладом у цьому відношенні є Велика Британія, яка навіть в умовах

скорочення загальних видатків на оборону у повоєнний період істотно наростила витрати на військові НДДКР, аналітичне забезпечення, освіту і підготовку кадрів для збройних сил і спецслужб. Так, лише протягом 2014-2019 рр. бюджет Центру урядового зв'язку (GCHQ) – розвідувальної структури, відповідальної за захист комунікацій та кібербезпеку, – зріс у понад півтора рази і склав майже 3,2 млрд. ф. ст. [76, с. 178]. Паралельно відбувалось системне оновлення аналітичних підрозділів ключових міністерств і відомств, запроваджувались нові формати ротації та підвищення кваліфікації управлінських кадрів, здійснювались масштабні закупівлі інноваційних ІТ-рішень.

Разом з цим Лондон послідовно курсує на поглиблення міжнародної кооперації у сфері безпекових досліджень та експертизи. Зокрема, поряд із традиційними двосторонніми форматами співробітництва з США та іншими союзниками по НАТО у 2010-х роках активно розвивається взаємодія з інституціями ЄС – Європейським оборонним агентством, Європейською службою зовнішньої діяльності, профільними дослідницькими консорціумами в рамках програми «Горизонт 2020». Це дозволяє британській стороні суттєво розширити доступ до передових розробок і прогнозів у безпековій сфері, брати участь у реалізації проривних проектів, зберігати провідні позиції на ринку оборонних інновацій навіть в умовах Брекзиту.

Дещо іншу модель розвитку інтелектуального потенціалу сектору безпеки демонструє в аналізований період Франція. На відміну від США та Британії з їх вираженою орієнтацією на комерціалізацію та аутсорсинг безпекових досліджень, французи зберігають домінуючу роль державних структур у цій царині. Як влучно зауважує О. Шаповалова, «у Франції історично склалася специфічна політико-адміністративна культура, заснована на картезіанській логіці, культі раціональності та технократичних підходах у державному управлінні... Це проявляється, зокрема, у тісному зрощенні державно-управлінської, військової та наукової еліт, високому рівні інкорпорованості «мозкових центрів» у систему формування оборонно-безпекової політики».

Ілюстрацією цієї тенденції є структура та діяльність провідного

французького аналітичного центру у сфері міжнародної та безпекової політики – Французького інституту міжнародних відносин (IFRI). Попри свій формально незалежний статус, він тісно афілійований з Міністерством оборони, МЗС та президентською адміністрацією, а переважна більшість його аналітичних матеріалів готується на замовлення та в інтересах державних відомств. Водночас IFRI зберігає доволі високий рівень експертної автономії, має розвинену мережу зарубіжних представництв і партнерів, активно працює в багатосторонніх форматах, що дозволяє йому органічно поєднувати функції внутрішнього консультанта та провідника французького впливу за кордоном [72, с. 39].

Загалом для Франції характерне домінування відносно великих державних або напівдержавних аналітичних центрів, чия діяльність спрямована на обґрунтування та реалізацію загальнонаціональної стратегії у сфері безпеки і оборони. Прикладами таких структур є Інститут стратегічних досліджень Військової школи (IRSEM), Центр аналізу, прогнозування та стратегії (CAPS) МЗС, Інститут досліджень національної оборони (IHEDN), Міжнародний інститут стратегічних досліджень (IRIS). На відміну від англо-саксонських країн, Франція не надто заохочує діяльність незалежних, приватних аналітичних центрів у безпековій сфері, розглядаючи це як прерогативу держави. Основна ставка робиться на акумуляцію кращих інтелектуальних ресурсів у провідних університетах, «великих школах», дослідницьких інституціях під егідою уряду.

Німеччина в аналізований період демонструє певну двоїстість у підходах до розвитку інтелектуального потенціалу національної безпеки. З одного боку, ФРН традиційно спирається на потужну академічну науку, яка виступає головним генератором безпекових досліджень і аналітичних розробок. Провідну роль у цій системі відіграють відомі науково-дослідні інститути: Інститут світової економіки (IfW), Німецький інститут економічних досліджень (DIW), Федеральний інститут досліджень безпеки (BIGS), Німецький інститут міжнародної політики та безпеки (SWP), а також низка університетських центрів [58, с. 221]. Вони забезпечують фундаментальне осмислення трансформації безпекового середовища, виходячи з німецьких національних

інтересів, економічних і геополітичних пріоритетів. При цьому фінансування, тематика та результати їх діяльності меншою мірою залежать від прямого урядового втручання порівняно з французькою моделлю.

З іншого боку, протягом останнього десятиліття в Німеччині помітно активізувались процеси «імпорту» англо-саксонських моделей експертно-аналітичного забезпечення політики безпеки. Йдеться, зокрема, про створення мережі спеціалізованих недержавних «мозкових центрів», діяльність яких спрямована на обґрунтування інтересів Берліна в контексті трансатлантичних відносин, участі в євроінтеграційних процесах та реагуванні на глобальні виклики. Прикладами таких think tanks є Німецький фонд Маршалла (GMF), Європейська рада з міжнародних відносин (ECFR), Центр прикладних політичних досліджень (CAP), Фонд науки і політики (SWP) та ін. [81]. На відміну від академічних інституцій, вони більше орієнтовані на поточні потреби політикуму та бізнесу, ширше використовують публічні платформи та лобістські інструменти. Проте, як справедливо зауважує М. Белінська, якісний вплив цих структур на формування безпекової політики ФРН все ще лишається досить обмеженим і ситуативним. До прикладу, жоден з німецьких аналітичних центрів не долучився до розробки ключових доктринальних документів у сфері безпеки і оборони на кшталт «Білої книги 2016», оновленої редакції «Концепції Бундесверу» тощо [8, с. 54]. Це свідчить про збереження традиційної для Німеччини моделі державно-центричного стратегування, в якій головна роль відводиться внутрішньовідомчій експертизі та міжміністерській координації, а не зовнішньому інтелектуальному забезпеченню.

Вельми повчальним для України є досвід Ізраїлю, який в умовах перманентної терористичної загрози зумів побудувати одну з найбільш ефективних у світі систем інтелектуального забезпечення національної безпеки. Її ключовими елементами стали:

1) розвинена мережа спеціалізованих аналітичних центрів як у структурі основних відомств (Служби зовнішньої розвідки «Моссад», Військової розвідки АМАН, контррозвідки ШАБАК, Генштабу Армії оборони Ізраїлю), так

і в провідних університетах та наукових установах (Тель-Авівський університет, Університет ім. Бар-Ілана, Міждисциплінарний центр у Герцлії та ін.) [25, с. 76];

2) тісне переплетіння діяльності цих центрів з системою прийняття рішень через інституціоналізовані канали міжвідомчої взаємодії, регулярні закриті брифінги за участі керівництва країни, а також практику призначення відомих експертів та аналітиків на ключові урядові посади;

3) залучення через спеціальні грантові та стипендіальні програми талановитих випускників провідних зарубіжних ВНЗ, стажування ізраїльських фахівців у США та Європі, що дозволяє підтримувати високий рівень інтелектуальної підживлення безпекової системи;

4) розгалужена система військово-технічної розвідки та моніторингу чутливих технологій, в рамках якої здійснюється цілеспрямований відбір перспективних ноу-хау, закупівля патентів, трансфер розробок подвійного призначення.

Завдяки поєднанню цих компонентів маленька країна з вкрай обмеженими природними ресурсами спромоглась забезпечити інноваційне лідерство в таких сферах, як космічні розвідувально-ударні системи, засоби радіоелектронної боротьби, високоточні боєприпаси, кібернетичні розробки, технології штучного інтелекту на полі бою. Переконливим свідченням ефективності інтелектуального потенціалу Ізраїлю стали успіхи в протидії ракетним обстрілам з боку «Хамас» та «Хезболли», створенні комплексу протиповітряної оборони «Залізний купол», здійсненні точкових операцій з ліквідації лідерів терористичних угруповань [73, с. 88]. Можна стверджувати, що в умовах асиметричних загроз саме якість розвідувально-аналітичного забезпечення, технологічна перевага та інноваційні рішення дозволяють Тель-Авіву надійно гарантувати безпеку своїх громадян.

Цікавим прикладом розвитку інтелектуальних спроможностей у безпековій сфері є і Сінгапур – невелика острівна країна, якій притаманна висока залежність від зовнішнього середовища, вразливість перед викликами регіональної нестабільності, міжнародного тероризму, піратства тощо. Протягом

останнього десятиліття Сінгапур цілеспрямовано працює над посиленням свого інноваційно-аналітичного потенціалу, виходячи з концепції «смарт-держави», здатної ефективно мобілізувати всі ресурси нації для протидії загрозам [70, с. 109]. Уряд ініціював низку стратегічних програм на кшталт «Розумної нації-2025», «Дослідницьких центрів майбутнього», які передбачають концентрацію інтелектуальних зусиль на проривних напрямах – кібербезпеці, аналітиці великих даних, робототехніці, нових матеріалах, міському плануванні, екологічних та «зелених» технологіях.

Знаковим проектом у безпековій сфері стало утворення на базі Наньянського технологічного університету Інституту майбутнього як потужного think tank, орієнтованого на довгострокове прогнозування загроз та моделювання сценаріїв розвитку Південно-Східної Азії. Завдяки залученню провідних фахівців та новітніх методологій форсайту Інститут перетворився на визнаний центр стратегічної експертизи, розробки якого знаходять практичне застосування в оборонному плануванні, розвідувальній роботі, антитерористичній діяльності силових структур Сінгапуру [80, с. 29]. Загалом сінгапурська модель інтелектуального забезпечення безпеки може розглядатись як приклад оптимального поєднання цілеспрямованих державних зусиль з ініціативою громадянського суспільства, вдалого застосування гнучких мережевих підходів у сфері традиційно закритій та ієрархізованій.

Досить специфічний досвід розвитку безпекової аналітики демонструють нові індустріальні гіганти – передусім Китай та Індія. У першому випадку інтелектуальне забезпечення національної безпеки здійснюється під жорстким контролем з боку комуністичної партії, в рамках pathos реалізації її доктринальних настанов щодо перетворення КНР на провідну світову державу. Ключовими генераторами безпекового знання виступають аналітичні центри при ЦК КПК, канцелярії держради, Міноборони та деяких провідних університетах (Інститут міжнародних досліджень Університету Цінхуа, Інститут міжнародних і стратегічних досліджень Пекінського університету, Шанхайська академія міжнародних досліджень та ін.). Попри проголошений курс на «відкритість

зовнішньому світу», більшість цих установ лишаються закритими та непрозорими для широкої громадськості, працюють під безпосереднім наглядом відповідних партійних органів [89, с. 162].

Утім, на відміну від традиційних китайських уявлень про пріоритетність «твердої» (військової) сили, в останнє десятиліття КНР робить значні інвестиції у розвиток інструментів «м'якої» та «розумної» сили – від нарощування іномовлення та розбудови мережі Інститутів Конфуція до масштабних кібернетичних ініціатив на кшталт «Цифрового Шовкового шляху» [85, с. 39]. Особливого значення набуває інтелектуальна експансія у сфері інформаційно-комунікаційних технологій, штучного інтелекту, аналітики big data, де Китай вже сьогодні претендує на глобальне лідерство. Попри те, що офіційно більшість таких розробок позиціонується як суто цивільні, експерти відзначають їх високий потенціал для посилення розвідувально-аналітичних та пропагандистських спроможностей Пекіна у гібридному протистоянні зі США та їх союзниками (таблиця 1.5.).

Таблиця 1.5 – Порівняльна характеристика моделей інтелектуального забезпечення національної безпеки окремих держав у 2011-2021 рр.

