Вахненко С. О.,
здобувач вищої освіти,
Національна академія Служби безпеки України
(м. Київ, Україна)

Гайдук А. В.,
здобувач вищої освіти
Національна академія Служби безпеки України
(м. Київ, Україна)

Кононова Д. В.,
кандидат філологічних наук, доцент, доцент кафедри романо-германських мов,
Національна академія Служби безпеки України
(м. Київ, Україна)

ВИКОРИСТАННЯ МІЖНАРОДНОГО ДОСВІДУ ОРГАНІЗАЦІЇ СЕКТОРУ БЕЗПЕКИ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Сектор безпеки та оборони України протягом останнього десятиліття зазнає глибокої трансформації, що зумовлено як внутрішніми реформаторськими пріоритетами, так і необхідністю інтеграції до євроатлантичних структур. Збройна агресія рф продемонструвала обмеженість традиційних підходів до організації оборонної системи та підкреслила важливість запозичення міжнародного досвіду, який показав свою ефективність у країнах із подібними безпековими викликами. Практика НАТО вирізняється системним підходом до стандартизації та взаємосумісності, впровадженням технічних і процедурних стандартів (STANAG, NISP), що забезпечують здатність збройних сил різних держав діяти спільно на тактичному, оперативному та стратегічному рівнях, а також оцінювати ступінь сумісності спроможностей союзників. У 2023 р. Альянс оновив процес оборонного планування (Comprehensive Defence Planning Process (NDPP)), визначивши пріоритети розвитку спроможностей партнерів, зокрема України, з акцентом на інтеграцію інформаційних систем, кіберзахист і стійкість оборонної логістики [1, 2].

Крім технічної стандартизації, НАТО реалізує комплексну політику реформування сектору безпеки (Defence and Security Sector Reform, D/SSR), що включає стратегічні консультації, навчальні програми та інституційні проєкти. Через комплексний пакет допомоги для України Альянс сприяє адаптації

системи оборонного менеджменту, стандартизації кадрової політики, розвитку оборонних освітніх інституцій і механізмів цивільного контролю, тоді як програми виховання доброчесності та удосконалення військової освіти (DEEP) підвищують прозорість, мінімізують корупційні ризики та сприяють підготовці керівних кадрів.

Досвід США демонструє ефективність жорстких механізмів парламентського, фінансового та операційного контролю: офіс урядової підзвітності США (GAO) постійно здійснює аудит видатків, контрактів і програм Міністерства оборони США та надає Конгресу оцінку результативності політики оборонних закупівель, логістики та кібербезпеки, а впровадження системи планування, програмування, бюджетування і виконання (PPBE) забезпечує чіткий зв'язок між стратегічним плануванням і ресурсним забезпеченням, підвищуючи прозорість управлінських рішень [3].

Практика Великої Британії демонструє ефективне поєднання парламентського контролю, здійснюваного через Комітет Палати представників США зі збройних сил, та незалежних аудитів - Національний аудиторський офіс Великобританії (NAO), які оцінюють ефективність оборонних видатків, управління персоналом і резервами, виконання програм модернізації та оборонних закупівель. Такий механізм формує стійку систему підзвітності, сприяє публічній довірі до військових інституцій та запобігає нецільовому використанню коштів, а його адаптація до українських реалій передбачає поєднання технічної сумісності (впровадження стандартів НАТО) з інституційними механізмами прозорості, включно з парламентським контролем, аудитом, публічною звітністю та довгостроковою підтримкою партнерів. Впровадження системи управління на засадах управління обороною, що базується на стандартах НАТО (зокрема BI Policy 2023), дозволить Україні підвищити ефективність оборонного планування та зміцнити демократичний контроль над сектором безпеки, що є ключовою умовою інтеграції до євроатлантичного простору.

Ізраїльська модель національної безпеки, заснована на принципі «тотальної оборони», інтегрує регулярні війська, резервістів, територіальну оборону, цивільний сектор та критичну інфраструктуру у єдину оборонну екосистему, що забезпечує гнучке та масштабоване реагування на комплексні загрози — від ракетних обстрілів до кібернетичних атак. Ключовим елементом є високотехнологічна складова, зокрема система протиракетної оборони «Залізний купол», що завдяки інтелектуальній системі управління вогнем здійснює аналіз траєкторій та пріоритизацію цілей у реальному часі, мінімізуючи ризики ураження цивільних об'єктів [4]. Інноваційною є система лазерної протидії «Залізний промінь», призначена для нейтралізації БПЛА, мінометних снарядів та ракет малого радіуса дії, що забезпечує значно нижчу вартість одиничного «пострілу» порівняно з традиційними перехоплювачами та підвищує економічну стійкість оборонної системи в умовах тривалого конфлікту [6]. Ізраїльська стратегія інтегрує штучний інтелект, автономні системи та енергоефективні технології, створюючи адаптивну і фінансово збалансовану архітектуру безпеки,

а кіберкомпонент «Кібер купол» забезпечує превентивне виявлення атак на критичну інфраструктуру, енергетичні системи, зв'язок і державні сервіси через взаємодію національного кібер-директорату, військових кібервідділів та приватного сектору. Цей досвід є релевантним для України з огляду на активний розвиток систем протидії БПЛА та впровадження технологій штучного інтелекту в оборонній сфері.

