НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
імені ІВАНА ЧЕРНЯХОВСЬКОГО

ГІБРИДНА АГРЕСІЯ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ: ДОСВІД ПРОТИДІЇ УКРАЇНИ, НАСЛІДКИ ДЛЯ ЄВРОПИ

Збірник матеріалів
міжнародної науково-практичної конференції
(Національний університет оборони України імені Івана Черняховського
17 листопада 2021 р. м. Київ)

Видання університету – 2022

УДК [355.45.02:005.21](477)

Укладачі: Корецький А.А., к.військ.н., с.н.с.
Семененко В.М., к.т.н., с.н.с.
Возняк С.М., к.т.н., с.н.с.
Черевко Р.М. д.ф.
Демешок О.О., к.е.н., доц.

Гібридна агресія Російської Федерації: досвід протидії України, наслідки для Європи: збірник матеріалів міжнародної науково-практичної конференції (Національний університет оборони України імені Івана Черняховського 17 листопада 2021 року м. Київ). – К.: НУОУ, 2022. – 227 с.

Збірник містить матеріали міжнародної науково-практичної конференції “Гібридна агресія Російської Федерації: досвід протидії України, наслідки для Європи”, яка була проведена 17 листопада 2021 року у Національному університеті оборони України імені Івана Черняховського.

Видання може бути корисним для наукових та науково-педагогічних працівників наукових установ, закладів вищої освіти, представників органів державної влади, недержавних організацій сектору безпеки і обороніУкраїни.

У випадку використання інформації, викладеної у збірнику, посилання на матеріали науково-практичної конференції обов’язкове.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

САЛКУЦАН Сергій Миколайович	Заступник начальника університету з навчальної роботи, к.військ.н., доцент, генерал майор
ДОБРОГУРСЬКИЙ Валерій Іванович	Заступник начальника університету, к.військ.н., полковник
ПАВЛІКОВСЬКИЙ Анатолій Казимирович	Начальник Центру воєнно-стратегічних досліджень, к.військ.н., доцент, полковник
КОРЕЦЬКИЙ Андрій Анатолійович	Заступник начальника Центру воєнно-стратегічних досліджень з наукової роботи, к.військ.н., с.н.с, полковник
БИЧЕНКОВ Василь Васильович	Заступник начальника Центру воєнно-стратегічних досліджень, д.т.н., с.н.с, полковник
ТИЩЕНКО Максим Георгійович	Начальник центру, к.т.н., підполковник
УШАКОВ Андрій Сергійович	Заступник начальника адміністративного управління, підполковник
СЕМЕНЕНКО В'ячеслав Михайлович	Заступник начальника Центру воєнно-стратегічних досліджень – начальник управління, к.т.н., с.н.с, полковник
ТКАЧЕНКО Володимир Анатолійович	Заступник начальника управління – начальник відділу Центру воєнно-стратегічних досліджень, к.військ.н., полковник
ФЕДЯНОВИЧ Дмитро Леонідович	Начальник відділу Центру воєнно-стратегічних досліджень, к.військ.н., с.н.с, полковник
ВОЗНЯК Степан Миколайович	Начальник відділу Центру воєнно-стратегічних досліджень, к.т.н., с.н.с, полковник
ФУЧКО Андрій Йосипович	Начальник відділу Центру воєнно-стратегічних досліджень, полковник
МУДРАК Юрій Миколайович	Начальник відділу Центру воєнно-стратегічних досліджень, полковник

ЗМІСТ

ВСТУП

Укладений у 2021 році Меморандум про співробітництво між Національним університетом оборони України імені Івана Черняховського та Коледжем університету оборони Норвегії заклав правові засади та відкрив нові можливості для започаткування наукової співпраці між провідними військовими навчальними закладами України та Норвегії.

Першим широкоформатним публічним заходом цієї співпраці стала міжнародна науково-практична конференція "Гібридна агресія Російської Федерації: досвід протидії України, наслідки для Європи", яка відбулась 17 листопада 2021 року у Національному університеті оборони України імені Івана Черняховського. Співорганізаторами конференції були Національний університет оборони України імені Івана Черняховського, Коледж університету оборони Норвегії та Інститут Джефферсона (США).

Конференція фактично дала старт для українсько-норвезького дослідницького проєкту "Україна і тотальна оборона".

Крім членів дослідницької проєктної групи – вчених Національного університету оборони України імені Івана Черняховського та Коледжу університету оборони Норвегії, у заході взяли участь співробітники Центрального науково-дослідного інституту Збройних Сил України, представники посольств держав – членів НАТО, Управління цивільно-військового співробітництва Генерального штабу Збройних Сил України, а також завідувач відділу історії України періоду Другої світової війни Інституту історії України НАН України Олександр Лисенко, політолог, історик, журналіст, директор Інституту світової політики Євген Магда, кінорежисерка, керівник громадської організації "Новий Донбас" Лариса Артюгіна, журналісти, аналітики, соціологи, представники громадської організації "International Center for Countering Russian Propaganda" Юрій Кочевенко, Валентина Бикова, Дмитро Громаков, Полянська Сніжана.

В ході конференції відбувся обмін результатами досліджень та експертними думками з актуальних проблем протидії України гібридній агресії Російської Федерації. Науковці та експерти мали можливість обговорити такі питання, як: російський вплив в Україні, військово-патріотичні організації та боротьба за ідентичність; військова освіта у розширеній реальності; російські підходи до ведення війни на суходолі, у повітрі, на морі та в інформаційній сфері.

До збірника матеріалів конференції увійшли матеріали доповідей, зроблених учасниками на пленарному засіданні та дискусійних панелях конференції.

Організатори конференції вдячні всім учасникам за активну роботу і сподіваються, що в подальшому щорічно у листопаді ми будемо проводити подібні зустрічі в стінах Національного університету оборони України імені Івана Черняховського з метою обговорення проблемних питань протидії агресії Російської Федерації.

Особливу вдячність висловлюємо директору Інституту Джефферсона (США) Аарону Преснелу, керівнику українсько-норвезького проекту “Україна і тотальна оборона” Тому Рьоссету, колегам з Норвегії за участь в організації конференції, цікаве для всіх учасників її змістовне наповнення та фінансово-матеріальну підтримку.

Матеріали науково-практичної конференції будуть корисними для наукових та науково-педагогічних працівників наукових установ, закладів вищої освіти, представників органів державної влади, недержавних організацій сектору безпеки і обороніУкраїни.

У випадку використання інформації, викладеної у збірнику, посилання на матеріали науково-практичної конференції обов’язкове.

Гібридна війна як форма глобального протистояння. Досвід України у протидії їй

Павло Грицай, кандидат військових наук, старший науковий співробітник
Начальник кафедри Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-1181-4523
Василь Телелим, доктор військових наук, професор, заслужений діяч науки і техніки України
Професор Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-5926-7680

Анотація. *В доповіді аналізуються витоки гібридної війни Російської Федерації проти України та заходи щодо протидії їй на початковому етапі та у сучасних умовах.*

Ключові слова: *гібридна війна, загроза, агресія.*

Вступ

Постановка проблеми. Сучасні воєнні конфлікти характеризуються появою нових форм і методів збройної боротьби. Збройна агресія Російської Федерації, яка мала прихований характер свого початку і проводилась в переважній більшості в політичні, економічній, соціальній, інформаційних сферах перейшла в гібридну війну проти України із прихованим залученням регулярних підрозділів.

Аналіз останніх досліджень та публікацій. Вивченню питань ведення гібридних війн присвячена велика кількість не лише наукових, а й художніх видань. В той же час, у роботах [1-8] приділена значна увага початку, веденню, а також досвід у протидії гібридній війні Російської Федерації проти України.

Мета доповіді. Метою доповіді є розгляд особливостей початку ведення Російською Федерацією гібридної війни проти України та досвіду отриманого в ході ведення антитерористичної операції та операції Об'єднаних Сил.

Виклад основного матеріалу

Тимчасова окупація півострову Крим та території Донбасу Російською Федерацією (РФ) сигналізувала початок нової ери у міжнародних відносинах, яку можемо означити як час "гарячої фази" "гібридної" війни, найбільш серйозною і цинічною агресією проти демократичних цінностей і міжнародного права, а на даний час ще й створення РФ міграційної кризи.

Загалом, оцінюючи події, які сьогодні прийнято називати "гібридною" війною РФ, враховуючи всі можливі чинники, що передували їй, стає можливим умовно виділити в її розвитку три основні фази: інноваційну, холодну та гарячу.

Однією з найбільших проблем України за часи незалежності, що передували відкритій агресії Росії, було те, що в зовнішньополітичній доктрині РФ ніколи не вважалася потенційним ворогом, який може здійснити ворожі дії по відношенню до України, я не говорю вже про військове вторгнення.

В той же час, саме РФ активно впливала на зовнішню політику України, намагаючись втягнути її у свою орбіту впливу, або, як мінімум, стримати від співпраці з країнами Заходу. На законодавчому рівні це вилилося в політику позаблоковості України.

Нажаль, незважаючи на "енергетичні" та "економічні" війни, включаючи торгові, фінансові та інші інструменти, на фактичну відмову від виплати повної вартості переданої Росії Україною ядерної зброї, небажання делімітації державного кордону між Росією та Україною не лише на його морських, але й на сухопутних ділянках, агресивну експансію російської культури, захват російським та проросійським бізнесом медіапростору України, підривну антиукраїнську і виключно проросійську діяльність УПЦ (МП) керівництво держави і значною мірою і населення по інерції продовжували вважати Росію гарантом незалежності і територіальної цілісності України.

Відповідно, про серйозну протидію "гібридним" загрозам Україні з боку РФ ніхто і не думав, та і в якості загроз безпеці держави це, нажаль, не сприймалось.

Деякі сумніви виникли після спроби РФ, так би мовити "легітимним" шляхом відокремити Крим від України і приєднати його до Росії. Ці спроби, завдяки енергійним, рішучим і своєчасно вжитим заходам, потерпіли фіаско. Але і тоді, протидія була досить виваженою, обережною, і обмежилась головним чином політичною та дипломатичною сферами.

Нажаль, повного розумінні "гібридності" або підступності задумів російського керівництва не наступило навіть після абсолютно неочікуваного інциденту зі спробою, нібито ніким не санкціонованого, захоплення українського острова Коса Тузла в Керченській протоці.

Воєнно-політичне керівництво України і тоді, в силу різних причин, прийняло рішення ситуацію до стану конфронтації із РФ не загострювати.

Водночас, варто зазначити, що і в цьому випадку протидія носила виключно ситуаційний і фрагментарний характер, а РФ в якості можливого військового противника, як і раніше, не розглядалась.

І лише відкрита окупація Криму, введення російських військ на територію України на Донбасі, намагання відокремити її східні та південні регіони, а з його провалом - утворення маріонеткових республік, формування та всебічне оснащення на їх території двох армійських корпусів Південного ВО ЗС РФ, розв'язання російськими військами та їх найманцями на сході України фактично відкритої форми збройної боротьби, яка може перейти в офіційний міждержавний збройний конфлікт та постійна загроза широкомасштабної агресії з декількох напрямків примусило керівництво України переглянути ці сподівання.

Перед Україною постав виклик знайти способи протидії "гібридній" агресії, яка мала на меті не тільки знищити Україну як державу, але й

дестабілізувати усю систему міжнародних відносин, і міжнародного права зокрема.

В момент фактичного початку РФ “гарячої” фази “гібридної” війни проти України реальний стан справ був загрозливим: боєздатність Збройних Сил через “перманентне” реформування була катастрофічно низькою, нове керівництво держави спочатку незрозуміло, як протидіяти такому безпрецедентному захопленню території суверенної держави, зокрема в контексті неоднозначної реакції міжнародної спільноти.

Згодом, реанімовані неймовірними зусиллями нового військово-політичного керівництва, добровольців, волонтерів, усього українського народу Збройні Сили України, в ході проведення антитерористичної операції, здійснюючи протидію “гібридним” загрозам Україні з боку РФ військовими засобами повною мірою, у всіх можливих формах, дозволених міжнародним правом війни, локалізували незаконні збройні формування. Створились умови для повної ліквідації конфлікту. В цей час Росія вводить на територію Донбасу формування своїх регулярних військ. Так, армія, не зважаючи на понесені втрати, вистояла, але конфлікт став довготривалим і загрожує перерости у міждержавний.

Безумовно, найбільш помітними стали заходи у військовій сфері, а саме: проведення мобілізації, зміцнення боєздатності держави, налагодження співпраці у військовій сфері з міжнародними партнерами, відновлення військової промисловості, співпраця з НАТО.

З подальшим усвідомленням феномену “гібридної” війни, а також її масштабів і вимірів виникла потреба вжити ряд заходів, які б допомогли нейтралізувати загрози і мінімізувати негативні наслідки агресії для України.

Серед них скасування позаблокового статусу України, введення економічних санкцій проти ряду підприємств та фізичних осіб РФ, у тому числі і в оборонній сфері, вжиття заходів активної протидії російській інформаційній агресії та пропаганді.

Крім того, не менш важливими подіями у протидії “гібридній” агресії РФ стали підписання Україною угоди про асоціацію з ЄС, активна співпраця України з НАТО, зокрема отримання статусу “країни-аспіранта”, робота щодо надання Україні збройної та не збройної допомоги від країн-партнерів, відмова від споживання російського газу, виграш України у Стокгольмському арбітражі щодо газових контрактів, тощо.

Окремою складовою протидії московській агресії є зустрічі у мінському та нормандському форматах. Ефективність мінського формату в сучасних умовах – то окрема тема.

Загалом, протидія України “гібридним” загрозам та “гібридній” агресії, яку здійснює РФ, являє собою комплекс заходів, які охоплюють усі сфери життєдіяльності країни. Серед них, основними вважаю, визначення та чітке дотримання суверенного зовнішньополітичного курсу щодо захисту національних інтересів; ведення активної міжнародної співпраці по питаннях безпеки та боротьба з проявами пацифізму у власному політичному середовищі; активізація прийняття політичних рішень міжнародних організацій, форумів,

конференцій щодо протидії “гібридним” війнам; удосконалення законодавчої бази з питань оборони держави; вступ держави до систем колективного захисту; розробка та впровадження дієвих Програм розвитку ЗС України з урахуванням перспективних напрямків розвитку інноваційних засобів збройної боротьби; проведення адміністративно-територіальної реформи, на базі якої створити дієву систему територіальної оборони держави, тощо.

В боротьбі з агресором за незалежність і територіальну цілісність України викристалізувалась мета протидії “гібридній” російській агресії як недопущення руйнування політичної системи України; захист її суверенітету і територіальної цілісності, забезпечення економічної та інформаційної безпеки країни; виявлення правдивої мети конфлікту і способів її досягнення; розкриття для міжнародної спільноти форм боротьби у “гібридній” війні.

Стосовно ж завдань протидії, то основними з них, на наш погляд, можна відмітити, насамперед, підвищення ефективності протидії міжнародного законодавства різним видам “гібридної” війни, необхідність визначитись з союзниками та партнерами, заключити з ними відповідні політичні угоди, що мають юридичну силу; стати членом Євроатлантичної колективної системи безпеки; досягнути оперативної і технічної сумісності ЗСУ зі збройними силами країн-партнерів; створити цілісну систему територіальної оборони; прийняти дієву нормативно-правову базу з питань підготовки держави до оборони; протидіяти впливу противника в інформаційному просторі держави; прийняти необхідні законодавчі акти щодо посиленого розвитку ОПК держави та її сфери національної безпеки і оборони, тощо.

У енергетичному протистоянні з РФ особливої уваги заслуговують відмова від “московського” газу, диверсифікація поставок газу, протидія створенню газогону “Північний потік-2”).

Вкрай важливими є законодавчі зміни, як, наприклад, відмова від позаблокового статусу, визнання РФ агресором і відповідальною за людські, матеріальні та фінансові втрати України, кардинальна зміна зовнішньополітичних пріоритетів, в яких раніше РФ ніколи не розглядалася як потенційний агресор.

Сучасна ситуація у світі, і зокрема, очевидне застосування РФ методів “гібридної” війни щодо країн Заходу, в тому числі газовий шантаж через запуск “Північного потоку-2”, організована Кремлем так звана “міграційна криза” на білорусько-польському кордоні, погрози поширення її на кордони України та країн Балтії, розміщення в західній частині Білорусі російських ракетних комплексів “Іскандер”, тощо, дає можливість прогнозувати подальшу дестабілізацію і необхідність активної мобілізації зусиль.

Висновки

Варто зазначити, що із досвіду протидії України військовими засобами “гібридній” війні Росії ЗС України зробили серйозні уроки. Серед них необхідність, ще тільки з появою вже перших ознак “гібридних” загроз, а ще краще – у превентивному порядку, реагувати на них. При цьому, форми і способи реагування на загрози також мають бути “гібридними”. Це – аксіома!

З іншого боку, очевидно, що зусилля агресора цілеспрямовані на знищення єдності партнерів України у протистоянні “гібридній” агресії, дестабілізації ситуації у Європі, зокрема, відвернення уваги від українського питання діями у Сирії, а також на пошук нових механізмів впливу задля відтворення Російської імперії. У цьому контексті потрібні об’єднані зусилля усього цивілізованого світу, водночас із розробкою комплексної системи протидії “гібридній” агресії.

Список літератури

1. Основи воєнної безпеки держави: підручник / Пунда Ю.В., Грищенко В.П., Грицай П.М. та ін. – К.: НУОУ ім. Івана Черняховського, 2017. –204 с.
2. Світова гібридна війна: український фронт. Монографія / За загальною редакцією В.П. Горбуліна. – К.: НІСД, 2017. – 496с.
3. Війна на Донбасі: реалії і перспективи врегулювання. – К.: Центр Разумкова, 2019. – 144с.
4. До 5-річчя від початку збройної агресії Російської Федерації проти України. Інформаційні матеріали Український інститут Національної пам’яті https://uinp.gov.ua/informaciyni-materialy/viyskovym/do-5-richchya-vid-pochatku-zbroynoyi-agresiyi-rosiyskoyi-federaciyi-proty-ukrayiny.
5. Сегеда С.П., Шевчук В.П. Гібридна війна Росії проти України: історичний вимір, Наука і оборона, № 1 (2019), Київ, С. 31-35.
6. Перепелиця Г. М. Україна – Росія: війна в умовах співіснування / Г. М. Перепелиця. – К. : Видавничий дім «Стилос», 2015. – 880 с.
7. Магда Є.В. Гібридна війна: вижити і перемогти / Є. В. Магда. – Харків: Віват, 2015. – 320 с.
8. Дузь-Крятченко О. П., Панкратов Є.Є. Досвід та уроки внутрішнього воєнного конфлікту та збройної агресії проти України. Труди університету: зб. наук. праць НУУО. – 2014. – № 4 (125). – С. 9–10.

Maritime combined threats in the High North

Ståle Ulriksen
Norwegian Naval College, NDU.
Oslo, Norwegia

Presenting main material

Since 2014 the military tension between Russia and the West in the European High North has escalated. The tension and friction in the Barents Sea may still be lower than in the Black Sea and in the Baltic Sea. Norway and Russia still cooperate relatively well in fields like search and rescue and in the regulation of the rich fisheries. Even so, the political climate has grown colder.

In addition to the increased military tension there seems to be a marked increase in Russian activities in other fields in and towards Norway. Some of these activities attempts to influence Norwegian policy making as well as the internal political climate in Norway. Other activities may be categorized as classic industrial espionage. A third category would seem to involve positioning and preparations in order to be able to target Norway in a crisis, conflict or war between Russia and the West. This brief paper mainly deals with the latter category. To better understand the Russian motivation for such behaviour, however, we need to take a look on the strategic situation in the European High North.

During most of the cold war, Norway and the surrounding waters was seen as NATO's northern flank. In the 1980s the tension and military presence increased to the point that the area was seen as the northern *front*. The change in perception of the area from flank to front reflected a both a dramatic change in US strategy and in Soviet capabilities. The US Maritime Strategy would allocate heavy forces, including multiple aircraft carrier groups, to attack the Russian forces in the north. One purpose was to utilise US Naval superiority in the north to relieve the central front where the Warsaw Pact where perceived to be stronger than NATO. The Russian strategy, in the west termed "the bastion defence", would attempt to block the Greenland-Iceland-United Kingdom (GIUK) gap and deny US forces access to the Norwegian Sea. If successful, the Russian strategy would isolate Norway behind the Russian lines of defence. At the time, the Soviet Northern Fleet consisted of almost 40 strategic submarines, some 130 nuclear- and diesel-propelled tactical submarines, forty large surface combatant warships, and a very large number of smaller vessels. Leningrad Military District had more than 500 bomber and fighter aircraft as well as at least eleven division of ground troops. The present Northern fleet is but a shadow of its former might, with just around ten operational non-strategic submarines and even fewer large surface combatants.

Still, the Northern Fleet includes the lions share of the most precious weapons in Russia's arsenal, the submarine launched intercontinental ballistic missiles with nuclear warheads that represents the Russian second-strike capability. In 2021 Russia has 12 such strategic submarines (SSBN), of which 9 are in the Northern Fleet. [1-2]. Most are equipped with 16 Sineva or Bulava missiles each. The missiles have a range

of at least 8300 kilometres, just about the distance from the Kola Peninsula to the Rio Grande if fired over the North Pole. Thus, these submarines may attack the whole of continental USA from their bases in Northern Russia. The missiles may, at full load, carry 10 nuclear warheads each. The warheads may be independently directed towards different targets. In theory then, each submarine may blow up 160 cities, airfields, or military bases with nuclear warheads. This capability is Russia's life insurance, a guarantee for Russia's status as a Great Power. In other words, this is a vital resource that Russia will have to defend, even at great cost.

The Northern Fleet became the fifth Russian Military District in early 2021, with command over naval, air and ground faces in the north-western parts of Russia. Even so, apart from the awesome power of the strategic submarines, and the few but advanced Severodvinsk-class guided missile submarines (SSGN), the Northern Fleet appears rather weak. The number of both operationally available submarines and large surface combatants is likely to fall during the 2020s. The Northern Fleets' ability to operate on the High Seas will probably decrease. There is a chance though, that the Northern Fleet, like the rest of the Russian navy, will be able to strengthen its forces in the "near seas", closer to the coast.

As seen from Murmansk the main threat to the strategic submarines and their bases are American hunter-killers (SSN/SSGN), very silent submarines with nuclear propulsion and armed with torpedoes and cruise missiles. American SSNs are probably able to track Russian SSBNs without being detected, at least if they can follow the SSBNs as they leave their bases. The Russians believe that once their SSBNs reach the polar ice cap, they are almost impossible to find. The main risk for these SSBNs is detection and destruction when in transit from their home bases to the ice cap. It is well known that US Navy SSNs regularly deploy to the Barents Sea, and that they use Norwegian harbours for supplies and change of crews.

Another serious threat to the Northern Fleet is attacks by American bombers, perhaps supported by Norwegian F-35s. The presence of US Air Force bombers over the Norwegian Sea and the Barents Sea have increased steeply in recent years. In 2020 B-52s, B-1Bs and B-2s all conducted flights in this area. Very often they exercised with Norwegian F-16s and F-35. Sometimes US bombers operate from Norwegian bases, sometimes they arrive directly from the USA.

In addition, the Russians may fear attacks by US Navy Carrier groups. In 2018 the USS Harry Truman arrived in the Vestfjord, just south of the Lofoten islands. This was the first time a US aircraft carrier deployed to northern Norway in almost three decades. American aircraft carriers have some 90 fixed wing aircraft and helicopters aboard, including advanced capabilities for electronic warfare and airborne early warning. Indeed, one carrier probably carry more operational airpower than the Northern Fleet Military District has at its disposal. The carriers are escorted by several destroyers and cruisers, and a hunter-killer submarine. At the time of writing a Norwegian frigate, the HNoMs Fridtjof Nansen, is part of the USS Harry Truman carrier group.

The renewed American presence in the north may be partly due to US worries about the advanced Severodvinsk-class SSGNs, but also in part be a result of Norwegian efforts to gain more support from allies in the face of a very aggressive

Russian posture since 2014. Norwegian forces have indeed increased their efforts to cooperate directly with US Forces, as shown in the examples above, but also in actual operations. On the 30th of August 2021 there were only coalition flags left over the airport in Kabul, those of the United States and Norway [3]. If recent Russian activities are meant to deter Norwegian policy from closer cooperation with the US, those attempts have failed.

In terms of population, Norway is a small country. In the commercial global maritime domain, however, Norway is a huge actor in several fields. Amongst them are fisheries, the merchant fleet and offshore oil and gas. Norway is a liberal country, and the economy is very open. While these policies are advantageous both politically and economically, they also create vulnerabilities. Skilled labour is expensive and fairly scarce in Norway. In the maritime sectors, and especially in shipping, it is common practice to hire people with competence and skills from abroad. We know that Russian authorities are actively pushing Russian sailors to gain employment in the Norwegian merchant fleet [4]. And some Norwegian shipowners run their own recruitment offices in Russia. One such company, Wilson of Bergen operates more than 120 small and medium sized freighters, on routes across Northern Europe – from the Baltic to the English Channel and northwards to the Kola Peninsula. The ships are crewed by some 1400 sailors. Wilson have recruiting offices in Arkhangelsk in Russia and Odessa in the Ukraine. The company reports that 80 percent of their sailors are from North-western Russia.

In order to protect themselves against the harsh weather in the North Sea, the Norwegian Sea and the Barents Sea, ships may choose to sail the Inner Leads along the Norwegian coast. These are relatively safe sailing routes. Still, the Norwegian coastline is difficult to navigate, with many fjords, often surrounded by mountains. There are more than 300 000 islands, islets and skerries. Crews with little experience in the area need to take aboard a pilot to be allowed to navigate here. However, officers on merchant ships may qualify for fairway certificates which allows them to sail without a pilot. Such certificates are granted for parts of the coastline. In 2015 a civilian Russian sailor revealed to Norwegian media that Russian authorities had encouraged sailors like him to qualify for fairway certificates in Norway. Presently some 250 Russian sailors have been granted fairway certificates, and a large number of these have such certificates for several coastal areas.

What could a fleet of more than a hundred small and medium-sized ships achieve in Norway and around the North Sea in a crisis if controlled from Moscow? I will that to the imagination of the reader, but there is no doubt that such assets could be used to delay, perhaps deny, western military operations and to destabilise the Norwegian economy. This fleet, and its crew, could also support regular Russian military operations.

The Norwegian Navy have developed tactics to utilise the coastal terrain as a force multiplier. In brief submarines, fast attack craft, coastal corvettes, and even larger vessels, exploits the oceanography and topography to hide. Very few antiship missiles are able to separate a fast attack craft from an islet. When hidden these vessels may attack from safe positions. Such operations require intimate knowledge of the littorals. If Russian civilian sailors have acquired such knowledge, they may be very

valuable assets for the Russian navy. Russian warships operating in the Norwegian littorals would be far less vulnerable to attack than if they were operating in the open sea.

Norwegian companies have developed a range of state-of-the-art technologies in several maritime sectors. This, of course, makes them attractive targets for industrial espionage. For years Norwegian authorities have warned against Russian, Chinese and Iranian activities in Norway. On the 23rd of October the Norwegian newspaper Dagens Næringsliv published a 14-page article describing, among other things, how Russian-flagged "research vessels" and Norwegian owned ships with mainly Russian crews navigated very close to an area where a new high tech underwater drone was tested [5]. The article presented strong indications, albeit not absolute proof, that this was a coordinated operation to gain information on the new technology that was being tested. Simultaneously it was pointed out that a Russian seismic ship may have charted a large part of the underwater infrastructure around Norway, i.e. pipelines carrying oil and gas, electric cables, internet cables etc.

In February 2021 the British company Rolls Royce announced the sale of its Norwegian subsidiary Bergen Engines to Transmashholding (TMH), a Russian company. The sale was eventually stopped by Norwegian authorities after harsh critique from the media and the political opposition. Bergen Engines builds high quality diesel engines. The technology is not very advanced, but Russian industry have been unable to produce such engines acceptable by the navy in the numbers needed. Before 2014 Russia imported gas turbines from the Ukraine and diesel engines from Germany for its frigates and corvettes. After the annexation of Crimea, the deliveries stopped. The result was huge delays in the production of new naval vessels. For instance: The Buyan-M class (project 21631) corvette *Uglich* was built in 29 months from 2011 to 2013. Its sister, the *Grayvoron*, took 70 months to build between 2015 and 2021. The latter were built with Chinese copies of German MTU diesels. The navy has experienced many problems with these engines. Later ships of the Buyan-M and Karakurt-class are planned with diesels from TMH, but production is very slow. If TMH had succeeded in buying Bergen Engines the Russian Navy would have got rid of one of the major bottlenecks in the renewal of its fleet.