Країна	**Модель інтелектуального забезпечення**	**Ключові актори**	**Сильні сторони**	**Слабкі сторони**
США	Плюралістична, з провідною роллю недержавних аналітичних центрів	Розвідувальне співтовариство, RAND Corp., галузеві асоціації, університети	Потужний науково-технологічний потенціал, розвинена експертна мережа, високий рівень аутсорсингу досліджень і розробок	Надмірна комерціалізація, вразливість перед лобістськими впливами, фрагментація аналітичного простору
Велика Британія	Гібридна, із залученням урядових і незалежних think tanks	Міноборони, МЗС, Центр урядового зв'язку, Chatham House, IISS	Розвинена мережа аналітичних центрів, тісні зв'язки з США та ЄС, увага до кібербезпеки та гібридних загроз	Брекзит ускладнив доступ до загально-європейських механізмів безпекових досліджень

Продовження таблиці 1.5.

Країна	**Модель інтелектуального забезпечення**	**Ключові актори**	**Сильні сторони**	**Слабкі сторони**
Франція	Державно-центрична, з домінуванням відомчих дослідницьких установ	Інститути МО, МЗС, президентської адміністрації, Військова школа, Sciences Po	Чіткість стратегічного бачення, потужні аналітичні традиції, інтеграція безпекової експертизи у систему держуправління	Закритість та ієрархічність, відставання в освоєнні новітніх безпекових практик
ФРН	Гібридна, заснована на потужній академічній науці та мережі приватних фондів	Університетські дослідницькі центри, SWP, GMF, ECFR	Фундаментальність досліджень, увага до невійськових аспектів безпеки, розвинені міжнародні зв'язки	Інерційність, переважання внутрішньої експертизи над зовнішньою
Ізраїль	Високоінтегрована, орієнтована на тісну взаємодію розвідувального співтовариства, ВПК та наукових установ	«Моссад», АМАН, Генштаб, Тель-Авівський ун-т, MDC в Герцлії	Інноваційність та адаптивність, увага до проривних технологій, ефективна система підбору кадрів	Невеликий масштаб аналітичного середовища, залежність від підтримки США та діаспори
Сінгапур	Мережева, заснована на поєднанні цілеспрямованої політики уряду та низових ініціатив громадянського суспільства	Наньянський технологічний ун-т, Ін-т майбутнього, галузеві асоціації	Ставка на форсайт-дослідження та моделювання ситуації, розвиток міждисциплінарних підходів	Малий розмір країни обмежує масштаб залученого експертного потенціалу

*Джерело: розробка автора.

Попри все розмаїття національних практик, спільним трендом для більшості країн Заходу є дедалі тісніша конвергенція діяльності державних, приватних і громадських інституцій в інтелектуальному забезпеченні безпеки, використання мережевих та краудсорсингових технологій, міждисциплінарних і крос-секторальних підходів. Як справедливо наголошує В. Смолянюк, «в сучасному світі, який стрімко змінюється під впливом процесів глобалізації, інформатизації та демократизації, традиційні ієрархічні моделі вироблення безпекових рішень вичерпують свій ресурс ефективності... Натомість майбутнє

за гнучкими, адаптивними системами стратегічного управління, які спираються на розгалужену експертно-аналітичну інфраструктуру, постійну ротацію ідей та кадрів» [52, с. 281].

Водночас важливо підкреслити, що кожна держава проходить унікальну траєкторію розвитку власного інтелектуального потенціалу безпеки, яка відображає її історичні традиції, ментальні особливості, ресурсні можливості та місце в архітектурі міжнародних відносин. Відтак універсальних рецептів у цій сфері не існує. Але креативне переосмислення та творча адаптація кращого світового досвіду з урахуванням національної специфіки є необхідною передумовою для зміцнення інтелектуального фундаменту безпекової політики України.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ РЕСУРСІВ У СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ УКРАЇНИ

2.1 Оцінка кадрового потенціалу та інтелектуального капіталу системи державного управління національною безпекою

Комплексна оцінка стану та перспектив розвитку інтелектуальних ресурсів у системі державного управління національною безпекою України неможлива без ґрунтовного дослідження її кадрового потенціалу та інтелектуального капіталу. Саме людський вимір є наріжним каменем системи забезпечення національної безпеки і оборони, від якості якого значною мірою залежать її функціональна спроможність, адаптивність та стійкість перед широким спектром сучасних викликів і загроз. Як справедливо зазначають Л. Чупрій та М. Карпенко, «в умовах динамізації безпекового середовища, появи нових, гібридних форм протиборства вирішальним фактором національної стійкості та конкурентоспроможності стає людський ресурс – його знання, вміння, мотивація, здатність до постійного самовдосконалення та інноваційної діяльності» [62, с. 148].

Відтак аналіз кадрового та інтелектуального виміру системи державного управління національною безпекою потребує врахування низки ключових параметрів – кількісних та якісних характеристик персоналу, рівня його професійної компетентності, механізмів підготовки та підвищення кваліфікації, мотиваційних чинників, інноваційної активності тощо. Водночас оцінка інтелектуального капіталу має охоплювати не лише безпосередньо людські ресурси, але й потенціал організаційних структур, баз знань, інформаційних систем, аналітичних моделей та експертних мереж, які опосередковують процес

вироблення та реалізації безпекової політики держави.

Згідно з даними РНБО України, чисельність особового складу сектору безпеки і оборони на кінець 2021 р. становила близько 495 тис. осіб (у т. ч. 250 тис. військовослужбовців та 245 тис. працівників правоохоронних органів і спеціальних служб). У відсотковому відношенні це становить близько 1,2% від загальної кількості населення країни [1, с. 23]. За цим показником Україна істотно поступається більшості країн-членів НАТО, де він коливається від 2 до 5%. Проте варто враховувати, що після початку повномасштабної збройної агресії РФ у лютому 2022 р. та запровадження воєнного стану відбувається суттєве нарощування сил оборони, яке вже найближчим часом може вивести Україну на загальноєвропейський рівень мілітаризації суспільства.

Утім, більш важливими видаються не кількісні, а якісні параметри кадрового забезпечення національної безпеки. Адже, як показує вітчизняний і зарубіжний досвід, в умовах асиметричних конфліктів та гібридних війн далеко не завжди чисельна перевага гарантує стратегічний успіх. Натомість визначального значення набуває інтелектуальний потенціал сил безпеки і оборони, рівень їх професіоналізму, технологічної оснащеності та психологічної готовності до виконання завдань за призначенням. Саме недооцінка цих факторів призвела до катастрофічних поразок ЗС України на початку збройної агресії РФ у 2014 р., коли чисельно переважаючі, але деморалізовані та слабо підготовлені війська виявились неспроможними адекватно реагувати на «гібридні» дії противника [46, с. 86].

Загалом за останні 5-7 років в Україні намітились певні позитивні зрушення в оновленні кадрового складу сектору безпеки і оборони. Зокрема, протягом 2014-2021 рр. до лав ЗСУ було залучено близько 400 тис. військовослужбовців-контрактників, переважна більшість яких мала реальний бойовий досвід участі в АТО/ООС [23, с. 14]. Відбулось певне омолодження командного складу – частка офіцерів віком до 30 років зросла з 12 до 18%, а середній вік командирів бригад скоротився з 45-47 до 38-42 років. У системі МВС та СБУ з’явилось нове покоління керівників середньої ланки, які пройшли

навчання за кордоном та мають прогресивне бачення реформ. Утім говорити про радикальні якісні зміни кадрового потенціалу все ще зарано.

За даними кадрового аудиту Міноборони України (2019 р.), частка військовослужбовців з вищою освітою в категоріях офіцерів становить 86%, у сержантському складі – лише 47%, у солдатському – взагалі 11%. При цьому менше 25% офіцерів володіють іноземною мовою на рівні стандартів НАТО, а серед сержантів цей показник не перевищує 4% [42, с. 31]. Аналогічна ситуація спостерігається і в правоохоронних структурах, де переважна більшість персоналу не має якісної освіти, досвіду роботи з аналітичними системами та сучасними технологіями. Показовим фактом є те, що станом на кінець 2021 р. в апараті МВС України працювало лише 11% фахівців з профільною освітою в галузі права та правоохоронної діяльності, у Нацполіції – 35%, у ДПСУ – 47% [43].

Особливо складним є стан інтелектуального забезпечення системи державної безпеки – органів СБУ, воєнної розвідки та контррозвідки, підрозділів кібербезпеки та інформаційного протиборства. Внаслідок тривалого недофінансування та кадрових «чисток» протягом останнього десятиліття ці структури істотно втратили свій аналітичний та прогностичний потенціал, здатність генерувати якісні інформаційно-розвідувальні продукти для вищого політичного та військового керівництва. За оцінками експертів, частка співробітників з науковими ступенями і званнями в центральних апаратах української спецслужб не перевищує 4-5%, що є одним з найнижчих показників у світі [36, с. 115]. При цьому середній вік аналітиків і «добувачів» інформації становить 47-52 роки, що свідчить про відсутність припливу молодих кадрів та існування суттєвих вікових дисбалансів у системі.

Негативно позначається на рівні інтелектуального забезпечення національної безпеки і слабкість наукового та експертного середовища, задіяного в розробці доктринальних і концептуальних засад безпекової політики держави. Зокрема, в країні досі відсутня цілісна мережа спеціалізованих аналітичних центрів, які б системно опрацьовували проблеми оборонного

будівництва, протидії гібридним загрозам, розвідувально-аналітичного супроводу зовнішньої політики тощо. Більшість існуючих недержавних «мозкових центрів» зосереджені на питаннях загальної зовнішньої політики та міжнародної безпеки (Центр Разумкова, Інститут світової політики, Рада зовнішньої політики «Українська призма» та ін.), тоді як військово-стратегічна та оборонно-промислова проблематика залишається на периферії їх інтересів [28, с. 103].

Вкрай обмеженим є й залучення потенціалу академічної науки до аналітичного забезпечення оборонної сфери. Попри наявність розвинутої мережі установ НАН України, університетів та галузевих НДІ, які мають високий рівень фундаментальних досліджень, їх практичний внесок у розв'язання прикладних проблем національної безпеки є мінімальним. Основними причинами цього є брак фінансування, відомча закритість силових структур, бюрократизованість процедур затвердження та впровадження результатів досліджень, інерційність мислення багатьох керівників. За даними Міноборони України, протягом 2015-2020 рр. питома вага витрат на оборонні НДДКР у структурі оборонного бюджету становила в середньому 0,4% проти 2-3% у провідних країнах НАТО [32, с. 18].

Характерною особливістю інтелектуального забезпечення системи національної безпеки України є його надмірна централізація та відомча замкнутість. На відміну від західних країн, де існує розвинутий ринок безпекових досліджень і розробок з високим рівнем міжвідомчої кооперації та аутсорсингу, в Україні практично всі види аналітичної діяльності монополізовані самими силовими структурами. Зокрема, організаційно-штатна структура СБУ передбачає наявність власних підрозділів стратегічного аналізу, ситуаційного прогнозування, моделювання ситуацій, психологічного забезпечення в центральному апараті та регіональних органах спецслужби.

Втім через низьку оплату праці, надмірне робоче навантаження та брак сучасного технічного оснащення ці структури мають обмежений функціонал і результативність [37, с. 124].

При цьому рівень міжвідомчої координації, обміну інформацією та спільного стратегування в українському безпековому секторі залишається доволі низьким. За оцінками експертів, більше 50% аналітичних продуктів дублюються різними суб'єктами системи забезпечення національної безпеки через відсутність спільних протоколів та форматів даних [33, с. 72]. Як наслідок, різні «гравці» часто формують суперечливе й неузгоджене бачення трендів і пріоритетів розвитку безпекової ситуації, що негативно позначається на рівні обґрунтованості державних рішень (таблиця 2.1.).

