

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Сучасна епоха відзначається глобалізаційними процесами, які передусім охоплюють інформаційну сферу. Ми живемо в інформаційному суспільстві, де поширення чи обмеження інформації, її змісту характеризують ступінь розвитку демократичних інститутів і процесів. Теза «хто володіє інформацією, той володіє світом» набула реального змісту у зв'язку із запровадженням новітніх інформаційних технологій, тому проблеми, що характеризують різні аспекти інформаційної діяльності, мають особливе як теоретичне, так і практичне значення.

У будь-якій інтерпретації поняття «безпека» пов'язане з умовами існування певного об'єкта. У залежності від складу об'єкта (особи, суспільства або держави, що є об'єктом загрози) ми можемо визначити міжнародну безпеку (безпеку багатьох держав), безпеку окремої держави, особисту безпеку та суспільну безпеку (безпеку невизначеного кола осіб) [1].

Для держави, усіх соціальних систем забезпечення безпеки є складним компромісом при вирішенні низки проблем, зокрема політичних, економічних, соціальних, воєнних, екологічних тощо. Їх вирішення потребує не тільки відповідних ресурсів і кількісних характеристик ймовірних загроз, а й визначення граничних значень їх існування. Система забезпечення національної безпеки (СЗНБ) передбачає систему моніторингу, збору, оброблення та аналізу інформації у різних сферах національної безпеки.

Чи не найбільшою проблемою національної безпеки нашої держави, **по-перше**, є її демографічний складник. Три голодомори 1921–1922, 1932–1933, 1946–1947 рр. – забрали життя до 15 млн українців, а під час Другої світової війни в окупованій Україні було знищено ще понад 5 млн цивільного населення та військовополонених [2, с. 55].

На сьогодні, за доповіддю ЦРУ під назвою «Міжнародна книга фактів» до ТОП-10 держав світу з найвищою смертністю населення віднесено й Україну, яка посідає восьме місце. Кількість смертей на 1 тис. осіб в Україні становить 15 осіб, і це перше місце в Європі.

Другим важливим індикатором національної безпеки згідно з Законом України «Про оборону України» є обороноздатність держави – як здатність держави до захисту в разі збройної агресії або збройного конфлікту.

Відповідно до редакції Закону «Про оборону України», що була чинна до 2008 р., потреби національної оборони держави мали фінансування

в розмірі не менше 3 % від запланованого обсягу валового внутрішнього продукту (ВВП). На жаль, за роки незалежності обсяг фінансування Збройних сил України (ЗСУ) в середньому не досягав і половини від цієї суми. Лівова частка державного ресурсу спрямовувалась на утримання ЗСУ, а не на їх розвиток. Це призвело до того, що минулі роки, за часів минулої влади, стали періодом подальшої деградації українського війська. Наслідок – рівень боєздатності та бойової готовності, наявне озброєння і військова техніка української армії на період агресії Росії до Криму і на сході України не відповідали сучасним вимогам. А належна інформація з цих питань практично була відсутня.

Передовий досвід рівня видатків на національну оборону у відсотках до ВВП є важливим показником обороноздатності держави. Нині нормою асигнувань на оборону в країнах НАТО є 2,2–2,5 % від ВВП. Наприклад у 2010 р він становив: у Франції – 2,3 %, Великій Британії – 2,7 %, США – 4,8 % ВВП. В абсолютних цифрах у середньому не менше 15 тис. дол. США на військовослужбовця на рік. У Польщі – 20 тис. дол. США.

Бідність і соціальна нерівність в Україні привела народ до Майдану в Києві і по всій Україні. Різниця в доходах 10 % найбагатших сімей і 10 % найбідніших не має перевищувати 10-разовий показник [2, с. 61]. Початок процесу стрімкої диференціації доходів населення України на 1990-ті роки і досяг критичної межі за часів попередньої влади Януковича та Азарова. За офіційними даними Державної служби статистики України найбільш забезпечені 10 % населення отримали у 5,7 разів більше грошових доходів, ніж 10 % найменш забезпечених. На думку автора, цей показник є значно заниженим.