When stopping the sale, Norwegian authorities also argued that the factory on Hordvikneset just north of Bergen, was too strategic a location to be sold to a potentially hostile country. The stopping of the sale, and the mentioned media disclosure of Russian activities in Norwegian waters signals, hopefully, that Norwegian society finally have recognized the fact that the country is vulnerable and exposed in an area that increasingly gains strategic importance.

Conclusions

To sum up, it would seem that the Russian not-so-friendly activities in the maritime sectors of Norway moves along two main tracks. The first attempts to get access to Norwegian technology and resources. The second track seems primarily to be an attempt to position Russian resources in Norway in order to be able to use them in crisis, conflict or war with the west – if the need should arise. My thesis is that these efforts has been reinforced lately in a recognition of the relative weakness of Russia's

conventional military capabilities in the north. The first track makes sense, from a Russian point of view, as Norway is major maritime actor in many maritime sectors. The second only makes sense in view of a major war between Russia and the US. In such a scenario it is on the one hand likely that Russia needs to deny the US the option to use Norwegian territory to stage attacks against Russa. On the other hand, it is also possible that Russian planners recognise that in a war with the US control over Norwegian territory, and the littorals in particular, would enable Russian forces to extend their defensive parameters.

List of references

1. This brief note is based on on-going research at the Norwegian Naval College.
2. In December 2021 the strategic submarine fleet is composed of one Typhoon class (project 941UM), six Delta IV class (project 667BRDM) and two Borey-class SSBNs (project 995/995A). The Typhoon is primarily used for testing of missiles, while one of the Delta IVs are due for decommissioning. Another Delta IV is at Sevmash shipyard in Severodvinsk for maintenance. In addition, a third, brand new Borey-class submarine is undergoing sea trials.
3. https://california18.com/norways-chief-of-defense-i-would-do-the-same-again/347082021/.
4. From interviews with shipowners and associated organisations.
5. Kibar, Osman (2021) «Operasjon Lazarev», in Dagens Næringsliv 23. October.

Місце, роль та місії сухопутного компонента у складі стратегічних угруповань військ у російських повномаштабних операціях

Василь Швалючинський, кандидат військових наук, доцент
Начальник кафедри Сухопутних військ Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-2775-4422
Віталій Хома, кандидат військових наук, доцент
Начальник науково-методичного центру організації наукової та науково-технічної діяльності Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-4821-4561

Анотація. *У доповіді наведені результати узагальненого аналізу деяких поглядів російських військових фахівців щодо дій військових формувань сухопутних військ під час ведення збройними силами Російської Федерації повномасштабних воєнних дій, а також припущення, зроблені на основі вище зазначеного аналізу, щодо ймовірних варіантів дій складових сухопутного компонента у випадку повномасштабної збройної агресії проти України.*

Ключові слова: *сухопутні війська, збройна агресія, оперативно-стратегічне командування, фаза операцій, тактична група.*

Вступ

Постановка проблеми. Починаючи з 2014 року Україна зіткнулася віч-на-віч з досить потужним у військовому відношенню противником – Російською Федерацією (РФ), яка розпочала війну проти нашої країни спочатку “гібридними” методами, а у серпні 2014 року здійснила вторгнення, застосовуючи військові формування зі складу регулярних збройних сил. Війна триває вже більше семи років і обстановка уздовж українсько-російського кордону лише загострюється. Окрім цього, РФ з кожним роком нарощує свою військову присутність у Білорусії, територія якої може бути використана як додатковий плацдарм для розв’язання агресії проти України з північного напрямку. Нарощування воєнного потенціалу також спостерігається на території Придністров’я, який може бути використаний для сковування частини Збройних Сил України на південно-західному напрямку.

Таким чином, воєнно-стратегічна обстановка довкола України свідчить, що РФ веде активну підготовку до повномасштабної збройної агресії проти нашої країни і усі складові сил безпеки та оборони держави повинні готуватися до відсічі цій агресії. Ефективно протидіяти агресору можна у тому випадку, коли відомі його підходи до підготовки і ведення воєнних дій, що може

забезпечити якісне прогнозування розвитку воєнно-стратегічної обстановки у майбутньому, а відповідно й планувати заходи протидії агресору.

Аналіз останніх досліджень та публікацій. Під час підготовки доповіді були проаналізовані деякі публікації, які розкривають склад, стан та основні завдання сухопутних військ збройних сил РФ [1-4], а також погляди російських військових фахівців щодо порядку дій сухопутного компонента під час повномасштабних воєнних дій. Дані, отримані з інформаційних ресурсів, дозволяють зробити висновок, що сухопутні війська є найбільш чисельним видом збройних сил РФ та налічують близько 40% усього особового складу, який проходить службу у збройних силах.

Командувач військами Південного військового округу генерал армії Олександр Дворніков стверджує [2], що під час формування програми навчання враховується досвід, набутий у процесі проведення спеціальної операції у Сирії. Її особливість – у відсутності чітких граней між завданнями стратегічного, оперативного і тактичного рівнів. Дворніков зазначив, що в основу бойового навчання закладається практика дій в умовах пустельної та гірської місцевості, ведення бою у населених пунктах, використання ударів авіації та високоточної зброї, ракетних з'єднань, Чорноморського флоту та Каспійської флотилії. Командирів вчать приймати випереджаючі, несподівані для противника рішення, щоб мати ініціативу під час бою. Нестандартним прийомом стало використання у контратакуючих військах тактичних груп прориву. Командири батальйонних груп отримали у підпорядкування підрозділи різних родів військ, а також можливість нешаблонно застосовувати весь арсенал їх озброєння.

Деякі військові експерти РФ на основі аналізу воєнних дій у Нагорному Карабаху розробили низку рекомендацій щодо напрямків розвитку тактики сухопутних військ [3], а саме: пошук та впровадження способів підготовки та застосування автономних тактичних груп, що синхронізують свої дії в рамках єдиного задуму; створення розвідувально-ударних комплексів (РУК) і розвідувально-вогневих комплексів (РВК) різного складу, дозволять впливати на об'єкти противника в реальному часі на усю глибину його бойових порядків; відпрацювання прийомів інтеграції функціоналу різних сил та засобів, що залучаються для впливу по противнику (завдання йому ураження).

Також відмічена тенденція переходу від лінійних до просторово-розподілених бойових порядків, яка виявилася у прагненні протиборчих сторін забезпечити максимальну автономність елементів бойового порядку шляхом створення у їхньому складі самодостатніх тактичних груп, що формуються за принципом функціонального призначення.

Мета доповіді полягає у тому, щоб зробити припущення щодо ймовірних варіантів дій сухопутного компонента зі складу збройних сил РФ у випадку повномасштабної збройної агресії проти України, зроблені на основі узагальненого аналізу деяких поглядів російських військових фахівців щодо порядку підготовки та ведення воєнних дій військовими формуваннями сухопутних військ.

Виклад основного матеріалу

Порядок застосування сил та засобів для досягнення цілей війни визначають способи воєнних дій. За поглядами російських військових фахівців основними способами воєнних дій у війні із застосуванням звичайних засобів ураження є одночасний чи послідовний розгром угруповань військ противника із поразкою життєво важливих об'єктів його військово-економічного потенціалу, інфраструктури та транспортних комунікацій. В умовах застосування зброї масового ураження, високоточної зброї великої дальності основним способом воєнних дій є одночасне ураження угруповань військ та об'єктів противника на всю глибину їх побудови (розташування).

У залежності від цілей і поставлених завдань, масштабів збройної боротьби, залучених сил і засобів застосування Сухопутних військ і родів збройних сил РФ у воєнний час здійснюватиметься у складі певних угруповань військ (сил) та об'єднань у тісній взаємодії з різними силами та засобами, що беруть участь. Застосування якогось виду, роду військ збройних сил окремо малоймовірне. Але необхідно зазначити, що оперативно-стратегічні командування формуються на базі військових округів, які організаційно входять до складу сухопутних військ. Отже, незважаючи на надзвичайно важливі ролі повітряно-космічних сил (ПКС), військово-морських сил (ВМС), ракетних військ стратегічного призначеня (РВСП), роль сухопутних військ збройних сил РФ у воєнних повномасштабних операціях є визначальною.

За результатами оперативної та бойової підготовки російські військові фахівці переконані, що для досягнення цілей операції доцільним є зосередження основних зусиль на визначенні та реалізації форм і способів вирішення двох-трьох найбільш важливих оперативних завдань, оскільки інші завдання грають, як правило, другорядну або допоміжну роль. Такий підхід реалізується під час навчань останніх років, що дозволяє їм застосовувати такі способи ведення бойових дій, як стримування наступаючого противника на одному напрямку та його розгром у поєднанні з маневреними діями на іншому напрямку; розчленування основних сил противника з утриманням вигідних районів; застосування оперативних мобільних резервів тощо.

Посилаючись на досвід воєн і збройних конфліктів початку XXI століття, російські військові експерти стверджують, що у сучасних умовах досягнення цілей війни можливо більшою мірою не шляхом знищення угруповань військ противника, а за рахунок дестабілізації обстановки у суспільстві та дезорганізації управління державою та збройними силами протилежної сторони шляхом впливу на ключові елементи, об'єкти енергетики, державного та військового управління, інфраструктури та систем життєзабезпечення.

Система підготовки сухопутних військ збройних сил РФ постійно корегується і можна виділити кілька підходів, які були запроваджені протягом кількох останніх років:

війська та сили навчаються лише у системі міжвидової підготовки на усіх рівнях, у тому числі оперативному і тактичному, особливу увагу при цьому приділяються питанням застосування бойових тактичних груп, повітряних

(морських) десантів, рейдових (обхідних, передових) загонів, а також їх взаємодії з авіацією;

під час проведення усіх заходів підготовки військ та сил передбачається використання АСУ, які діють у єдиному інформаційному просторі, домагаючись досягти сумісності автоматизованих систем управління видів та родів військ збройних сил та прийняття рішень у реальному масштабі часу;

з урахуванням проведення спільних заходів із підрозділами іноземних держав (країни організації договору про колективну безпеку (ОДКБ)) до тематики заходів підготовки з'єднань включаються питання застосування їх у складі коаліційних угруповань військ (сил);

у практику навчання військ та органів управління введено відпрацювання прийомів та способів ведення спеціальних (партизанських) та контрпартизанських (контрповстанських) бойових дій, боротьби з силами спеціальних операцій.

З наданням системі управління сухопутних військ ЗС РФ нового вигляду організація міжвидової підготовки значно спростилася. У підпорядкування командувачам передано практично усі з'єднання видів та родів військ збройних сил РФ (за винятком повітряно-десантних військ (ПДВ), РВСП та війська повітряно-космічної оборони (ВПКО)). Це дозволяє вже на етапі планування підготовки військ, організувати злагодження органів управління та підрозділів для дій у складі міжвидового та міжвідомчого угруповання військ (сил).

На основі вище зазначеного аналізу можна зробити припущення щодо ймовірних дій сухопутного компонента ЗС РФ у випадку повномасштабної агресії.

Щодо ймовірного наміру стратегічної наступальної операції то метою операції може бути окупація України або її окремих територій, встановлення прямого або опосередкованого контролю над Україною та позбавлення її державного суверенітету і територіальної цілісності силовим шляхом. Ключовими завданнями можуть бути:

1. Спровокувати Об'єднані сили, Збройні Сили України до відновлення активних воєнних дій на території Донецької та Луганської областей та звинуватити у порушенні Мінських домовленостей.
2. Завоювати панування у повітрі та на морі.
3. Скувати головні угруповання Сил оборони України на Донецькому та Луганському напрямках.
4. Розгромити головні угруповання Сил оборони та оволодіти Лівобережною та південною частиною Правобережної території України.
5. За сприятливих умов розвинути наступ у західному напрямку та захопити усю територію України.
6. Провести стабілізаційні дії та встановити окупаційний режим на усій території України.

Кінцеве положення: територія України знаходиться під повним контролем РФ.

Концепція операцій може полягати у наступному:

Вирішальними діями противника можуть бути нанесення ударів військами оперативного-стратегічного командування (ОСК) “Захід” та ОСК “Південь” з метою оволодіти правобережною та на приморському напрямку частиною лівобережної території України, оточити головні угруповання Сил оборони України у районі проведення операції Об’єднаних сил.

Формуючими діями, які повинні забезпечити успіх вирішальної операції, можуть бути:

1 Фаза – війська ОСК “Південь” за 10–15 діб до початку активних дій збільшують інтенсивність обстрілів та активізують дії ДРС і НЗФ з метою спровокувати ЗС України до активних воєнних дій у районі операції Об’єднаних сил. У той же час розпочинають стратегічне розгортання угруповань військ ОСК “Південь” та ОСК “Захід”. Збройні сили Росії розпочинають повітряну наступальну операцію з метою завоювання панування у повітрі, порушення систем управління та логістичного забезпечення Сил оборони України, створення сприятливих умов для успішних наступальних операцій сухопутних та повітрянодесантних угруповань військ.

Одночасно слід очікувати дії ВМС РФ щодо блокування військово-морських баз, портів по трьох напрямках з метою нейтралізувати дії ВМС України та позбавити її можливості отримувати підтримку з моря, постачання зброї, боєприпасів, інших матеріально-технічних засобів з боку країн-партнерів.

2 Фаза – (2-3 доби) ОСК “Південь” розпочинає наступальні дії з метою нанести ураження головному угрупованню військ ЗС України, скувати їх дії у районі операції Об’єднаних сил.

3 Фаза – (1-2 доби) ОСК “Захід” наносить удар у фланг угрупованням Об’єднаних сил ЗС України.

4 Фаза – у подальшому слід очікувати наступальні дії ударних угруповань “Східних” по всьому фронту:

5 Фаза – (2-3 доби) У подальшому після перегрупування противник ймовірно нарощуватиме зусилля та буде продовжувати наступ з метою захоплення столиці нашої держави.

Після завершення даної фази операцій можна очікувати ультиматуму від керівництва РФ щодо можливості припинення воєнних дій за умов капітуляції України та виконанні нею усіх вимог, продиктованих РФ.

Отримавши відмову України щодо складання зброї та за сприятливих для противника умов, слід очікувати подальші наступні фази операцій, які можуть бути спрямовані на захоплення решти території нашої країни.

Висновки

Ухвалення керівництвом Російської Федерації політичного рішення щодо ескалації збройного протистояння (шляхом проведення стратегічної наступальної операції) певним чином залежатиме від збереження підтримки України з боку міжнародної спільноти, безпекових організацій, а також готовності України до стримування та відсічі збройній агресії. Тому співпраця з країнами – членами НАТО – це надзвичайно важлива складова діяльності іншої держави загалом та Збройних Сил зокрема щодо зміцнення нашої безпеки, а

також колективної безпеки у Європі. Наш противник досить потужний, і лише його сухопутний компонент спроможний при підтримці інших видів збройних сил завдати незворотних втрат нашій країні. Тому наша мета – створити такі умови, щоб агресор змушений був відмовитися від ідеї ведення воєнних дій проти України та будь-якої іншої європейської країни.

Список літератури

1. Сухопутні війська Російської Федерації [Електронний ресурс]: 2021 // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki.
2. Командующий войсками ЮВО рассказал о новой тактике [Електронний ресурс]: 2021 // Російська газета. – Режим доступу: https://rg.ru/2021/11/08/reg-szfo/komanduiushchij-vojskami-iuvo-rasskazal-o-novoj-taktike.html.
3. Основные направления развития тактики Сухопутных войск (по опыту вооруженного конфликта в Нагорном Карабахе) [Електронний ресурс]: 2021 // Военная мысль. – Режим доступу: https://vm.ric.mil.ru/upload/site178/ljRu2qkJR5 pdf.
4. Учения “Запад-2021”: Россия дистанцировалась от Лукашенко? [Електронний ресурс]: 2021 // DW Akademie. – Режим доступу: https://www.dw.com/ ru/uchenija-zapad-2021-rossija-distancirovalas-ot-lukashenko/a.

The Russian Way of Regular Land Warfare

Amund Osflaten, MA, PhD-student
Teacher in Combined Arms Warfare, The Norwegian Defence University College
Oslo, Norwegia

Annotation. *This report looks at Russian military behavior after the Cold War and makes generalizations about the conduct of the Russian Armed Forces in operations. It is primarily concerned with Russian regular warfare, in contrast to irregular or political warfare, but it still analyzes the relevance of the different modes of warfare in the cases of Russian use of military force. Also, the report will analyze and describe the general characteristics of Russian regular land warfare. However, it is important to note that these characteristics are based on preliminary findings in the author's PhD-project. The overall research approach comprises several case-analyses of Russian use of military force. These case-analyses are primarily based on open-source material. Finally, in conclusion, this report will argue that the Russian Federation prefer the use of regular force also when other approaches appear viable, and, secondly, that the Russian way of regular land warfare is characterized by a general effort to penetrate the defensive system and quickly reach decisive objectives. This approach is realized through rapid operations, the exploitation of the initial period of conflict, secrecy and deception, sophisticated methods for pre-conflict deployment and the comprehensive utilization of electronic warfare (EW). However, note that these conclusions only become evident when looking at Russian behavior in a broad timeframe.*

Introduction

The object of study in this report is the Russian way of regular land warfare. Thus, it is placed in the "way of warfare" tradition. This assumes that there are general characteristics in how the Russians conduct warfare, and that these characteristics stay valid over a long timeframe. Consequently, this report looks at a generalization of Russian conduct of warfare that transcends today's conflict in Donbas. Further, this generalization will be limited to regular land warfare. In this report, regular warfare is defined as warfare aimed at seizing and retaining territory, and decisively destroy enemy military forces. Consequently, in addition to conventional warfare, regular warfare also includes battlefield nuclear warfare. Regular forces are the forces best suited for conducting regular warfare; however, importantly, irregular forces may be used to conduct regular warfare and regular forces may be used in irregular warfare. Land warfare simply means warfare on and about land territory. Thus, land warfare does not exclude joint operations.

As a research subject, Russian regular land warfare is perhaps under-researched today. In contrast, modes of warfare that combine regular, irregular and non-military warfare, such as "hybrid warfare," are very prevalent in analyses of Russian behavior. Additionally, the analyses are often preoccupied with the strategic and political aspects. Therefore, this report, and the PhD project it is derived from, aims at

elucidating the regular aspects of the Russian use of military force. Next, it will be argued that Russian behavior shows a persistent emphasis on regular military force. Subsequently, the report will describe general characteristics of Russian regular operations; that is, the Russian way of regular land warfare.

Presenting main material

The primacy of conventional force

While few would contest that the Russian Federation is partly relying on their conventional capabilities in recent conflicts, the degree of this reliance is more debated. This report will argue that conventional force is not only important to the Russian Federation, but it is also, within the constraints of any particular situation, a preference. By looking at the conflicts in which the Russian Federation have been involved after the Cold War, a picture of conventional predominance appears. In the following section, a historical argument for the Russian preference for conventional force is presented. In this, it is often equally interesting to analyze what the Russian Federation is not doing than their factual actions.

In the aftermath of the collapse of the Soviet Union, the Chechen republic tried to secede from the newly established Russian Federation. This became the origin of a long a bloody war between Chechen separatist and the federal forces. In this conflict, between a militarily superior counterinsurgent and a Chechen insurgency, the Russian Federation chose a strategy of counterinsurgency by punitive conventional firepower. This conventional and indiscriminate firepower was aimed at subduing the Chechen forces and population in general (Miakinkov, 2011, pp. 673–674). The Russian could have chosen a population-centric counterinsurgency strategy, popularly known as a "hearts-and-minds," capitalizing on political and other non-military means; however, the Russians preferred using their superior conventional firepower.

Later, when the long and bitter conflict between South-Ossetia and Georgian central authorities made a turn towards open hostility in 2008, the Russian Federation launched a full-scale invasion of Georgia. Again, a conflict local in scope was resolved through the extensive use of conventional force. Moscow could have chosen to isolate the conflict to South-Ossetia, which, in turn, could create more international sympathy towards the Russian declared objective of protecting the South-Ossetian population from atrocities (The Council of the European Union, 2009, pp. 24–25). The Russian invasion involved a joint force constituting 40.000 soldiers and thus a large portion of the available combat-ready Russian forces (Bukkvoll, 2009, p. 57). In the end, the Russian advance halted just short of the Georgian capital.

The Russian invasion of Crimea was another example of large-scale use of regular force. While there were minimal casualties on both sides the invasion was largely conducted by regular elite forces, and not for example covert irregular forces. The bulk of the Russian servicemen participating in the invasion were from regular forces, albeit light and elite in character. Examples of Russian units in Crimea were the 810 Naval Infantry Brigade based in Sevastopol and several units from the VDV, the airborne troops (Kofman et al., 2017, pp. 5–10). The practice of removing badges, flags and other marks from their uniforms and equipment would not be sufficient to hide their nationality to the Ukrainian forces, authorities and local population. A

Russian soldier with Russian uniform, equipment and a Moscow accent would not be mistaken to be an ad hoc locally mobilized militiaman, even if the Russian flag on his arm was removed. The Ukrainian address to the UN Security Council, made already 1 March 2014, demonstrates this clearly. The Ukrainian UN Permanent Representative claimed that: "[Russian] troops were already in country and their numbers were increasing, constituting an act of aggression" (United Nations Security Council, 2014). While the presence of Russian troops was not disputed, the intent and scale of the Russian operation would be harder to discern. It was primarily the strategic circumstances that caused the Ukrainian restraint. Simultaneously as Russian forces were flowing into Crimea, a large invasion force was deployed at the eastern border of Ukraine (Kofman et al., 2017, p. 8). The tangible threat of invasion, combined with the experience of Georgia in 2008, made the Ukrainian very wary of unnecessary escalation. This paper will argue that these considerations were the primary reason for the Ukrainian restraint during the Russian invasion of Crimea, not any ambiguity about the Russian presence on the peninsula. In fact, a successful Russian denial of any involvement in Crimea would increase the possibility of Ukrainian resistance. Even more important, a successful denial would also increase the possibility of NATO or any foreign assistance to Ukrainian authorities. If the forces in Crimea were perceived to be local militiamen, and not forces from a nuclear armed major military power, the risk to Ukraine and NATO of intervening militarily would be lower.

In the Donbas conflict, starting in 2014, a similar preference for conventional force is visible. The pro-Russian separatists, heavily supported by the Russian Federation, are organized and equipped as regular forces and has chosen an approach of retaining territory by a continuous defensive frontline. This is a symmetrical confrontation, in which the separatists expose themselves to conventional firepower. In other words, the Ukrainian Armed Forces, significantly militarily stronger than the separatists if unsupported, would smash the separatist forces in the case of a full-scale confrontation. This was clearly seen in the initial phase of the Ukrainian Anti-Terrorist Operation (ATO), in which the Ukrainian forces were close to neutralizing the separatists before the regular forces from the Russian Federation intervened (The White Book of the Anti-Terrorist Operation in the East of Ukraine in 2014–2016, 2017, pp. 30–31). The separatist could have chosen an approach of guerilla-warfare, using the porous border with Russia to deploy into Donbas and then retreat back to the safety of Russian territory. Also, a terrorist approach would also be imaginable, which would include assassinations and terrorist acts towards the Ukrainian civil society, creating a divide between the Russian and Ukrainian ethnicities within the Ukrainian state. In these counter-factual approaches the pro-Russian separatists would, to a larger degree, use irregular methods to avoid direct regular confrontation. Then, what is the reason for the Ukrainian and Western restraint in combatting the separatists? This report argues that it is the Russian potential of regular warfare, and thus the tangible specter of full-scale invasion, that is the crucial factor in protecting the separatists from destruction.

Finally, when looking at a broader historical picture, the Russian preference for conventional force appears to be a Soviet legacy. The Soviet invasion of Hungary in 1956, Czechoslovakia in 1968 and Afghanistan in 1979 did all follow a similar pattern.

A large conventional force, both "in country" and inserted in the initial period of war, was rapidly and with a relatively low signature completing the occupation with low opposition. Importantly, politically sensitive situations were resolved with brute conventional force and the Soviets left little room for concessions when the operations were ongoing.

The characteristics of the Russian way of regular land warfare

Based on preliminary findings from my PhD-project, this report will continue to describe the characteristics of a Russian way of regular land warfare. The overall hypothesis, admittedly a broad generalization, is that the Russian way of warfare follows a fundamental logic that includes two central aims. The first aim is the rapid penetration of the defensive system, preferably by a powerful conventional force and, secondly, quickly reach decisive objectives. Often, the rapid and forceful development of the military situation reduces or thwarts the defenders' resistance. This emphasis on affecting the depth of the enemy defensive system is not new in Soviet and Russian military theory. In the 1920s and 1930s, the "deep operations" theory, devising a method for penetrating the incredibly strong elastic defense in depth of WWI and re-introduce the operationally decisive maneuver to the battlefield, was developed by Tukhachevsky, Isserson and other theorists (Kelly & Brennan, 2009, pp. 43–48).

The introduction of nuclear weapons and the ballistic missile in the early Cold War made access to the enemy depth and achieving decisive effects less of a problem. However, at the end of the Cold War, the realization that nuclear warfare would be detrimental for all parties involved, made the Soviets again to consider conventional approaches to warfare. Consequently, the deep operations theory increased again in importance. In addition, the emerging technologies of the 1980, primarily precision-strike weaponry and information technology, induced a generation of Soviet military theorists to look for new methods of gaining access to the depth of the enemy system. Non-contact warfare, of which Ogarkov and Slipchenko were well-known proponents, described the use of long-range precision strike weapons and real-time targeting, without contact between large regular formations, as a new method of warfare (McDermott & Bukkvoll, 2017).

The fundamental aims of the Russian way of regular land warfare are achieved through a set of measures and methods. Firstly, the initial period of war, and similarly the beginning of an operation, is exploited to insert the conventional force before the defenders are fully organized. Importantly, the exploitation of the uncertainties in the initial period of conflict makes ultimatums and political signaling less likely. This was clearly visible in the Russian invasion of Georgia and Crimea (See Barabanov et al., 2010, pp. 37–75; Flikke, 2015). On the other hand, for example the US coalitions' final warnings and political efforts before the war against Iraq in 1991 and 2003 would be less likely to happen before a similar Russian operation.

Secondly, the early and rapid insertion of the conventional force is often conducted by multiple methods and categories of forces. For example, in the Russian invasion of Crimea, the Russian forces were inserted by aircraft to Simferopol airport, ships to Sevastopol port, landing craft along the coastline of Crimea or ferried across the Perch strait. Additionally, significant forces were already in-country through the

permanent deployment of the 810 Naval Infantry Brigade at Sevastopol (Kofman et al., 2017, pp. 6–12).

Thirdly, Russian tactics are, to a larger extent than in the West, based on norms and set procedures. This facilities for rapid decision-making and responsiveness on the operational level of war. In other words, flexibility in the lower command-levels is forsaken for operational level efficiency – tactics are subordinate to the operational level of war. This is a persisting trait of Soviet and Russian way of warfare (Donnelly, 1988, pp. 224–228).

While the above-described bold approach might quickly reach decisive outcomes, it also produces risks and vulnerabilities. For example, the Russian forces airlifted into Simferopol airport in the early stages of the invasion of Crimea could easily be surrounded by superior Ukrainian forces. Thus, the Russian way of regular land warfare includes several characteristics aimed at mitigating these risks and vulnerabilities. Firstly, secrecy and deception, known as maskirovka in Russian, is crucial. Rapid and procedural decision-making, and centralization of command at the operational level of war at the expense of flexibility at the lower tactical echelons, creates a predictable behavior if the operation is revealed. Consequently, secrecy and deception are necessary to delay the enemy's realization of impending operation.

Secondly, and closely connected to secrecy and deception, the Russian forces often use large-scale exercises and other means of pre-conflict deployment to shuffle large forces around in peacetime. This extensive use of unannounced exercises and mobilization inspections in peacetime creates less sensitivity for large troop movements in a potential opponent. Consequently, in case of a Russian decision to use military force, the deployment of a large conventional force, under the pretext of an exercise, does not drift far from what is normally expected. For example, this approach seems to be used before the invasion of Georgia and Crimea in which a large part of the forces used in the invasions were recently mobilized for large exercises or mobilization inspections.

Finally, in the Russian way of regular land warfare the activity of actively changing the operational environment to allow for the effective use of conventional force are crucial. Traditionally, Soviet and Russian forces have used smoke and aerosols not only to screen own forces and blind the enemy, but also to change the entire area of operations of a force formation (Hines, 1988, p. 67). Electronic Warfare (EW), extensively used in Russian operations in Ukraine, is a similar measure. The proliferation of EW in Russian units is a method of creating favorable conditions for Russian use of conventional force. It reduces the effectiveness of weapon systems and the cohesion of the opposing force; particularly against a technologically sophisticated opponent such as NATO. This again reduces the overall risks and vulnerabilities to the conventional force.