Таблиця 2.1 – Виявлені автором проблемні аспекти кадрового та інтелектуального забезпечення системи державного управління національною безпекою України

Параметр оцінки	**Сутність проблеми**	**Причини**	**Наслідки**
Освітній та компетентнісний рівень кадрів	Дефіцит фахівців з вищою освітою, знанням іноземних мов, навичками роботи з сучасними технологіями	Відсутність цілеспрямованої кадрової політики, престижності служби, низька оплата праці	Зниження якості аналітичної роботи, ефективності реагування на загрози
Вікова та кваліфікаційна структура	Старіння кадрів, недостатній приплив молодих фахівців, дисбаланси в кар'єрному зростанні	Низький рівень соціальних гарантій, неконкурентні умови служби, відсутність системи безперервного навчання	Зниження адаптивності й інноваційності безпекових інституцій
Інституційно-функціональне забезпечення аналітичної діяльності	Брак потужних мозкових центрів, слабкість експертних мереж, низька залученість наукового потенціалу до безпекових досліджень	Обмеженість бюджетної підтримки, бюрократичні перепони, відомча закритість силових структур	Недостатня якість доктринальних документів, ситуативність рішень, брак альтернативних опцій політики
Міжвідомча координація та комунікація	Відомча замкнутість, дублювання аналітичних функцій, слабкі канали «горизонтальної» взаємодії	Відсутність єдиних протоколів та форматів обміну даними, незбалансованість завдань і ресурсів	Неузгодженість оцінок розвитку безпекової ситуації, субоптимальне використання сил і засобів

*Джерело: розробка автора.

Усвідомлення зазначених дисбалансів спонукало керівництво держави до започаткування протягом останнього десятиліття низки ініціатив із реформування системи кадрової політики та інтелектуального забезпечення безпекової сфери. Зокрема, у 2014 р. було створено Міжвідомчу комісію з питань розвитку сектору безпеки і оборони при РНБО України, у рамках якої вперше вдалось налагодити координацію зусиль різних силових структур у формуванні єдиних вимог до підготовки персоналу. Поступово впроваджуються нові освітні стандарти та програми навчання у військових вишах, запроваджуються модульні системи перепідготовки та підвищення кваліфікації офіцерів і держслужбовців у сфері нацбезпеки [39].

Активізувались і контакти профільних наукових та експертних установ з органами державної влади. Зокрема, НІСД, Центр Разумкова, Інститут міжнародних відносин КНУ ім. Т. Шевченка та інші провідні аналітичні структури почали регулярно залучатися до розроблення стратегічних документів у сфері безпеки, проведення комунікаційних кампаній та заходів публічної дипломатії. З 2019 р. у структурі РНБО діє Національний координаційний центр кібербезпеки, який уперше об’єднав під одним «дахом» представників усіх ключових міністерств і відомств, наукових установ, громадських організацій та ІТ-бізнесу для вироблення ефективної стратегії протидії кіберзагрозам [59].

Утім ці кроки поки що не призвели до кардинального покращення якості інтелектуального забезпечення національної безпеки України. Брак кваліфікованого персоналу, розпорошеність наукового потенціалу, збереження міжвідомчих бар’єрів та відсутність цілісного бачення реформ серйозно гальмують інноваційний розвиток сектору безпеки і оборони, його адаптацію до вимог воєнного часу. Особливо критичною ця ситуація є для органів військово-цивільних адміністрацій, розвідувальних та контррозвідувальних служб, підрозділів інформаційної та кібербезпеки, державної охорони та захисту критичної інфраструктури. Без подолання вказаних вузьких місць навіть суттєве збільшення чисельності особового складу та обсягів фінансування не зможе якісно змінити спроможності української держави в умовах повномасштабної

збройної агресії РФ.

Відтак на сучасному етапі державотворення актуалізується завдання цілісного переосмислення кадрової політики та моделі інтелектуального забезпечення національної безпеки України, формування концептуальних засад та практичних механізмів нарощування людського капіталу сектору безпеки і оборони відповідно до кращих світових практик та викликів воєнного часу. Ключовими пріоритетами державної політики у цій сфері мають стати:

1) створення єдиної міжвідомчої системи стратегічного планування та координації інтелектуальних ресурсів на основі діяльності спеціально створеного органу типу Ради оборонних досліджень і розробок;

2) організація безперервної підготовки, перепідготовки та підвищення кваліфікації управлінських кадрів за програмами національної безпеки на базі оновлених стандартів і методик;

3) централізований моніторинг та оцінювання якості людського капіталу силових відомств з використанням сучасних метрик і показників ефективності;

4) налагодження ефективного партнерства в освітній і науковій сфері зі стратегічними партнерами України, отримання консультативно-дорадчої та технічної допомоги з питань інтелектуального забезпечення безпеки;

5) кардинальне збільшення фінансування НДДКР в інтересах оборони та безпеки, формування довгострокових програм замовлення досліджень і розробок на основі проектного підходу;

6) стимулювання розвитку мережі незалежних аналітичних центрів у сфері безпеки та посилення їх впливу на розробку державної політики;

7) створення єдиного координаційного центру зі стратегічних комунікацій для забезпечення консолідованої інформаційної політики у протидії агресору.

Лише системне впровадження комплексу взаємопов’язаних заходів за цими напрямами дозволить суттєво підвищити адаптивність, ефективність та стійкість національної системи інтелектуального забезпечення безпеки,

наростити її здатність протистояти загрозам в умовах триваючої «гібридної» агресії з боку РФ. Україна зобов’язана зробити серйозні висновки з уроків минулого і рішуче розірвати порочне коло кадрової деградації та управлінської неефективності, яка вже не раз відгукувалася трагічними поразками та численними жертвами. В умовах, коли на кону стоїть саме виживання нації, ми не маємо права на інтелектуальну демобілізацію та кадровий непотизм заради вузькокорпоративних чи бюрократичних інтересів.

Я певен, що наш воєнний час 2024 року вимагає рішучого і невідкладного оновлення інтелектуального фундаменту національної безпеки на засадах патріотизму, професіоналізму та синергії всіх державних і суспільних ресурсів.

2.2 Проблеми та виклики у сфері використання інтелектуальних ресурсів системи державного управління національною безпекою України

Здійснений у попередньому параграфі аналіз сучасного стану кадрового та інтелектуального потенціалу системи державного управління національною безпекою України дозволяє виокремити низку системних проблем і викликів, подолання яких є необхідною передумовою суттєвого зміцнення інституційної спроможності держави в умовах триваючої російської агресії.

Я хотів би насамперед акцентувати увагу на проблемі відсутності цілісного та науково обґрунтованого стратегічного бачення розвитку інтелектуальних ресурсів сектору безпеки і оборони. Попри наявність окремих концептуальних документів у кадровій сфері (Стратегічний оборонний бюлетень України, Концепція військової кадрової політики у ЗСУ тощо), в Україні й досі не сформовано узгодженого розуміння того, яким має бути оптимальний формат інтелектуального забезпечення національної безпеки в умовах гібридної війни, на основі яких принципів і механізмів повинна вибудовуватися система управління знаннями, компетентностями та інноваціями [48, с. 42]. Це породжує

високий рівень фрагментарності та різновекторності діяльності органів влади, спонтанність і кон'юнктурність рішень, що ухвалюються під тиском обставин.

Промовистим прикладом вказаних розбіжностей є ситуація в секторі безпеки і оборони в перші місяці повномасштабного вторгнення РФ, коли на тлі критично важливих завдань забезпечення територіальної оборони та мобілізації тривав затяжний міжвідомчий конфлікт щодо підпорядкування та розподілу повноважень між підрозділами ЗСУ, Нацгвардії, ТерО та нарешті утворених військово-цивільних адміністрацій [31, с. 29]. За відсутності чітких процедур координації дій та обміну інформацією це призводило до суттєвих прорахунків і втрат, негативно позначалося на ефективності протидії агресору. І хоча завдяки героїзму і самовідданості захисників більшість цих вад вдалося поступово подолати, вони оголили фундаментальні інституційні проблеми вітчизняного безпекового сектору.

Іншою системною вадою, що стримує ефективне використання інтелектуального потенціалу у сфері національної безпеки, є надмірна бюрократизація та забюрократизованість процесів управління. «…Існуюча система державного управління в секторі безпеки і оборони України демонструє очевидну неадекватність щодо викликів сьогодення, оскільки здебільшого продовжує відтворювати застарілі, ієрархічні форми мислення та роботи, що уповільнюють циркуляцію ідей, послаблюють зворотний зв'язок, позбавляють управлінців можливості вчасно реагувати на динамічні зміни безпекового середовища» [17, с. 63]. Органи влади просто «тонуть» у потоці другорядних, формальних процедур, штучно створюваних міжвідомчих і внутрішньовідомчих бар'єрах, що унеможливлює повноцінну реалізацію наявного інтелектуального капіталу.

Особливо гостро ця проблема постає у науково-дослідній та інноваційній діяльності, де існують численні «вузькі місця», пов'язані з надмірною зарегульованістю, закритістю та непрозорістю відповідних процесів. За оцінками незалежних експертів, близько 90% перспективних наукових розробок у сфері національної безпеки України припадають на фундаментальні та

прикладні дослідження, що здійснюються в рамках програм і проектів Державного оборонного замовлення [44, с. 11]. Утім вельми складні та забюрократизовані процедури затвердження технічних завдань, фінансування, приймання результатів НДР, а також режимні обмеження щодо їх апробації та оприлюднення суттєво знижують ефективність та практичну віддачу досліджень.

Іншим «вузьким місцем» щодо інноваційного забезпечення безпекової сфери є надто обмежена залученість до оборонних НДДКР незалежних наукових установ та комерційних структур. На відміну від провідних країн НАТО, в Україні основним виконавцем наукових досліджень військового призначення виступають профільні відомчі НДІ та заклади вищої освіти МОУ, Мінстратегпрому. При цьому частка позаурядових «мозкових центрів» та приватних високотехнологічних компаній у загальному фінансуванні оборонних НДДКР становить лише 10-12%, що звужує спектр залучених наукових шкіл, обмежує конкуренцію ідей та підходів [18, с. 172]. В умовах обмежених бюджетних можливостей це стримує інвестиції в амбітні проривні проекти, змушує концентруватися на вдосконаленні наявних зразків ОВТ, обмежує доступ до світових трендів розвитку критичних технологій.

Треба також відзначити недостатній рівень інтегрованості інтелектуального забезпечення безпекової сфери України в міжнародну архітектуру досліджень і розробок. Попри наявність низки двосторонніх і багатосторонніх угод про наукову співпрацю, участь у програмах і заходах під егідою НАТО, ЄС, ОБСЄ, наша держава все ще не має стійких механізмів обміну досвідом, повноцінного доступу до наукових мереж і баз даних союзників. За даними Центру досліджень армії, конверсії та роззброєння, протягом 2015-2021 рр. частка іноземного фінансування в загальному обсязі науково-технічної діяльності ДК «Укроборонпром» не перевищувала 2-3% [15]. З іншого боку, режимні обмеження ускладнюють залучення іноземних фахівців та експертів до реалізації вітчизняних оборонних проектів, стримують трансфер технологій і know-how.

Найбільш наочно ці прогалини проявились в умовах масштабної військової агресії з боку РФ. Зокрема, в ситуації обмеженого доступу до сучасних технологічних рішень (засобів зв'язку, навігації, розвідки, цілевказання тощо) ЗСУ та інші складові сектору безпеки змушені були витрачати критично дорогоцінні людські та часові ресурси на «винахід велосипеда», самотужки розробляючи ті системи, що давно апробовані в арміях країн НАТО. Водночас окремі позитивні приклади кооперації з провідними компаніями та think tanks ЄС і США (у сферах тактичної розвідки, планування операцій, інформаційного протиборства) засвідчили величезний потенціал інтелектуальної співпраці, використання якого дозволяє частково компенсувати відсутні ресурси та згенерувати асиметричні рішення [5, с. 43].

Серед інших прогалин кадрового та інтелектуального забезпечення національної безпеки України варто відзначити недостатній рівень координації та взаємодії суб'єктів сектору безпеки і оборони, в тому числі щодо вироблення узгоджених оцінок, планування та проведення спільних аналітичних досліджень. Як відзначає К. Войтовський, «проведений у 2019-2020 рр. комплексний огляд сектору безпеки засвідчив вкрай низькі рівні сумісності інформаційних систем, методологічних підходів і протоколів аналітичної діяльності між різними силовими відомствами. Подекуди ситуація доходила до абсурду: з 14 індикаторів оцінки стану безпекового середовища, які незалежно застосовували МОУ та СБУ, лише 2 збігалися за змістом, решта – мали принципові розбіжності» [40, с. 181].