Скандинавські держави, такі як Фінляндія та Швеція, послідовно впроваджують концепцію тотального захисту або комплексної безпеки, яка базується на всеохоплюючій участі державних інституцій, приватного сектору та громадянського суспільства з акцентом на цивільну готовність і стійкість. У Фінляндії концепція закріплена в стратегічних документах і передбачає системне планування дій у надзвичайних ситуаціях, підтримку стратегічних резервів, розвиток місцевих мереж реагування та тісну взаємодію між адміністративними структурами, громадами й добровільними формуваннями, зокрема через навчальні програми для населення та розвиток територіальної оборони [5]. У Швеції нова Стратегія оборони на 2025–2030 роки передбачає інвестиції близько 170 млрд шведських крон у військову сферу та 37,5 млрд шведських крон у цивільну оборону, модернізацію арсеналу й оборонної інфраструктури, збільшення призовників, посилення кібер- та інформаційної безпеки, а також інтеграцію добровольчих організацій і підготовчих програм для молоді, спрямованих на набуття навичок виживання та першої допомоги.

Український досвід 2022–2025 років демонструє унікальні підходи до адаптивної оборони: масове застосування безпілотників трансформувало розвідку, корекцію вогню та логістику, волонтерські мережі забезпечили ефективну мобілізаційну та логістичну підтримку фронту, територіальна оборона зміцнила тилові рубежі, а цифровізація управлінських процесів із використанням ШІ та великі дані (Big Data) підвищила координацію між військовими та цивільними структурам. Водночас зберігаються системні виклики: дублювання функцій між відомствами знижує ефективність координації, існують ризики корупції в закупівлях і логістиці, а швидка цифровізація створює загрози кібербезпеці й алгоритмічним ризикам, що потребує запровадження стандартів кіберзахисту, незалежного аудиту і прозорих політик управління даними. Таким чином, модернізація українського сектору безпеки вимагає інтегрованого підходу, що поєднує технологічні інновації (БПЛА, цифровізація), розвиток територіальної оборони та волонтерських мереж із інституційними реформами, спрямованими на підвищення координації, підзвітності та кіберстійкості, створюючи умови для формування стійкої, гнучкої та технологічно спроможної системи національної безпеки [7].

Аналіз міжнародного та українського досвіду свідчить, що підвищення обороноздатності держави в сучасних умовах неможливе без комплексного підходу, який поєднує технологічні інновації, інституційну зрілість, суспільну участь та інтеграцію у міжнародні системи безпеки. Для України це означає необхідність одночасного розвитку сучасних оборонних технологій (БПЛА,

кіберзахист, ШІ), удосконалення координації між складовими сектору безпеки, посилення цивільного контролю, формування культури національної безпеки та активної участі громадян, а також поглиблення взаємосумісності із стандартами НАТО та ЄС. Такий інтегративний підхід забезпечує формування стійкої, гнучкої та технологічно спроможної системи, здатної ефективно протидіяти багатовимірним загрозам сучасної війни.

Список використаних джерел:

1. NATO. Comprehensive Defence Planning Process. URL: https://www.nato.int/cps/en/natolive/topics_49202.htm (accessed: 08.11.2025)
2. NATO. Comprehensive Assistance Package for Ukraine. URL: https://www.nato.int/cps/en/natolive/topics_231639.htm (accessed: 08.11.2025)
3. U.S. Government Accountability Office (GAO). (2024). FY 2023 Financial Statement Audit Progress and Challenges. URL: https://www.gao.gov/products/gao-24-107478 (accessed: 08.11.2025)
4. Israel’s defence industry: adaptation and growth in a changing arms market. ResearchGate. 2024. URL: https://www.researchgate.net/publication/389872609_Israel%27s_defence_industry_adaptation_and_growth_in_a_changing_arms_market (accessed: 02.11.2025)
5. Finland's Comprehensive Security Strategy. URL: https://www.government.fi/en/policies/comprehensive-security (accessed: 08.11.2025)
6. Israel's Iron Beam High-Energy Laser Weapon System. URL: https://www.rafael.co.il/system/iron-beam/
7. Ukraine's Army of Drones Initiative. URL: https://www.ukrainianworldcongress.org/united24/ (accessed: 02.11.2025)