Conclusions

This report has provided a broad picture of the Russian way of regular land warfare; however, as it is based on an ongoing PhD-project the findings are, at the moment, preliminary. Overall, both the Soviet and Russian military behavior has shown a preference for the use of conventional force. This preference will lead to a

forceful approach that require a penetration of any defenses, and, subsequently, moving to secure decisive outcomes. This is achieved through a series of trademark measures: the exploitation of the initial period of war (operation), multiple methods of inserting the conventional force into the area of operations, and the procedural, and thus rapid, approach to tactics and decision-making. These trademark measures create risks and vulnerabilities as the integrity and cohesion of the invasion force is potentially at stake. Consequently, these risks and vulnerabilities are mitigated by another set of characteristics: the traditional Soviet and Russian use of secrecy and deception to delay the enemy's realization of the operation, the use of large-scale exercises and other sophisticated methods to deploy forces to the theater without revealing the operation, and to actively change the operational environment on a grand scale, in recent conflicts exemplified by the extensive use of EW.

List of references

1. Barabanov, M., Lavrov, A., Pukhov, R., & Tseluyko, V. (2010). The Tanks of August (R. Pukhov, Ed.). Centre for Analysis of Strategies and Technologies.

Bukkvoll, T. (2009). Russia's military performance in Georgia. Military Review, 89(6), 57–62.

2. Donnelly, C. (1988). Red Banner: The Soviet Military System in Peace and War. Jane's Information Group Ltd.

3. Flikke, G. (2015). A timeline for the conflict and war in Ukraine: Vol. 2015: 4. The Norwegian Atlantic Comittee.

4. Hines, K. L. (1988). Competing concepts of deep operations. The Journal of Soviet Military Studies, 1(1), 54–80. https://doi.org/10.1080/13518048808429897.

5. Kelly, J., & Brennan, M. (2009). Alien: How Operational Art Devoured Strategy. https://apps.dtic.mil/sti/citations/ADA506962.

6. Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., & Oberholtzer, J. (2017). Lessons from Russia's Operations in Crimea and Eastern Ukraine. RAND Corporation.

7. McDermott, R. N., & Bukkvoll, T. (2017). Russia in the Precision-Strike regime: Military theory, procurement and operational impact (p. 50). Norwegian Defence Research Establishment FFI. http://rapporter.ffi.no/rapporter/17/00979.pdf.

8. Miakinkov, E. (2011). The Agency of Force in Asymmetrical Warfare and Counterinsurgency: The Case of Chechnya. Journal of Strategic Studies, 34(5), 647–680. https://doi.org/10.1080/01402390.2011.608946.

9. The Council of the European Union. (2009). Independent International Fact-Finding Mission on the Conflict in Georgia (Volume I). The Council of the European Union.

10. The White Book of the Anti-terrorist Operation in the East of Ukraine in 2014–2016. (2017). Ukrainian Ministry of Defence, General Staff and research institutions of the Armed Forces of Ukraine.

11. United Nations Security Council. (2014). Security Council Meeting Report 7124. United Nations.

Уроки з аналізу гібридних дій Російської Федерації у Чорному і Азовському морях у 2014-2021 роках та рекомендації щодо спільної з НАТО та ЄС протидії на гібридні загрози

Степан Яким'як, кандидат військових наук, доцент
Начальник кафедри Військово-Морських Сил Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-1530-271X

Анотація. *В статті на підставі аналізу досвіду гібридних дій Російської Федерації в Азовському та Чорному морях у 2014-2021 роках визначено сфери (галузі) здійснення гібридних впливів та особливості комплексного проведення відповідних заходів, зокрема інформаційно-психологічних, політичних, дипломатичних, економічних, спеціальних, військових. За підсумками проведеного аналізу визначено основні висновки та уроки з досвіду гібридних дій, до яких, у першу чергу, віднесено такі: РФ використовує технологію гібридного впливу ("стратегію обмежених дій") для досягнення власних геостратегічних та воєнно-політичних цілей; внаслідок гібридних дій РФ відбувається масштабне порушення прав людини на окупованих територіях та принципу свободи судноплавства у цих морях, здійснюється негативний вплив на регіональну і глобальну безпеку.*

Для протидії гібридним загрозам у праці запропоновано основні принципи, цілі, завдання та форми застосування сил на морі, а також рекомендації щодо спільних дій, зокрема проведення морської безпекової операції, операцій із захисту судноплавства та, у разі потреби, операції з примушення РФ до миру і виконання нею вимог міжнародного права.

Ключові слова: *гібридний вплив, уроки з досвіду гібридних дій на морі, принципи протидії гібридним загрозам, морська безпекова операція, міжнародна операція із захисту судноплавства.*

Вступ

Постановка проблеми. Аналіз гібридних дій РФ в Азово-Чорноморському регіоні у 2014-2021 роках, зокрема проти України, засвідчує про розширення їх масштабів та використання Росією різних сфер для здійснення комплексного дозованого впливу для досягнення визначених цілей без переходу до повномасштабного застосування сил (військ) [1]. Слід зазначити, що гібридні дії відбуваються у різних районах морів та різних умовах, зокрема в різні пори року, у тому числі в умовах холодної погоди.

Водночас, існує проблема, яка полягає в наявності такого протиріччя: з одного боку РФ постійно удосконалює технологію практичного здійснення гібридного впливу на морі, що вимагає відповідного реагування, а з іншого боку – поглиблюється відставання у розвитку теоретичних засад для здійснення такого реагування і пошуку раціональних способів протидії противнику на морі,

у тому числі в умовах холодної погоди. Також слід зазначити, що Україна як воююча держава накопичила певний досвід протидії гібридним впливам РФ, зокрема й на морі, але висновки й уроки з цього досвіду доцільно мати й країнам-партнерам України, у першу чергу – державам-членам НАТО, які мають схожі умови приморського розташування та прилеглих морських районів, наприклад – прибалтійські держави, а також Румунія, Болгарія, Норвегія та інші.

Аналіз останніх досліджень і публікацій. У працях [2–3] було розглянуто загальні підходи до сутності гібридних дій та їх порівняння з іншими видами дій і застосуванням сил (військ) у мирний час, кризових ситуаціях та воєнних конфліктах. Закордонними та вітчизняними авторами у працях [1, 4–9] було проаналізовано досвід гібридних дій РФ в Азово-Чорноморському регіоні, визначено певні уроки та запропоновано шляхи протидії гібридним загрозам на морі. Таким чином, не вирішеним у вказаних вище працях завданням є визначення сфер (галузей) здійснення гібридних впливів на основі накопиченого досвіду, аналіз особливостей комплексного проведення відповідних інформаційно-психологічних, політичних, дипломатичних, економічних, спеціальних, військових заходів, зокрема в умовах холодної погоди, та визначення основних принципів, цілей, завдань і форм застосування сил для протидії гібридному впливу на морі, у тому числі у випадку спільних дій держав-партнерів, НАТО і ЄС.

Метою доповіді є визначення уроків з досвіду гібридних дій в Азово-Чорноморському регіоні та вироблення відповідних рекомендацій щодо принципів, цілей, завдань та форм застосування сил під час протидії гібридним загрозам на морі спільно з країнами-членами НАТО та в різних умовах обстановки, у тому числі в умовах холодної погоди.

Виклад основного матеріалу дослідження

У ході триваючої збройної агресії РФ проти України накопичено значний бойовий досвід щодо застосування сил на морі і в прилеглих приморських районах. До основних складових такого досвіду слід віднести:

ведення дій щодо недопущення захоплення військових частин, пунктів базування аеродромів, озброєння і військової техніки у ході спеціальної міжвідомчої операції РФ щодо захоплення Криму (лютий – березень 2014 року);

проведення протидиверсійних та інших дій щодо недопущення захоплення Росією з моря окремих районів Одеської, Миколаївської, Херсонської областей (з березня 2014 року);

ведення дій в умовах нанесення противником ураження по двох катерах Морської охорони Державної прикордонної служби України (серпень 2014 та червень 2015 року);

посилення оборони пунктів базування і портів, та ведення демонстраційних дій зі стримування противника;

захист судноплавства в умовах масштабних затримок цивільних суден в Керченській протоці та Азовському морі;

нарощування угруповання сил ВМС ЗС України в Азовському морі;

ведення бойової діяльності з контролю обстановки та захисту судноплавства в умовах провокаційних дій противника та масштабного закриття для плавання значних за площею районів.

Під час здійснення РФ гібридного впливу на морі (з моря) у ході захоплення Криму та в подальших діях проводились такі взаємоузгоджені заходи:

інформаційно-психологічні дії щодо:

деморалізації особового складу військових частин ВМС, інших видів ЗС й інших відомств, що були розташовані у Криму;

дискредитації Збройних Сил;

негативного впливу на населення у приморських та інших районах зі спотворенням відомостей (поширення фейків) про загальну соціально-політичну обстановку у державі і регіонах та налаштуванням на позитивне сприйняття дій агресора;

негативного впливу на керівництво і визначені цільові групи громадян іноземних держав зі спотворенням відомостей (поширення шейків) про обстановку в Україні, дії її керівництва, міжнародно-правову та оперативну обстановку у Чорному та Азовському морях;

дезінформації та спотворення відомостей (поширення фейків) про діяльність у морських районах кораблів і підрозділів ВМС ЗС України та держав-членів НАТО, зокрема щодо проведення ними навчань, маневрування, використання військовими кораблями іноземних держав права мирного проходу через територіальне море України поблизу Криму.

політичні і дипломатичні щодо:

здійснення заходів дипломатичними каналами з поширенням неправдивої інформації про обстановку в Україні та здійсненням тиску на керівництво інших держав з метою протидії Україні на морі;

військові і спеціальні дії, у тому числі міжвідомчі, щодо:

захоплення важливих об’єктів в Криму;

прихованого перевезення морем військових підрозділів з території РФ до Криму;

ведення перемовин, шантажу, підкупу посадових осіб військових частин;

блокування та фізичного штурму берегових військових частин у Криму підрозділами без розпізнавальних знаків із залученням агентів під видом “народної самооборони” та цивільного населення, що діє попереду військових;

блокування з моря пунктів базування у Криму та штурмові дії із захоплення кораблів;

посилення бойового складу сил на Азовському морі та створення міжвідомчого угруповання сил “з охорони Керченського мосту”, фактично створеного для зриву цивільного судноплавства та недопущення перебазування сил ВМС ЗС України з Чорного моря в Азовське;

здійснення масштабних позазаконних зупинок цивільних суден, що здійснюють плавання до українських портів в Азовському морі та у зворотному напрямку, у трьох районах (на підходах до Керченського мосту, на підходах до портів) та проведення доглядових операцій на їх борту;

перешкоджання перебазуванню сил ВМС ЗС України з Чорного в Азовське море із застосуванням міжвідомчого угруповання сил, ведення штурмових дій із захоплення військових кораблів та їх ураження надводними кораблями та авіацією;

поширення фейків про закриття районів для плавання та надання міжнародного повідомлення мореплавцям;

фактичне закриття значних за площами районів для плавання, що обмежують можливості зі здійснення міжнародного цивільного судноплавства та повсякденної (бойової) діяльності кораблів причорноморських держав;

здійснення незаконного радіоелектронного впливу та порушення функціонування засобів зв'язку та навігації, у тому числі глобальної системи навігації GPS ("спуфінг");

незаконне використання цивільних систем та засобів для ведення військових заходів, зокрема встановлення на газодобувні платформи військових засобів виявлення цілей;

приховане розгортання підводних засобів контролю за обстановкою за межами власного територіального моря та, ймовірно, на підводних трубопроводах;

ведення постійних демонстраційних, провокаційних та розвідувальних дій у визначених районах морях, наближених до протокових зон, територіального моря України та інших причорноморських держав.

Слід підкреслити, що у 2018-2021 роках РФ продовжила ведення гібридних дій в Азово-Чорноморському регіоні та здійснювала відповідні заходи із загальною метою щодо дестабілізації обстановки в Україні. Реагуючи на розпочаті РФ у 2018 році тривалі зупинки торговельних суден у трьох районах в Азовському морі та на підходах до Керченської протоки, у жовтні 2018 року було розпочато протидію противнику на морі українськими бойовими катерами, перебазованими в Азовське море. Завдяки цьому було частково припинено дії РФ щодо зупинки цивільних суден. У подальшому РФ вдалася до прямого акту агресії 25 листопада 2018 року, провівши позазаконне захоплення трьох військових кораблів України, які здійснювали легальний прохід через Керченську протоку для перебазування в Азовське море.

Таким чином, під час гібридних дій на морі РФ здійснює нарощування військово-морської присутності та перешкоджання судноплавству у визначених морських районах. У певний момент противник може перейти до встановлення зони контролю на морі та повного блокування морської, у тому числі військово-морської діяльності.

Важливою особливістю протидії гібридному впливу в Азовському морі є складні умови виконання завдань, зокрема умови холодної погоди, яка панує у зимові місяці – у грудні, січні та лютому. Так, на застосування сил в Азовському морі взимку (в умовах холодної погоди) суттєво впливають такі чинники:

загальне погіршення гідрометеорологічних умов у період з листопада по квітень, зокрема підвищена швидкість вітру і зростання інтенсивності штормів;

покриття кригою значних за площею частин моря: м'яка зима – близько 15% (лимани, затоки); сувора зима – до 100%;

товщина криги становить: у прибережних районах – 0,2-0,8 м; в центральній частині моря – 0,1-0,3 м;

утворення торосів на прибережних ділянках висотою 1-5 м:

тривалість періоду покриття моря кригою – 22-145 днів.

Аналіз досвіду воєнних конфліктів засвідчив про необхідність врахування таких стратегічних аспектів впливу холодних погодних умов на початок і ведення бойових дій:

перенесення початку військових кампаній і найважливіших операцій на період року, що характеризується більш сприятливими погодними умовами (приклади – Фолклендська війна 1982 р., російсько-грузинська або «восьмиденна» війна 2008 р., російсько-українська війна 2014 року – до теперішнього часу);

загальний негативний вплив умов холодної погоди на якість виконання оперативних (бойових) завдань силами під час дій, зокрема:

уповільнення темпів розгортання сил (військ);

погіршення маневреності та мобільності сил (військ);

зниження активності та темпу наступальних та інших дій;

погіршення продуктивності фізичної активності людини;

зниження морально-психологічного стану сил і, відповідно, зниження боєздатності підрозділів;

наявність ризиків або погіршення стратегічних можливостей створених угруповань для своєчасного та якісного досягнення конкретної мети застосування сили в операціях, походах, у війні.

Для вивчення і прогнозування особливостей дій сил в умовах холодної погоди важливо використовувати набутий досвід застосування сил у даному районі дій у попередніх роках. Стосовно умов Азовського моря важливо враховувати досвід дій радянських ті інших військ в цьому районі в зимових умовах під час Другої світової війни. До основних уроків з цього досвіду слід віднести такі:

в умовах холодної погоди (у період з листопада по квітень) суттєво знижувались можливості надводних сил (Азовської флотилії) з виконання завдань на морі та надання допомоги військам, що діяли у прибережних районах;

важливим завданням було своєчасне переведення кораблів з акваторії замерзаючих баз у райони дій та бази, що не замерзали взимку;

у разі замерзання значної частини моря – перехід до використання екіпажів кораблів як об'єднаних сил спеціального призначення для проведення рейдів по кризі до місць розташування на суші військ противника (приклад – протягом зими 1941-1942 рр. було здійснено понад 70 таких нічних рейдів).

На підставі аналізу дій сил в Азовському морі у 2014-2021 роках визначено основні особливості застосування сил та уроки. До особливостей дій сил слід віднести такі:

значне ускладнення або неможливість навігації та виконання бойових завдань на морі для ведення розвідки, демонстраційних дій, патрулювання, супроводження суден, протидії ударним силам противника, сприяння військам, які діють у прибережних районах;

обмерзання суден, особливо низькобортних;

погіршення можливостей застосування корабельної зброї під час виконання завдань у морі та під час несення служби в пунктах базування;

обмежені можливості застосування корабельної зброї, зокрема в єдиній системі протиповітряної оборони, після підйому малих кораблів на причали на час зимових умов;

ускладнення або неможливість утримувати в робочому стані інженерні загородження у воді в умовах криги та торосів;

обмерзання причалів, обладнання та інших гідротехнічних споруд;

загроза стиснення і пошкодження льодом корпусів малих суден і необхідність їх підняття на причали та ін.

З аналізу досвіду дій на морі у зимових умовах у 2014-2021 роках визначено такі основні уроки:

значне зменшення внеску надводних сил у складі об'єднаних сил в умовах покриття моря кригою і, відповідно, підвищення ролі інших складових сил у відбитті ударів противника з морських напрямків;

необхідність створення додаткових спроможностей для криголамної підтримки надводних сил;

необхідність створення сприятливих умов для базування маломірних суден, зокрема обладнання пунктів базування необхідними комплексами для підйому їх на причали та їх зберігання в зимових умовах;

визначення та використання відповідних способів застосування екіпажів кораблів, що не залучені до дій на морі в умовах наявності криги, з виконання завдань в спеціальних операціях на суші та для виконання інших бойових завдань;

необхідність створення системи спеціальних курсів для підготовки особового складу до дій в умовах холодної погоди.

Для подальшого врахування уроків з дій у холодну погоду в практику підготовки сил та під час підготовки операцій доцільно передбачити:

проведення комплексу досліджень щодо створення та використання перспективних моделей застосування сил для ведення операцій в умовах холодної погоди;

проведення комплексу дослідно-випробувальних робіт зі створення нових зразків озброєння для застосування в умовах холодної погоди, в тому числі малих надводних носіїв амфібійного, модульного та багатосферного типів, малого озброєння та транспортних засобів для дій на льодовій поверхні, морських роботизованих систем для дій в умовах холодної погоди;

започаткування та проведення в Національному університеті оборони України спеціалізованих курсів з підготовки та ведення операцій. в умовах холодної погоди

Аналіз досвіду бойової діяльності сил оборони на морі, зокрема сил і засобів Військово-Морських Сил (далі – ВМС) та інших видів (окремих родів сил і військ) Збройних Сил України, морської охорони Державної прикордонної служби України та органів (підрозділів) інших відомств України, а також результати проведених досліджень у Національному університеті оборони

України дозволили сформувати певну сукупність положень щодо мети, завдань та форм застосування міжвідомчих міжвидових угруповань сил на морі в умовах гібридних дій противника.

Під час гібридних дій з боку противника метою застосування угруповань різнорідних сил ВМС може бути стримування противника та стабілізація обстановки у морських операційних зонах і прилеглих приморських районах, забезпечення національної стійкості на морі та захист морської економічної діяльності держави і міжнародного судноплавства в українських водах.

Для виконання вказаних вище завдань усі сили, визначені від міністерств та відомств держави, застосовуються спільно у складі угруповання об'єднаних сил під єдиним керівництвом та за єдиним замислом і планом. Основною формою застосування такого угруповання об'єднаних сил, що діє на морі і приморських районах, буде об'єднана морська операція.

З урахуванням стандартів НАТО доцільно використовувати підходи, що існують до проведення подібних операцій в умовах кризових ситуацій, а саме – таку форму застосування, як морська безпекова операція (Maritime Security Operation) [10]. За підходами, що використовуються в НАТО, під морською безпековою операцією розуміють сукупність узгоджених дій на морі, що виконуються військовими формуваннями та правоохоронними органами, оснащеними відповідними засобами та уповноваженими діяти у відповідь на ризики та загрози, пов'язаними з морською безпекою. Водночас, під терміном "морська безпека" розуміють стан безпеки на морі зі зниження ризиків та протидії загрозам неправомірних та небезпечних дій у морському просторі, а також реагування на них з метою забезпечення законності, захисту громадян та захисту національних та міжнародних інтересів. Морська безпека зосереджується на протидії незаконному використанню морського простору.

Для досягнення зазначеної вище мети дій в умовах гібридного впливу противника доцільно виконувати такі основні завдання:

ведення спостереження та розвідки в морських операційних зонах та інших визначених районах в інетересах забезпечення національної безпеки, відсічі та стримування збройної агресії;

участь у проведенні інформаційних та спеціальних дій (операцій) в морських операційних зонах та інших визначених районах;

підтримання сприятливого оперативного режиму у визначених районах моря, у тому числі створення спеціальних умов (режимів) використання визначених морських районів та повітряного простору над ними;

ведення дій зі стабілізації обстановки в морських операційних зонах та визначених прилеглих районах узбережжя, у тому числі здійснення ізоляції з моря визначених ділянок морського узбережжя та протидії терористичним угрупованням і диверсійно-розвідувальним силам противника;

ведення демонстраційних дій на морі та в прилеглих районах узбережжя;

сприяння угрупованням військ (сил) та підрозділам сил оборони і безпеки, зокрема Об'єднаних сил, що діють у приморських районах;

посилення охорони державного кордону на морі та суверенних прав України в її виключній (морській) економічній зоні;

захист морських комунікацій України в морських операційних зонах та торговельних суден іноземних держав у визначеній зоні відповідальності держави;

забезпечення перевезень морем важливих державних та військових вантажів;

охорона та оборона районів базування (дислокації) своїх сил (військ).

З урахуванням особливостей спільних дій в умовах здійснення противником гібридного впливу, а не ведення ним повномасштабних воєнних дій, така морська операція матиме свої особливості. У першу чергу, ця операція буде проводитися з використанням різноманітних міжвідомчих заходів, веденням дій із забезпечення військової і військово-морської присутності у визначених районах, несення бойової служби у визначених районах і бойового чергування визначеним складом сил, веденням демонстраційних дій, виконанням завдань бойової і службово-бойової діяльності та ін.

В умовах подальших гібридних дій РФ на морі важливим є поглиблення безпекової співпраці між державами. Спільні дії держав на морі забезпечать належну протидію гібридному впливу. З урахуванням висновків з вивчення досвіду діяльності сил сторін в Азово-Чорноморському регіоні у 2014-2021 роках та результатів проведених досліджень, визначено такі рекомендації щодо спільних з НАТО та іншими партнерами основних заходів та дій у військовій (оборонній) сфері на морі:

забезпечення цілорічної безперервної військово-морської присутності визначеного складу військових кораблів нечорноморських держав НАТО і країн-партнерів (перш за все, кораблів з відповідними ударними і спеціальними спроможностями) у форматі “24/7/365” (18 почергових ротацій сил, послідовно протягом року);

забезпечення охоплення спільними заходами (навчання, бойові патрулювання, спостереження та ін.) до 100% площі визначених районів обох морів (в усіх частинах Чорного та Азовського морів, у тому числі центральній та північно-східній частині Чорного моря);

запровадження і постійне проведення (з урахуванням наведених вище положень) таких спільних операцій:

морських безпекових операцій (бойова служба, бойове патрулювання) згідно стандартів НАТО;

операцій з контролю за судноплавством та дотриманням норм міжнародного морського права, особливо щодо суден, що порушують законодавство України і відвідують Крим (несанкціоновані заходи/виходи до/з портів Криму), проведення доглядових операцій та арештів суден-порушників;

операції з примушення до миру (у разі отримання резолюції/мандату РБ ООН) та відновлення контролю над тимчасово окупованими територіями та водними просторами України і Грузії.

Насамкінець слід наголосити, що відсіч збройної агресії РФ та протидія гібридним діям противника на морі можуть бути успішними лише за умови завчасної підготовки і ведення ефективних спільних міжвідомчих та коаліційних дій на морі.

Висновки

1. За підсумками проведеного аналізу досвіду ведення РФ гібридних дій на у Азово-Чорноморському регіоні у 2014-2021 роках визначено такі основні висновки та уроки: РФ використовує та постійно удосконалює технологію гібридного впливу для досягнення визначених цілей; внаслідок гібридних дій РФ відбувається масштабне порушення прав людини на окупованих територіях, право свободи судноплавства в Азовському та Чорному морях, знижується рівень міжнародної безпеки; протидія гібридним загрозам вимагає уточнення завдань та пошуку відповідних форм застосування сил.

2. В умовах холодної погоди (в зимових умовах) існують істотні особливості застосування сил на морі, які обумовлюють врахування висновків та уроків з досвіду, а також: запровадження заходів щодо збереження малорозмірних катерів в умовах криги; визначення нових бойових завдань підрозділам з ведення рейдових дій через морські райони, покриті кригою; створення нових зразків озброєння для ведення дій на кризі, зокрема спеціальних мобільних засобів доставки та ураження.

3. Для протидії гібридним загрозам запропоновано основні принципи, цілі, завдання та форми застосування сил на морі, а також рекомендації щодо спільних дій, зокрема проведення морської безпекової операції, операцій із захисту судноплавства та, у разі потреби, операції з примушення РФ до миру і виконання нею вимог міжнародного права.

Перспективи подальших досліджень. Напрямом подальших досліджень є обґрунтування положень до керівних документів (стандартів) застосування сил з урахуванням досвіду протидії гібридним загрозам на морі та визначення оперативно-тактичних вимог до нових зразків озброєння, необхідних для ведення дій в районах, покритих кригою, в умовах гібридних дій противника на морі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The White Book of the Anti-terrorist Operation in the East of Ukraine in 2014-2016 / Ivan Rusnak, Vitaliy Bydniy, Sergiy Segeda, Stepan Yakymiak and etc. – Kyiv: MOD of Ukraine, National Defence University of Ukraine, 2017. – 162p.
2. The World Hybrid War: Ukrainian Forefront: monograth abridget and translated from Ukrainian/Volodymyr Horbulin. – Kharkiv: Folio, 2017. – 158p.
3. Stocer, Donald and Whiteside, Craig. Blurred Lines: Gray-Zone Conflict and Hybrid War – Two Failures of American Strategic Thinking // Naval War College Review. – 2020, Winter. – Volume 73, number 1. – P. 13-48.
4. Flanagan, Stephen J., Chindea, Irina A. Russia, NATO, and Black Sea Security Strategy. Regional Perspectives from a 2019 Workshop. – RAND Corporation, Santa Monica, Calif. (USA), 2019. – 18 p.
5. Perepelytsia, Grigoriy. Current geopolitical trends in the Black Sea region // UA: Ukraine Analytica. – №3(5). – 2016. – P. 20-28.
6. Клименко А., Гучакова Т. Чорноморська небезпека та реакція НАТО. Випуск 2, травень 2019. – К.: Чорноморські новини (Blackseanews), 2019. – 20с.
7. Yakymiak, S. Naval Forces of Armed Forces of Ukraine and their plase and

roie in deterrence of armed agression, protection of sovereignty and territotial integrity of the state / Strategic appraisal: Naval Forces of Ukraine, 2018. ISBN 978-617-7157-815.

8. Яким’як С.В. Висновки та уроки з досвіду діяльності Військово-Морських Сил Збройних Сил України під час окупації Криму та антитерористичної операції // Воєнна історія. – 2014. - № 3-4. – С.76-86.

9. Яким’як С.В. Проблемні питання протидії гібридному впливу противника на морі та шляхи їх вирішення / С.В. Яким’як // Наука і оборона. 2020. № 2. – С. 31–36.

10. Allied Joint Doctrine for Maritime Operations (AJP-3.1, Edition Version 1). – Brussels (Belgium): NATO Standardization office, 2016.

Military Education in Extended Reality

Stian Kjeksrud, Associate Professor
Norwegian Defence University College,
Oslo, Norwegia

Annotation. *Using immersive educational technology to improve teaching and learning on human security and the role of military force in higher military education.*

Presenting main material

The research and development project **Military Education in Extended Reality** (hereafter the XR-project) explores immersive technologies and new pedagogical approaches to improve teaching and learning at the master's degree level at NDUC on the role, utility, and limitations of force in protecting civilians from violence in contemporary armed conflict. The XR-project builds on more than a decade of research on protection of civilians and the military role, synthesized and conceptualized for military planners (and master's degree students) as a *Threat-based approach to protection of civilians* (Beadle 2014; Beadle and Kjeksrud 2014, 2018; Kjeksrud 2016, 2019; Kjeksrud, Beadle, and Lindqvist 2016; Lindqvist et al. 2020).

The XR-project runs from 2020 through 2022, while the quasi-experiment described here-which forms an important part of the overall research and development process-will be run and finalized in 2022. The first year (June 2020-June 2021) was used to develop a conceptual idea for a pilot version of a future educational program, providing a well-informed starting position.The quasi-experiment described here, however, will scrutinize a subset of the most promising ideas captured in that concept, based on existing knowledge about learning and teaching in Extended Reality. As such, the future version of the XR-programme and the current conceptual idea will be modified according to findings in the quasi-experiment, both to increase learning effects and to make sure funds are well spent on a viable technological solution.

The XR-project studies whether and how a combination of immersive technologies-including, but not limited to, 360°-videos and interactive Virtual Reality-applications-can provide teachers with powerful educational tools. The aim is to increase students' immediate interest in a new topic for military planners and influence life-long learning about the ideas underpinning the threat-based approach to protection of civilians. The project employs cutting edge pedagogical theories**,** exemplified through *embodiment,* where students virtually experience armed conflict situations through other's eyes and virtual bodies, including as victims of violence, perpetrators of violence, and as military protectors. Embodiment can trigger affective and cognitive empathy that involve strong emotions-both personal and logical-while learning, potentially leading to longer lasting impressions and life-long learning. The XR-project combines new technological approaches with well-tested pedagogy, such as facilitated peer-to-peer learning, where students discuss dilemmas amongst themselves, guided by a mentor.