Не кращим є становище і з координацією науково-експертного забезпечення у сфері безпеки. Попри наявність розгалуженої мережі дослідницьких установ і аналітичних центрів, рівень системності їх роботи та взаємодії є вкрай низьким. Як наслідок, відомчі науково-дослідні інституції подекуди працюють над схожими темами, не погоджуючи планів та дублюючи завдання. Зусилля різних державних і недержавних «мозкових центрів» дуже часто розпорошені, спрямовані на різні цілі, що не дозволяє повною мірою використати їх інтелектуальний ресурс в інтересах обороноздатності

країни [45, с. 202].

На загальну неефективність аналітичної діяльності накладаються також міжвідомчі конфлікти та суперечності, пов’язані з різним позиціонуванням та інтересами суб’єктів безпекової політики. Особливо проблемним у цьому контексті є питання розмежування завдань і повноважень розвідувальних органів та військових формувань. Зокрема, поширеною є практика, коли МОУ чи ГУР МОУ продукують аналітичні матеріали, що прямо стосуються сфер відповідальності СЗР (економічна, науково-технічна, інформаційна безпека), дублюючи їх напрацювання або «перетягаючи ковдру» [36, с. 95]. Своєю чергою розвідка неохоче ділиться здобутою інформацією з військовими через побоювання її витоку та розголошення джерел, що також не сприяє формуванню цілісної картини загроз національній безпеці.

Застосування методології SWOT-аналізу дозволяє чіткіше побачити спектр внутрішніх і зовнішніх факторів, що впливають на ефективність використання інтелектуальних ресурсів у системі державного управління національною безпекою України. До сильних сторін можна віднести збереження кваліфікованого кадрового ядра сектору безпеки й оборони, наявність усталених науково-аналітичних шкіл, відносно розвинуту освітньо-наукову інфраструктуру. Водночас серед внутрішніх вразливостей чітко проявляються недосконалість нормативно-правового поля, фрагментарність державної політики, міжвідомча неузгодженість, застарілість методів управління та кадрові дисбаланси [4, с. 214].

Що стосується зовнішнього контексту, то ключовими можливостями, безперечно, є доступ до передових знань і технологій країн-партнерів по НАТО, отримання матеріально-технічної та консультативно-дорадчої допомоги, використання навчальних та тренувальних програм під егідою Альянсу. З іншого боку, триваюча збройна агресія РФ, гібридні загрози і виклики національній стійкості, ускладнені геополітичні умови партнерства з Заходом є тими зовнішніми викликами, що визначатимуть перспективи розвитку безпекового сектору України на найближче десятиліття. І від того, наскільки ефективно ми

зуміємо використати наявний інтелектуальний потенціал в умовах обмежених ресурсів, значною мірою залежатиме успішність протистояння ворожим планам [55, с. 137].

Таблиця 2.2 – Стислий SWOT-аналіз проблем і перспектив розвитку інтелектуальних ресурсів системи державного управління національною безпекою України

Сильні сторони	**Слабкі сторони**	**Можливості**	**Загрози**
- Висококваліфіковане кадрове ядро - Потужні галузеві наукові школи - Розгалужена мережа профільних ЗВО та НДІ - Креативність і патріотизм персоналу - Здобутий в АТО/ООС досвід асиметричного реагування на загрози	- Недосконалість законодавства - Брак цілісного бачення реформ - Відомчі конфлікти і неузгодженість - Забюрократизованість та інерційність процесів управління - Недостатній рівень інновацій та оновлення знань - Розпорошеність зусиль і ресурсів	- Доступ до передових знань і технологій НАТО - Отримання технічної та консультативної допомоги - Участь у програмах професійного розвитку під егідою НАТО і ЄС - Розвиток партнерської взаємодії з провідними державами світу - Імплементація євроатлантичних стандартів і практик	- Триваюча збройна агресія РФ - Посилення гібридних загроз, насамперед в інформаційній та кібер-сфері - Ускладнення геополітичних умов партнерства із Заходом - Дефіцит кваліфікованих кадрів внаслідок мобілізації та міграції - Обмеженість бюджетного ресурсу для фінансування реформ

*Джерело: розробка автора.

Резюмуючи викладене, слід констатувати, що наявні підходи та механізми використання інтелектуального потенціалу в системі державного управління національною безпекою України на сьогодні не повною мірою відповідають масштабам існуючих викликів. Попри певні зрушення останніх років, зумовлені досвідом відсічі російській агресії та співпраці з країнами-партнерами, в цілому якість аналітичного забезпечення безпекової політики залишається

недостатньою. Фрагментарність стратегічного бачення, міжвідомчі протиріччя, слабка координація різних суб'єктів, брак кваліфікованих кадрів та інноваційних рішень є «хронічними хворобами» української системи безпеки, які в умовах війни проявляють себе з новою силою.

Водночас успішний досвід оборони Києва, Харкова, Миколаєва, звільнення окупованих територій у 2022 році переконливо довів, що навіть в екстремальних умовах українські військові та правоохоронці здатні демонструвати креативність та ефективність у протистоянні набагато сильнішому противнику – насамперед завдяки синергії зусиль, винахідливості та самовідданості. Відтак нагальним завданням держави є закріплення цього безцінного досвіду та його інкорпорація у практику державного стратегічного управління. На наше переконання, серед ключових кроків у цьому напрямі мають бути:

1) формування єдиної Стратегії розвитку інтелектуального потенціалу системи забезпечення національної безпеки України із залученням провідних фахівців сектору оборони, представників академічної спільноти, незалежних аналітичних центрів та громадськості;

2) нормативно-правове закріплення функцій і повноважень органів державної влади щодо координації наукової, аналітичної та кадрової роботи у безпековій сфері, створення відповідних міжвідомчих робочих органів;

3) створення загальнонаціональної мережі ситуаційно-аналітичних центрів на базі провідних наукових установ та вищих навчальних закладів, уніфікація методологій та протоколів обміну інформацією між ними;

4) розроблення інноваційних підходів до підготовки, перепідготовки та підвищення кваліфікації особового складу сектору безпеки і оборони з урахуванням вимог війни та впровадження новітніх освітніх технологій;

5) інтенсифікація міжнародного співробітництва у науково-технічній сфері, імплементація кращих практик і процедур аналітичної роботи з безпекових питань, набуття членства в профільних експертних мережах і консорціумах;

6) кардинальне нарощення фінансової підтримки наукових досліджень і прикладних розробок у сфері національної безпеки, впровадження механізмів державного замовлення, проектного менеджменту та грантової підтримки відповідних НДДКР;

7) запровадження національної системи оцінювання та атестації кадрів сектору безпеки відповідно до стандартів НАТО, забезпечення конкурсності та прозорості кар'єрного зростання, інституціалізація ротацій між відомствами [35, с. 94].

Реалізація зазначених напрямів дозволить суттєво підвищити інституційну спроможність держави, наростити людський та інтелектуальний капітал сектору безпеки і оборони України, що є головною передумовою нашої перемоги на полі бою та після її завершення. Адже історія неодноразово доводила, що саме народи з потужним інтелектуальним стрижнем здатні долати найбільші труднощі і виклики, відновлюватися після руйнівних воєн та виходити на нові горизонти розвитку. Таким є і стратегічний орієнтир для України, яка, загартувавшись у нинішніх випробуваннях, неодмінно посяде гідне місце у колі успішних, безпечних та інноваційних держав світу.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ РЕСУРСІВ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ УКРАЇНИ

3.1 Реалістичні стратегічні напрями розвитку інтелектуального потенціалу системи державного управління національною безпекою України

Здійснений у попередніх розділах комплексний аналіз сучасного стану та проблем формування й використання інтелектуальних ресурсів у системі державного управління національною безпекою України засвідчив необхідність розроблення та впровадження цілісної стратегії нарощування інтелектуального потенціалу сектору безпеки і оборони відповідно до стандартів НАТО та викликів війни. В умовах обмежених фінансових, кадрових та часових можливостей першочергова увага має бути зосереджена на реалізації найбільш пріоритетних та результативних напрямів реформування, здатних у стислі терміни забезпечити якісні зрушення в адаптивності, ефективності та стійкості вітчизняної безпекової системи.

На моє переконання, серед таких пріоритетних напрямів у короткостроковій перспективі (1-2 роки) мають бути насамперед наступні кроки:

1) Розроблення та затвердження Стратегії розвитку кадрового потенціалу сектору безпеки і оборони України на період до 2025 року, яка на основі ґрунтовного аудиту визначить реальний стан і проблеми кадрового та інтелектуального забезпечення, сформулює амбітне бачення його трансформації у відповідності до сучасних викликів та окреслить цілісну «дорожню карту» реформ. Координацію розроблення та впровадження Стратегії доцільно покласти на робочу групу під егідою РНБО за участі профільних міністерств,

науково-експертних установ, громадянського суспільства та зацікавлених міжнародних партнерів.

2) Створення єдиної міжвідомчої системи підготовки, перепідготовки та підвищення кваліфікації управлінських кадрів для сектору безпеки і оборони на базі Національного університету оборони та інших провідних вишів. Йдеться про формування інноваційної освітньої платформи для централізованого навчання цивільних і військових керівників середньої та вищої ланки, здатних ефективно взаємодіяти та генерувати нестандартні управлінські рішення в умовах війни. Ключовими елементами цієї системи мають стати:

– уніфіковані програми та стандарти підготовки відповідно до вимог НАТО, орієнтовані на розвиток лідерських якостей, аналітичних компетентностей та soft skills;

– широке застосування ділових ігор, кейс-методів та симуляційних технологій, максимально наближених до реальності російсько-української війни;

– залучення провідних іноземних та вітчизняних фахівців і тренерів, у т.ч. з досвідом участі у миротворчих операціях, антитерористичній діяльності та asimetric warfare;

– розвинені механізми дистанційного навчання та електронних освітніх ресурсів, що дозволяють охопити максимальну аудиторію управлінців в умовах обмежених можливостей очного навчання.

3) Започаткування цільової державної програми «Інтелектуальний безпековий резерв України», спрямованої на цілеспрямований відбір, підтримку та залучення до аналітичної й експертної роботи на потреби сил оборони талановитої молоді – випускників ЗВО, аспірантів, молодих учених із найширшого спектру галузей знань (право, економіка, ІТ, психологія, соціологія, лінгвістика тощо). Реалізація програми передбачатиме:

– проведення на конкурсній основі щорічного набору до 100 молодих фахівців з усіх регіонів України для участі у 6-місячній інтенсивній програмі підготовки за напрямом «Аналітика та експертиза у сфері національної безпеки»;

– забезпечення учасникам програми стипендій, грантів на реалізацію

дослідницьких проектів, стажування у провідних аналітичних центрах країн-членів НАТО;

– створення активної мережевої спільноти випускників програми для обміну досвідом, комунікації та залучення до виконання аналітичних завдань в інтересах сектору безпеки і оборони.

4) Радикальне спрощення процедур проведення, фінансування та впровадження результатів наукових досліджень і розробок оборонного та безпекового спрямування, впровадження принципів «розумної дерегуляції» у цій сфері. Це передбачає, зокрема:

– перехід до проектної моделі фінансування перспективних НДДКР через запровадження фондової та грантової форм, що забезпечують оперативніше виділення та освоєння бюджетних і позабюджетних коштів;

– скорочення термінів експертизи та затвердження ТЗ і результатів НДДКР, спрощення вимог до звітності за проектами, зменшення кількості обов’язкових експертиз та узгоджень;

– лібералізацію режимних обмежень у частині залучення цивільних дослідників і підрядників, запровадження практики державно-приватного партнерства в інноваційній сфері.

За попередніми оцінками, реалізація зазначених невідкладних заходів дозволить уже протягом найближчих 12-18 місяців:

– на 15-20% підвищити рівень професійної кваліфікації та аналітичних навичок персоналу структур сектору безпеки й оборони;

– збільшити частку молодих фахівців в аналітичних і науково-експертних підрозділах з 10 до 25-30%;

– у 1,5-2 рази скоротити час «реакції» наукового та експертного середовища на запити безпекових інституцій та відповідно підвищити актуальність і затребуваність аналітичних продуктів;

– розширити коло представників громадянського суспільства, залучених до обговорення та вироблення безпекової політики (з 30-40 до 100-120 осіб щорічно) [34, с. 36].