Третім фактором національної безпеки є проблема тінізації економіки України, що стало причиною революції гідності на майданах всієї України з листопада 2013 року. За різними оцінками рівень тінізації становить у розвинених країнах – 8 % від ВВП, у країнах з перехідною економікою – близько 20 % від ВВП. За офіційними даними, в Україні спостерігається високий рівень тінізації економіки – 39 % від ВВП на початку 2011 року. Ці дані, на думку автора, також суттєво занижені.

Тіньова економіка має значний негативний вплив на всі соціально-економічні процеси, що відбуваються в суспільстві. В останні роки попередня влада навіть ухвалювала українські та законодавчі рішення з урахуванням тіньової економіки, що гальмують соціально-економічні реформи.

Четвертим фактором національної безпеки є рівень розвитку науки. «Критичний рівень.

який необхідний для виживання науки в Україні. – 0,9 % ВВП, тільки після цього порогу починається економічний ефект від науки», – наголосила голова парламентського Комітету з питань освіти й науки, народний депутат Лія Григнєвич [2, с. 62]. Проте в 2012 р. влада виділила на науку з бюджету найменшу кількість коштів за всі роки незалежності, а саме – 0,25 % ВВП, що призвели до суттєвого скорочення фінансування науковців і освіти, які очолили коженні маніфестації та Євромайдани в Києві і в регіонах України в 2013–2014 навчальному році.

П'ятим фактором національної безпеки слід вважати рівень витрат на природоохоронні заходи. Україна – одна з найбільших за територією, чисельністю населення та економічним потенціалом держав Європи.

На її території зосереджені дуже великі природні багатства, але суто колонізаторський підхід і безгосподарність призвели не тільки до порушення, а й до руйнування природних ландшафтів. Сучасні масштаби економічних змін створили реальну загрозу життю та здоров'ю громадян України й національній безпеці.

Відсутність належної інформації призвела до сучасного накопичення промислових відходів в Україні – 35 млрд т, а це найбільші обсяги відходів у ЄС. Капіталовкладення на природоохоронні заходи не мають бути меншими за 8–10 % ВВП, а для країн з напруженою екологічною ситуацією (до яких, до речі, відноситься й Україна) – навіть вище: до 12–15 % ВВП. Проте природоохоронні витрати в Україні за останні роки склали близько 0,6 % ВВП [2, с. 68].

Очевидно, що сучасний екологічний і соціально-економічний фактор України визначає гостру актуальність постійної уваги з боку держави до забезпечення її екологічної та природно-техногенної безпеки. Слід зауважити, що діяльність Міністерства та Міністерства праці і соціальної політики сьогодні розділені, а стала держава – це та, в якій відходи не накопичуються, а безпосередньо перетворюються.

Наступним, **шостим фактором** національної безпеки слід вважати соціально-політичні небезпеки, які за характером походження можна поділити на:

- а) політичні (терористичні акти, масові заворушення, страйки, війни та збройні конфлікти та ін.);
- б) соціальні (алкоголізм, наркоманія, злочинність тощо);
- в) комбіновані (небезпеки в соціально-економічній сфері, природно-техногенні небезпеки та небезпеки в інформаційній сфері) [3, с.169].

З точки зору безпеки життєдіяльності будь-які конфлікти можуть об'єднувати небезпечні і шкідливі фактори, які властиві майже всім стихійним лихам чи техногенним катастрофам. Та найбільшою національною небезпекою для людства, населення України і довкілля в наш час є війна.

Війна, яка відбувається на сході України викликає масове зниження кількості людей і руйнування державних закладів, мостів, заводів, шахт і всієї інфраструктури. Сепаратисти, терористи та російські найкращі війська під прапорами ДНР та ЛНР проти місцевого населення і збройних військ АТО використовують артилерійські снаряди, ракети, міни, торпеди, мають сучасну високоточну зброю «Град», безпілотні літаючі апарати.

Терористи ДНР і ЛНР захоплюють у заручники місцеве населення, застосовуючи підпали, вбивства, тортури, залякують населення і органи влади. Попередня влада Януковича та Азарова застосовувала електромагнітний тероризм під час страйку на Майдані в Києві. Застосовуючи малогабаритні електромагнітні генератори потужністю 200–800 млн Вт, створювали могутній електромагнітний імпульс, що вразливо впливав на всі електронні елементи інфраструктури – від комп'ютера до автомобіля зв'язку.