Compared to existing training and educational tools in XR, this project aims to influence the joint operational planner, the professional military officer who translates military strategy into joint operations through comprehensive planning processes. As such, it is not suited for the training of individual soldiers, rather it seeks to sharpen joint operational officers' analytical skills, critical thinking, and ability to communicate and cooperate to solve complex and wicked problems.

The pedagogical puzzle

Civilians are regularly targets of physical violence in armed conflict. Increasingly, military forces are tasked to protect civilians from perpetrators that target civilians with the intent and purpose of causing harm. This is a new task for military forces and still not well understood in policies, doctrines, military education, and practices in operations. This new understanding of protection-as defined in both United Nations (UN) and North Atlantic Treaty Organization (NATO) policies-conflicts with how we usually think about the role of military force as protectors. The traditional view leans heavily on International Humanitarian Law (IHL), which regulates how force can be used during war to avoid unlawful and unnecessary harm to civilians. These laws of armed conflict still provide the most important rules and regulations for the conduct of war and armed conflict. But they do fall short of addressing a major protection gap: providing physical protection against armed groups that target civilians intentionally as part of their warfare. Today, armed conflict usually plays out where people live, not on some distant battlefield. As such, IHL considerations are more important than ever to avoid so-called collateral damage, which can be detrimental to the success of any operations, and needless to say, devastating for victims, their families, and communities. In addition, military forces must also protect civilians from violence instigated by others-including rebel groups, rouge security forces, and violent mobs-which complicates the conduct of operations and human security concerns considerably.

New knowledge about the utility of force to protect civilians-developed at the Norwegian Defence Research Establishment (FFI) and NDUC-points to the necessity of better understanding the perpetrators of violence, i.e. why, how, and to what effect they attack civilians, simply to facilitate tailored military responses to particular threats. This so-called threat-based approach to protection provides a systematic and holistic way of considering "when to do what", based on a deeper understanding of why and how perpetrators target civilians. Nevertheless, experience from several years of teaching this new approach to master's degree students at NDUC and to military staff officers world-wide, indicate that it is challenging to convey this new knowledge effectively. There are many possible explanations for this pedagogical puzzle, but we suspect that the following are some of the most important:

a) It may be that protection of civilians is seen as "too soft" for military forces, something better left to humanitarian and development actors.

b) protection of civilians possibly challenges deeply founded understandings of what military force is and should be and represents a threshold for students to cross intellectually, culturally, and professionally.

c) the pedagogical challenge may also be linked to whom militaries are meant to protect (a distant third person vs. your own country, society, and family).

d) It may also be that the threat-based approach to protection is too complex in itself and represents another "threshold" for further learning to occur.

There are probably many other reasons that can explain the educational puzzle. The preparatory phase of the quasi-experiment will seek to investigate systematically how students relate to this topic and identify potential thresholds that might limit learning of this new task. Moreover, the project will explore whether immersive educational tools may "nudge" the students over the hypothesized threshold and into a new way of thinking about military force and civilian protection. If successful, the knowledge and technology may easily be scaled and modified to provide NATO and the UN with a unique educational tool that can be distributed worldwide.

Learning outcomes

The project seeks to improve engagement in and knowledge about the subject *Human Security and the Military Role* among master students at the Norwegian Defence University College with the help of innovative and immersive pedagogical tools (XR). More specifically, three learning outcomes capture what a future pilot iteration of the educational XR-program should contribute towards. Students should be able to:

1. **(Knowledge)** Explain the role, utility, and limitations of military force in protecting civilians from physical violence in armed conflict.
2. **(Skills)**: Analyze variations in threats to civilians in armed conflict
3. (**General competence):** Evaluate how military forces can reduce different types of violence against civilians in armed conflict, without causing more harm in the process

While we believe that all three learning outcomes are equally important, we have decided to limit the quasi-experiment to address **learning outcome two primarily**, i.e. the student's **skill** in analyzing variation in threats to civilians in armed conflict. However, skills are also dependent on knowledge and general competence, and we acknowledge that we cannot construct illogical hard walls between these three learning outcomes. Still, understanding the perpetrators of violence is the most important building block of the threat-based approach. The added value of the approach is based on a systematic understanding of threats, drawn from generic traits across historic cases of violence against civilians in armed conflict.

As such, the experiment will be designed to capture student's ability to identify threats to civilians based on five generic questions about perpetrators' characteristics, supported by a threat-typology consisting of eight threat-categories, from genocide to mob violence. Some of the baseline knowledge about this topic will be conveyed through a flipped classroom lecture before the XR-"treatment". In addition, we will add an element in the XR-experience that will touch upon learning outcome three, where students are meant to be able to evaluate and discuss "what works" in different threat situations, based on insights provided by the threat-based approach. However, due to financial limitations, we will not fully develop this part of the XR-experience in the quasi-experiment.

What do we know about learning in extended reality?

The threat-based approach to protection of civilians provides students (and joint military planners) with systematic ideas on how to analyze physical threats to civilians.

However, as already described, there seems to exist specific pedagogical challenges linked to teaching and learning this topic. In general, we know that the new understanding of the military role as protectors from others' violence is new and unfamiliar to most militaries. This wanting understanding, combined with only marginal doctrinal and practical knowledge to lean on, creates a significant gap between the practice of operations and new demands for critical thinking about the utility of force in armed conflict. To address these challenges, the XR-project is therefore leaning on existing literature about learning in higher education to understand more about pedagogies, technologies, and learning strategies that may assist in overcoming some of these pedagogical obstacles. The research and literature review process moves in parallel with the preparations for the quasi-experiment, informing every step. As of mid-October 2020, there are **four** main themes guiding the project's theoretical framework, while we also expect to discover other explanations than those identified in the literature during the actual experiment:

a) **Threshold concepts** relate to those aspects of a learning trajectory that are troublesome to the learner, require a shift in how to perceive the world (i.e. an ontological shift), and also require the learner to let go of previously accepted understanding of the world (Cousin 2006). This shift, of leaving the well-known behind, leaves the learner in a state of uncertainty before the new knowledge and understanding has become accepted. This period of transition may be seen as similar to a rite of passage, and is described as a liminal stage, as a stage of uncertainty, of doubt, but also of affordances and expectations (van Gennep 1909, Turner 1990). In present learning theory this is perceived to be a particularly valuable yet complex learning space (Meyer and Land 2003, Meyer and Land 2005). This framework is now listed as a High Impact Pedagogy by the Higher Education Academy (HEA) (Evans. Mujis and Thomlinson 2015). Seen from a broader perspective, the threshold concept framework sits well within the so-called VUCA perspective—social events characterized by volatility, uncertainty, complexity, and ambiguity—and with the increased multi-scientific interest in complexity, ill-defined and wicked problems, and radical uncertainty (Kay and King 2020). Initial threshold concepts are suggested to be situational awareness, i.e.how to "read the world" (Freire 1970), issues of *Otherness* and *Othering,* and balancing the highly complex ontological pair of tolerance of uncertainty with confidence to challenge.

b) **Empathy.** One way of learning is by imitating others. Mimicry is a decisive factor that consciously and unconsciously transforms the way people think and feel (Pentland, 2008). The brain mirrors actions, even when we observe others as if we were doing them ourselves (Iacoboni, 2009). Iacoboni's (2009) book, Mirroring People: the science of empathy and how we connect with others, claims that there are smart cells in the brain allowing people to understand others. From imitation to morality, from political affiliations to consumer choices, mirror neurons are relevant to myriad aspects of social cognition. Surprisingly, mirror neurons also become active when individuals are completely still and watching those same actions performed by other people. By watching the activities on a video, subjective experiences are reflected like a mirror to the brain through simulation. These cells help to understand

other people's mental states; all the gestures made when people speak and when they see (and hear) other people gesturing and speaking.

Drama-rich pedagogies (Ewing, 2019b) and the guidelines of process drama' (Bowell & Heap, 2013) can facilitate the design of a transformative learning experience (Grady,2020). 360 videos for training, fueled by the impact of mirror neurons, could influence students to experience a scenario to a certain extent as the actors do. In brief, they could affect the way people think and feel. Moreover, we seek to study the physiological response to empathy as embodied cognition and body language that seem to be automatic and universally similar. The embodied cognition theory is promising in providing a theoretical approach to investigate empathy better as it is expressed in cognitive, affective, and somatic levels (Wilson, 2002). The 360 video-scenarios that the XR-project will develop and test offer an opportunity to investigate cognitive empathy (as threshold concept), affective empathy (as emotional changes) and somatic-embodiment (sensor data variation).

c) Embodiment is a powerful tool that could be used in immersive story-telling and the one with probably the best documented effect in terms of induced empathy, attitude and behaviour change. Embodiment in VR is substituting a person's body by a virtual body (Slater et al, 2010) that "is apparently spatially coincident with their real body" (Neyret et al, 2020). By using various mechanisms, such as real-time motion capture, the virtual body/avatar can be programmed to move in synchronously and correspondence with the user's real body movements, invoking the perceptual illusion of the virtual body ownership (Neyret et al, 2020), similar to the rubber hand illusion (Botvinick & Cohen, 1998). In other words, VR can place people virtually in the body of another, "such that an "ingroup" member can temporarily occupy the body and position of an "outgroup" member" (Slater et al, 2020), resulting in changes in attitudes and behaviours. While the optimal embodiment implementation suggests use of advanced sensors and bodysuits, a simplified version is possible just by using HMD controllers and widely commercially available sensors such as Kinect and recently also with 360 video (Landau et al, 2020).

d) **measurement and sensors.** Physiological data will be recorded from sensors during the quasi-experiment. Electrodermal activity (in short EDA; sometimes also referred to in the scientific literature as skin conductance or galvanic skin responses) and heart-rate are the types of physiological data that will be recorded. EDA is calculated based on the conductivity of human skin, and it is generally detected using two electrodes (commonly placed on the palm-side of two fingers of the user). EDA is not consciously controllable, instead, the phenomenon is modulated autonomously by the sympathetic activity. EDA activity correlates to human behavior and cognitive and emotional states, and therefore skin conductance, offers optimal insights into autonomous emotional regulation (Boucsein, 2012). Heart rate can be measured with a number of different sensors, and the one that is planned to be used in the present study is the photoplethysmography (PPG). PPG is an easy and inexpensive measurement method that exploits characteristics of the infrared light for heart rate monitoring purposes. This method uses a light source and a photodetector placed on the skin (usually on a finger) to measure the volumetric variations of blood vessels due to blood circulation dynamics (Shelley, 2007).

Research question

The overarching aim of the quasi-experiment is to explore whether and how the use of immersive digital learning tools may influence students' skills in analyzing variation in threats to civilians caught in armed conflict. The main research question asks:

How (and to what degree) do immersive educational tools/technologies (including VR-embodiment, 360°- videos, map applications) influence learning about threshold concepts (the threat-based approach to protection of civilians)?

A mixed-methods approach

The quasi-experiment will employ a mixed-methods approach. Surveys and interviews will be employed at three points in the process: pre-, in-, and post-experiment, each fulfilling different tasks. The pre-experiment self-reporting survey aims to capture students' attitudes towards human security and the role of military force, where we expect marginal earlier knowledge and exposure to this topic in education and practice. We consider employing an Implicit Association Test, a self-reporting attitude questionnaire, for this purpose. The in-experiment survey aims to capture immediate impressions after (each) XR-experience, concentrating on affective and cognitive empathy, as well as the ability to analyze threats to civilians. We will also consider running group/individual interviews immediately after each experiment iteration, to capture more details and insights about a broader set of variables, including friction, motion-sickness, user friendliness of goggles, etc. Finally, we seek to combine surveys and interviews post-experiment to capture knowledge and attitude retention some time after the quasi-experiment. Importantly, we will design the quasi-experiment in a way that will demand student deliberations about relevant choices when considering different threats to civilians, to measure if they have undergone some mental change during the process, possibly indicating deeper/new understanding and over the threshold-thinking. We will alo employ various sensors collecting physiological data to capture biological reactions to 360°videos and VR-programs, with the aim of evaluating and quantify the level of empathy/engagement/learning experienced by the user. We also aim to capture body heat variations, using thermal cameras, as well as traditional cameras and sound recordings for observation and analysis of body movement and discussions.

Experiment audience

The 2021-2022 master's degree class consists of 55 students. They come from all branches of the armed forces, including land, air, maritime, and cyber(?). There is a clear majority of men, which is representative for the armed forces in general. They have a varied background, educationally, professionally, and personally. They are generally between 30 and 40 years old. Common to all is that they are selected by their branch as a candidate to the master's degree, rather than through open competition. To increase the validity of our findings we aim to reach as many of them as possible-preferably all-in the same experiment, which possibly indicates that we must run seven iterations of the experiment, where one group will consist of only seven students. We will consider possibilities for randomized selection into groups, but more likely the students will already be assigned to a group of eight/seven. It might be possible to run seven iterations over five days, although five iterations is more realistic. Some of the

students might not be able or willing to join. The following description concerns one iteration. We will also consider using a control group that is subjected to a learning process without XR-tools, depending on the manpower and resources available.

Quasi-experiment design

Based on the research questions and hypotheses developed above, the XR-project will design a quasi-experiment-consisting of five steps-to generate empirical data that will be used to explore the presence or absence of our theoretical expectations and possibly other, yet to be identified mechanisms concerning learning in Extended Reality:

- **Step one**: Creating a common intellectual platform through a flipped classroom lecture including discussion, introducing the core ideas underpinning the threat-based approach to protection of civilians
- **Step two:** Triggering affective empathy for victims of both ethnic cleansing and political insurgency and perpetrators of violence (ethnic cleansing) through embodiment in combined VR and 360°-video narratives.
- **Step three:** Influencing cognitive empathy through dialogue-based simulations with AI-avatars (political insurgents) in realistic virtual surroundings.
- **Step four:** Affecting cognitive empathy and analytical skills through group discussions and practical threat-analysis in VR in a virtual 3D-map application
- **Step five:** Honing cognitive empathy and analytical skills through facilitated peer-to-peer process about courses of action development and potential outcomes of operations.

List of references

1. Beadle, Alexander William. 2014. Protection of Civilians - Military Planning Scenarios and Implications. Kjeller: Norwegian Defence Research Establishment (FFI).

2. Beadle, Alexander William, and Stian Kjeksrud. 2014. Military Planning and Assessment Guide for the Protection of Civilians. Kjeller: FFI. FFI-report. https://www.ffi.no/no/Rapporter/14-00965.pdf.

3. Boucsein, W. (2012). Electrodermal activity. Springer Science & Business Media.

4. “The Utility of Military Force to Protect Civilians in UN Peace Operations.” In The Use of Force in UN Peacekeeping, Routledge.

5. Bowell, P., & Heap, B. S. (2013). Planning Process Drama, Enriching Teaching and Learning (2nd ed.). Abingdon, England: Routledge.

6. Cousin, G. (2006). An Introduction to Threshold Concepts. Planet No1, December 2006, pp. 4 - 5.

7. Daniel H. Landau, Béatrice S. Hasler, Doron Friedman: Virtual Embodiment using 180º Stereoscopic Video. June 07, 2020 Frontiers in Psychology https://www.frontiersin.org/ articles/10.3389/fpsyg.2020.01229/full.

8. Evans et al. (2015). Engaged student learning. High Impact strategies to enhance student achievement. Web: https://www.advance-he.ac.uk/knowledge-hub/engaged-student-learning-high-impact-strategies-enhance-student-achievement.

9.Ewing, R. (2019b). Embedding Arts-Rich English and Literacy Pedagogies in the Classroom. Literacy Learning: The Middle Years, 27(1), 7–17.

10. Freire, P. (1970). Pedagogy of the oppressed. New York, NY: Seabury.

11. Grove O'Grady A. (2020) Towards a Pedagogy of Empathy. In: Pedagogy, Empathy and Praxis. Palgrave Pivot, Cham. https://doi.org/10.1007/978-3030-3952614

12. Kay,J. And King, M. (2020). Radical Uncertainty. Decision-Making Beyond the Numbers. NY: Norton.

13. Iacoboni, M. (2009). Mirroring people: the science of empathy and how we connect with others. New York, N.Y.: Picado

14. Kjeksrud, Stian. 2016. "The Utility of Force for Protecting Civilians." In Protection of Civilians, Oxford University Press.

15. "Using Force to Protect Civilians. A Comparative Analysis of United Nations Military Protection Operations." University of Oslo. http://urn.nb.no/URN:NBN:no-71600.

16. Kjeksrud, Stian, Alexander William Beadle, and Petter H. F. Lindqvist. 2016. Protecting Civilians from Violence: A Threat-Based Approach to Protection of Civilians in United Nations Peace Operations. Oslo/Kjeller: NODEFIC/FFI. https://www.ffi.no/no/Publikasjoner/Documents/Protecting-Civilians-fromViolence.pdf.

17. Lindqvist, Petter H. F., Stian Kjeksrud, Alexander William Beadle, and Gustav Nyqvist. 2020. "Human Security and the Military Role: Finding the Utility of Force to Protect Civilians from Violence." https://forsvaret.inkrement.no/.

18. Meyer, J.H.F. and Land, R. (2003). Threshold concepts and troublesome knowledge: linkages to ways of thinking and practicing. In: Rust, C. (ed.), Improving Student Learning - Theory and Practice Ten Years On. Oxford: Oxford Centre for Staff and Learning Development (OCSLD), pp 412-424.

19. Meyer, J., and Land, R (2005) 'Threshold concepts and troublesome knowledge (2) epistemological considerations and a conceptual framework for teaching and learning. Higher Education, 49, 373-88.

20. Pentland, A. (2008). Honest signals: How they shape our world. Cambridge, MA: MIT Press.

21. Shelley, K. H. (2007). Photoplethysmography: beyond the calculation of arterial oxygen saturation and heart rate. Anesthesia & Analgesia, 105(6), S31-S36.

22. Wilson M (2002) Six views of embodied cognition. Psychonomic Bulletin & Review 9(4): 625–636. Rivkin, J. (2010). The Empathic Civilization: The Race to Global Consciousness in a World in Crisis. Cambridge: Polity.

Використання Російською Федерацією суспільно-центричних стратегій як складової гібридної війни проти України та Заходу

Юрій Цурко
Старший викладач кафедри застосування інформаційних технологій та інформаційної безпеки інституту забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-7481-8399

Анотація. *Виступ відбувся 17 листопада 2021 року на міжнародній науково-практичній конференції "Гібридна агресія Російської Федерації: досвід протидії Україні, наслідки для Європи" і присвячений аналізу комунікаційних заходів РФ на підтримку її зовнішньої політики, зокрема щодо України та країн Європи.*

Ключові слова: *інформаційна війна, наратив, Російська Федерація, стратегія, суспільство, Україна.*

Вступ

Постановка проблеми. Розвиток інформаційних технологій, зростання залежності суспільства від таких технологій, збільшення його відкритості, а також вразливість вільних демократичних держав до гібридних загроз створює вигідні умови для авторитарних і диктаторських режимів, передусім – Російської Федерації щодо тиску на сусідні країни та реалізації агресивних цілей політики. Одна із важливих сфер впливу, що використовуються в рамках гібридної війни / загроз, є суспільство, яке потрібно захищати і підвищувати його стійкість проти ворожої пропаганди, дезінформації, ідеології.

Аналіз останніх досліджень та публікацій. У публікаціях [1-2] описані бачення РФ навколишнього світу, стратегії та завдання, які РФ намагається реалізувати для досягнення цілей національної безпеки. Публікації [3-5] містять детальний аналіз соціально-орієнованих стратегій, наративів, комунікаційних напрямів, тем і меседжей РФ. Публікації [6-10] містять поточне бачення вищого керівництва РФ проблем у відносинах з Україною та його наміри щодо силового втручання у внутрішні справи України із порушенням її державного устрою, суверенітету, територіальної цілісності та незалежності.

Мета доповіді. Доповідь призначена для інформування широкого кола наукової спільноти та суспільства України і країн Заходу про агресивну суть політики РФ і загрози у соціальній сфері, що вона несе.

Виклад основного матеріалу

Слово "стратегія" означає – загальний план досягнення цілей певної діяльності з визначенням шляхів досягнення та засобів, які будуть

використовуватися. Вміння розробляти стратегії є надзвичайно цінним і є запорукою успіху.

Отже, чи є у Москви стратегії, спрямовані проти суспільства України? Певен, що є. На відміну від України, яка 30 років тому була регіональним актором, не мала державності та, відповідно не розробляла ніяких стратегій національної безпеки (СНБ), оборони тощо, РФ після розпаду СРСР зберегла відповідні знання та вміння.

Тому пропоную звернутися до стратегії національної безпеки РФ і подивитися, що там написано, як Москва сприймає світ навколо і що хоче робити. Згідно витягу із СНБ у редакції 2015 року та оновленої її версії від липня цього року. Зміст останнього документу у порівнянні із попереднім є суттєво розмитим, багато речей не називається прямо і чітко, а навпаки, дуже узагальнено. Водночас, бачення загроз залишається тим самим – Захід є ворогом.

При цьому значна увага приділяється соціальній складовій, наприклад: “размыванию традиционных ценностей, искажению мировой истории”, проведенню “информационных кампаний, направленных на формирование враждебного образа России”, “ограничение использование русского языка, запрет на деятельность российских СМИ и использование информационных ресурсов” [1].

Відповідно до бачення “загроз”, формується перелік цілей, що Москва хоче досягти, та відповідних завдань. Так, розділ ІІІ [1] містить перелік національних інтересів, частина з яких відноситься до соціальної сфери.

Одним із так званих “стратегических национальных приоритетов” визначено “защиту традиционных российских духовно-нравственных ценностей, культуры и исторической памяти”, водночас інші пріоритети також містять соціальну складову [1].

Частина із цілого переліку завдань пов’язана із захистом населення РФ від “тлєтворного” впливу Заходу та виховання патріотизму, частина – на активне просування так званого “культурного суверинитета” РФ [1].

При цьому загрозу для України несуть завдання щодо розвитку “добровольческого движения”, “поддержки религиозных организаций традиционных конфессий”, “защиты исторической правды”, “защиты российского общества от внешней идейно-ценностной экспансии”, “повышение роли России в мировом гуманитарном, культурном, научном и образовательном пространстве” [1].

Подібні завдання ставляться і для досягнення цілей зовнішньої політики, основним інструментом якої є дипломатія. Особливо загрозливою є “оказание поддержки соотечественникам, проживающим за рубежом” та “укрепление братских связей между русским, белорусским и украинским народами” [1]. Цікаво, що це єдина згадка про українське; Україна як держава, суб’єкт взагалі не розглядається, на відміну від попередньої редакції СНБ від 2015 року, де, як ми бачили, вона характеризувалась як нелегітимне утворення внаслідок антиконституційного державного перевороту за підтримки Заходу і “долгосрочный очаг нестабильности в Европе и непосредственно у границ России”.

Інший документ “Концепція зовнішньої політики РФ” також містить завдання щодо захисту співвітчизників, посилення ролі російської мови у світі, розвиток і державна підтримка ЗМІ РФ за кордоном [2].

Тобто ми маємо справу з добре розробленою стратегією, включаючи суспільно-центричні компоненти, із комплексним і творчим вибором шляхів та інструментів її реалізації. РФ діє за сімома напрямами, використовуючи значно більше інструментів, ніж традиційні – дипломатія, інформація, військова сила, економіка (англійська абревіатура DIME) [3]. Чітко видно ознаки гібридності підходу: міграційні кризи 2015 та 2021 років, пропагандистська тематика про COVID-19, “Північний потік-2” є ланками одного ланцюга.

Інформаційна війна (головний інструмент впливу на суспільство), що проводить РФ, є суттєвим удосконаленням комуністичної пропаганди та активних заходів “радянського” зразка. В першу чергу це стосується застосування нових інструментів, які стали доступними внаслідок розвитку інформаційних технологій – електронних ЗМІ, соціальних мереж та відкритої структури мережі Інтернет.

Смислову основу інформаційної війни складають комплекс наративів або комунікаційних напрямів, які є основними або глобальними [4].

Ці головні наративи мають регіональні відгалуження, спрямовані більш конкретно проти України, Європи, США та інших країн [4, 5].

Є також комунікаційні напрями спеціально для внутрішнього користування [4, 5].

Хоча ці наративи розроблені та використовуються давно, вони лишаються актуальними і зараз.

Уваги заслуговують так звані “статті” В. Путіна та Д. Медвєдєва. У путінському “творі” артикулюється історична штучність і несамостійність України, а також використання її Заходом як інструмент для стримування РФ. Особливий акцент робиться на зростанні в країні нацизму та наявності “внутрішньоукраїнського конфлікту” або “громадянської війни” на сході [6].

Довідково. 12 липня цього року на офіційному сайті президента РФ було опубліковано статтю його авторства «Про історичну єдність росіян і українців». У ній В. Путін оголосив росіян, українців і білорусів одним народом, якому слід бути разом. Як заявляв минулого року В. Сурков, колишній кремлівський “куратор” Донбасу, “до братерства краще за все примушувати силою” [7]. Статтю В. Путіна в Росії було включено в перелік обов’язкових тем для занять з військовослужбовцями з військово-політичної підготовки.

Медвєдєвські тези спрямовані проти керівництва України, при чому артикулюється його несамостійність, слабкість, корумпованість та ведуть до висновку про “бессмысленность и даже вредность отношений с нынешними руководителями” [8]. Фрази про “дождаться появления на Украине вменяемого руководства”, “Россия умеет ждать. Мы люди терпеливые” містять приховану погрозу силової зміни політичної системи в Україні.

На такі ж висновки спрямовує і нещодавні “Валдайські тези” [9] В. Путіна та інтерв’ю минулого тижня [10], які є логічним продовженням цього

комунікаційного напряму. Путін відкрито заявляє про тупик у стосунках з Україною і неможливістю досягти своїх цілей щодо її підкорення старими способами.

Висновки

Отже, чого нам чекати? Враховуючи чітке законодавче та персональне ігнорування України як незалежної і суверенної держави, Москва, ймовірно спрямовуватиме свої інформаційні заходи на делегітимізацію органів державної влади України, формування розколу в українському суспільстві, посилення позицій про-російських сил з можливим силовим приведення їх до влади.

Навряд чи слід очікувати згоду та присутність РФ на міжнародних форумах, як Мінській, Нормандський формат або якийсь новий, наприклад за участю США.

Смислову основу інформаційних заходів, ймовірніше за все, складатиме удосконалений наратив “Русского мира” щодо необхідності об’єднання братських слов’янських народів.

Інформаційні заходи будуть добре скоординовані із застосуванням інших “жорстких та м’яких” силових інструментів, у тому числі – проти країн ЄС і НАТО та із можливим суттєвим зниженням порогу застосування ЗС і підготовленими збройними провокаціями.

Список літератури

1. Указ Президента Российской Федерации от 02.07.2021 № 400 “О Стратегии национальной безопасности Российской Федерации”, Интернет-портал Администрации Президента России. http://www.kremlin.ru/acts/bank/47046/page/1.

2. Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В.Путиным 30 ноября 2016 г.), Интернет-портал Министерства иностранных дел Российской Федерации, 01.12.16. https://archive.mid.ru/web/ guest/foreign_policy/official_documents/-/asset_publisher/ CptICkB6BZ29/content/id/2542248.

3. Bob Seely (2018), A definition of contemporary Russian conflict: how does the Kremlin wage war?, The Henry Jackson Society, 2018. http://henryjacksonsociety.org/wp-content/uploads/ 2018/06/A-Definition-of-Contemporary-Russian-Conflict-new-branding.pdf.

4. Hybrid Warfare Analytical Group Research, 2018. https://uacrisis.org/wp-content/uploads/2018/02/Europe-image-in-Russian-TV-1.pdf.

5. Putin’s asymmetric assault on democracy in Russia and Europe: implications for U.S. National Security, a minority staff report prepared for the use of the Committee on foreign relations United States Senate, January 10, 2018. U.S. Government Publishing Office, Washington, 2018. https://www.congress.gov/115/cprt/SPRT28110/ CPRT-115SPRT28110.pdf.

6. Путин В. (2021), Об историческом единстве русских и украинцев, Интернет-портал Администрации Президента России,12.07.2021. http://kremlin.ru/ events/president/ news/66181.

7. Сурков В. (2019), Долгое государство Путина. О том, что здесь вообще происходит, Интернет-портал “Независимая газета”, 11.02.2019. https://www.ng.ru/ ideas/2019-02-11/5_7503_surkov.html

8. Медведев Д. (2021) Почему бессмысленны контакты с нынешним украинским руководством. Пять коротких полемических тезисов, Газета “Коммерсантъ”, №184/П, 11.10.2021, стр. 3. https://www.kommersant.ru/doc/ 5028300.