Водночас у середньостроковій перспективі (3-5 років) ключовими пріоритетами у розвитку інтелектуального потенціалу національної безпеки України мають стати наступні напрями:

1) Впровадження комплексної системи безперервного професійного розвитку фахівців сектору безпеки і оборони на основі принципу «освіта протягом життя». Це передбачає поступовий перехід від періодичного підвищення кваліфікації за відомчим принципом до постійного вдосконалення компетентностей персоналу відповідно до індивідуальних освітніх траєкторій та актуальних потреб служби. Для цього необхідно:

– оновити кваліфікаційні вимоги та запровадити наскрізні рамки компетентностей для всіх посад і рівнів управління у безпековому секторі;

– сформувати об’єднаний банк освітніх програм і курсів у сфері безпеки, провести їх акредитацію та уніфікацію за стандартами НАТО;

– налагодити систему валідації результатів неформального та інформального навчання за профілем службової діяльності;

– запровадити практику регулярного оцінювання професійної компетентності фахівців із застосуванням зовнішнього незалежного аудиту.

2) Створення Національної мережі ситуаційно-аналітичних центрів при Апараті РНБО, Міноборони, МВС, СБУ та інших ключових суб’єктах сектору безпеки і оборони. Основним призначенням цих структур має стати:

– цілодобовий збір, накопичення, аналітичне опрацювання та поширення даних про стан безпекового середовища з усіх можливих джерел;

– підготовка моделей, прогнозів і сценаріїв розвитку ситуації на їх основі, розробка проектів управлінських рішень для вищого керівництва держави;

– налагодження оперативного «горизонтального» обміну даними та аналітикою між усіма зацікавленими суб’єктами у режимі реального часу;

– організація взаємодії з незалежним експертним середовищем, комунікація з іноземними партнерами та міжнародними інституціями.

Важливою умовою успішного функціонування мережі є розроблення і

затвердження єдиних протоколів та форматів інформаційного обміну, процедур аналітичної діяльності, критеріїв оцінки достовірності даних та моделей верифікації прогнозів.

3) Заснування Міжвідомчого центру оборонних інновацій та критичних технологій у структурі Міноборони, призначеного для координації та підтримки НДДКР оборонного спрямування, у т.ч.:

– вироблення єдиної політики замовлень на дослідження і розробки відповідно до Державної цільової програми реформування та розвитку ОПК;

– експертизи та оцінки перспективності інноваційних проектів і технологічних рішень подвійного призначення;

– налагодження співпраці військових НДІ і КБ з недержавними науково-дослідними установами, ЗВО, високотехнологічними компаніями;

– організації транскордонних консорціумів і проектних груп для реалізації спільних НДДКР в рамках двостороннього та багатостороннього ВТС;

– здійснення трансферу передових іноземних технологій та імплементації досвіду інноваційної діяльності провідних країн НАТО [6, с. 71].

4) Запровадження цілісного механізму стратегічного планування та координації досліджень у сфері національної безпеки на основі принципів проектного менеджменту. Це передбачає:

– розроблення щорічних та середньострокових планів наукових досліджень і розробок за участю всіх суб’єктів сектору безпеки і оборони, незалежних аналітичних центрів та профільних наукових установ;

– організацію відкритих конкурсів проектів і програм у сфері безпеки, їх об’єктивну експертизу та селекцію за чіткими критеріями актуальності, реалістичності, інноваційності;

– запровадження механізмів проектного управління НДДКР – від розроблення концепцій і ТЗ до організації виконання, прийняття результатів та оцінки ефективності впровадження;

– регулярний моніторинг ходу реалізації проектів та програм, їх коригування відповідно до зміни безпекової ситуації та потреб замовників;

– підвищення прозорості та підзвітності використання бюджетних видатків на НДДКР, запровадження зовнішнього незалежного audeet [60].

Показовим у цьому контексті є досвід Ізраїлю – країни, яка протягом останніх десятиліть перебуває в епіцентрі збройного протистояння і водночас демонструє разючі успіхи в розвитку безпекових інновацій. Вкрай обмежений у природних ресурсах, Ізраїль зробив ставку на розвиток інтелектуального капіталу нації, максимальне сприяння креативності та винахідливості в інтересах зміцнення обороноздатності. Завдяки запровадженню спеціальних урядових програм, податкових та митних преференцій, механізмів державно-приватного партнерства в інноваційній сфері, ізраїльтянам вдалося сформувати потужний науково-технологічний та підприємницький потенціал, залучити масштабні іноземні інвестиції в сектор безпекових стартапів [3, с. 217].

Як наслідок, сьогодні Ізраїль входить до топ-5 світових експортерів продукції ВПК, контролює до 10% глобального ринку кібербезпеки, залишається одним із лідерів у сферах штучного інтелекту, робототехніки, безпілотних авіаційних систем. Наявність розгалуженої мережі венчурних фондів, акселераторів та бізнес-інкубаторів, орієнтованих на сектор безпеки і оборони, дозволяє невеликій країні генерувати до 1000 технологічних стартапів щорічно і швидко впроваджувати їх у війська. За оцінками експертів, близько половини оборонного бюджету Ізраїлю витрачається саме на перспективні НДДКР, тоді як у країнах НАТО цей показник не перевищує 10-15% [22].

Звісно, сліпе копіювання ізраїльського досвіду в українських умовах навряд чи можливе з огляду на відмінності масштабів держав, специфіку безпекового середовища, стан і структуру ОПК, ментальність та традиції управлінської культури.

Втім певні інституційні механізми та організаційні підходи цілком можуть бути запозичені. Зокрема, на часі є розроблення окремої Національної програми безпекових інновацій із виділеним фінансуванням, яка передбачала б:

– формування галузевих інноваційних кластерів і технопарків подвійного призначення довкола провідних технічних університетів та наукових

центрів (КПІ, ХПІ, «Харківський авіаційний», «Південмаш», КБ «Південне» та ін.);

– поглиблення кооперації державного і приватного секторів шляхом розміщення довгострокових замовлень ОПК у підприємців, створення інжинірингових шкіл та лабораторій спільного користування;

– надання тендерних преференцій та податкових пільг для інвесторів, які вкладають кошти в перспективні оборонні стартапи, запровадження програм їх акселерації та виходу на глобальні ринки;

– організацію бізнес-місій та виставкових заходів для просування вітчизняних безпекових інновацій за кордоном, приєднання до спільних проектів в рамках ЄС та НАТО [21, с. 14].

На мою думку, реалізація такого комплексу заходів із розвитку інтелектуального потенціалу системи державного управління національною безпекою України на горизонті 3-5 років дозволить досягти амбітних результатів, а саме:

– скоротити відставання від провідних країн світу за показниками фінансування безпекових НДДКР і підготовки кадрів з 5-7 до 2-3 разів;

– збільшити частку інноваційних технологій і розробок у виробництві ОВТ з нинішніх 3-5 до 15-20%;

– наростити експорт високотехнологічної продукції оборонного та подвійного призначення в 1,5-2 рази;

– довести щорічний випуск фахівців у галузі національної безпеки за програмами вищої освіти до 3-3,5 тис. осіб.

Таблиця 3.1 – Стратегічні напрями та очікувані результати розвитку інтелектуального потенціалу системи державного управління національною безпекою України у середньостроковій перспективі

Напрям реформ	**Зміст заходів**	**Очікувані результати**	**Індикатори успішності**
Розроблення Стратегії розвитку кадрового потенціалу	- Комплексний аудит стану кадрового забезпечення - Формулювання амбітного бачення трансформації - Розроблення цілісної «дорожньої карти» реформ	- Підвищення професійної кваліфікації персоналу - Оптимізація вікової та освітньо-кваліфікаційної структури - Наближення до стандартів НАТО	- Частка фахівців з вищою освітою – 90-95% - Частка персоналу до 35 років – 30-40% - Відповідність вимогам НАТО – на 70-80%
Створення єдиної системи підготовки управлінських кадрів	- Розроблення уніфікованих програм та стандартів - Впровадження інноваційних освітніх технологій - Забезпечення міжвідомчої та міжнародної кооперації	- Формування нової генерації лідерів з інноваційним мисленням - Досягнення оперативної сумісності та синергії зусиль - Обмін кращими управлінськими практиками	- Охоплення навчанням 100% управлінців середньої та вищої ланки - Підвищення рівня професійних компетентностей на 25-30%
Започаткування програми «Інтелектуальний безпековий резерв»	- Щорічний конкурсний набір талановитої молоді - Організація інтенсивної фахової підготовки - Грантова підтримка дослідницьких проєктів - Створення спільноти випускників	- Омолодження аналітичного середовища - Залучення кращих інтелектуальних ресурсів нації - Формування інноваційних ідей і підходів - Поширення культури критичного мислення	- Участь у програмі 100 осіб щороку - Працевлашту-вання 70% випускників за фахом - Реалізація 30-40 дослідницьких проектів
Радикальна дерегуляція сектору безпекових НДДКР	- Перехід до проєктної моделі фінансування - Спрощення процедур експертизи і звітності - Лібералізація режимних обмежень - Розширення публічно-приватного партнерства	- Скорочення циклу «ідея-розробка-впровадження» - Активізація недержавного сектору безпекових досліджень - Зростання частки високотехнологічних розробок	- Скорочення термінів виконання НДДКР на 30-40% - Зростання приватних інвестицій в ОПК на 20-25% - Підвищення рівня серійності нових ОВТ до 70-80%

Продовження таблиці 3.1.

Напрям реформ	**Зміст заходів**	**Очікувані результати**	**Індикатори успішності**
Розвиток безперервної професійної освіти	- Запровадження наскрізних компетентністних рамок - Об'єднання ресурсів відомчих систем підготовки - Валідація неформального та інформального навчання - Регулярне незалежне оцінювання компетентності	- Забезпечення актуальності знань і навичок персоналу – Підвищення практичної зорієнтованості підготовки – Визнання самоосвіти як способу розвитку – Об'єктивізація рівня професіоналізму	- Оновлення компетентностей кожні 3-5 років – Зменшення відриву від службових обов'язків на 15-20% – Покриття оцінюванням до 90% фахівців
Створення мережі ситуаційно-аналітичних центрів	- Налагодження цілодобового багатоканального моніторингу - Продукування прогнозно-аналітичних матеріалів - Забезпечення міжвідомчої координації та комунікації - Організація взаємодії з експертним середовищем	- Створення цілісної ситуаційної обізнаності - Підвищення обґрунтованості прийняття рішень - Досягнення синергії інформаційно-аналітичних зусиль - Формування довірчих експертних мереж	- Скорочення часу реагування на загрози на 40-60% - Підвищення достовірності прогнозів на 20-30% - Охоплення експертною підтримкою до 80% управлінських рішень
Заснування центру оборонних інновацій	- Вироблення єдиної інноваційної політики – Запровадження проєктно-грантових механізмів - Налагодження кооперації науки, ОПК та ІТ-сектору - Забезпечення трансферу передових технологій	- Консолідація ресурсів на проривних напрямах - Інтенсифікація циклу досліджень і розробок - Конвергенція військових і цивільних технологій - Прискорена імплементація стандартів НАТО	- Зростання частки інновацій в ОПК на 10-15% – Подвоєння кількості оборонних стартапів - Скорочення циклу розробки ОВТ на 30-40%

*Джерело: розробка автора.

Безперечно, реалізація такого амбітного бачення потребуватиме не лише політичної волі керівництва держави, а й широкої суспільної підтримки,

готовності до справжнього «інтелектуального стрибка», зміни ментальних моделей та управлінської культури. Без подолання інерції мислення, бюрократичних бар'єрів та міжвідомчих протиріч, без «вбудовування» інновацій в усі «пори» системи національної безпеки будь-які, навіть найкращі стратегії та програми реформ ризикують лишитися на папері.