Інформаційно-психологічний вплив використовують як державна влада деяких країн, так і терористи. Наприклад, Президент Росії В. Путін деінформував усю світову громадськість, заявляючи про те, що в Криму російських військ немає, а «зелені» чоловічки – це внутрішні сепаратисти Криму, які просять нашої допомоги, і яким він допоможе загарбав Крим. Тепер зізнається, що в Криму російські війська дійсно були, а на сході України їх немає. Хоча військові заручники, російські танки та високоточне обладнання з Росії свідчить про інше.

Людям, чий близькі або знайомі опинилися в руках терористів, необхідно відразу звернутися до компетентних органів. Якщо ви потрапили до числа тих, хто звільняється, то повинні максимально допомогти тим, хто залишається у терористів, перш за все повідомити: число терористів, в якій частині будівлі вони знаходяться, їх озброєння, число заручників, де вони знаходяться, фізичний стан терористів, особливості їх поведінки, хто головний у групі.

Національна безпека України в глобальному контексті більш чітко окреслена в Законі України «Про основи національної безпеки» та наукових підручниках і статтях С. Ковжого, О. Малько, А. Пролєжаєв, Л. Наладовської та інших авторів [3, 4, 5].

Таким чином, аналіз останніх досліджень і публікацій свідчить, що всім вище наведеним складовим національної безпеки не дістає належної інформаційної безпеки.

З огляду на висловлене, **метою написання статті** є аналіз сучасного стану інформаційної безпеки в Україні та у світі, особливо в період військових дій, та обґрунтування основних завдань забезпечення інформаційної безпеки людини, військ та держави із застосуванням новітніх безпілотних літальних апаратів з урахуванням сучасних викликів та загроз.

Інформаційна революція, до речі, стала джерелом найтривалішого економічного зростання в історії США. Інформаційна епоха справляє свій вплив не тільки на економіку держави, а й на види цілей та їх озброєнь [6, с. 38].

Новітні комунікаційні й комп'ютерні інформаційні технології зумовлюють розвиток мереж у три найважливіші способи:

а) по-перше, новітні технології значно скорочують час проходження сигналу, даючи змогу розпорощеним організаціям підтримувати зв'язок і координувати дії;

б) по-друге, інформаційні технології значно скорочують вартість зв'язку, забезпечуючи життєздатність військовим підрозділам, що потребують постійного інтенсивного обміну інформацією – таких як військові підрозділи АТО на сході України;

в) по-третє, новітні технології значно розширили різноманітність видів інформації, що передається, та підвищили її складність – завдяки інтеграції комунікаційних комп'ютерних технологій на прикладі застосування безпілотних літальних апаратів.

Особливістю сучасної збройної боротьби іноземні фахівці та військовослужбовці України, які сьогодні воюють на сході України, вважають інтегрований підхід до ведення інформаційної розвідки, передачі даних, управління військами й зброєю, вогневого ураження противника у часі, наближеному до реального.

Фахівці вважають, що в сучасній бойовій обстановці безпілотні літальні апарати здатні більш ефективно й оперативніше, ніж пілотовані літаки, вирішувати завдання тактичної повітряної розвідки і коректування вогню бойового управління й зв'язку сил АТО.

Середня вартість літака неухильно зростає від покоління до покоління. Так, наприклад, вартість одного американського літака А-4 становила у 1997 р. 6 млн дол. США. Вартість літаків МІГ-29 і F-16 в межах 22–28 млн, літаків СУ – 30 млн, F-15, F-18 – від 25 до 37 млн дол. США, а найбільш коштовний літак-винищувач F-22A Raptor – 177 млн дол. США. Крім того, для підготовки льотчика до певного рівня майстерності потрібен щорічний наліт упродовж декількох років не менше 100–120 год на літаку і близько 200 год на тренажері.

Іншим найбільш ефективним шляхом отримання інформації розвідки та підвищення економічної ефективності авіації вважається, є поступова відмова від пілотованої авіації і перехід до використання безпілотних літальних апаратів (БПЛА). «Хоча розвідка не гарантує успіх у бою, її відсутність може привести до поразки», – наголосив військовий фахівець Д. Гланц [7, с. 67]. Одні з перших відчували необхідність застосування розвідувальних БПЛА тактичного рівня ізраїльські війська, котрі таємно закупили в США 12 БПЛА Firebee Model 7241

(ізраїльська назва «МАБАТ») і на базі яких була створена перша ескадрилья БПЛА.