9. Мисливская Г. (2021), Путин об Украине: Это тупик, и я не очень понимаю, как из него выйти, Интернет-портал “Российской газеты”, 21.10.2021. https://rg.ru/2021/10/21/putin-ob-ukraine-eto-tupik-i-ia-ne-ochen-ponimaiu-kak-iz-nego -vyjti.html.

10. Зарубин П. (2021), Интервью телеканалу “Россия”, Интернет-портал Администрации Президента России,13.11.2021. http://kremlin.ru/events/president/ news/67100.

Мілітаризація молоді як складова російської політики на тимчасово окупованих територіях Донецткої і Луганської областей

Ольга Пашкова, кандидат історичних наук
Науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-6525-4613

Анотація. *Молодь, яка проживає на тимчасово окупованій території України, зокрема окремих районів Донецької і Луганської областей, перебуває у фокусі інтересів Російської Федерації. Запровадження так званого військово-патріотичного виховання мешканців цих територій розглядається як політика мілітаризації, що спрямовується на формування "нової ідентичності" молоді, яка має ототожнювати себе із псевдореспубліками, та підготовку до військової служби у незаконних збройних формуваннях. Мета дослідження полягає у висвітленні основних напрямів мілітаризації дітей та підлітків тимчасово окупованих територій Донецької і Луганської областей.*

Загальнонаукові методи дослідження (аналіз, синтез, індукція та дедукція, порівняння) дали змогу студіювати предмет дослідження у безперервній динаміці та діалектичній взаємопов'язаності. Специфіка предмета дослідження передбачала застосування спеціальних методів воєнно-історичного дослідження, зокрема історико-порівняльного та історико-генетичного.

Окупаційні адміністрації, керовані військово-політичним керівництвом Російської Федерації, створили "систему" освіти, а також позаосвітньої діяльності, що дає змогу залучати максимальну кількість місцевої молоді та всебічно впливати на підростаюче покоління на тимчасово окупованих територіях України. Заходи, що здійснює Україна із протидії російському впливу, насамперед, полягають у залученні молоді до українського соціокультурного середовища, зокрема через спрощений доступ до освітніх послуг.

Отримані результати дослідження свідчать про необхідність подальшої системної роботи у напрямі заохочення молоді з тимчасово окупованих територій Донецької і Луганської областей отримувати українську освіту, адаптації її до інформаційного простору України.

Ключові слова: *молодь, мілітаризація, військово-патріотичне виховання, тимчасово окуповані території України, незаконні збройні формування.*

Вступ

Постановка проблеми. Після окупації окремих районів Донецької і Луганської областей України у 2014 році діяльність військово-політичного керівництва Росії через окупаційні адміністрації цих територій спрямовувалася на поступову втрату місцевою молоддю української ідентичності. "Виховання" дітей та підлітків у дусі відданості псевдореспублікам, що розглядається як

підготовка молоді до участі у збройній агресії проти України, стало викликом для нашої держави. Поступова втрата зв'язків із Україною через перебування в антиукраїнському середовищі зумовлює потребу протидії російському негативному впливу.

Аналіз останніх досліджень і публікацій. Проблема мілітаризації молоді тимчасово окупованих територій України залишається у фокусі уваги державних органів влади України, а також громадських організацій. Окремі аспекти впливу на молодь окремих районів Донецької і Луганської областей висвітлювалися вітчизняними дослідниками. Зокрема, у роботах [7; 8] узагальнено використання наративів періоду Другої світової війни, здійснення візуальної пропаганди з історичними наративами на тимчасово окупованих територіях України.

Мета дослідження **–** висвітлення основних напрямів мілітаризації дітей та підлітків тимчасово окупованих територій Донецької і Луганської областей.

Виклад основного матеріалу

Мілітаризація ("військово-патріотичне виховання") дітей на тимчасово окупованих територіях Донецької і Луганської областей здійснюється системно та цілеспрямовано у ході освітньої та позаосвітньої діяльності. **На рівні освітніх закладів** вплив на молодь здійснюється *через викладання навчальних дисциплін*. Упродовж років окупації у псевдореспубліках було розроблено навчально-методичні матеріали для провадження освітньої діяльності, а шкільні навчальні програми було адаптовано під ідеологічні потреби окупаційних адміністрацій. Значний акцент в освітньому процесі було сконцентровано на посиленні так званого регіонального "патріотизму". Безперечно, найбільший виховний потенціал належить дисциплінам гуманітарного циклу. Для цього у програму закладів середньої освіти було введено навчальний предмет "Уроки громадянськості Донбасу" та "Історія Вітчизни", що утверджують "особливість" Донбасу, його "окремішність" від України та "нерозривність зв'язку з Росією". Таким чином здійснюється спроба "обґрунтувати" утворення так званих республік через начебто неукраїнську ідентичність населення Донбасу.

На уроках історії у закладах середньої освіти окрема увага приділяється періоду промислового розвитку Донбасу в XIX ст., створенню "Донецько-Криворізької республіки", подіям на Донбасі у період Другої світової війни. Культивуються постаті "трудового Донбасу" – Олексія Стаханова, Петра Кривоноса тощо, а також символи Донбасу – меморіальний комплекс "Твоїм визволителям, Донбас", Савур-Могили тощо. Значне місце у "республіканських" посібниках із історії відводиться подіям весни 2014 року. Створюється проекція історичної пам'яті про німецько-радянську війну 1941–1945 років на сучасний збройний конфлікт на Донбасі, що проголошується "прямим продовженням війни з фашизмом", зокрема, через виконання навчальних завдань по здійсненню історичних паралелей тощо.

"Уроки мужності", присвячені подіям становлення псевдодержавності на тимчасово окупованих територіях (так звані День Республіки, День прапору, День Донецько-Криворізької Республіки), Другої світової війни (День визволення Донбасу, День Перемоги), а також іншим датам, пов'язаним із

історією Радянського Союзу (День виводу військ з Афганістану, День захисника Вітчизни). До проведення уроків залучаються представники "МДБ", "народної міліції", інших незаконних збройних формувань.

Комеморація ("увічнення пам'яті героїв"). Одним із об'єктів комеморації виступають учасники незаконних збройних формувань, зокрема через присвоєння їхніх імен середнім закладам освіти, встановлення на будівлях закладів меморіальних дошок тощо. Іншим напрямом увічнення пам'яті залишається тематика Другої світової війни. Так, у закладах освіти "ЛНР" 2020 рік був оголошений "Роком пам'яті і слави" із проведенням заняття, присвяченого подіям 1941–1945 років.

Крім того, на тимчасово окупованих територіях ОРДЛО почали діяти окремі заклади з "посиленою військовою підготовкою" ("кадетський корпус імені О. Захарченка" на базі закладу середньої освіти № 4 у Донецьку, "козачий кадетський корпус імені маршала авіації Олександра Єфимова" в Луганську). Загалом, у 2018–2019 навчальному році у закладах середньої освіти "ЛНР" діяло вісім так званих кадетських (козачих) класів, у 2019–2020 – їх кількість збільшилася до 18 [1].

Військові ігри, військово-польові збори. Залучення дітей до навчально-практичних польових зборів за темами "Виживання в лісовій зоні", "Виживання в зимових умовах", "Виживання під час бойових дій", змагань з початкової військової підготовки "Майбутній воїн" і відкритої першості "ДНР" з військово-прикладного семиборства, "військово-патріотичних" змагань "Юний десантник", навчально-практичних занять з курсу "Початкова військова підготовка / Медико-санітарна підготовка" на полігонах військових частин тощо.

Російська Федерація через окупаційні адміністрації здійснює вплив на свідомість молоді тимчасово окупованих територій України і **у ході позаосвітньої діяльності**, зокрема через фінансування та всебічну підтримку *псевдопатріотичних організацій та воєнізованих таборів* (тривалістю від двох до десяти днів) для дітей і підлітків віком 10–17 років.

Лише на окупованій території Донецької області Офісом Генерального прокурора України встановлено понад 10 так званих військово-патріотичних клубів, зокрема "Молода Гвардія Донбасу", "Амазонки", "Патріот", "Бастіон", "Степові Вовки". За даними, оприлюдненими у "ДНР", кількість "патріотичних" клубів, гуртків та об'єднань у цій частині окупованого Донбасу наприкінці 2019 року становила 62, а кількість їхніх "вихованців" нараховувала 2014 осіб [2]. Схожі об'єднання діяли і на окупованій території Луганської області ("Амазонки", "Доброволець", "Редут" тощо). У 2020 році їх нараховувалося 32, до складу яких входило 987 неповнолітніх [3].

Дозвілля дітей та молоді тимчасово окупованих територій Донецької і Луганської областей здійснюють через організацію воєнізованих "військово-патріотичних" таборів як у самих псевдореспубліках, так і на території тимчасово окупованої Автономної Республіки Крим та м. Севастополь та самої Російської Федерації. Так, у 2016 році у м. Коврові (РФ) у таборі, сформованому на базі навчального центру Міністерства оборони Російської Федерації, неповнолітні громадяни України проходили базову військову підготовку разом із

дітьми з Росії та Сирії [4]. У цей же час у Євпаторії (Автономна Республіка Крим) проходив молодіжний "військово-патріотичний" табір-форум "Донузлав 2016", учасниками якого були підлітки з Росії, Білорусі, а також окупованих Російською Федерацією територій: частини Донбасу, Південної Осетії, Абхазії та Придністров'я [5]. Програма подібних таборів передбачала проведення вогневої, медичної, фізичної, стройової підготовки. Діти проходили смугу перешкод, вивчали техніки рукопашного бою та скелелазіння, основи виживання, методи поводження з вибухонебезпечними предметами, техніки огляду і конвоювання тощо.

Невід'ємною складовою програми таких таборів залишається ідеологічна робота з молоддю тимчасово окупованих територій України. Російське керівництво використовує маніпуляції з історією як інструмент формування антиукраїнських настроїв серед підростаючого покоління [6].

Публічні заходи, приурочені "історичним датам", культивація яких здійснювалася ще за радянських часів, або подіям, пов'язаним із так званим державотворенням псевдореспублік. Зокрема, заходи з нагоди 9 травня в окупованих містах окремих районів Донецької та Луганської областей носять масовий характер, супроводжуються мітингами за участю представників окупаційних адміністрацій, учасників німецько-радянської війни 1941–1945 років, членів незаконних збройних формувань, а також представників влади Російської Федерації, нерідко депутатів Державної Думи РФ. Крім того, молодь "ДНР-ЛНР" активно залучається до численних науково-культурних, гуманітарних обмінів делегаціями з регіонами РФ, до політико-ідеологічних заходів у Росії. Сакралізація дат 9 травня, 22 червня, 23 лютого спрямовується на збереження радянських комеморативних практик для створення зв'язку між поколіннями "захисників" Донбасу від "фашистів" [7-8].

Водночас держава Україна продовжує здійснювати заходи, спрямовані на протидію російському впливу на молодь тимчасово окупованих територій України. Зокрема, у жовтні 2020 року Офіс Генерального прокурора України направив до Офісу прокурора Міжнародного кримінального суду повідомлення щодо політики пропаганди та нав'язування військової служби серед дітей на тимчасово окупованій території Автономної Республіки Крим [9] через включення місцевих освітніх установ у систему "військово-патріотичного" виховання Російської Федерації, діяльність воєнізованих класів у закладах середньої освіти, функціонування літніх військових таборів тощо. Така політика Росії на території півострова є інструментом примусу молоді до служби в армії держави-окупанта.

Включення молоді тимчасово окупованих територій у соціокультурний простір України, зокрема через отримання української освіти, стало перспективним напрямом державної політики реінтеграції окупованих районів Донбасу та Автономної Республіки Крим. Так, з 2016 року в Україні під патронатом Міністерства освіти і науки України працює програма "Доступна освіта", завдяки якій у мешканців тимчасово окупованих територій з'явилася можливість вступати до закладів вищої освіти України за спрощеною процедурою і отримати український документ про освіту. Упродовж 2019/2020

навчального року понад 4,5 тис. дітей із цих територій здобували освіту в Україні за дистанційною формою навчання. Наприкінці травня 2020 року в межах гуманітарної підгрупи Тристоронньої контактної групи було вирішено питання спрощеного механізму перетину дітьми КПВВ, які мають бажання отримати освіту на території, підконтрольній Україні. Ці питання було врегульовано на законодавчому рівні, що дало змогу забезпечити реалізацію права на освіту для понад 2 000 дітей із тимчасово окупованих територій, з яких понад 300 осіб – з тимчасово окупованої території Автономної Республіки Крим та м. Севастополя [10, с. 119, 220]. До закладів вищої освіти України у 2020 році з окупованих територій Донбасу та Криму вступило 2026 осіб. Відповідно до Державної цільової соціальної програми "Молодь України" на 2021–2025 роки, затвердженої Кабінетом Міністрів України, передбачається збільшення кількості вступників з цих територій до закладів вищої освіти України до 10 тисяч.

Водночас залишається низка проблемних питань, що ускладнюють процес реінтеграції дітей та молоді з тимчасово окупованих територій. Зокрема, недостатній рівень поінформованості мешканців окупованих територій про можливості реалізації прав і свобод в інших регіонах України, перешкоджання отриманню освіти у навчальних закладах України з боку окупаційних адміністрацій, масована антиукраїнська пропаганда, гостра потреба у соціально-психологічній адаптації дітей у соціокультурний простір України після їх вступу до українських закладів освіти. Так, у квітні 2021 року Кабінет Міністрів України затвердив бюджетну програму "Забезпечення реінтеграції молоді з тимчасово окупованих територій Донецької та Луганської областей, тимчасово окупованої території Автономної Республіки Крим та міста Севастополя", що передбачає підготовку, забезпечення та проведення безоплатного навчання на курсах з підготовки до вступу до державних закладів вищої освіти молоді; проведення інформаційних кампаній, реалізацію проєктів, здійснення культурно-мистецьких, спортивних та інших заходів, спрямованих на особистісний та патріотичний розвиток молоді тощо.

Висновки

Таким чином, мілітаризація (так зване військово-патріотичне виховання) молоді стала елементом політики держави-окупанта на тимчасово окупованих територіях Донецької і Луганської областей України, що має на меті втрату української ідентичності мешканцями цих територій, у першу чергу дітьми та юнацтвом. З огляду на це питання реінтеграції дітей і молоді з тимчасово окупованих територій України до українського конституційного, культурного, інформаційного, освітнього простору та створення передумов для відновлення територіальної цілісності та суверенітету України залишається важливим напрямом державної політики України.

Список літератури

1. Поддержка и развитие кадетского/казачьего компонента в системе образования Луганской Народной Республики [Електронний ресурс]. – Режим доступу: https://minobr.su/ks-parioticheskoe-vospitaniye/8355-podderzhka-i-razvitie-

kadetskogo-kazachego-komponenta-v-sisteme-obrazovaniya-luganskoy-narodnoy-respubliki.html

2. Постанова донецької народної республіки № 22-3 “Про затвердження республіканської програми патріотичного виховання громадян донецької народної республіки на 2020–2022 роки” від 30.04.2020» [Електронний ресурс]. – Режим доступу: https://pravdnr.ru/npa/postanovlenie-pravitelstva-doneczkoj-narodnoj-respubliki-ot-30-aprelya-2020-goda-%E2%84%96-22-3-ob-utverzhdenii-respublikanskoj-programmy-patrioticheskogo-vospitaniya-grazhdan-doneczkoj-narodnoj.

3. Почти тысяча молодых людей ЛНР участвуют в работе военно-патриотических клубов Республики [Електронний ресурс]. – Режим доступу: https://mklnr.su/6096-pochti-tysyacha-molodyh-lyudey-lnr-uchastvuyut-v-rabote-voenno-patrioticheskih-klubov-respubliki.html

4. Дітей окупованого Донбасу і Сирії навчають військовій справі в Росії [Електронний ресурс]. – Режим доступу: https://jfp.org.ua/rights/porushennia/violation_categories/dity-u-zbroinomu-konflikti/rights_violations/kovrov

5. У кримському таборі «Донузлав 2016» влітку «виховували» дітей з окупованих територій [Електронний ресурс]. – Режим доступу:

https://jfp.org.ua/rights/porushennia/violation_categories/dity-u-zbroinomu-konflikti/rights_violations/krym

6. Нелиберальное воспитание в Луганской Республике [Електронний ресурс]. – Режим доступу: https://gtrklnr.com/2019/11/06/neliberalnoe-vospitanie-v-luganskoj-respublike/

7. Маєвський О. (2020), Формування інформаційного простору в так званих “ДНР” та “ЛНР” методами експлуатації візуальних образів Другої світової війни, Інформація і право, № 2 (33), С. 132–140.

8. Топальський В.Л., Іваненко С.М. (2020), Використання конструкту «Велика вітчизняна війна» в російській антиукраїнській пропаганді, Воєнно-історичний вісник, № 3 (37), С. 42–54.

9. Офіс Генпрокурора направив в МКС інформаційне повідомлення щодо пропаганди військової служби серед дітей в окупованому Криму [Електронний ресурс]. – Режим доступу: https://www.gp.gov.ua/ua/news?_m=publications &_c=view&_t=rec&id=281213

10. Щорічна доповідь уповноваженого Верховної Ради України з прав людини за 2020 рік про стан додержання та захисту прав і свобод людини і громадянина в Україні (2021), Київ, 354 с.

What Russia's IPb behavior towards Ukraine can teach Norway: Reflections from NDUUs Hybrid War Conference

Karen-Anna Eggen, PhD Fellow
Norwegian Institute for Defence studies. Norwegian Defence University College.
Oslo, Norwegia

Introduction

Russia loves symbolism. This is reflected in both Russia's domestic celebrations and external behavior. From grand parades celebrating forgone heroes or feats, to mock attacks on Western military vessels on various anniversaries and the Sputnik vaccine, symbolically named after the first mission to space. As we approach the 30th anniversary of the collapse of the Soviet Union, Russia seem set on reestablishing its lost power, having already seized de-facto control of Belarus, now escalating the conflict on the border of Ukraine [1]. Some also call this Putin's legacy building, as a young KGB officer during the collapse, now an ageing 70-year-old tsar.

Russia's "hybrid war" [2] approaches to Ukraine have implications beyond the Ukrainian border. Most notably it has resulted in heightened tensions in Europe and alongside Russia's Western border, including in the shared Arctic space with Norway. Russia's hybrid war approaches towards Ukraine have also provided insight into Russian strategic thought and behavior. How can a country, such as Norway, with vastly different cultural, historical, and geographical ties with Russia, learn from what Ukraine has gone through the past eight years?

Presenting main material

The Great Confrontation: Informatsionnoe Protivoborstvo (IPb)

In my doctoral project, the aim is to examine Russian information confrontation, "informatsionnoe protivoborstvo" (IPb), in the Nordic region. IPb is by many translated as information warfare, which is of course a term suitable to a country such as Ukraine, where information is used on the higher end conflict scale, i.e., in actual warfare. Information warfare as a term had an uptick in popularity following Russia's annexation of Crimea and continued incursions in Eastern Ukraine.

IPb reflects a concept and belief that Russia is in a constant information confrontation with, particularly, the West, and the increased importance placed on information tools (non-military tools) as a means and methods to meet objectives and achieve gains beneficial to Russian state power. IPb encompass the entire conflict spectrum, from peace to war, where information warfare is the extension of IPb on the higher end. However, most of Russia's IPb activities take place on the lower end, during peacetime, with the aim to influence perceptions and behavior, as well as gather information and intelligence that can be used in the event of a conflict escalation.

The military is still of crucial importance. Together with Russia's nuclear arsenal they are always lurking in the background, ready to be used as a threat. Except for Georgia 2008, Ukraine 2014, and Syria 2015, where physical military operations were (and in

the latter cases continues to be) used, the military most often serves to gain psychological effects towards Russia's Western adversaries. As for the case of Ukraine, it is Putin's iron bar to break open the door of bilateral talks with President Joe Biden and ensure Russa a better bargaining position.

The key goal of IPb is to affect information management systems and infrastructure of the target state, but also achieve desired effects in the mind if the target populations' perceptions and decision-making processes. And, equally important, protect Russia's society and infrastructure from the same type of influence attempts.

Ukraine – of Particular Importance to Russia

There is little doubt that Ukraine holds a special place in Russian thinking. Since the 2014 annexation, and increasingly so in 2021, the Russian elite has argued that Ukraine it historically, culturally, and rightfully a part of Russia. It is firmly embedded in Russian sphere of interest. This sphere is reserved for Russian influence and should not be interfered with by Western actors, most notably the EU, NATO, and the U.S.

In Russian strategic thinking, Ukraine also serves as an important security buffer. Historically this is something Russia has placed heavy emphasis on maintaining, that is, making sure to have buffer states separating it from Western (or other) competing powers. With Ukraine's Western pivot, Russia sees both its sphere of influence and its security buffer threatened. The implications of this threat perception were evident in 2014 but is manifesting itself in 2021 as the closest Europe has been to actual large-scale war in modern times.

Russia has used the latter eight years of the frozen war with Ukraine to test various tools on the Ukrainian government and society to try and force it away from its Western pivot. Such a pivot undercuts Russia's hope of re-integrating the post-Soviet space, a particular hard blow as we are approaching the 30th commemoration date of the collapse of the former Soviet empire.

However, Kyiv has proved itself as a resilient force set on integrating the country in a westward direction. Russia, now having exhausted most of its other means – economic, information, cyberattacks, subversion, proxy war, influence through oligarchs and so on – is left with is its military might and is, in the words of Nobel laureate Dmitry Muratov, "actively selling the idea of war" (Carnegie.ru, Dec 9).

Norway – of Growing Importance?

Turning briefly towards Europe and NATO countries in particular, Russia has also spent considerable IPb efforts the last eight years. Like Ukraine, such IPb efforts have taken many shapes and forms and the entire Russian state toolbox has been available for use. According to Russia analyst, Mark Galeotti, the key aim has been to divide, distract, and demoralize. The different measures range from disinformation campaigns to corruption, cyber-attacks, use of NGOs (or government-controlled NGOs) and criminal groups. Russia has sought to destabilize societies within the alliance as a way of weakening its unity. Moscow knows that NATO, at least on paper, is militarily more powerful and perceive the alliance as a threat to its national security. The recent decision to withdraw its diplomatic mission to NATO over allegations of intelligence gathering could also be seen in this light. Such a decision also increases Russia's bilateral leverage over NATO states because Russia no longer has "any

relations with NATO", as commented by Russia's Minister of Foreign Affairs, Sergey Lavrov.

The sentence was uttered while Lavrov was visiting Norway to participate at the Barents Council's Ministerial Meeting and meet with his Norwegian counterpart, Anniken Huidtfelt. Norway, also bordering to Russia in the Arctic High North, has a very different historical and cultural connection with Russia. It is firmly embedded in the "Western club" and NATOs "eyes in the North". Historically, relations have been good and despite Norway's western embeddedness, the countries have cooperated in several areas and maintained a peaceful coexistence in the High North.

As mentioned, the Russian annexation of Crimea in 2014 had repercussions beyond Ukrainian borders. Russia's actions created tensions and uncertainty in Norway, and since 2014 Norwegian authorities have followed Russian military build-up in the Arctic more closely and the focus on Russian attempts to influence and shape Norwegian information systems and societal preferences is heightened. Norway experiences a more active Russian military, ready to intimidate, particularly during NATO exercises in Norway. Its diplomatic mission is highly active and ready to refute any allegations made toward Russia as russophobia and hysteria. The Erna Solberg government (2013-2021) attributed a cyber-attack on the Norwegian Parliament and other critical infrastructures to Russia. Furthermore, a continuous concern in Oslo is Russia's attempt to play on existing tensions between Norway's northern population and the political decision-makers in the South-East, as well as the continuous challenging of Norwegian jurisdiction on Svalbard. The disagreement of whether or not the Svalbard Treaty applies in the seas around the archipelago, as well as the geographical position of the islands in a strategically important area, makes Svalbard an ongoing security policy issue for Norway. In recent years, Russia has ramped up its accusations of Norwegian discrimination of Russian economic activities on the island and accused Norway of breaching the Svalbard Agreement [3].

The North-South divide stems from people living closer to the Norwegian border disagreeing with the deteriorating state of relations between Norway and Russia, and what some perceive as an unconstructive and US led security policy towards Russia. The northern region has extensive experience with cross-border cooperation, visits, and friendly activities. Many people living in Finnmark (the northernmost Norwegian county) still remember, or have been told stories about, the Soviet liberation of Northern Norway during World War II. These are emotional and important stories and a part of Norwegian-Russian shared history that the Russian regime has spent considerable time and effort keeping alive. The latter evident through the many Soviet soldier commemorations and memorial sites in Northern Norway and the fact that Russian state officials make sure to mention this shared history whenever possible. This is not to downplay the importance and gratitude of the Soviet liberation, but to show how this is part of the larger Russian use of history to gain leverage.

Russia has also actively commented on developments in Norway's security and defense policy. Historically, Norway has sought a policy of both deterring and reassuring Russia. The former consists, among other, of Norwegian NATO membership. The reassuring policy is tied to what limitations Norway place on alliance presence and activity on Norwegian soil, the most central being the

declaration of not allowing foreign bases on Norwegian soil and storing nuclear weapons on Norwegian territory during peacetime. After 2014, Norway has heightened its cooperation with NATO and the U.S., as well with its Nordic neighbors Sweden and Finland. A short remark is warranted here. In a Nordic context, Sweden and Finland are seen as important buffers and Russia places heavy emphasis on both countries remaining non-aligned. Extensive Norwegian (but also other allied) military cooperation with the countries is perceived as an attempt to draw Sweden and Finland closer to NATO and a breach with – in Russia's eyes – the region's security status quo.

Russia has increasingly blamed Norway for moving away from its reassurance policy, particularly as military cooperation was stopped, and sanctions imposed, after the annexation of Crimea. Furthermore, sharp critique has been tied to increased Norwegian bilateral cooperation with the US, and Russia see the increased presence as a threat and a break with the historic reassurance guarantees. The debate has also been raised in Norway as the Parliament now is considering a "Supplementary defense cooperation agreement between Norway and the *United States* of America" [4]. This supplement the already existing, and close, cooperation between Norway and the US, where U.S. troops are in Norway on a rotational basis. Some Norwegian voices worry that this is a move away from Norwegian base policy and the US through the supplementary agreement gain exclusive access to, and right to use, four Norwegian military bases [5].

Russia has primarily met such concerns with harsh diplomatic responses, but also increasingly since 2014 sought to intimidate by amassing large scale military exercises close to Norway's border or near ongoing NATO exercises. These are often surprise exercises. Russia has also several times warned about meeting increased NATO presence in the North with "necessary countermeasures". By building its security and defense policy explicitly on the idea of deterrence and reassurance, Norway has in some regards given Russia a bargaining card – and they are using it for what its worth to enhance their interests.

The key question in this regard is how we distinguish between what is rhetoric and what is reality? This is the case for both Norway and Ukraine. The Russian rhetoric is, to a large extent, not new and some phrases and viewpoints can be tracked back to the Cold War era. The problem today is the context in which they are voiced. With heightened international tensions, a growing gap between perceptions of reality and "facts on the ground", and increased uncertainty regarding each other's intentions, do we still know what Russia *actually* means or intends to do? It certainly does not seem to be the case with regards to Russia's troop buildup on Ukraine's border.

The Norwegian society has in general proven itself a quite resilient when it comes to disinformation and influence attempts. It is a society with high trust towards politicians, state institutions, and media. However, as most other open, democratic societies, the problem is that there are several societal and digital vulnerabilities ready to be exploited. Today this is particularly true of social media and attacks on digital infrastructures (from state to local level and private enterprises). But also "traditional" methods of influence are used. Critical infrastructure is analyzed and mapped, and social tensions or cultural-historical debates and conflict lines are, if not used today, stored to be pressured when deemed necessary.

This is where Norway has a lot to learn from Ukraine, especially as Norwegian decision-making (from a Russian perceptive) increasingly is seen – or attempted portrayed – as US led. Because Norway, but also its Nordic neighbors, seem more resilient toward Russian influence and pressure, it might lower the stakes of using the military to apply pressure or deter. Especially as the Russian Arctic play an increasingly significant role in both Russian socio-economic planning, with the development of the Northern Sea route, and national security thinking, as most of Russia's nuclear arsenal is located on the Kola Peninsula close to Norway's border.

Conclusions

While political contact between Norway and Russia has improved in some areas since 2017, the military and defense-political contact between the two countries remains low. The Jonas Gahr Store government (2021) has emphasized in its political platform that it intends to increase dialogue with Russia and it is clear that Russia is waiting to see what this means in practice (ref. the visit by Foreign Minister Lavrov). It might be a smart move as Norway is increasing its military cooperation with the US and experienced a heightened influence and intelligence pressure, in line with the Russian IPb playbook.

As for lessons learned, Russia will not reveal any information of strategic or responsive nature in various publications. But given the fact that Russia in other arenas, such as Ukraine, play on already invented ideas/technology, this could indicate that Russia will use the same approaches, but add a context-specific flavor to them. In other words, it is not impossible to imagine what Russia can do, although military planners should envision various scenarios.