У цьому контексті повчальним для України є досвід посткомуністичних країн Центрально-Східної Європи, які протягом останніх десятиліть доклали титанічних зусиль для перебудови своїх безпекових систем на шляху до членства в НАТО та ЄС. Польща, Чехія, Угорщина, країни Балтії змогли за історично стислий період подолати радянську спадщину, наростити кадровий та інтелектуальний потенціал, досягти високих стандартів оперативної сумісності з партнерами по Альянсу. Безперечно, цьому сприяли потужні зовнішні стимули та фінансово-технічна допомога в рамках програм НАТО, однак не менш важливими виявились і «м'які» фактори – зміна світоглядних та ціннісних орієнтирів, утвердження принципів демократичного контролю, транспарентності та підзвітності безпекових інституцій [64, с. 315]. Натомість в Україні все ще зберігаються певні рудименти «пострадянськості» в роботі оборонних відомств та спецслужб – закритість, бюрократизм, непотизм, недовіра до незалежної експертизи. Відтак справжня «демілітаризація» суспільної свідомості, імплементація принципів демократичного врядування та належного врядування (good governance) в секторі безпеки мають розглядатися як наріжні камені перезавантаження вітчизняної безпекової системи, її адаптації до викликів гібридної війни.

3.2 Удосконалення мережевої взаємодії зацікавлених суб'єктів та інституційних механізмів використання інтелектуальних ресурсів

Іншим надважливим імперативом розвитку інтелектуального потенціалу

системи державного управління національною безпекою України є налагодження ефективних механізмів мережевої взаємодії та координації діяльності всіх зацікавлених суб'єктів – як державних (профільні міністерства та відомства, спецслужби, науково-дослідні установи, заклади вищої освіти), так і поза державних (мозкові центри, громадські організації, ЗМІ, бізнес-структури тощо). Лише в такий спосіб можна досягти синергетичного ефекту, уникнути дублювання зусиль і марнотратства ресурсів, забезпечити своєчасне реагування на динамічні зміни безпекового середовища.

На жаль, наявні інституційні механізми використання інтелектуальних ресурсів в Україні все ще залишаються недостатньо ефективними та скоординованими. Як і раніше, мають місце відомчий сепаратизм, ревниве ставлення до інформації, інерція закритості та непрозорості оборонного планування. Недержавний експертний потенціал залучається спорадично і вибірково, а широка громадськість переважно виключена з процесів формування і реалізації безпекової політики. За оцінками аналітиків Центру Разумкова, усунення цих застарілих практик і перехід до всеосяжної моделі публічно-приватного партнерства є ключовою передумовою перезавантаження вітчизняного безпекового сектора [48, с. 18].

Тож які ж кроки доцільно здійснити в цьому напрямі найближчими роками?

По-перше, необхідним є створення постійно діючого Міжвідомчого координаційного центру з питань аналітично-прогнозного супроводження реалізації національних безпекових стратегій під егідою РНБО України. Його основним завданням має стати забезпечення узгодженості та послідовності дій усіх державних структур в імплементації Стратегії національної безпеки, Стратегії воєнної безпеки, Стратегічного оборонного бюлетеня та інших системоутворюючих документів. Для цього Центр повинен мати достатні повноваження для інтеграції інформаційно-аналітичних ресурсів міністерств та відомств, здійснення регулярного контрою над відповідними заходами, підготовки пропозицій щодо коригування політики. Окрім апарату РНБО, до

роботи Центру доцільно залучити представників силових структур, Мінекономіки, Мінфіну, провідних «мозкових центрів» та громадських рад.

По-друге, важливим кроком може стати запровадження регулярної практики спільних міжвідомчих навчань і тренувань за сценаріями реагування на комплексні безпекові загрози – як класичні військові, так і гібридні. Це дозволить відпрацювати алгоритми та процедури взаємодії різних суб'єктів в умовах кризових ситуацій, виявити найбільш вразливі елементи системи, «протестувати» різні моделі і формати скоординованого застосування сил та засобів сектору оборони і безпеки. Досвід країн НАТО переконливо довів високу ефективність подібних навчань для формування спільної ситуаційної обізнаності, досягнення оперативної сумісності та взаємодоповнюваності зусиль цивільних і військових структур, налаштування механізмів кризового менеджменту. Показово, що окрім представників силового блоку, в них активно беруть участь й інші державні агенції, органи місцевого самоврядування, громадські організації та бізнес-асоціації [83, с. 217].

По-третє, вкрай назрілим є радикальне розширення форматів і механізмів залучення позадержавних інтелектуальних ресурсів до експертного супроводу процесів вироблення і реалізації безпекової політики. Йдеться про налагодження сталої співпраці владних структур з провідними аналітичними центрами, науковими та освітніми установами, професійними об'єднаннями, волонтерськими рухами на основі прозорих і зрозумілих «правил гри». Для цього, з одного боку, необхідно законодавчо закріпити форми, процедури та гарантії такої взаємодії (зокрема, при підготовці щорічних послань Президента, доктринальних документів, проєктів бюджету, державних цільових програм). З іншого боку, варто запровадити систему конкурсного розміщення замовлень на незалежну експертизу й аналітичний супровід у недержавному секторі на умовах відкритого тендеру, рівного доступу та неупередженого оцінювання пропозицій. Це сприятиме «демонополізації» експертної сфери, розвитку конкуренції ідей та підходів, залученню найбільш кваліфікованих і креативних фахівців.

По-четверте, актуальним завданням є поглиблення транскордонної

комунікації і мережування українських суб'єктів безпекового сектору з відповідними структурами країн-членів і партнерів НАТО. Зокрема, йдеться про розширення участі в спільних багатонаціональних проектах у сфері стратегічного аналізу, оборонних НДДКР, розвитку кадрового потенціалу. Формування сталих професійних мереж між аналітиками, експертами, менеджерами безпекових програм по обидва боки Атлантики матиме безцінне значення для обміну кращими практиками, запозичення передових методик і технологій, поширення спільних ціннісних установок та безпекової культури. При цьому важливо, щоб міждержавна взаємодія не обмежувалася виключно офіційними міжурядовими контактами, а здійснювалася на всіх рівнях – між університетськими і науковими центрами, професійними асоціаціями, громадськими організаціями.

По-п'яте, потребує вдосконалення нормативно-правова база, що регламентує процедуру надання грифів секретності, режими зберігання та доступу до інформації з обмеженим доступом. Чинні правила в цій сфері все ще залишаються надмірно забюрократизованими та непрозорими, створюючи невиправдані перепони для комунікації між державними та недержавними суб'єктами та обміну важливими даними. Як свідчить закордонний досвід, спрощення та раціоналізація системи охорони державної таємниці не підриває національних інтересів, а навпаки – сприяє підвищенню довіри й більш ефективному використанню позаурядового експертного ресурсу в інтересах зміцнення обороноздатності. Тож Україні слід рухатися в напрямку відкритого діалогу з громадянським суспільством щодо визначення розумного балансу між легітимним правом держави на збереження секретів та об'єктивними потребами демократичного контролю й широкого фахового обговорення чутливих питань безпекової політики.

Нарешті, вкрай важливим напрямом діяльності має стати розбудова горизонтальних аналітично-комунікаційних мереж між різними відомчими підрозділами, відповідальними за стратегічний аналіз та експертне супроводження процесу прийняття рішень. Наразі діяльність цих структур

переважно зосереджена «всередині» силових міністерств та служб, а міжвідомча співпраця має спорадичний характер. Створення сталих майданчиків для професійної взаємодії аналітиків-управлінців (постійно діючих семінарів, конференцій, робочих груп) дозволило б суттєво інтенсифікувати обмін кращими практиками, порівняння методик та підходів, вироблення спільного бачення актуальних безпекових викликів. Саме такі неформальні аналітичні мережі в багатьох країнах НАТО є потужним генератором свіжих ідей, інноваційних концепцій та «проривних» аналітичних продуктів.

Підсумовуючи викладений у цьому параграфі №3.2 аналіз, доцільно навести зведену таблицю, яка системно презентує ключові напрями, пріоритетні заходи, очікувані результати та індикатори успішності процесу вдосконалення мережевої взаємодії суб'єктів вітчизняного безпекового сектору на осяжну перспективу (див. таблицю 3.2.).

Таблиця 3.2 – Пріоритетні напрями та очікувані результати вдосконалення мережевої взаємодії суб'єктів сектору безпеки і оборони України

Напрям удосконалення	**Зміст заходів**	**Очікувані результати**	**Індикатори успішності**
1) Створення Міжвідомчого координаційного центру	- забезпечення узгодженості дій держструктур - інтеграція інформаційно-аналітичних ресурсів - контроль імплементації стратегій	- підвищення рівня координованості на 30-40% - скорочення випадків дублювання функцій - 100% охоплення контролем ключових заходів	- налагодження регулярних (що)тижневих нарад - створення єдиної бази даних і звітності - впровадження системи kpi для виконавців
2) Запровадження міжвідомчих навчань за сценаріями гібридних загроз	- формування спільної ситуаційної обізнаності - досягнення оперативної сумісності - удосконалення кризового менеджменту	- скорочення часу реагування на 25-30% - участь 90% суб'єктів безпекового сектору - опрацювання 15-20 кризових сценаріїв	- проведення навчань що(квартально) - долучення місцевої влади і волонтерів - створення універсальних соп реагування

Продовження таблиці 3.2.

Напрям удосконалення	**Зміст заходів**	**Очікувані результати**	**Індикатори успішності**
3) Розширення механізмів залучення недержавної експертизи	- налагодження сталого публічно-приватного партнерства - запровадження прозорої тендерної системи - формування конкурентного ринку ідей	- зростання частки зовнішньої експертизи до 30% - залучення провідних «мозкових центрів» - підвищення якості аналітичних продуктів	- ухвалення закону про публічні консультації - виділення бюджету на аутсорсинг послуг - створення урядового аналітичного порталу
4) Поглиблення міжнародного мережування в рамках НАТО	- участь у багатонаціональних дослідницьких проєктах - формування сталих експертних мереж - трансфер передових практик і підходів	- входження в топ-5 країн-контрибуторів програм нато - проведення 5-7 спільних навчань щорічно - стажування 200-250 фахівців у нато	- створення українського офісу зв’язку в нато - збільшення фінансування двосторонніх r&d - запуск програм академічної мобільності
5) Вдосконалення системи охорони держтаємниці	- спрощення процедур надання грифів секретності - запровадження механізмів демократичного контролю - налагодження діалогу з громадянським суспільством	- скорочення частки інформації з грифом на 40% - забезпечення доступу до 90% відкритих даних - зростання довіри до безпекових інституцій	- інвентаризація масивів секретної інформації - створення комісії з розсекречування даних - запуск платформи безпекового краудсорсингу
6) Розбудова міжвідомчих аналітичних мереж	- створення сталих майданчиків професійної взаємодії - інтенсифікація обміну досвідом та методиками - продукування інноваційних ідей та концепцій	- проведення 30-40 фахових заходів щорічно - долучення 80% аналітиків держсектору - підвищення якості стратегічного аналізу на 25%	- заснування асоціації аналітиків силового блоку - видання фахового журналу і бюлетеня - запровадження грантової підтримки проєктів

*Джерело: розробка автора.

Вважаю, що реалізація окреслених у таблиці 3.2. першочергових кроків щодо оптимізації механізмів міжвідомчої координації, державно-приватної

співпраці та міжнародного мережування в секторі безпеки і оборони України є необхідною передумовою нарощування сукупного інтелектуального потенціалу країни в умовах триваючої «гібридної» агресії з боку РФ. Тому впровадження відповідних новацій та підходів, навіть попри ймовірний інституційний спротив та ресурсні обмеження воєнного часу, має розглядатися політичним керівництвом держави, і зокрема Офісом Президента України, як один із пріоритетів національного рівня, що потребує особливої уваги, політичної волі та цілеспрямованих управлінських зусиль.

ВИСНОВКИ

Проведені вище дослідження дозволяють зробити такі агреговані висновки.