Цікавий той факт, що початок власних розвідувальних БПЛА в Ізраїлі був покладений у гаражі одного з ентузіастів та отримав назву Mastiff: це невеликий за розмірами БПЛА, оснащений телекамерою. А у 1978 році в Ізраїлі було розроблено ще один БПЛА-Scout.

На відміну від російських військових (які створили модифікацію БПЛА «Пчела-1Т», «ПчелаПМ»), значно активніше застосовували тактичні БПЛА збройні сили США, провідні країн НАТО та Ізраїль. Так в США БПЛА Pioneer вагою від 40 до 190 кг та розмаху крил 5,15 м забезпечував інформацію американським військам на глибину до 90 км з території Саудівської Аравії під час операції «Буря в пустелі» в 1991 р. Більш сучасні БПЛА, створені в США – це Predator, Global Hawk RQ-4A, які пройшли випробування в Югославії та Афганістані.

На основі досвіду застосування безпілотних літальних об'єктів, узагальнених зібраних даних щодо існуючих БПЛА, аналізу їх основних характеристик, таких, як зміна ваги, тривалість польоту, максимальна висота та радіус дії, встановлено, що найбільш затребуваним є БПЛА оперативного-тактичного рівня зі змінною вагою близько 200 кг, тривалістю польоту до 5 годин, можливістю ведення розвідки з малих і середніх висот (100–5000 м) на глибину до 300 км.

Серед БПЛА іноземного виробництва, які успішно зарекомендували себе під час збройних конфліктів і характеристики яких підпадають під визначені вище вимоги: ізраїльські безпілотники оперативного-тактичного класу Searcher II і Hermes 450, БПЛА ближньої розвідки з радіусом дії 5–10 км типу Skylark, Skylark II, Seagull [4, с. 152].

Сьогодні в Україні розроблені і проходять випробування вітчизняні БПЛА під час збройного конфлікту з російськими найманцями на сході України. Одночасно для створення сучасної армії в Україні слід добре володіти світовими тенденціями перспектив розвитку безпілотної авіації та подальші зміни в розвитку збройної боротьби, які свідчать про те, що в перспективі людство перейде в епоху воїнського покоління. Основними рисами збройної боротьби може стати перенесення основних зусиль у космічний простір, де широкое застосування космічних розвідувальних, навігаційних та ударних систем по супротивнику; поява роботизованої бойової техніки, поступове витіснення людини з поля бою; поява інтелектуального, інформаційного й інших видів несмертельної зброї, що наведено на рис. 1 [4, с. 169].

Ці війни будуть мати широкий просторовий розмах, удари можуть наноситись одночасно з усіх можливих напрямків театру воєнних дій по всій території супротивника практично без обмежень.