List of references

1. See for example, Brian Whitmore (December 15, 2021), "Belarus joins Vladimir Putin's Russia behind Europe's new Iron Curtain", *Atlantic Council.*

2. The term "hybrid warfare" is highly debated but will be used in this paper as it was the key term used during the NDUU Conference.

3. Traktat mellem Norge, Amerikas Forente Stater, Danmark, Frankrike, Italia, Japan, Nederlandene, Storbritannia og Irland og de britiske oversjoiske besiddelser og Sverige angående Spitsbergen [Svalbard.. – Lovdata.

4. https://www.regjeringen.no/dokumenter/kglres_forsvarssamarbeid/id284534.

5. For example, see question posed in Parliament by the leader of the Norwegian communist party (Rodt), Bjornar Moxnes: https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=84689.

6. Barabash, Viktor V. Elena A. Kotelenets, Irina S. Karabulatova, Maria Y. Lavrentyeva, and Yulia S. Mitina (2019), "The confrontation between the Eastern and Western worldviews in the conceptual space of the information war against Russia: the genesis and evolution of the terminological apparatus", Amazinia Investiga, Vol. 8(19), 246-254.

7. Charap, Samuel, Dara Massicot, Miranda Priebe, Alyssa Demus, Clint Reach, Mark Stalczynski, Eugeniu Han, Lynn E. Davis (2021), "Russian Grand Strategy: Rhetoric and Reality", RAND Corporation, Research Report.

8. Darczewska, Jolanta (2014), “The autonomy of Russian information warfare. The Crimean operation, as case study”, Centre for Eastern Studies, Point of View no.

9. Eggen, Karen-Anna (2020), “Russia’s strategy towards the Nordic region: Tracing continuity and change”, Journal of Strategic Studies.

10. Galeotti, Mark (2016), “Heavy Metal Diplomacy: Russia’s Political Use of its Military in Europe since 2014”, European Council on Foreign Affairs.

11. Information Security Doctrine (2016), “Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii, 5 Dec. Accessed from http://kremlin.ru/acts/bank/41460.

12. Joe Cheravitch (2021), “The Role of Russia’s Military in Information Confrontation”, CAN Occasional Paper, IOP-2021-U-030078-Final.

13. Jonsson, Oscar (2019), The Russian Understanding of War: Blurring the Lines between War and Peace, Washington D.C.: Georgetown University Press.

14. Lata, V. F., V. A. Annenkov and V. F. Moiseev (2019), “Informatsionnoye protivoborstvo: Sistema terminov i opredeleniy”, Vestnik Akademii voyennykh nauk, Vol. 2 (67), 128-138.

15. Polyakova, Alina, Flemming Splidsboel-Hansen, Robert Van der Nordaa, Oystein Bogen, and Henrik Sundbom (2018),), “The Kremlin’s Trojan Horses: Russian Influence in Denmark, The Nederlands, Norway, and Sweden”, The Atlantic Council.

16. President of Russia (2016), “Soveshchaniye poslov i postoyannykh predstaviteley Rossiyskoy Federatsii [Meeting of Ambassadors and Permanent Representatives of the Russian Federation], 30 Jun., http://kremlin.ru/events/president/news/52298.

17. President of Russia (2020), “Yezhegodnaya press-konferentsiya Vladimira Putina [Vladimir Putin’s annual press conference]”, 17 Dec., http://kremlin.ru /events/president/news/64671.

18. Tchikalova, Lidia (2015), “Informatsionnoye protivostoyaniye Rossii I SSHA v period siriyskogo konflikta”, University of St. Petersburg, Dissertation. Accessed from http://jf.spbu.ru/upload/files/file_1431687357_8838.pdf.

19. Thomas, Timothy (2014), “Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?”, The Journal of Slavic Military Studies, Vol. 27(1), 101-130.

Визначення співвідношення військових і невійськових сил та засобів протидії гібридної агресії

Анатолій Павліковський, кандидат військових наук, доцент
Начальник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-0637-368X
Степан Возняк, кандидат технічних наук, старший науковий співробітник
Начальник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-9015-813X
Андрій Іващенко, кандидат технічних наук, доцент
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-8131-5463
Ольга Демешок, кандидат економічних наук, доцент
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-6297-3241

Анотація. Розглядаються індикатори моніторингу району гібридної агресії та методика визначення раціонального складу співвідношення військових і невійськових сил та засобів протидії гібридної агресії.

Ключові слова: гібридна агресія, протидія, військові і невійськові сили та засоби, співвідношення.

Вступ

Постановка проблеми. Керований характер збройного насильства в сучасних військових конфліктах, використання не лише військової сфери для протистояння, варіативна інтенсивність бойових дій і зростаюча кількість сторін конфлікту в сукупності характеризують сучасний воєнний конфлікт (СВК) як системний багатовимірний процес.

Процес врегулювання таких конфліктів ускладнений. Кількість угод з підтримання миру зростає, але їх ефективність сумнівна. Збільшується кількість запитів на інститути глобального і регіонального партнерства, зростає їх роль в процесах врегулювання.

Для врегулювання СВК гібридного типу ООН в рамках свого статуту проводить миротворчу діяльність та організує і координує різні типи миротворчих операцій. Порівняно з періодом 1990-х рр., сучасні операції ООН з

підтримання миру і безпеки розгортаються на більш тривалі терміни та не завжди досягають своїх цілей. Це обумовлює необхідність проведення більш глибокого аналізу проблемних питань сучасних міжнародних операцій з підтримання миру і безпеки. Як варіант вирішення СВК розглядається багатопрофільна інтегрована міжнародна операція з підтримання миру і безпеки (БІМОПМБ).

Аналіз останніх досліджень та публікацій. Питання щодо розвитку сучасних тенденцій та поглядів на проведення міжнародних операцій з підтримання миру і безпеки неодноразово висвітлювалися як у вітчизняних, так і у зарубіжних наукових працях і публікаціях [1]. Водночас питанням оцінки співвідношення військових і невійськових сил та засобів у складі БІМОПМБ в умовах СВК приділяють недостатньо уваги [2].

Мета доповіді. На основі проведеного аналізу конфліктів гібридного типу пропонується перелік індикаторів для визначення фази конфлікту для визначення раціонального складу військових і невійськових сил та засобів у складі БІМОПМБ.

Виклад основного матеріалу

Сучасні воєнні конфлікти – це надзвичайно складні комплекси різних форм насильства різного типу, рівня, інтенсивності, сфер протиборства. Вони носять більш фрагментарний характер (ведуться за участю значної кількості учасників, в більшості своїй – недержавних структур, від локальних угруповань до квазідержавних утворень) і розгортаються в умовах слабкості або відсутності державної влади [3].

Тенденції щодо зростання кількості сторін – учасників СВК наведено в на рис. 1 [4].

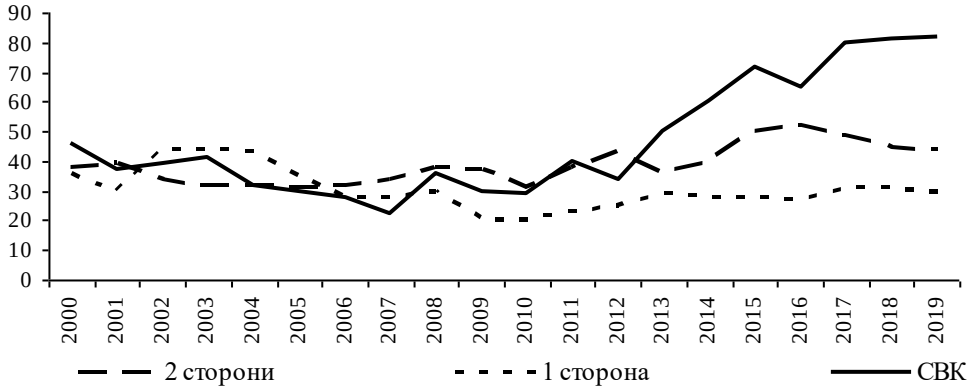

Рисунок 1 – Загальна тенденція зміни кількості сторін СВК

СВК характеризується як конфлікти низької або середньої інтенсивності з багатьма учасниками, основні з яких приховані, при якому дії ведуться у всіх сферах, для досягнення цілей якого використовують невоєнні сили і засоби, а кордони розповсюдження конфлікту є нечіткими. При цьому традиційні підходи з боку держави до запобігання та врегулювання СВК переважно не спрацьовують, так як і дії міжнародних безпекових організацій в особі ООН та регіональних організацій.

Сьогодні миротворчість серйозно видозмінилася. Крім традиційної миротворчості, ООН реалізує багатосторонню миротворчість і комплексну багатосторонню миротворчість. Термін “миротворчість”, який зазвичай включає в себе невоєнні засоби досягнення миру, часто використовують для характеристики будь-якої діяльності, спрямованої на зупинення конфлікту та відновлення миру. Відповідно до ст. 33 статуту ООН визначені основні невоєнні засоби врегулювання воєнного конфлікту: переговори; посередництво; примирення; звернення до регіональних організацій, тощо.

У БІМОПМБ військова компонента взаємодіє з усіма іншими компонентами місії, такими як цивільна та поліцейська, щоб максимізувати обмін інформацією та інтеграцію для ширшого колективного впливу ООН. Взаємодія з цивільною компонентою (особливо в політичній площині) включає спільне стратегічне планування імплементації мандату операції та коригування завдань військової компоненти в залежності від обстановки, що склалася [5].

Проте конкретна політика щодо конфліктних ситуацій багато в чому залишається реактивною, тобто в основному дії вживаються після того, як та чи інша подія відбулася − лише у відповідь на неї. Однією з причин є те, що виникають проблеми, пов’язані з пошуком індикаторів, за якими можна судити про потенційно конфліктні райони. Незважаючи на те, що розгорнуто й реалізується програма моніторингу ООН за можливими вибухонебезпечними зонами, чітких критеріїв, за якими можна було б прогнозувати, коли й де виникне, а також у якій формі виявиться черговий конфлікт, не існує.

По-друге, виникають проблеми обґрунтування необхідності втручання; прийняття відповідних рішень про те, якого виду дії будуть початі; отримання необхідних дозволів для впливу на конфлікт і, нарешті, фінансування дій, що вживаються. Також істотну роль відіграють і суто психологічні чинники, зокрема, необхідність запобігання загрози, якої поки не існує реально.

Тобто існують проблеми як визначення індикаторів для моніторингу зони СВК так і визначення раціонального складу місії (операції).

Для оцінювання ситуації в зоні конфлікту пропонується використовувати результати дослідження аналітичного центру The Fund for Peace [6] та “Індекс слабкості держав” (Fragile States Index) – комплексний показник, що характеризує здатність (нездатність) влади контролювати цілісність своєї території, політичну, економічну, соціальну та демографічну ситуацію в країні, а також стійкість її державних інститутів.

Для визначення Індексу проводиться аналіз країн світу за допомогою спеціального системного інструменту оцінки конфліктів (Conflict Assessment System Tool). Аналіз проводиться на підставі 12 індикаторів вразливості держави, які об’єднані в чотири групи (див. табл. 1).

Показник зовнішнього втручання розглядає вплив зовнішніх суб’єктів на функціонування держави особливо у безпековій, економічній та політичній сфері. З одного боку, зовнішнє втручання фокусується на аспектах безпеки держави шляхом втручання зовнішніх суб’єктів, як прихованих, так і явних, у внутрішні справи держави. Це втручання може вплинути на баланс влади (або вирішення конфлікту) всередині держави. З іншого боку, зовнішнє втручання

зосереджується на економічному залученні сторонніх суб'єктів, що створює економічну залежність.

Таблиця 1

Індикатор вразливості держави.

Групи	Індикатори
Політичні	P1 – легітимність держави; P2 – державні послуги; P3 – права людини та верховенство права.
Згуртованості	C1 – сектор безпеки і оборони; C2 – державні інституції; C3 – суспільство.
Економічні	E1 – економічний спад; E2 – нерівномірний економічний розвиток; E3 – відтік технічного та інтелектуального капіталу.
Соціальні та зовнішнього втручання	S1 – демографічний тиск; S2 – біженці та внутрішньо переміщені особи; X1 – зовнішнє втручання.

Ця методика не враховує інформаційного впливу.

Сторони конфлікту, які мають доступ до найсучасніших інформаційних технологій, отримують переваги над іншими сторонами конфлікту. Мета будь-якої війни і політики уряду будь-якої країни – змусити супротивника, конкурента, партнера прийняти вигідне для своєї країни рішення. Здійснюючи вплив за допомогою тієї або іншої інформації, що доводиться по засобах комунікації, на світогляд, свідомість, психіку людей, вдається досягати того, що уряди країн, які піддалися інформаційній дії, приймають "нав'язані", невигідні для країни рішення.

У квітні 2015 р. на парламентській асамблеї НАТО було представлено доповідь Д. Калхи "Гібридна війна: новий стратегічний виклик НАТО?". У цій доповіді зокрема підкреслюється, що Росія використовує внутрішню слабкість України за рахунок, насамперед, невійськових методів (таких як політичне, інформаційне, економічне залякування та маніпуляції), які підкріплюються загрозою використання регулярних військ. Також, порівнюючи гібридні війни, яку ведуть Росія, Ісламська держава Іраку та Леванту, дослідник підкреслює що Росія скоординовано застосовувала широкий спектр 52 тактик, від політичного й економічного примусу, кібератак, дезінформації і пропаганди до відкритих і прихованих бойових дій.

В розрізі цього пропонується розширити показник "X1 – зовнішнє втручання" наступними параметрами інформаційного втручання (див. табл. 2).

Таблиця 2

Параметри інформаційного втручання

Зовнішнє втручання	Вид
Інформаційне	Інформаційно-психологічний вплив. Інформаційно-технічний вплив. Кібернетичний вплив.

Висновки

Протидія гібридній агресії вимагає консолідації зусиль всіх можливих сил та засобів міжнародного співтовариства в інтересах врегулювання збройного конфлікту мирним шляхом. Для цього необхідна інтеграція військових та невійськових сил та засобів, що забезпечить результативність заходів, які доцільно вжити для формування складу міжнародної операції. При моделюванні причин і умов, що викликають СВК, раннього попередження конфліктів на своїй території необхідно враховувати параметри інформаційного втручання. В подальших дослідженнях необхідно зосередитись на розробці методики визначення співвідношення військових і невійськових сил та засобів у складі багатопрофільної інтегрованої міжнародної операції з підтримання миру і безпеки в умовах сучасних військових конфліктів.

Список літератури

1. Іващенко А. М., Возняк С. М. Аналіз можливих форм і способів проведення миротворчої операції ООН на Сході України. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2018. № 2(63). С.32 – 38.
2. Сиротенко А.М. Методологія комплексного використання військових та невійськових сил та засобів сектору безпеки і оборони для протидії сучасним загрозам воєнній безпеці України: монографія / В.Ю. Богданович, І.С. Романченко, І.Ю. Свида, А.М.. – Л.: НАСВ, 2019. – 268 с.
3. Бочарніков В. П., Свєшніков С. В. Погляди на характер сучасних воєнних конфліктів. Наука і оборона. 2017. № 1. С. 3 – 8.
4. Uppsala Conflict Data Program, 2018. Department of Peace and Conflict Research, Uppsala University, Sweden
5. Prinsloo B. Hybrid Peacekeeping – A Deeper Understanding of Evolving Peacekeeping Practices. Oxford research group. 2017. URL:https://www.oxfordresearchgroup.org.uk/blog/hybrid-peacekeeping-a-deeper-understanding-of-evolving-peacekeeping-practices (дата звернення: 23.11.2021).
6. Індекс слабкості держав світу (Fragile States Index) URL:https://fragilestatesindex.org (дата звернення: 23.11.2021).

Об’єднана операція як основна форма відсічі гібридній агресії Російської Федерації

В’ячеслав Семененко, кандидат технічних наук, старший науковий співробітник

Заступник начальника Центру – начальник управління Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0001-5774-0868

Михайло Лобко, кандидат військових наук, доцент

Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0002-8131-5463

Андрій Фучко,

Начальник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0002-8941-2217

Анотація. *На основі аналізу сучасних тенденцій розвитку збройної боротьби, поглядів науковців, фахівців, експертів розкриваються основні особливості сучасних воєнних конфліктів. Досліджуються питання змісту та особливостей “гібридної” війни. На основі проведених досліджень, досвіду відсічі збройній агресії Росії на Сході України визначаються питання об’єднаної операції як основної форми відсічі збройній агресії “гібридного” типу. Розкриваються особливості та визначаються сутність і найбільш загальні теоретичні основи об’єднаної операції. Надається визначення об’єднаних сил, що здійснюють підготовку і проведення об’єднаної операції.*

Ключові слова: *“гібридна” війна, “гібридна” агресія, форми застосування військ (сил), військова операція, об’єднана операція, сили оборони, об’єднані сили, воєнні, невоєнні, спеціальні засоби збройної боротьби.*

Вступ

Постановка проблеми. РФ здійснила збройну агресію проти України, застосувавши концепцію “гібридної” війни, яка багато в чому є унікальною зі структурно-функціонального погляду: за формою вона “гібридна”, а за змістом – “асиметрична”. Хоча кожен конкретний елемент цієї “гібридної” війни не новий по суті і використовувався майже в усіх війнах минулого, однак унікальними є узгодженість і взаємозв’язок цих елементів, динамічність та гнучкість їх застосування [1].

Аналіз останніх досліджень і публікацій. Дослідженню нового "феномену" XXI століття, який отримав назву "гібридної" війни, присвячена значна кількість публікацій вітчизняних і іноземних науковців, фахівців, експертів, де розглядаються цілі, механізми, технології і засоби російської "гібридної" агресії в Україні і в інших воєнних конфліктах [2–6]. "Гібридна" війна у їх дослідженнях розглядається як сукупність воєнних дій, поєднання мілітарних, парамілітарних, політико-дипломатичних, інформаційних, економічних та інших засобів з метою досягнення встановлених стратегічних політичних цілей. Однак, слід зазначити, що досліджуючи власне "гібридну" війну як феномен сучасності та її певні сторони, у наведених та інших публікаціях автори не надають конкретних заходів, форм і способів протидії "гібридній" агресії.

Метою доповіді є вирішення проблеми пошуку ефективних форм та способів протидії "гібридній" агресії, її відсічі. Зазначена мета є вкрай актуальною для України як в умовах сьогодення, так і у перспективі.

Виклад основного матеріалу

Як відомо, основним змістом воєнних конфліктів минулого була збройна боротьба, яка здійснювалась у традиційних формах: операцій, бойових дій, битв, боїв, ударів тощо, що охоплювали практично всі природні сфери: суходіл, повітря, море, космос. Наведене відноситься до суто *воєнних засобів*.

Зміна характеру сучасних воєнних конфліктів пов'язана першочергово зі стрімким розвитком технологій виробництва й особливо цифрових інформаційних технологій. Неодмінною складовою сучасних воєнних конфліктів стали політико-дипломатичне, економічне, інформаційне, кібернетичне протистояння, масовий вплив пропаганди на населення й військовослужбовців та інші, тобто *невоєнні засоби*. Невоєнні засоби вплинули на характер воєнних конфліктів і на розвиток форм застосування військ (сил). Зокрема, з'явилися такі операції (дії), як інформаційні, інформаційно-психологічні, кібернетичні, гуманітарні, рятувальні тощо. Слід наголосити, що для воєнних конфліктів минулого також було притаманне використання невоєнних засобів боротьби. Однак через недосконалість розвитку технологій того часу їхній вплив на перебіг і результати збройного протистояння був, в основному, допоміжним і незначним порівняно з воєнними засобами.

Поєднане використання даних форм застосування свідчить про зміну змісту і надає воєнним конфліктам так званого "гібридного" характеру. Необхідність протидії цим явищам ставить завдання перед всіма органами державної влади та необхідність їх широкої участі у відсічі збройній агресії шляхом запровадження *спеціальних засобів*.

Необхідно констатувати, що основним змістом сучасних воєнних конфліктів залишається збройна боротьба. В той же час, чітко простежується використання трьох основних компонентів протиборства: воєнних засобів; невоєнних та спеціальних засобів.

Отже, для забезпечення досягнення визначеної мети оборони держави, гарантованої відсічі збройній агресії «гібридного» типу необхідно *об'єднати*

завдання, які випливають з характеру сучасних воєнних конфліктів щодо протидії цим явищам, *поєднати зусилля сил і засобів* силових структур сектору безпеки та оборони, органів державної влади, інших державних органів у протидії згаданим вище компонентам воєнних конфліктів, сили і засоби, які залучаються для здійснення оборони держави, відсічі збройній агресії, повинні перебувати під *єдиним керівництвом* на стратегічному, оперативному і тактичному рівнях та виконувати завдання за *єдиним замислом і планом* [7].

Для поєднання вказаних складових необхідно визначити форму, яка б могла їх об'єднати. Проведене дослідження показало, що такою формою доцільно обрати "операцію".

У сучасному розумінні "***військова операція***" розглядається як сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом бойових дій, битв, боїв, ударів і маневру видів і родів військ (сил), що проводяться одночасно і послідовно за єдиним замислом і планом, під єдиним керівництвом для виконання поставлених завдань та досягнення визначених воєнно-політичних (воєнно-стратегічних) цілей. Однак, для відсічі збройній агресії "гібридного" типу об'єднавчою формою має стати "об'єднана операція".

Об'єднана операція становить собою сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом воєнних, невоєнних та спеціальних засобів боротьби, що проводяться одночасно й послідовно за єдиним замислом і планом складовими сектору безпеки та оборони, органами державної влади, іншими державними органами, органами місцевого самоврядування під єдиним керівництвом для виконання поставлених завдань з відсічі збройній агресії та досягнення визначених воєнно-стратегічних цілей. *Воєнними засобами* об'єднаної операції є традиційні форми застосування військ (сил): операції (меншого масштабу); бойові дії (як форма застосування з'єднань видів військ (сил); битви (форма застосування родів військ (сил), складова операції); спеціальні дії спеціальних військ; дії служб, сил і засобів підтримки, логістики тощо.

До операцій слід віднести оборонну, наступальну (контрнаступальну), повітряну, морську, спеціальну, стабілізаційну та ін., які проводитимуться в зоні об'єднаної операції визначеними силами й засобами.

До *невоєнних засобів* мають належати операції, дії, заходи, що проводяться в рамках об'єднаної операції для забезпечення виконання покладених завдань і досягнення її визначеної мети. Операціями (діями) можуть бути інформаційні, інформаційно-психологічні, кібернетичні (дії, заходи, акти, акції), гуманітарні, рятувальні (пошуково-рятувальні), евакуаційні тощо.

Під час проведення об'єднаної операції у визначених зонах (районах) визначеними силами і засобами проводитимуться заходи: правового режиму воєнного (надзвичайного) стану; місцевих державних адміністрацій з питань оборони; обласних рад оборони (в разі їх створення); органів місцевого самоврядування; заходи, що проводитимуть військово-цивільні (військові) адміністрації (в разі їх створення); заходи єдиної державної системи цивільного захисту (надзвичайних ситуацій, евакуаційні, епідеміологічні (епізоотичні, епіфітотичні) тощо.

Спеціальними засобами об'єднаної операції будуть спеціальні, антитерористичні операції (дії), службово-бойові, оперативно-розшукові заходи, дії сил і засобів правоохоронних органів, інші форми, притаманні їм, а також силам територіальної оборони. Спеціальні засоби в об'єднаній операції використовують в основному правоохоронні органи держави.

Загальною метою застосування сил оборони буде зрив та відсіч збройній агресії, примушення противника до відмови від подальшого ведення воєнних дій з повним відновленням територіальної цілісності й суверенітету держави. Визначена мета досягатиметься проведенням усього комплексу воєнних, невоєнних і спеціальних засобів, як то: операцій, дій, заходів, що проводитимуться одночасно і послідовно за єдиним замислом і планом під єдиним керівництвом у рамках об'єднаної операції за участі всіх складових сил безпеки та сил оборони держави.

Саме наведена сутність об'єднаної операції забезпечують утілення "засад всеохоплюючої оборони України", викладених у Стратегії воєнної безпеки України. Зазначена Стратегія передбачає для здійснення оборони держави застосування всіх традиційних форм і способів збройної боротьби, проведення превентивних, асиметричних та інших дій і стійкого опору агресору.

Об'єднану операцію готують і проводять угруповання об'єднаних сили. Для цього рішенням Президента України – Верховного Головнокомандувача Збройних Сил України (Головнокомандувача Збройних Сил України) визначається склад угруповання об'єднаних сил. Об'єднані сили утворюються зі складу сил оборони.

Сили оборони – Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави.

Отже, до складу сил оборони входять органи військового управління, з'єднання, військові частини видів, родів, спеціальних військ (сил), логістики видів, родів військ (сил) Збройних Сил України, а також визначені Генеральним штабом Збройних Сил України згідно зі *стратегічним планом застосування сил оборони*, органи управління, інші органи, військові частини, підрозділи зі складу інших військових формувань, правоохоронних і розвідувальних органів. Об'єднані сили становлять тимчасове оперативно-стратегічне (оперативне) угруповання (об'єднання) військ (сил і засобів), для виконання завдань об'єднаної операції з використанням воєнних, невоєнних і спеціальних засобів.

Крім того, до складу угруповання об'єднаних сил включаються місцеві органи державної влади, інші державні органи, органи місцевого самоврядування, їх сили і засоби, які беруть участь у виконанні завдань оборони у рамках об'єднаної операції.

Для підготовки і проведення об'єднаної операції у складі об'єднаних сил утворюються: оперативні (оперативно-тактичні) угруповання військ (сил) для проведення всього діапазону операцій (бойових дій, битв) із відсічі збройній агресії; система органів, сил і засобів для підготовки та проведення операцій, дій,

заходів з використанням невоєнних засобів; система органів, сил і засобів для виконання завдань з використанням спеціальних засобів. Оскільки об'єднані сили виконують покладені на них завдання в різних умовах обстановки, з використанням різних засобів, то їхній склад буде не постійним.

Склад об'єднаних сил залежатиме від кількох факторів, основними з яких будуть: мета й завдання операції; склад і ймовірний характер дій противника; склад військ (сил), органів, сил і засобів, що залучаються до виконання завдань; умови виконання поставлених завдань операції тощо.

Об'єднані сили очолює командувач об'єднаних сил. Командувач об'єднаних сил підпорядковується Головнокомандувачу Збройних Сил України та здійснює особисто й через Об'єднаний оперативний штаб (командування об'єднаних сил) Збройних Сил України оперативний контроль за набуттям ними оперативних (бойових) спроможностей, планування застосування та безпосереднє управління об'єднаними силами й засобами Збройних Сил України, інших складових сил оборони, переданими в його підпорядкування.

Об'єднані сили включають кілька оперативно-тактичних (оперативних) угруповань військ (сил), які розгортаються на ймовірних напрямках дій угруповань противника і виконують визначені завдання з використанням форм відповідно до встановленої системи застосування сил оборони.

До складу зазначених угруповань мають входити сили й засоби інших військових формувань, правоохоронних, розвідувальних органів зі складу сил оборони, на які покладається виконання завдань у формах, що належать до спеціальних засобів. Зазначені сили й засоби мають включатися до складу створених оперативно-тактичних (оперативних) угруповань військ (сил) і бути елементами оперативної побудови цих угруповань, а їхні органи управління мають входити до органів (пунктів) управління Об'єднаного оперативного штабу (командування об'єднаних сил) Збройних Сил України й утворених угруповань військ (сил).

Висновки

Отже, однією з форм відсічі збройній агресії "гібридного" типу слід вважати об'єднану операцію. Об'єднана операція є формою застосування військ (сил) для відсічі збройній агресії, яка охоплює та об'єднує воєнні, невоєнні і спеціальні засоби боротьби. Її підготовка і здійснення мають проводитися під єдиним керівництвом.

Об'єднана операція готується і проводиться об'єднаними силами. Угруповання об'єднаних сил утворюється зі складу сил оборони, а також включаються органи державної влади, інші державні органи та органи місцевого самоврядування з їх силами і засобами. За такого підходу об'єднана операція забезпечує об'єднання завдань та поєднання зусиль сил і засобів силових структур сектору безпеки та оборони, органів державної влади, інших державних органів і протидіяти всім компонентам збройної агресії "гібридного" типу з використанням державних і місцевих ресурсів та значно збільшує можливості успішної відсічі збройній агресії.

Також, проведення об’єднаної операції забезпечує реалізацію окремих положень Стратегії воєнної безпеки України із забезпечення підготовки і ведення всеохоплюючої оборони України.

Список літератури

1. Світова гібридна війна: український фронт [Електронний ресурс]: монографія / за заг. ред. В. П. Горбуліна. – К.: НІСД, 2017. – Режим доступу: https://niss.gov.ua/publikacii/monografii/svitova-gibridna-viyna-ukrainskiy-frontmonografiya.