1. За підсумками параграфу 1.1. можна сказати про зростаючу роль інтелектуальних ресурсів у системі державного управління національною безпекою як визначального чинника стратегічної конкурентоспроможності та стійкості держави в умовах глобальної невизначеності та «гібридних» загроз. На відміну від традиційних складових безпекового потенціалу (територія, населення, збройні сили, економіка тощо), які є важливими, але не вирішальними в постіндустріальну епоху, саме інтелектуальний капітал у формі знань, навичок, організаційних компетенцій та соціальних зв'язків уможливлює ефективне реагування на асиметричні виклики, забезпечує гнучкість та інноваційність безпекової політики держави. Підтвердженням цьому є практика провідних країн світу, в яких протягом останніх десятиліть простежується чітка тенденція до нарощування інвестицій у розвиток «мозкових центрів», аналітичних структур та експертних мереж при одночасному скороченні витрат на традиційні військові потреби.

Водночас історичний досвід колишніх імперій (Британської, Німецької, Османської) та наддержав часів «холодної війни» (США і СРСР) засвідчує, що ефективна система інтелектуального забезпечення безпеки є не лише результатом цілеспрямованих зусиль держави, але й продуктом тривалої соціокультурної еволюції суспільства, його здатності продукувати й абсорбувати інновації. З урахуванням цього стратегічним завданням України має стати розбудова власної моделі інтелектуального забезпечення національної безпеки та стійкості, яка, з одного боку, враховуватиме кращий світовий досвід та сучасні безпекові imperatives, а з іншого – спиратиметься на самобутні ментально-ціннісні та інституційні підвалини розвитку української державності, особливості її геостратегічного положення та історичної ролі як форпосту демократичного Заходу у протистоянні з євразійським неототалітаризмом.

2. Аналіз особливостей формування та використання інтелектуальних ресурсів у системі забезпечення національної безпеки дозволяє дійти висновку про зростаючу роль наукових знань, аналітичних компетентностей та стратегічного мислення як вирішального фактора адаптивності та стійкості держави в умовах турбулентного безпекового середовища. Ефективна протидія гібридним загрозам, забезпечення національної безпеки та обороноздатності країни вимагають не лише розвиненого кадрового та технологічного потенціалу сектору безпеки, але й наявності потужної «мережі знань», інтегрованої у глобальний простір безпекової аналітики. Світовий досвід свідчить, що продуктивна робота такої мережі можлива лише за умов демократичності, інклюзивності та транспарентності політичної системи, широкого залучення потенціалу академічної науки, незалежних аналітичних центрів та громадянського суспільства. Відтак, розбудова в Україні цілісної та збалансованої моделі інтелектуального забезпечення національної безпеки є не лише питанням інституційного дизайну чи ресурсної оптимізації, але й індикатором зрілості вітчизняної демократії, здатності еліти та соціуму до критичного мислення, обґрунтованого вибору стратегічних пріоритетів розвитку. Від того, наскільки ми зуміємо пройти цей непростий шлях, значною мірою залежить майбутнє України як суверенної, сильної та інтелектуальної держави.

3. Підсумовуючи огляд сучасного досвіду провідних країн світу, можна констатувати, що ефективне інтелектуальне забезпечення національної безпеки вимагає органічного поєднання низки взаємопов’язаних складових. По-перше, держава повинна здійснювати цілеспрямовану політику нарощування кадрового потенціалу сектору безпеки, яка передбачає модернізацію системи підготовки та підвищення кваліфікації фахівців, впровадження інноваційних освітніх методик і технологій, налагодження міжвідомчого наукового обміну. По-друге, інтелектуальний потенціал безпекової сфери значною мірою залежить від рівня технологічного оснащення аналітичних структур, їх здатності продукувати інноваційні розробки світового рівня, креативно використовувати наявні

ресурси. По-третє, ключовою передумовою адекватності стратегічного аналізу та прогнозування є забезпечення щільних і довірчих зв'язків державних безпекових інституцій з незалежним експертним середовищем, налагодження постійного «мозкового штурму» щодо викликів національній безпеці. Нарешті, по-четверте, інтегрованість безпекової аналітики у глобальні експертні мережі, міжнародний трансфер знань і технологій дозволяє малим та середнім державам компенсувати ресурсні обмеження, «підживлювати» свій інтелектуальний потенціал за рахунок кооперації із зовнішніми гравцями. Попри все розмаїття національних практик, спільним трендом для більшості країн Заходу є дедалі тісніша конвергенція діяльності державних, приватних і громадських інституцій в інтелектуальному забезпеченні безпеки, використання мережевих та краудсорсингових технологій, міждисциплінарних і крос-секторальних підходів.

4. Проведений аналіз сучасного стану кадрового та інтелектуального потенціалу системи державного управління національною безпекою України засвідчив наявність низки проблемних аспектів. Зокрема, попри певне зростання кількісних параметрів особового складу сектору безпеки і оборони (до 495 тис. осіб або 1,2% населення), його якісні характеристики все ще не повною мірою відповідають вимогам часу. Частка військовослужбовців з вищою освітою у ЗСУ становить 86% серед офіцерів, 47% серед сержантів і лише 11% серед солдатів. У МВС фахівці з профільною освітою складають від 11% в апараті до 47% у ДПСУ. Найбільш критичною є ситуація в органах безпеки, де частка співробітників з науковими ступенями не перевищує 4-5%, а середній вік аналітиків сягає 47-52 років. Загалом, попри локальні зрушення, інтелектуальне забезпечення національної безпеки України й досі не відповідає кращим світовим практикам.

5. Стислий аналіз (параграф 2.2.) проблем і викликів у сфері використання інтелектуальних ресурсів системи державного управління національною безпекою України дозволив виокремити низку ключових прогалин, серед яких: відсутність цілісного стратегічного бачення розвитку інтелектуального потенціалу сектору безпеки і оборони; надмірна

бюрократизація та забюрократизованість управлінських процесів; домінування відомчої закритості та обмежена залученість незалежного експертного середовища до формування безпекової політики (частка позаурядових аналітичних центрів і приватних компаній у фінансуванні оборонних НДДКР не перевищує 10-12%); низький рівень інтегрованості до міжнародної науково-технологічної співпраці (частка іноземних коштів у структурі фінансування безпекових досліджень складає 2-3%); слабка координація діяльності різних суб'єктів сектору безпеки (з 14 індикаторів оцінки безпекового середовища, що застосовуються МОУ та СБУ, лише 2 повністю співпадають). Подолання цих викликів вимагає системних інституційних, організаційних та ресурсних трансформацій моделі інтелектуального забезпечення національної безпеки України.

6. Згідно результатів параграфу №3.1, ключовими стратегічними напрямами розвитку інтелектуального потенціалу системи державного управління національною безпекою України протягом наступних 5 років мають стати: 1) розроблення цілісної Стратегії розвитку кадрового потенціалу сектору безпеки і оборони на основі викликів сучасності та стандартів НАТО; 2) створення єдиної міжвідомчої системи підготовки управлінських кадрів з використанням інноваційних освітніх технологій; 3) започаткування цільової програми «Інтелектуальний безпековий резерв» для залучення талановитої молоді; 4) радикальне спрощення процедур замовлення та впровадження безпекових НДДКР; 5) перехід до моделі безперервної професійної освіти персоналу; 6) розбудова мережі ситуаційно-аналітичних центрів та 7) заснування єдиного Центру оборонних інновацій і критичних технологій. Системна реалізація цього комплексу заходів, попри ймовірний спротив та ресурсні обмеження, здатна забезпечити справжній «інтелектуальний стрибок» вітчизняної безпекової системи, її адаптацію до сучасних викликів гібридної війни та наближення до стандартів євроатлантичної спільноти.

7. Налагодження ефективних механізмів мережевої співпраці та координації діяльності державних і недержавних суб'єктів безпекової сфери є

найважливішою передумовою розкриття потужного інтелектуального потенціалу українського суспільства в інтересах зміцнення обороноздатності. Ключовими пріоритетами на цьому шляху мають стати: створення єдиного міжвідомчого координаційного центру; запровадження регулярних навчань за сценаріями комплексного реагування на гібридні загрози; розширення форматів публічно-приватного партнерства в безпековій аналітиці; поглиблення міжнародного мережування в рамках євроатлантичної спільноти; раціоналізація системи охорони державної таємниці; розбудова тематичних професійних спільнот. Послідовна реалізація цього комплексу заходів, попри ймовірний інституційний спротив та ресурсні обмеження, здатна забезпечити синергію зусиль усіх зацікавлених гравців, мінімізувати міжвідомчі бар’єри, налагодити сталі канали генерування, обміну та використання передових аналітичних компетенцій. Без такої всеосяжної «мережевізації» годі й сподіватися на розв’язання амбітних завдань адаптації вітчизняного безпекового сектору до вимог і викликів сучасності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННННЯ

1. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2020 році». Київ : НІСД, 2020. 264 с.

2. Аналітична доповідь Національного інституту стратегічних досліджень до позачергового Послання Президента України до Верховної Ради України про внутрішнє та зовнішнє становище України у сфері національної безпеки. К. : НІСД, 2022. 99 с.

3. Атаманенко І. Інноваційна екосистема національної безпеки: ізраїльський досвід для України. *Стратегічна панорама*. 2021. № 1-2. С. 211-225.

4. Бегма В. М., Загорка О. М., Косевцов В. О. Механізми управління щодо реструктуризації і реорганізації оборонної промисловості : світовий досвід для України : монографія. Київ : ІПНБ, 2021. 310 с.

5. Бегма В. М., Шемаєв В. М. Оборонно-технічне співробітництво в умовах глобалізації: український вимір : монографія. Київ : НІСД, 2011. 85 с.

6. Бегма В., Шемаєв В. Необхідність трансформації державного управління оборонними ресурсами України в нових реаліях світового порядку. *Збірник наукових праць НАДУ*. 2022. № 1. С. 67-74.

7. Бегма В. М., Шемаєв В. М., Радов Д. Г. Нові підходи до забезпечення інтелектуальної складової воєнної безпеки. Наука і оборона. 2013. № 4. С. 36-41.

8. Белінська Н. Є. Політика безпеки та стратегічної культури ФРН в умовах нових викликів європейській безпеці : дис. ... канд. політ. наук : 23.00.04. Чернівці, 2021. 226 с.

9. Бєлай С., Споришев К. Системи підтримки прийняття рішень у державному управлінні силами безпеки в умовах сучасних викликів для України. Актуальні питання у сучасній науці. 2024. №2/20. URL: https://perspectives.pp.ua/index.php/sn/article/download/9146/9195 (дата

звернення: 19.11.2024).

10. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук. праці. Київ : НІСД, 2016. 528 с.

11. Власюк О. С., Кононенко С. В. Кремлівська агресія проти України: роздуми в контексті війни : монографія. К. : НІСД, 2017. 304 с.

12. Власюк О. С., Кононенко С. В. Актуальні аспекти вдосконалення моделі національної безпеки України. *Стратегічна панорама*. 2017. № 1. С. 17-23.

13. Глобалізація і безпека розвитку : монографія / О. Г. Білорус та ін.; за ред. О. Г. Білоруса. К. : КНЕУ, 2001. 733 с.

14. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки. К. : НІСД, 2010. 288 с.

15. Горбулін В. П., Шеховцов В. С., Шевцов А. І. Проблемні питання імпортозаміщення та розвитку оборонно-промислового комплексу в контексті науково-технічного співробітництва України з країнами НАТО і ЄС. *Вісник Національної академії наук України.* 2018. № 9. С. 3-10.

16. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки. Київ : НІСД, 2010. 515 с.

17. Державне управління у сфері національної безпеки України : словник-довідник / уклад. : О. Г. Бондаренко та ін. Київ : НАДУ, 2021. 492 с.

18. Деякі питання реформування державного управління України : розпорядження Кабінету Міністрів України від 24.06.2016 № 474-р. URL: https://zakon.rada.gov.ua/laws/show/474-2016-p#n9 (дата звернення: 15.06.2024).

19. Дубов Д. В., Баровська А. В. Інформаційне забезпечення системи державного управління в умовах гібридної війни. *Стратегічні пріоритети*. 2019. № 1 (49). С. 143-152.