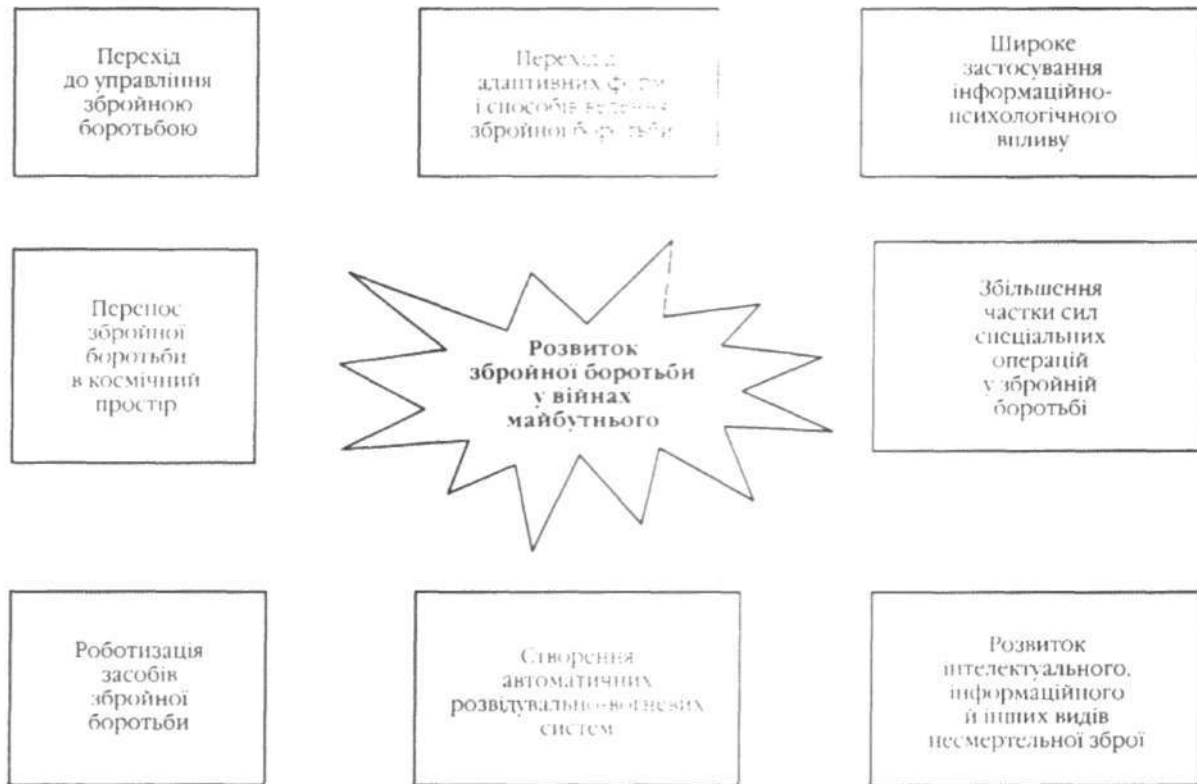


Рис. 1. Напрямок подальшого розвитку збройної боротьби у війнах майбутнього

Метою війни стане не фізичне знищення ворога, а його внутрішній розрив, підрив морального середовища населення противника й послідовне знищення культурного середовища його проживання. Війна може вестися одночасно по всій території країни, проти якої здійснюється агресія. За деякими оцінками американських експертів до 2025-го року 90 % усіх бойових літаків можуть стати безпілотними.

У цілому, на думку автора й експертних прогнозів, у зв'язку з наростанням регіональних загроз, територіальних суперечок і виконанням планів з модернізації збройних сил попит на БПЛА щорічно зростатиме для отримання своєчасної інформаційної розвідки.

Отже, основними напрямами державної політики з питань національної безпеки в інформаційній сфері слід вважати:

1. Забезпечення інформованості населення та військ АТО, і на цій основі його довіри до влади.
2. Забезпечення прозорості діяльності державних органів та прийняття управлінських рішень.
3. Однією з обов'язкових вимог до країн-кандидатів на приєднання до ЄС є створення умов для побудови інформаційного суспільства, і в першу чергу розроблення та впровадження новітніх вітчизняних конкурентоспроможних інформаційно-комунікаційних технологій в усі сфери суспільного життя, зокрема в «інформаційну безпеку», з урахуванням нових загроз для України.

Література

1. Корнич Б. А. Організаційно-правові засади політико-інформаційної безпеки України: Монографія. – Одеса: Юридична література, 2003. – 472 с.
2. Качинський А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень. Монографія. – К.: НІСД, 2013. – 104 с.
3. Ковжог С. О., Малько О. Д., Полежаєв А. М. Безпека життєдіяльності: навч. посібник. – Х.: Право, 2014. – 304 с.
4. Закон України «Про основи національної безпеки» від 19.07.2003 № 964-IV. – К.: 2005. – 14 с.
5. Паников А. П., Нападовська Л. В. Національна безпека України у глобальному контексті // Безпека життєдіяльності. – 2009. – № 4. – С. 4–9.
6. Мережі і мережні війни: майбутнє терору, злочинності та бойових дій / За ред. Дж. Арквіллі, Д. Монфельдта: Пер. з англ. А. Ішенка. – К.: Вид. дім «Києво-Могилянська Академія», 2005. – 350 с.
7. Застосування безпілотних літальних апаратів у воєнних конфліктах / О. О. Горошко, Ю. К. Зіатдінов, О. А. Льяшов та ін. – К.: Вид. дім «Києво-Могилянська Академія», 2013. – 248 с.

А. П. Пашков,
доцент кафедри екології факультету природничих наук Національного університету «Києво-Могилянська Академія»,
академік Міжнародної академії безпеки життєдіяльності