2. Хоффман Ф. «Гибридная» война и ее вызовы. [Електронный ресурс] / Фрэнк Хоффман. – Режим доступу: https://pub.wikireading.ru/123633.

3. Уізер К. Джеймс. – Смисл гібридної війни [Електронный ресурс] / Джеймс К. Уізер. – Режим доступу: http://connections-qj.org/ru/article/smysl-gibridnoy-voyny.

4. Г. П. Мідттун. Битва умів. Гібридна війна – це вплив на людей, з метою підвести їх до свідомого чи несвідомого вибору, корисного для агресора [Електронный ресурс] / Ганс Петтер Мідттун // Euromaidan Press, 2020-05-22, переклад з англійської Ю. Каздобіна, – Режим доступу : https://texty.org.ua/articles/101043/.

5. Житник О. Осмислення поняття «гібридна» війна у західному та українському наукових дискурсах [Електронний ресурс] / Житник О.М. – Режим доступу: https://repository.mruni.eu handle Zhytnyk.

6. Military Aspects of Countering Hybrid Aggression: Ukrainian Experience. Publication NATO. North Atlantic Treaty Organization. Science and Technology Organization. AC/323 (SAS-161) TP/999. STO TECHNICAL REPORT. TR-SAS-161. www.sto.nato.int

7. Лобко М. Об’єднана операція як основна форма відсічі збройній агресії “гібридного” типу. Наука і оборона, №2, 2021. DOI 10. 33099/2618-1614-2021-15-2-24-33.

Підхід до прогнозування фаз розвитку конфліктів гібридного типу

Андрій Іващенко, кандидат технічних наук, доцент
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-8131-5463
Андрій Корецький, кандидат військових наук, старший науковий співробітник
Заступник начальника Центру воєнно-стратегічних досліджень з наукової роботи
Київ, Україна
https://orcid.org/0000-0002-6346-3083

Анотація. *Розглядається проблема прогнозування розвитку конфліктів гібридного типу (Hybrid War), які включають одночасне протиборство в різних сферах та велику кількість об'єктів і суб'єктів конфлікту. Розглядається можливість застосування великих даних (Big Data) та методів їх обробки з метою прогнозування їх розвитку. Пропонується послідовність обробки великих обсягів різнорідних даних, які отримуються як з оцінок воєнно-політичної обстановки, так і з району конфлікту..*

Ключові слова: *конфлікти гібридного типу, великі дані, технології обробки великих даних, аналіз великих даних, прогнозування.*

Вступ

Постановка проблеми. Глобалізація і інформаційно-технологічна революція стали інтеграторами класичних і нових форм, способів, методів і технологій сучасних конфліктів. Набули поширення конфлікти гібридного типу, які направленні на досягнення політичних цілей та характеризуються збільшенням кількості об'єктів, які задіяні в конфлікті, їх різними комбінаціями, одночасним проведенням декількох фаз конфлікту і застосуванням військових та невійськових засобів [1]. Такі конфлікти характеризуються петабайтами (10^{15} байта) даних, які генеруються в процесі конфлікту. Аналіз поточного стану таких конфліктів вимагає врахування значної кількості різнорідних параметрів (політичних, військових, економічних, інформаційних тощо), а прогнозування наступних фаз – встановлення кореляцій між об'єктами і суб'єктами конфлікту, які, як правило, ретельно приховуються. Відомі методи прогнозування, які засновані на встановленні причинно-наслідкових зв'язків не забезпечують необхідного рівня вірогідності реалізації. Актуальним є пошук якісно нових підходів до прогнозування розвитку конфліктів гібридного типу.

Аналіз останніх досліджень та публікацій. Різним аспектам конфліктів гібридного типу війни присвячена значна кількість досліджень як провідних аналітичних центрів світу так і ряду вітчизняних науковців. Не зважаючи на те, що цей термін почав широко використовуватися в наукових публікаціях з

2014 року, проблема прогнозування фаз розвитку таких конфліктів не достатньо теоретично обґрунтована і потребує подальшого вивчення.

Методи аналізу великих даних та питання їх практичного застосування для вирішення широкого колу завдань досліджені в монографії Кейта [2]. Монографія [3] присвячена проблемним питанням застосування великих даних при плануванні операцій коаліційних сил в Іраку, авторами встановлено прямий зв'язок між обсягом даних, який використовувався при оперативному плануванні та кількістю жертв під час бойових дій. В роботі [4] проведено аналіз використання великих даних при плануванні операції в Афганістані. В [5] розглядаються питання застосування великих даних на тактичному рівні. У статті [6] надаються рекомендації щодо внесення змін у стратегії національної безпеки та воєнні доктрини з питань застосування великих даних.

В той же час питання аналізу та прогнозування розвитку конфлікту гібридного типу між Україною і Росією [1], де задіяна велика кількість об'єктів і суб'єктів, існує значний обсяг накопичених за сім років однорідних та неоднорідних даних, в науковій літературі досліджено не повністю.

Мета доповіді **–** обґрунтування можливості застосування технологій великих даних для аналізу та прогнозування розвитку конфлікту гібридного типу та визначення послідовності їх обробки та аналізу.

Виклад основного матеріалу

Аналіз досліджень та публікацій дозволив встановити чіткий зв'язок між революційними змінами в сучасних інформаційних технологіях та застосуванням нових підходів до ведення сучасних конфліктів і війн, який наведений в табл.1. Квінтесенцією чергової етапу розвитку технологій – набуття можливостей збору, накопичення та аналізу великих обсягів даних стала розробка та практичне застосування стратегій ведення конфліктів гібридного типу. Будь-яка протидія гібридній агресії стає неможливою без наявності та застосування низки сучасних технологій, які стають елементами систем великих даних.

Таблиця 1

Зв'язок між розвитком інформаційних технологій і сучасними воєнними стратегіями

Інформаційна технологія	**Воєнні стратегії і операції**
Мережеві обчислювання	Мереже-центричні бойові дії і операції
Хмарні обчислювання	Єдина інформаційне поле збройних сил- Об'єднане багатодоменне командування і управління - багатодоменні операції
Великі дані *(Big Data)*	Конфлікти і операції гібридного типу

Інформаційно-технологічні аспекти конфліктів гібридного типу полягають у здатності синхронізувати дії декількох засобів сили одночасно, застосувати

інформаційно-аналітичні підходи, багатозначність, нелінійний характер та когнітивні елементи війни. Конфлікти гібридного типу ведуться, як правило, нижчою інтенсивністю, ніж звичайні пороги виявлення та реагування і напряму залежать від швидкості, обсягу та засобів збору та поширення даних. Як кількість таких конфліктів, так і обсяги даних, які їх супроводжують, будуть зростати за геометричною прогресією [1].

Однією із визначальних рис сучасного конфлікту гібридного типу є одночасне використання різних типів структурованих та неструктурованих даних для його опису. Як правило, аналіз поточної фази конфлікту здійснюється описом наступних даних: DIME/PMESII/ASCOPE: де DIME - дипломатія, інформація, збройні сили та економіка; PMESII - політичні, безпекові, економічні, соціальні, інформаційні та інфраструктурні параметри; ASCOPE - райони, структури, спроможності, організація, люди та події.

Починаючи з певних числових значень обсягу даних і далі по мірі їх зростання, відбуваються якісні зміни, які дозволяють з великим рівнем ймовірності визначити нові взаємозв'язки (кореляції) всередині сукупності об'єктів і суб’єктів конфлікту, інформація про які зосереджена в одному масиві даних. Водночас кореляції не відповідають на запитання, необхідні в процесі оперативного планування: коли і яка мета? Вони дозволяють оцінити, з якою ймовірністю зміна одного чинника конфлікту призведе до зміни інших чинників цього конфлікту. Виявлення таких кореляцій є особливо корисним на етапі оперативного планування операцій. Як правило, ці фактори тісно взаємопов'язані, на один із факторів можна ефективно впливати з метою організації протидії. Однак слід враховувати, що встановити ці кореляції при малих обсягах масиву даних неможливо.

Великі дані розділяються на дві категорії: структуровані та неструктуровані. Структуровані дані упорядковані і мають чітку структуру і, як правило, зберігаються у вигляді таблиць. Неструктуровані дані різнорідні (документи, зображення, відео), надходять із різних джерел (системи спостереження, дрони, супутникові дані тощо) та різних мереж, включаючи соціальні. З такими даними складніше працювати, оскільки для отримання інформації з них необхідні відповідні інструменти, методи зберігання та обробки.

Різнорідність великих даних зумовлює специфічні методи їх аналізу. Для аналізу великих даних застосовується сукупність різних методів. Насамперед, це методи математики, статистики, методи інтелектуального аналізу та штучного інтелекту, розпізнавання образів, імітаційного моделювання, методи OSTIN та інші. Вони дають можливість отримувати необхідну інформацію з великих даних, визначати наявність або відсутність зв'язків між суб’єктами і об’єктами конфлікту гібридного типу, визначати причини та наслідки різних подій, перевіряти версії тощо.

В загальному вигляді процес прогнозування конфліктів гібридного типу на основі великих даних наведено на рис. 1.

Генерація даних здійснюється із різних джерел, включаючи дані візуальної розвідки, відео спостереження, дронів, файлів журналів, датчиків, веб-камер,

засобів радіотехнічної розвідки. Зібрані дані передаються в інфраструктуру зберігання та обробки даних для подальшої обробки та аналізу.

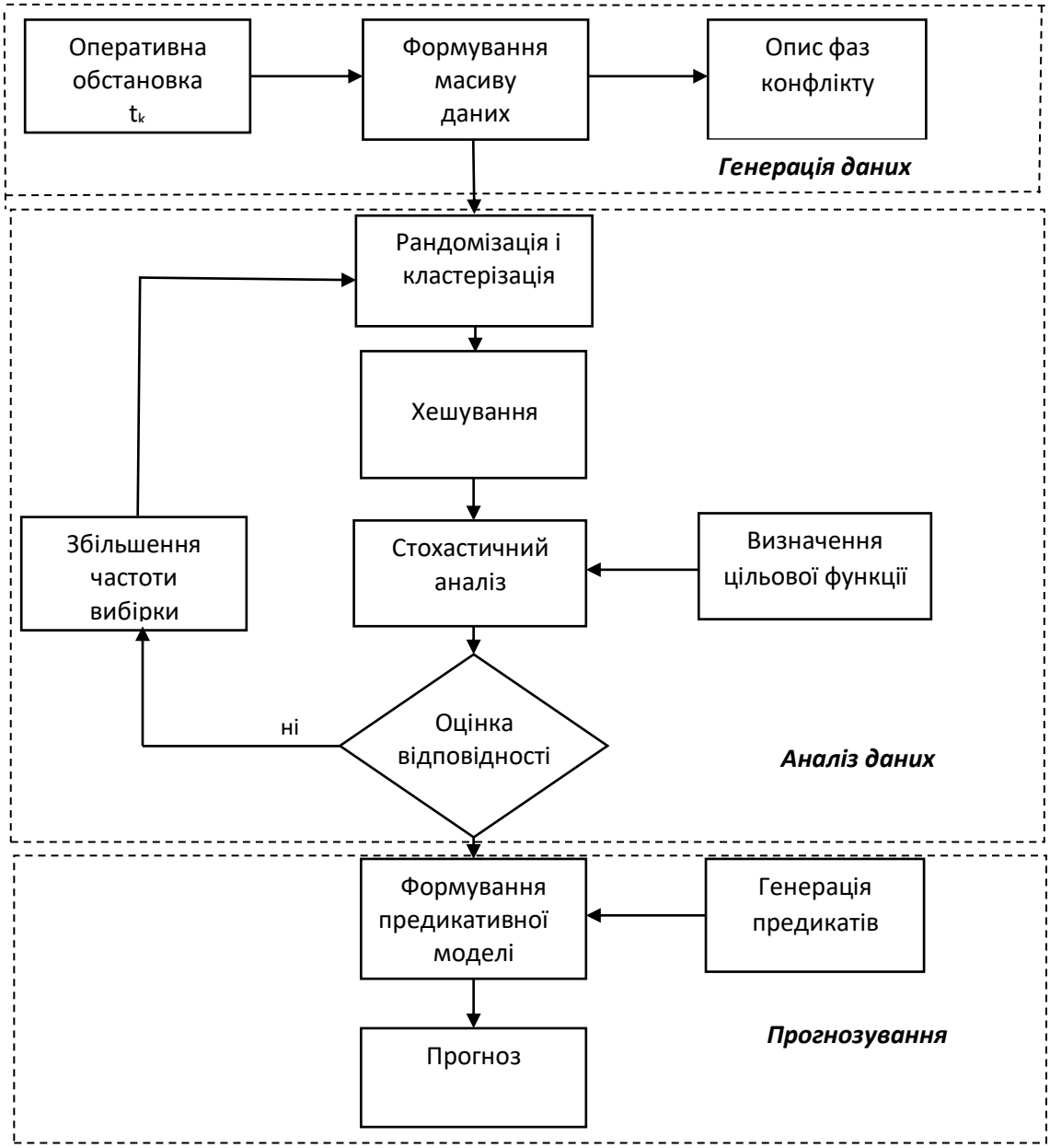

Рис. 1 Загальна послідовність процесу прогнозування конфліктів гібридного типу на основі великих даних аналізу.

Аналіз даних (*Data Mining*) включає застосування класичних та сучасних процедур і алгоритмів для перетворення різнорідних неструктурованих даних на необхідну для прогнозування інформацію, тобто отримати нову, приховану та корисну інформацію з набору великих даних.

Прогнозування включає визначення набору показників для конкретної проблеми, вибір архітектури та методів аналізу великих даних.

Разом з тим, прогнозування на основі великих даних, незважаючи на широке розповсюдження технологій та алгоритмів для їх аналізу, має наступні обмеження: масштабованість, зберігання, своєчасність аналізу, подання неоднорідних даних, обмеженість систем аналітики даних, відсутність кадрового

резерву, конфіденційність та безпека, необхідність обмеження даних, цифровий розрив, помилки даних.

Висновки

1. З появою конфліктів гібридного типу обсяг генерованих у процесі конфлікту даних різко виріс. Жодна технологія не дозволяє отримати прогноз розвитку конфлікту гібридного типу з повною достовірністю, однак, враховуючи переваги та недоліки мережецентричних або хмарних обчислень, може виявитися корисним застосувати технології обробки великих обсягів даних для отримання достовірних прогнозів.

2. Крім визначення великих даних, необхідно розробляти методики застосування великих даних для прийняття рішень та прогнозування.

3. Необхідно враховувати три основні умови перед впровадженням аналітики великих даних: чи можливо отримати корисну інформацію на додаток до даних, які вже отримуються з існуючих систем; як підвищиться точність даних, які будуть отримані за допомогою аналітики великих даних; як впровадження аналітики великих даних підвищить точність прогнозів розвитку конфліктів гібридного типу.

4. Аналітика великих даних має широко застосування у різних сферах гібридного конфлікту, включаючи військову. Застосування технологій великих даних допомагає у аналізі та побудові сценаріїв розвитку конфлікту. Разом з тим, незважаючи на переваги, у аналітики великих даних є свої обмеження та проблеми застосування.

Таким чином, великі дані відкривають нові можливості для прогнозування сучасних конфліктів гібридного типу.

Список літератури

1. Semenenko V.M., Ivashchenko A.M. Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices. NATO Science and Technologies Organization, Paris, 2020, 188 p.
2. Кейт О. Зброя математичного знищення. К., Book Chef, 2020, 336 с.
3. Berman E., Felter J., Shapiro J. Small Wars, Big Data: The Information Revolution in Modern Conflict. Princeton NJ, Princeton University Press, 2018, 408 p.
4. Zorri D.M., Derezovski M. Big Data Conflict Forecasting: Operationalizing the Data Science Team. Occasional paper. Joint Special Operating University, Department of Strategic Studies, June 2021, 32 p.
5. Tunnell H.D. Tactical Data Science. Military Review. Vol. 100, Iss. 4, (Jul/Aug 2020). Kanzas, Fort Leavenworth, p. 123-137.
6. Morabito D. National Security and the Third-Road Threat: Toward a Comprehensive Theory of Information Warfare. Air & Space Power Journal; Vol. 35, Iss. 3 (Fall 2021), Maxwell AFB, p. 19-39.
7. The Biggest Data Management News Items During the First Half of 2021. Melbourne, New Bites, Jun 27, 2021, 127 p.

Інформаційні аспекти ймовірного сценарію розвитку гібрибної агресії Російської Федерації проти України

Володимир Башинський, доктор технічних наук, старший науковий співробітник

Начальник Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки,

Чернігів, Україна

https://orcid.org/0000-0003-1712-7772

Геннадій Пєвцов, доктор технічних наук, професор

Заступник начальника Харківського національного університету Повітряних Сил імені Івана Кожедуба з наукової роботи,

Харків, Україна

https://orcid.org/0000-0002-0426-6768

Павло Опенько, кандидат технічних наук, старший дослідник

Начальник науково-дослідного відділу інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0001-7777-5101

Антон Козир, кандидат технічних наук

Начальник науково-дослідного відділу Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки,

Чернігів, Україна

https://orcid.org/0000-0002-1888-2553

Анотація. *Характерною ознакою воєнних конфліктів XXI століття є поява нового виду війн – інформаційних, коли перемога здобувається не за рахунок знищення збройних сил і економіки противника, а через вплив на його морально-психологічний стан. В умовах сьогодення, все частіше використовуються методи, засновані на комплексному застосуванні політичних, економічних, інформаційних та інших невоєнних заходів, що реалізуються з опорою на військову силу. Сукупність цих методів реалізує концепцію гібридної війни, провідною ідеєю якої є досягнення політичних цілей з мінімальним військовим впливом на противника за рахунок застосування сучасних інформаційних технологій з опорою на "м'яку силу" і "тверду силу".*

З метою дослідження розвитку гібридної агресії Російської Федерації (РФ) проти України в довгостроковій перспективі (до 2035 року) був проведений аналіз розвитку інформаційного аспекту взаємовідносин між Україною та іншими впливовими регіональними та світовими акторами щодо розвитку ситуації довкола України.

За результатами проведеного аналізу, ситуація, що склалася, містить передумови декількох сценаріїв майбутнього розвитку подій довкола України в умовах гібридної агресії РФ. Однак, вочевидь, на найближчі роки це майбутнє буде обмежено двома ключовими константами – широкомасштабна збройна агресія і остаточне врегулювання політичної ситуації між Україною та РФ. Отримані у процесі наукових досліджень результати, доцільно враховувати при прогнозуванні варіантів розвитку інформаційних аспектів ймовірного сценарію розвитку гібридної агресії РФ проти України в довгостроковій перспективі.

Ключові слова: *національна безпека, інформаційна безпека, гібридна агресія, інформаційна війна.*

Вступ

Постановка проблеми. Актуальність дослідження обумовлена необхідністю формування сценаріїв інформаційного протистояння в рамках гібридної агресії РФ проти України з метою пошуку шляхів мирного врегулювання та протидії існуючій агресії.

Основою для прогнозування варіантів розвитку інформаційного аспекту гібридної агресії РФ проти України є аналіз подій та тенденцій в інформаційному просторі навколо України.

Виходячи з трендів розвитку міжнародної безпеки у довгостроковій перспективі, визначених російськими аналітичними центрами, можна зробити висновок, що РФ розглядає гібридну агресію проти України, як визначальний чинник у майбутніх міжнародних відносинах. Її інформаційна політика стосовно України, в майбутньому, матиме виключно агресивний характер.

Аналіз останніх досліджень і публікацій. Через гібридну агресію РФ проти України, воєнно-політичну нестабільність на Близькому Сході, боротьбу за вплив на світові фінансові та енергетичні потоки посилюється глобальна воєнно-політична нестабільність. Провідні держави збільшують розміри воєнних витрат, активізують розробку нових зразків озброєння, підвищують інтенсивність військових навчань.

Основні тенденції формування та розвитку безпекового середовища у світі розглядаються як вітчизняними [1] так і закордонними авторами [2]. В той же час, постійні зміни в геополітичні обстановці, викликають оновлення доктринальних документів з інформаційної безпеки, як в Україні [3–4], так і в країні агресорі – РФ [5–6].

Зважаючи на зазначені динамічні зміни, інформаційний аспект гібридної агресії РФ проти України розглядається як безпосереднє протистояння сторін в інформаційній війні, спрямованій:

з російського боку – на утримання населення України у своїй системі координат, що повністю відповідає цілям РФ щодо України;

з нашого боку – на формування національної ідеї, сутність якої може полягати в єдності України з цивілізованим “західним” світом, встановленні

європейської (“західної”) системи цінностей і повному розриві з російською імперською ідеологією.

Мета доповіді. Визначення на основі методу сценарного прогнозування варіантів інформаційних аспектів ймовірного сценарію розвитку воєнного конфлікту з РФ в довгостроковій перспективі (до 2035 року).

Виклад основного матеріалу

Основою некласичних форм реалізації російської агресивної політики є дестабілізація суспільно-політичної обстановки в країні, використання протестного потенціалу місцевого населення, дискредитація на міжнародній арені, вплив на політичну, економічну, енергетичну, соціальну, фінансову та інші сфери життєдіяльності країни. В основі цих форм лежать способи та технології інформаційної боротьби, що знайшли своє відображення у стратегічних документах, які визначають політику РФ у сфері військового будівництва та застосування збройних сил, а саме Стратегія національної безпеки (грудень 2015 р.) [7] та Воєнна доктрина (грудень 2014 р.) [8]. Для реалізації своїх планів у складі збройних сил РФ були створено війська та сили інформаційних операцій. До проведення заходів інформаційної боротьби широко залучаються засоби масової інформації (далі - ЗМІ), також набули широко використання інтернет-центри так звані “фабрики тролів”.

На підставі вищевикладеного можна визначити дві групи чинників, які визначають інформаційний аспект воєнного конфлікту РФ з Україною.

Перша група (відношення провідних країн світу та міжнародних безпекових організацій до України):

відношення провідних країн світу до України;

відношення провідних країн світу до РФ;

відношення (сприйняття конфлікту) міжнародних безпекових організацій до України;

відношення (сприйняття конфлікту) міжнародних безпекових організацій до РФ;

ступінь присутності російських (проросійських) інформаційних джерел (ЗМІ, впливові особи, політичні партії, громадські організації тощо) в інформаційному просторі провідних країн світу;

ступінь присутності українських (проукраїнських) інформаційних джерел (ЗМІ, впливові особи, політичні партії, громадські організації тощо) в інформаційному просторі провідних країн світу;

ступінь впливу російських (проросійських) інформаційних джерел (ЗМІ, впливові особи, політичні партії, громадські організації тощо) на рішення міжнародних безпекових організацій;

ступінь впливу українських (проукраїнських) інформаційних джерел (ЗМІ, впливові особи, політичні партії, громадські організації тощо) на рішення міжнародних безпекових організацій;

сприйняття провідними країнами світу української та російської спільної історії (за версією України чи РФ);

рівень підтримки провідними країнами світу факту створення Православної Церкви України;

захищеність інформаційного простору провідних країн світу від кібератак російських (проросійських) хакерів;

спільність історії, культури, мистецтва України з провідними країнами світу;

спільність історії, культури, мистецтва України з РФ;

наявність та активність російської діаспори в провідних країнах світу;

наявність та активність української діаспори в провідних країнах світу.

Друга група (сприйняття населенням України державної інформаційної політики):

сформованість національної ідеї України;

ступінь самоідентифікації громадян України;

єдність поглядів громадян України на питання релігії (підтримки створення Православної Церкви України);

єдність поглядів громадян України на питання мови (провідного статусу української мови у всіх регіонах України);

рівень життя населення в РФ;

рівень життя населення в Україні;

можливість етнічних конфліктів в Україні;

можливість етнічних конфліктів в РФ;

сили і засоби, які РФ використовує (може залучити) до інформаційної кампанії проти України;

сили і засоби, які Україна використовує (може залучити) до забезпечення власної інформаційної боротьби та інформаційного впливу на РФ;

захищеність інформаційного простору РФ від інформаційних впливів;

захищеність інформаційного простору України від інформаційних впливів;

наявність та активність проросійських сил в Україні;

наявність та активність проукраїнських сил в РФ;

авторитет та рівень довіри населення України до керівництва держави, державних інститутів та складових сектору безпеки і оборони України;

авторитет та рівень довіри населення РФ до керівництва держави, державних інститутів та силових структур РФ;

втомленість населення України від воєнного конфлікту;

втомленість населення РФ від конфлікту.

Обрані комплексні чинники дають можливість отримати один базовий і чотири похідних сценарії розвитку ситуації.

Висновки

У доповіді авторами визначені дві найбільш впливові групи чинників, які визначають інформаційний аспект гібридної агресії РФ проти України: відношення провідних країн світу та міжнародних безпекових організацій до України; сприйняття населенням України державної інформаційної політики.

На підставі проведеного дослідження визначено, що, по-перше, Україна у довгостроковій перспективі (до 2035 року) постійно буде знаходиться під інформаційним впливом РФ; по-друге, інформаційний простір України недостатньо захищений від інформаційних впливів РФ; по-третє, в українському суспільстві ще не сформована національна ідея. Саме тому, необхідно здійснювати комплекс заходів щодо забезпечення інформаційної безпеки України, реалізація якого дозволить створити умови для сталого та гарантованого задоволення національних інтересів держави, упередження та нейтралізації загроз національним інтересам та національній безпеці України в інформаційній сфері.

Список літератури

1. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства Аналітичний документ. Київ, 2018. [Електронний ресурс]. – Режим доступу: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok XXI-end 0202.pdf.
2. Foresight 2018: systemic world conflicts and global forecast for XXI century / International Council for Science etc.; Scientific Supervisor M. Zgurovsky. – K.: NTUU “Igor Sikorsky Kyiv Polytechnic Institute”, 2018. – 226 p.
3. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020.
4. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017.
5. Военная доктрина Российской Федерации, утвержденная Президентом РФ 25.12.2014 № Пр-2976.
6. Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента РФ от 5.12.2016 № 646.
7. Стратегия национальной безопасности Российской Федерации. – [Електронний ресурс]. – Режим доступу: http://www.consultant.ru/document/cons _doc_LAW_191669/61a97f7ab0f2f3757fe034d11011c763bc2e593f/
8. Президент утвердил новую редакцию Военной доктрины. – [Електронний ресурс]. – Режим доступу: http://static.kremlin.ru/media/events/files/ 41d527556bec8 deb3530.pdf

Аналіз проблемних питань протимінної діяльності в Україні та можливі шляхи їх вирішення

Володимир Коцюруба, доктор технічних наук, професор, заслужений винахідник України

Професор кафедри оперативного та бойового забезпечення Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0001-6565-9576

Олександр Смальков, кандидат технічних наук

Доцент кафедри оперативного та бойового забезпечення Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0001-7351-393X

Василь Полюляк, ад'юнкт кафедри оперативного та бойового забезпечення Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0002-6536-5612

Михайло Гритчук, слухач інституту державного та військового управління Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0003-1038-3175

Анотація. *У доповіді стисло наведений аналіз проблем протимінної діяльності та шляхи їх вирішення.*

Ключові слова: *протимінна діяльність, вибухонебезпечні предмети, мінна небезпека, розмінування.*

Вступ

Постановка проблеми. В результаті збройної агресії Російської Федерації проти України на звільнених територіях Донецької та Луганської областей, територіях, окупованих незаконними збройними формуваннями, виникла проблема забруднення вибухонебезпечними предметами (у тому числі найбільш небезпечними – саморобними вибуховими пристроями (ВНП)) та надання допомоги жертвам, постраждалим від них [1-2].

Аналіз застосування ВНП в зоні операції Об'єднаних сил (ООС) показує, що ВНП розкидані по всій території конфліктної зони, особливо уздовж лінії бойового зіткнення і являють собою серйозну загрозу для особового складу, озброєння і техніки, цивільних осіб, включаючи дітей. На сьогодні замінована територія складає понад 7000 кв. м [3].

Україна входить до числа країн з найбільшою у світі кількістю жертв мін та інших вибухонебезпечних залишків війни. Підриви на мінах і боєприпасах, що не розірвалися, досі залишаються основною причиною жертв серед дітей у 2017-2018 роках, склавши близько двох третин від усіх зареєстрованих випадків

смерті і травм, через що багато дітей залишилися з інвалідністю на все життя [4-5].

Ці статистичні дані є безпосереднім результатом триваючої агресії Російської Федерації на Сході України, де значна площа земель як на підконтрольній, так і на тимчасово окупованій території наповнена мінами та боєприпасами, що не вибухнули.

Аналіз останніх досліджень і публікацій. Проведений аналіз існуючих публікацій вказує, що в напрямку протимінної безпеки та розмінування було проведено багато досліджень [6-8], але проблемні питання протимінної діяльності в Україні та можливі шляхи їх вирішення не розглядалися.