20. Дунаєв І., Кудь А. Конструювання майбутнього для України: від інтуїтивного пророцтва до наукового синтезу. *Вісник післядипломної освіти. Вип. 12 (41). (Серія «Соціальні та поведінкові науки»).* С. 142-159. DOI: https://doi.org/10.32405/2522-9931/2522-9958-2020-12(41)-142-

159 (дата звернення: 19.11.2024).

21. Загородня С. Напрями вдосконалення державної політики України у сфері безпекових інновацій. *Ефективність державного управління*. 2022. Вип. 1. С. 13-20.

22. Іванов О. Досвід трансформації оборонно-промислового комплексу Ізраїлю: висновки для України в умовах збройної агресії Росії. *Наука і оборона*. 2022. № 1. С. 46-51.

23. Інформаційно-аналітичний огляд Міністерства оборони України «Біла книга 2021. Збройні Сили України». К. : МОУ, 2022. 185 с.

24. Коваленко М. М., Дунаєв І. В. Складові публічної політики в умовах реалізації мобілізаційної моделі розвитку економіки. *Теорія та практика державного управління*. 2023. Вип. 1 (76). С. 7–25. DOI: 10.26565/1727-6667-2023-1-01. URL: https://periodicals.karazin.ua/tpdu/article/view/22287/20607 (дата звернення: 19.11.2024).

25. Кондратьєва О. В. Інтелектуальний капітал в системі забезпечення інноваційного розвитку держави. *Економічний аналіз*. 2021. Т. 31. № 3. С. 73-79.

26. Кравченко С. І., Кладченко І. С. Основні підходи до визначення поняття «інтелектуальний капітал». *Економічний вісник Донбасу*. 2017. № 3 (49). С. 75-81.

27. Крамар О. Л. Радянська історіографія холодної війни. *Український історичний журнал.* 2019. № 3. С. 91-103.

28. Мадіссон В., Шахов В. Сучасна українська геополітика : навч. посіб. для студ. гуманіт. спец. вищ. навч. закл. Київ : Либідь, 2003. 174 с.

29. Мандрагеля В. А. Інтелектуальні ресурси забезпечення національної безпеки. *Науково-інформаційний вісник Академії національної безпеки*. 2018. № 3-4 (19-20). С. 109-119.

30. Марченко О. С. Інтелектуальні ресурси: сутність та види. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Економічна теорія та право*. 2018. № 4 (35). С. 129-142.

31. Нікітін Ю. В., Чорний В. С. Особливості міжвідомчої взаємодії

складових сектору безпеки і оборони України в сучасних умовах. *Вісник Національного університету оборони України*. 2022. № 2 (65). С. 26-32.

32. Оборонна реформа: системний підхід до оборонного менеджменту : монографія / А. Павліковський та ін. ; за заг. ред. А. Сиротенка. Київ : НУОУ, 2020. 274 с.

33. Поляков Л. І. Воєнна реформа в Україні: здобутки та втрати. *Наука і оборона*. 2022. № 2. С. 67-75.

34. Поляков Л. Інтелектуальні виклики для сектору безпеки і оборони України в умовах війни. *Національна безпека і оборона*. 2022. № 1-2. С. 33-38.

35. Поляков Л. Процеси розвитку та реформування системи забезпечення національної безпеки. *Політичний менеджмент*. 2022. № 5. С. 90-99.

36. Пошедін О. І. Взаємовідношення розвідувальних та військових структур. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2015. № 1. С. 90-96.

37. Пошедін О. І. Воєнна розвідка України: шляхи реформування та підвищення ефективності функціонування. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2021. № 1 (44). С. 120-127.

38. Пошедін О. І., Мудрак Ю. М. Наукове забезпечення розвитку кадрового потенціалу розвідувальних органів України. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки.* 2019. № 2 (80). С. 111-121.

39. Про затвердження Положення про особливості організації освітнього процесу у вищих військових навчальних закладах Міністерства оборони України та військових навчальних підрозділах вищих навчальних закладів України : наказ Міністерства оборони України від 20.07.2015 № 346. URL: https://zakon.rada.gov.ua/laws/show/z1126-15#n16 (дата звернення: 15.06.2023).

40. Проблеми і напрями підвищення ефективності функціонування

системи забезпечення національної безпеки України : наук.-інформ. зб. Вип. 1 / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2012. 256 с.

41. Резнікова О. О., Цюкало В. Ю., Паливода В. О., Дрьомов С. В. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналіт. доп. Київ : НІСД, 2020. 328 с.

42. Результати кадрового аудиту Міністерства оборони України: аналітична доповідь / О. Ф. Сальнікова та ін. К. : НУОУ, 2020. 60 с.

43. Розпорошений сектор: оцінка ефективності урядування у секторі безпеки й оборони України станом на 2021 рік : аналіт. звіт / Д. Ю. Ляпін та ін. Київ : Заповіт, 2022. 82 с.

44. Сальнікова О. Ф., Кушнір В. О. Упровадження інновацій в оборонній сфері України: проблеми та перспективи. *Наука і оборона.* 2019. № 4. С. 8-14.

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

46. Сектор безпеки і оборони України: реформи в умовах гібридної війни : аналітична доповідь Центру Разумкова / ред. В. Горбулін, О. Литвиненко. Київ : Заповіт, 2022. 130 с.

47. Сектор безпеки і оборони України: стратегічне лідерство та військовий професіоналізм : монографія / В. С. Фролов та ін. Київ : НУОУ, 2022. 176 с.

48. Сектор безпеки і оборони України: теорія, стратегія, практика : монографія / Ф. В. Саганюк та ін. Київ : Академпрес, 2017. 180 с.

49. Семенченко А. І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України : монографія. Київ : НАДУ, 2008. 428 с.

50. Ситник Г. П. Державне управління у сфері національної безпеки (концепт. та організаційно-правові засади) : підруч. К. : НАДУ, 2012. 544 с.

51. Скиба О. П. Розвідувальне забезпечення національної безпеки США як чинник глобального лідерства. *Актуальні проблеми міжнародних відносин*. 2012. Вип. 111 (Ч. 1). С. 90-96.

52. Смолянюк В. Ф. Системні засади національної безпеки України. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. 2018. № 2 (37). С. 107-126.

53. Спільник С. І. Теоретичні та організаційно-правові засади забезпечення національної безпеки в умовах боротьби з тероризмом : монографія. К. : ФОП Кандиба Т. П., 2020. 300 с.

54. Тютюнник В. П., Горовенко В. К. Забезпечення національної безпеки України в контексті сучасних євроінтеграційних процесів. *Наука і оборона.* 2015. № 4. С. 134-139.

55. Україна 2030: Доктрина збалансованого розвитку / О. Жилінська та ін. Львів : Кальварія, 2017. 164 с.

56. Українські Think Tanks у дзеркалі експертного опитування / підгот. Н. Харченко, Ю. Романюк, О. Заславська. Київ : Фонд «Демократичні ініціативи», 2003. 44 с.

57. Фесенко М. В. Державна політика забезпечення інтелектуальної безпеки як складник державної безпеки: досвід ФРН. *Державне управління: удосконалення та розвиток.* 2020. № 3. URL: http://www.dy.nayka.com.ua/?op=1&z=1596 (дата звернення: 15.06.2023).

58. Фесенко М.В. Роль «мозкових центрів» у формуванні зовнішньополітичної стратегії США. 2016.

59. Функціонування Національного координаційного центру кібербезпеки як складової національної системи кібербезпеки / Г. П. Ситник та ін. *Публічне управління і адміністрування в Україні.* 2019. Вип. 14. С. 29-34.

60. Черніховська О. Гнучке управління оборонними дослідженнями і розробками в країнах НАТО: уроки для України. Національна безпека: український вимір. 2021. № 4. С. 132-147.

61. Чорний В. С., Шемаєв В. М., Зубарєв В. В. Концептуальні засади розвитку системи забезпечення національної безпеки України : монографія. Київ : НУОУ, 2015. 216 с.

62. Чупрій Л., Карпенко М. Проблеми формування нової ідентичності і

соціокультурної безпеки в Україні в процесі євроінтеграції. *Вісник Нац. академії керівних кадрів культури і мистецтв*. 2022. № 2. С. 145-157.

63. Abelson D. E. Think Tanks and the Global Influence on Public Policy. Cambridge : Cambridge University Press, 2022. 255 p.

64. Alexandrov O., Popova I., Yatsubyn M. Intellectual security of the state as an object of strategic public administration. *Public Administration and Law Review*. 2021. Issue 4. P. 312-318.

65. Brown E. L. Organizational and Legal Aspects of National Security During Counterterrorism Operations. Oxford : Oxford University Press, 2020. 305 p.

66. Соснін О. В., Воронкова В. Г., Ажажа М. А. Інформаційне суспільство як виклик глобалізації : монографія. Запоріжжя : Просвіта, 2017. 388 с.

67. Harris P., Thompson R. National Security Strategy and Policy Planning. Cambridge : Cambridge University Press, 2012. 520 p.

68. Johnson L. M. Arms Control: Searching for New Approaches. *World Economy and International Relations Journal*. 1990. Vol. 22, No. 7. P. 55-65.

69. Johnson T. R., Bradley M. S. The Use of «Soft Power» in U.S. Foreign Policy. *Journal of Diplomatic Studies*. 2017. Vol. 12, No. 1. P. 200-210.

70. Koh A. T. H. Singapore's perspectives on national security and resilience. *PRISM*. 2019. Vol. 8, No. 2. P. 102-117.

71. Koshka D., Melnyk S. «Intellectual Security» of a State: the Content and the Essence. *International Journal of Educational Policy Research and Review. 2023. Vol*. 2 (9). P. 136-140.

72. La France face aux défis du XXIe siècle: Revue stratégique de défense et de sécurité nationale. Paris : DICOD, 2017. 111 p.

73. Magen A. Fighting terrorism: The democracy advantage. Journal of Democracy. 2018. Vol. 29, No. 1. P. 111-125.

74. McChrystal S. Team of Teams: New Rules of Engagement for a Complex World. New York : Penguin, 2015. 290 p.

75. Müller F. K. German Think Tanks and Their Role in Shaping Foreign

Policy in the Early 20th Century. *Contemporary European Issues*. 2018. Vol. 29, No. 2. P. 120-140.

76. National Security Strategy and Strategic Defence and Security Review 2015. London : TSO, 2015. 94 p.

77. National Security Strategy of the United States of America. Washington : White House, 2017. 55 p.

78. Nye J. S. Soft Power: The Means to Success in World Politics. New York : Public Affairs, 2004. 352 p.

79. Nye J. S. The future of power. New York : Public Affairs, 2011. 320 p.

80. Petrella S. Combining intelligence with science in security and defense issues: the experience of the S. Rajaratnam School of International Studies. *Revista Brasileira de Inteligência*. 2017. Vol. 12. P. 27-34.

81. Piel R., Schulze P. W. Think Tanks in Germany: The Bertelsmann Foundation. In Think Tanks, Foreign Policy and the Emerging Powers. Palgrave Macmillan, 2018. P. 189-207.

82. Smith J. P. British Political Elites: The Intellectual Resource of Governance. *Political Studies Journal*. 2016. Vol. 64, No. 3. P. 85-92.

83. Stoltenberg J. The Secretary General's Annual Report 2021. Brussels : NATO, Public Diplomacy Division, 2022. 236 p.

84. Stone D. Think tanks and policy analysis in countries in transition. Budapest : Central European University Press, 2005. 317 p.

85. Trubinová M. Is China a cyber security threat? European View. 2018. Vol. 17, No. 1. P. 36-44.

86. Weaver K. R., McGann J. G. Think Tanks in Public Policy: A Comparative Analysis of Global Practices. New York : Brookings Institution Press, 2012. 250 p.

87. Williams K. R., Meyer D. S. Strategic Approaches to National Security: Challenges and Solutions. New York : Palgrave Macmillan, 2010. 495 p.

88. Williams M., Suzuki H. Japan in the 20th Century: Political, Economic, and Cultural History. Oxford : Oxford University Press, 2007. 530 p.

89. Zhao K. The motivation behind China's public diplomacy. *The Chinese Journal of International Politic*s. 2015. Vol. 8, No. 2. P. 167-196.