Метою доповіді є висвітлення проблемних питань протимінної діяльності в Україні та можливі шляхи їх вирішення.

Виклад основного матеріалу

За останні роки міжнародна спільнота все більше усвідомлює масштаби і серйозність проблеми, які пов'язані із ВНП і прийшла до розуміння, що це глобальна проблема, яка потребує узгоджених глобальних заходів реагування. Організація Об'єднаних Націй (ООН) відіграє ключову роль у формулюванні заходів реагування та забезпеченні необхідної міжнародної підтримки та механізмів взаємного узгодження. Питання протимінної діяльності (ПМД) регулярно виносяться на розгляд Генеральної асамблеї ООН. З часом стратегічні цілі і завдання ПМД коригуються, але мета залишається незмінною: зменшення соціального, економічного та екологічного впливу мін та вибухових залишків війни на населення та економіку країни.

Протимінна діяльність – комплекс заходів, спрямованих на захист національних інтересів, а також на зменшення соціального, економічного та екологічного впливу мін та вибухонебезпечних предметів на життя та діяльність населення [9]. Протимінна діяльність зазвичай представляє собою комплекс п'яти взаємодоповнюючих груп діяльності [10]:

гуманітарне розмінування, тобто пошук мін і вибухонебезпечних залишків війни, звільнення земель, картографування і маркування небезпечних ділянок та очищення від мін;

навчання ризикам життєдіяльності населення, пов'язаним з вибухонебезпечними предметами (Risk education (RE));

надання допомоги постраждалим, включно з реабілітацією та реінтеграцією;

знищення запасів зброї;

адвокація з метою сприяння розробки політик та практик, що дадуть змогу зменшити загрозу від мін та вибухонебезпечних залишків війни.

Термін "протимінна діяльність" позначає заходи, що включають інформування про мінну небезпеку, розвідку і розмінування, допомогу жертвам, інформаційну роботу, направлену на розуміння небезпеки ВНП. Втім, ПМД і заходи, які вона включає, не можуть розглядатися окремо, оскільки вони значною мірою співпадають з додатковими гуманітарними програмами та програмами розвитку, та у деяких випадках із миротворчими операціями. ПМД

потребує планування і управління на глобальному, національному і місцевому рівнях та передбачає роботу зацікавлених осіб серед представників міжнародної, національної громадськості, сфери комерції, неурядових організацій та збройних сил за різних умов.

Основну відповідальність за ПМД несе уряд країни, ураженої мінами. Ця відповідальність зазвичай покладається на національний орган (НО) ПМД, який відповідає за регулювання, управління і координування національної програми протимінної діяльності. НО ПМД несе відповідальність за створення національних і місцевих умов для ефектного управління ПМД. Цей орган несе одноосібну відповідальність за всі етапи та всі аспекти програми ПМД в межах своїх державних кордонів, у тому числі за розробку національних стандартів та інструкцій з ПМД.

Із прийняттям Закону України від 22 грудня 2004 р. №2281-IV "Про прийняття Протоколу про вибухонебезпечні предмети-наслідки війни" [11] наша держава взяла на себе зобов'язання проводити операції в галузі ПМД згідно з міжнародними стандартами ПМД.

З *початком агресії Росії,* ситуація на території Донецької та Луганської областей стала просто катастрофічною. Генеральний секретар ООН Антоніу Гутерреш у доповіді на засіданні Генеральної асамблеї 31 липня 2017 року [12] назвав Україну серед країн, в яких найбільше потерпілих від ВНП. В цій же доповіді визначені стратегічні цілі ООН у сфері ПМД.

На європейській конференції, присвяченій гуманітарній кризі на сході України, що проходила у березні 2018 року у Брюсселі, заступник генерального секретаря ООН з гуманітарних питань Урсула Мюллер заявила, що Східна Україна швидко стає однією з найбільш замінованих територій у світі. Тільки на території підконтрольній Україні майже 7 000 км^2 місцевості забруднено ВНП, а отже виключені із використання в господарській діяльності. З початку бойових дій від ВНП постраждало 1858 осіб, з них 102 дитини. Основною причиною загибелі мирного населення є нерозуміння небезпеки, яку несуть ВНП і незнання правил поведінки на території забрудненій ВНП.

Відповідно до міжнародної практики та Міжнародних стандартів ПМД в державі, територія якої забруднена ВНП, повинна створюватися відповідна система ПМД, що регламентується відповідним законодавством. Система ПМД повинна включати: суб'єкти ПМД, їх повноваження, зв'язки між ними та процеси, які вони виконують, об'єкти ПМД та вимоги до них і спрямована на якісне виконання завдань ПМД.

Найважливішим продуктом ПМД є розмінована місцевість, а найскладнішим процесом – процес розмінування. Саме розмінування дозволяє досягти мети ПМД – зменшити масштаби соціального, економічного і екологічного впливу ВНП на населення та економіку.

На основі аналізу стану питання функціонування існуючої системи ПМД в Україні встановлено:

механізми та інструкції координаційної роботи наявні, але вони потребують удосконалення. Розроблена нормативна база спрямована на вдосконалення співпраці та взаємодії між різними учасниками. Крім цього,

функціонує штаб, який об'єднує представників усіх залучених відомств, для звітування про заходи та проблемні питання;

координаційний центр міжнародної підтримки у ПМД не визначений, але уряд працює над удосконаленням структури системи ПМД у країні. Розроблені проекти нормативних актів, які допоможуть у створені національного органу (НО) з питань ПМД та центру ПМД. До НО ПМД будуть залучені всі відповідні відомства;

відповідальність за гуманітарне розмінування наразі покладена на ДСНС України. Однак, основні заходи з ПМД на нещодавно звільнених територіях виконують переважно підрозділи Збройних Сил України;

зазвичай донори не виявляють бажання надавати фінансування установам, які знаходяться під військовим керівництвом або які переслідують військові цілі. Це є додатковою підставою для створення базової структури цивільного органу, відповідального за ПМД.

Можливими шляхами вирішення проблемних питань щодо НО ПМД є: створення в межах існуючих інституційних структур; надання повноважень представляти інтереси Уряду та інших організацій відповідно до міжнародних стандартів та законодавства. Членами НО ПМД повинні стати представники міністерств та відомств. Регіональні адміністрації також повинні брати участь у роботі НО ПМД на ротаційній основі; управління екологічної безпеки та ПМД Міністерства оборони має виконувати функції секретаріату НО ПМД.

Стосовно центру протимінної діяльності (ЦПМД) слід зазначити наступне: має бути підзвітним НО ПМД; має безпосередньо звітувати перед головою НО ПМД; керівник ЦПМД має призначатися членами НО ПМД; положення про ЦПМД розробляє НО ПМД; несе відповідальність за збирання та розповсюдження інформації; виконує контроль якості результатів ПМД; несе відповідальність за навчання протимінній справі та нарощування потенціалу у країні.

При цьому, ЦПМД повинен головним чином фінансуватися за рахунок державних коштів, через незалежний бюджет; на власний розсуд отримувати технології та обладнання для виконання своїх обов'язків; мати можливість залучати кошти від міжнародних партнерів та донорів, з міжнародними учасниками ПМД.

Як показав досвід Хорватії, якщо структури ПМД створюються багато років потому після завершення конфлікту, то існує ризик втрати інформації, а значна територія потребуватиме повторної перевірки та повторного очищення. Внаслідок цього така ситуація неминуче призведе до дублювання завдань та марного витрачання обмежених ресурсів. На прикладі Хорватії було показано, що залучення міжнародних фондів може бути простішим, якщо в країні діє цивільний НО ПМД.

Висновки

Як висновок слід зазначити наступне. НО ПМД та ЦПМД повинні створюватись в межах існуючих державних структур. Очолювати НО ПМД повинен Прем'єр-Міністра України, а його заступниками мають бути заступник

Міністра оборони України та Голова ДСНС України. Членами НО ПМД мають бути всі члени Державної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій. Управління екологічної безпеки та ПМД Міністерства оборони України має виконувати функції секретаріату НО ПМД. НО ПМД визначатиме державну політику в сфері ПМД та представлятиме інтереси Уряду та інших організацій відповідно до міжнародних стандартів та законодавства. ЦПМД має бути підзвітним НО ПМД і виконувати функції його оперативного підрозділу і реалізовувати державну політику в сфері ПМД.

Список літератури

1. Воєнна доктрина України: Указ Президента України від 24.09.2015 р. № 555/2015 К.: АПУ, 2015. URL: https://zakon.rada.gov.ua/laws/show/555/2015.
2. Концепція розвитку сектору безпеки і оборони України: Указ Президента України від 14.03.2016 р. №92/2016. К.: АПУ, 2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016Text.
3. Україна – п’ята в світі за кількістю жертв вибухів мін. URL: https://m.censor.net.ua/news/ 3161155/ ukraina_pyataya_v_mire_po_kolichestvu_ jertv_vzry vov_min_doklad (дата звернення: 05.03.2020).
4. Анатомия армии. URL: http://armor.kiev.ua/army/engenear/razminir- ova-2. shtml.
5. Допомога в діяльності, пов’язаній з розмінуванням. Доповідь Генерального секретаря ООН Антоніу Гутерреш на 72 сесії Генеральної асамблеї 31 липня 2017 року. URL: https://www.kmu.gov.ua/news/250123740.
6. Курсеітов Т. Л., Нероба В. Р. Прихована загроза. Військовий вісник. №10, 2019.
7. Особливості гуманітарного розмінування. URL: https://www.radiosvoboda.org/a/29685254.html (дата звернення: 27.02.2020).
8. Ворович Б.О. Шляхи вирішення проблемних питань розмінування території України. Збірник наукових статей ЦВСДІ НУОУ. Воєнно-прикладні питання системного аналізу та математичного моделювання. 24.03.2020.
9. Протимінна діяльність [Електронний ресурс] – Режим доступу до ресурсу: http://audm.org.ua/nashi-proekti/komertsijna-struktura/.
10. Mine action [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Mine_action.
11. Закону України від 22 грудня 2004 р. №2281-IV “Про прийняття Протоколу про вибухонебезпечні предмети-наслідки війни”.
12. Допомога в діяльності, пов’язаній з розмінуванням. Доповідь Генерального секретаря ООН Антоніу Гутерреш на 72 сесії Генеральної асамблеї 31 липня 2017 року. URL: https://www.kmu.gov.ua/news/250123740.

Особливості воєнних аспектів ведення гібридної війни

Ігор Романченко, доктор військових наук професор
Директор Центрального науково-дослідного інституту Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-2008-5649
Анатолій Зварич, кандидат військових наук, старший дослідник
Провідний науковий співробітник Центрального науково-дослідного інституту Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0002-7136-0295

Анотація. *За результатами проведеного аналізу виконання завдань під час антитерористичної операції та операції об'єднаних сил визначено характерні риси бойових дій в умовах ведення "гібридної" війни. У доповіді висвітлюються особливості воєнних аспектів такої війни.*

Зазначені риси стосуються складу сил і засобів, що беруть участь у бойових діях в умовах "гібридної" війни, часових та просторових параметрів ведення бойових дій, форм і способів застосування військ в умовах такої війни.

Ключові слова: *гібридна війна, форма ведення воєнних дій, регулярні та іррегулярні військові формування, бойовий склад.*

Вступ

Постановка проблеми. З трансформацією та формуванням безпекового середовища в світі відбувається еволюція воєнних конфліктів. Вони дедалі набувають комбінованого ("гібридного") характеру, поєднуючи ознаки класичної війни між державами, внутрішнього збройного конфлікту, політичного, дипломатичного, економічного та інформаційного протиборства, тероризму й організованої злочинності.

При цьому, найбільш складними у конфлікті є воєнні аспекти його ведення, які недостатньо досліджені. Отже питання визначення особливостей воєнних аспектів ведення "гібридної війни", яка на сьогодні триває проти України, є актуальним.

Аналіз останніх досліджень і публікацій. Проведений аналіз останніх публікацій у відкритих джерелах свідчить про те, що таке явище, як гібридна війна вже добре відоме. Цій темі присвячено багато публікацій, серед яких слід відмітити [1–4]. Але у своїй більшості ці публікації мають загальний характер і фрагментарно висвітлюють окремі аспекти гібридної війни. Особливості воєнних аспектів в зазначених публікація окремо не досліджуються і не систематизовані.

Мета доповіді. Мета доповіді полягає у викладенні поглядів на особливості воєнних аспектів ведення "гібридної війни".

Виклад основного матеріалу

Найбільш складними у сучасних конфліктах залишаються воєнні аспекти його ведення. Це пов'язано з тим, що в таких конфліктах реалізуються національні інтереси та приховано застосовуються регулярні та іррегулярні військові формування декількох держав, а представляється конфлікт як внутрішній.

Конфлікт охоплює територію, на якій одночасно з веденням бойових дій продовжується функціонування об'єктів цивільної інфраструктури. При цьому, на збройні сили та інші військові формування покладаються завдання, які для них не були б притаманними в умовах відкритого міждержавного воєнного конфлікту.

Форми ведення воєнних дій в умовах "гібридної" війни наповнюються новим змістом. Розширюються часові та просторові параметри їх ведення. Підвищується роль військових формувань тактичного рівня у вирішенні оперативних та, навіть, стратегічних завдань. Бій стає основною складовою воєнних дій і характеризується високою активністю, мобільністю та автономністю частин і підрозділів, різноманітністю та нетиповістю способів виконання завдань.

У конфлікті, в який втягнуто сьогодні Україну, вищезазначені особливості мають комплексний характер.

За результатами проведеного аналізу виконання завдань під час антитерористичної операції та операції об'єднаних сил визначено характерні риси бойових дій в умовах ведення "гібридної" війни.

Зазначені риси стосуються складу сил і засобів, що беруть участь у бойових діях в умовах "гібридної" війни, часових та просторових параметрів ведення бойових дій, форм і способів застосування військ в умовах такої війни.

На відміну від класичної, в "гібридній" війні бойові дії, локальні бої, бойові зіткнення ведуться незначними за чисельністю та різнотипними військовими формуваннями. При цьому, їх бойовий склад, зазвичай, не має типової структури, він постійно зазнає змін, відповідно до умов обстановки.

Характерною особливістю бойових дій в такій війні є те, що в них беруть участь не тільки регулярні війська та інші державні військові формування, а й іррегулярні формування, добровольчі батальйони, найманці, приватні охоронні компанії, цивільне населення. У воєнному конфлікті на Сході України частина особового складу іррегулярних формувань становить 30-40 % (добровольчі підрозділи, ополченці, донські козаки, кадирівці, різноманітні кримінальні угруповання), що майже у вісім разів більше ніж у класичних війнах.

У війні "гібридного" типу, відмічається така специфічна ознака як наявність у бойовому складі частин і підрозділів озброєння та військової техніки різних поколінь, широке використання цивільного транспорту, і підвищення ролі вогневого ураження противника засобами ближнього бою (протитанковими комплексами, крупнокаліберними кулеметами, снайперською зброєю), артилерією тощо.

На відміну від класичної, "гібридна" війна відрізняється часовими та просторовими параметри і може тривати десятиріччями (приклад –

Придністров'я, Абхазія, Осетія, Нагірний Карабах). Її просторовий розмах не обмежується самою зоною бойових дій, а поширюється на всю територію країни. Так, територія, охоплена антитерористичною операцією становила понад 16 тисяч квадратних кілометрів, площа окупованої автономної республіки Крим – 27 тисяч. 13 районів Донецької та Луганської областей не контролюються органами державної влади України. Терористичні акти, збройні провокації, масові сутички мали місце на території Харківської, Запорізької, Одеської та інших областей, а потужний інформаційний вплив поширюється не тільки на громадян країн, що тим чи іншим чином беруть участь у воєнному конфлікті, а й на світову спільноту.

При цьому, спостерігається значне збільшення ступеня розосередження військ на полі бою, смуг та районів відповідальності частин і підрозділів, наявність значних відстаней між підрозділами у бойових порядках, які в два-три рази перевищують просторові характеристики бойових порядків частин та підрозділів в класичних операціях.

Побудова бойових порядків в таких війнах спрямовується на те, щоб встановити контроль у районах населених пунктів, над важливими автомобільними та залізничними шляхами і вузлами. При цьому, низька щільність військ та практична відсутність вогневої взаємодії між ними зумовлює легкість проникнення диверсійно-розвідувальних груп у тил частин і підрозділів. Зазначене вказує на важливість територіальної оборони у виконанні завдань боротьби із диверсійно-розвідувальними силами противника.

Крім того, "гібридна" війна відрізняється наявністю різних за інтенсивністю періодів ведення бойових дій.

Найбільш інтенсивними такими періодами в Україні можна вважати: звільнення від бойовиків понад 30 населених пунктів та взяття під контроль частини україно-російського кордону; бойові дії підрозділів сил АТО в районах населених пунктів Іловайськ, Старобешеве та Амвросіївка, бої за Донецький аеропорт та за населений пункт Дебальцеве.

Також слід зазначити, що характерною рисою "гібридних" війн, особливо початкового, прихованого етапу їх ведення, є потужна інформаційна протидія сторін, широке застосування сил спеціальних операцій, масові акції протесту та безлади на вулицях, погроми державних установ, соціальні, політичні, міжнаціональні та релігійні сутички тощо.

Фактично всі зазначені вище прийоми були використані під час анексії Автономної Республіки Крим, розв'язання війни на Сході України та дестабілізації внутрішньополітичної ситуації в державі.

У таких умовах головна роль у виконанні завдань щодо стабілізації обстановки відводиться іншим військовим формуванням і правоохоронним органам, а також державним і воєнним структурам, які пов'язані із веденням інформаційної боротьби. При цьому, від результатів виконання, покладених на них завдань, напряму залежить перероставання конфлікту у відкрите збройне протистояння або його припинення.

Специфічною ознакою "гібридної" війни, можна вважати також те, що все різноманіття змісту та порядок дій сил і засобів, які беруть участь у збройному

протистоянні, складно представити у вигляді якоїсь конкретної відомої форми застосування військ.

У нашій країні такою формою стала антитерористична операція, в Російській Федерації наприкінці минулого сторіччя – контртерористична, в Грузії у 2008 році – операція з примушення до миру або з відновлення конституційного ладу.

Характерною властивістю цих, а також інших операцій стало сполучення в межах однієї операції класичних оборонних та наступальних бойових дій, повітряних та протиповітряних боїв, спеціальних операцій, партизанських дій (засідок, нальотів, терористичних актів), інформаційно-психологічних, кібернетичних операцій, контрдиверсійних та інших дій.

При цьому, як свідчить досвід, роль спеціальних та інформаційних операцій (інформаційних компаній) у досягненні стратегічних цілей щодо встановлення контролю на певній території або забезпечення територіальної цілісності, останнім часом, значно зросла. Широкомасштабні наступальні та оборонні операції великих угруповань військ поступилися місцем бойовим діям, боям незначних за чисельністю військових формувань.

Відрізняє "гібридну" війну від класичної і принципове змінення в умовах такої війни змісту основних видів бойових дій – оборони та наступу.

Сьогодні в основу оборони, замість позиційної лінійної багатоешелонованої тактики її ведення покладено мобільні дії військ, які означають не тільки швидке пересування військ до початку та у ході бойових дій, а й своєчасне здійснення маневру вогнем, виходу з-під ударів противника, високоточний вогонь по його критичних об'єктах.

Мобільні дії, передбачають обов'язкове ефективне функціонування системи розвідки і управління, побудову оборони без акцентування на завчасному зосередженні більшості сил і засобів на обраному напрямку, а натомість із послідовною концентрацією сил і засобів у необхідному місці в інтересах розгрому противника по частинах: спочатку головної, а потім інших його ударних або обхідних угруповань завданням коротких контрударів чи потужних вогневих ударів із зайнятих вогневих рубежів.

Досвід ведення оборони показав, що більш ефективним способом її ведення залишається маневрена оборона. Успішному веденню маневреної оборони сприяє те, що бій ведеться в населеному пункті під прикриттям будівель, а лінія оборони має воронкоподібне розташування. Така організація оборони дозволяє уникнути значних втрат і зв'язати боєм значні сили противника для забезпечення виконання завдання на інших напрямках.

У наступі традиційно масовані вогнева підготовка та підтримка атаки, розгортання військ у батальйонні, ротні, взводні колони для переходу в атаку, прорив, що полягає у зламі оборони противника на обраних напрямках, оволодіння опорними пунктами, першою позицією, поступаються сьогодні місцем, вибірковому високоточному ураженню критичних об'єктів противника, рішучому обходу противника з флангів та його оточенню, широкому застосуванню маневру військами та вогнем, рейдових, десантно-штурмових, пошуково-ударних дій, дій повітряних десантів та їх поєднання.

Одним із таких прикладів є проведення рейдових дій 95 оаембр у період з 18 липня по 10 серпня 2014 року в напрямку ЛИСИЧАНСЬК, ДЕБАЛЬЦЕВЕ, САВУР-МОГИЛА, та вихід у район зосередження СЛОВ'ЯНСЬК загальною протяжністю маршруту 455 км.

Висновки

Отже враховуючи результати наукових досліджень та бойового досвіду в умовах "гібридної" війни можна зробити висновки, що в інтересах підвищення оперативних та бойових можливостей військ для реагування на сучасні загрози актуальним є:

визначення завдань іншим військовим формуванням та правоохоронним органам щодо їх участі у відсічі збройної агресії;

уточнення правил застосування зброї та бойової техніки іншими військовими формуваннями та правоохоронними органами в мирний час та під час введення в державі правового режиму надзвичайного стану з метою своєчасного реагування на "гібридні" загрози;

визначення порядку залучення підприємств, організацій всіх форм власності до оборони держави в особливий період.

Зміст підготовки військ (сил) необхідно адаптувати до умов ведення "гібридної" війни. При цьому, основні зусилля зосередити на підготовці військовослужбовців до виконання завдань під час ведення бойових дій в населених пунктах, на блокпостах, опорних пунктах на лінії бойового зіткнення (розмежування), у складі бойових двійок-трійок, мобільних підрозділів, а також спільно з іншими військовими формуваннями та правоохоронними органами.

Список літератури

1. Протидія гібридній війні: досвід України.: аналітична доповідь / Київ: Національний інститут стратегічних досліджень, 2016. 70 с.

2. Аналіз ведення антитерористичної операції та наслідків вторгнення Російської Федерації в Україну у серпні-вересні 2014 року: посіб. Київ: ГШ ЗС України, 2015. 24 с. URL: https://www.mil.gov.ua/content/other/anliz_rf.pdf.

3. Аналіз Генерального штабу ЗС України щодо бойових дій на Дебальцевському плацдармі з 27 січня до 18 лютого 2015 року. URL: http://www.mil.gov.ua/analitichni-materiali/analiz-generalnogo-shtabu-zsu-shhodo-bojovih-dij-na-debalczevskomu-placzdarmi-z-27-sichnya-do-18-lyutogo-2015-roku.html.

4. Іловайська операція. Упорядник М. Жирохов. Чернігів: Княжий Вал, 2021, 84 с.

Аналіз дій противника і протидія йому в гібридній війні проти України

Олег Кравець, кандидат військових наук, старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0001-7253-5360
Мстислав Случайний, кандидат військових наук, старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-3497-130X
Максим Ніколаєнко, кандидат військових наук
Центральний науково-дослідний інститут Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-3468-0879

Анотація. *Доповідь аналізу дій противника і протидія йому в "Гібридній війні" проти України.*

Ключові слова: *противник, гібридна війна, нейтральні сили, антитерористична операція.*

Вступ

Постановка проблеми. Після анексії Криму і з початком конфлікту на сході України термін "гібридна війна" став все частіше використовуватися військовими фахівцями для відображення дедалі зростаючої складності війни. Саме в Україні Російська Федерація (РФ), реалізуючи "гібридну війну", комплексно здійснює підрив військового та економічного потенціалу країни, чинить інформаційно-психологічний тиск, надає активну підтримку внутрішній опозиції, застосовує партизанські та диверсійні методи.

Отже, виникає необхідність пошуку заходів адекватної протидії. Для цього, насамперед, потрібно визначити особливості дій противника за етапами ведення "гібридної війни" для подальшого розроблення заходів адекватної протидії, що і є актуальним науковим завданням.

Аналіз останніх досліджень та публікацій. У статті [1] розглянуто основний склад сил та характер дій противника, який протистоїть військовим частинам та підрозділам Сухопутних військ ЗС України, під час проведення антитерористичної операції (АТО). У процесі аналізу складу сил та характеру дій противника автор наводить опис основних незаконних збройних формувань (НЗФ), які були створені на сході України за участі диверсійно-розвідувальних сил ЗС РФ.

У статті [2] наголошується на причинах протистояння України і РФ. Також робиться акцент на тому, що військова складова конфлікту об'єктивно залишається основним фактором його розгортання.

У статті [3] пропонується розглядати такі етапи збройних конфліктів за сценарієм "гібридної війни": інноваційна агресія (економічний тиск, інформаційно-психологічні атаки тощо), застосування НЗФ або приватних армій

(повстанський, партизанський рух, тероризм); офіційні військові дії або демонстрація сили (ідентифікована уніформа, зброя, офіційне визнання участі у конфлікті).

Однак у роботах [1–3] не розкриваються основні особливості дій противника в межах складових "гібридної війни", зокрема військової.

Мета доповіді. Метою доповіді є проведення аналізу дій противника в "гібридній війні" проти України.

Викладення основного матеріалу

Аналіз дій противника в гібридній війні проти України свідчить про те, що гібридні загрози одночасно створюють обстановку економічної нестабільності, сприяють зростанню настроїв недовіри до чинної влади, ставлять під удар інформаційні мережі, висуваючи привабливі гасла, що відповідають їхнім цілям, ініціюють штучну гуманітарну кризу й фізично погрожують опонентам. Вони мають місце в інформаційній, соціальній, економічній і військовій сферах.

Ключовими елементами гібридної загрози є: збройні сили держави-агресора; недержавні військові сили; повстанські групи, партизанські загони; кримінальні організації; нейтральні сили.

Нейтральні сили не беруть участі у бойових діях, але їхня присутність, діяльність та інтереси, як правило, впливають на здатність Збройних Сил України виконувати свої завдання. До них належать: біженці та внутрішні переселенці; міжнародні організації; транснаціональні корпорації; засоби масової інформації тощо.

Досвід показує, що на різних етапах характер "гібридної війни" залежить від політичних цілей воюючих сторін, соціальної структури, військових, економічних і духовних можливостей держав (або інших учасників), що безпосередньо беруть участь у війні, засобів збройної боротьби, які застосовуються сторонами конфлікту, а саме:

об'єктом конфлікту є території, на які агресор має приховані претензії, що не можуть бути висловлені відкрито, зважаючи на існуючу систему міжнародного права;

суб'єктами конфлікту є: Україна, яка має суверенітет над спірною територією, та сукупність незаконно створених збройних формувань, найманців, кримінальних елементів, диверсійно-розвідувальних сил за всебічної (інформаційної, фінансової, військової) підтримки Російської Федерації, котра має приховані претензії;

формування незаконно створених організованих збройних формувань і здійснення ними різних акцій збройного насильства (зокрема блокування військових об'єктів, захоплення органів державної влади, банків тощо), що є можливим за умови значного зростання обсягів прихованої матеріальної та консультативної підтримки з боку країни-агресора;

загострення збройного протистояння із силами безпеки і оборони України, пряма військова допомога незаконно створеним збройним формуванням з боку агресора;

формування в окремих регіонах України псевдоуряду, який намагається легітимізуватися на міжнародній арені;

забезпечення політичної підтримки псевдоуряду з боку інших держав і подальша легітимізація його матеріальної та консультативної підтримки;

переформатування або ухвалення нового національного законодавства України в інтересах агресора;

надання агресором значної матеріальної допомоги на відновлення цілковито або частково зруйнованої економіки для поглиблення залежності від нього квазідержавного утворення.

Російська Федерація намагається досягти мети "гібридної війни" проти України виконанням низки завдань щодо: дестабілізації суспільно-політичної та економічної ситуації, підриву основ громадянського миру в країні; економічного виснаження внаслідок необхідності значного збільшення витрат на технічне оснащення та підготовку сектора безпеки і оборони в умовах перманентної воєнної загрози, відновлення зруйнованих конфліктом об'єктів інфраструктури, промисловості тощо; позбавлення України союзників; відволікання фінансових і матеріальних ресурсів України від вирішення нагальних проблем розвитку держави; формування свого лобі в державних інститутах, офіційних структурах України, у політичних партіях; створення у складі України анклавів з контрольованим маріонетковим режимом, що має забезпечити можливість постійного впливу на внутрішню і зовнішню політику та легітимізація анексованої території.

З урахуванням наведеного вище, "гібридну війну" проти України умовно можна поділити на три основних етапи: підготовчий, активний та завершальний.

На підготовчому етапі, який тривав кілька років, керівництвом Російської Федерації, за активного залучення його спецслужб, вживалися заходи з формування ідеологічних, політичних, військових передумов для майбутньої агресії, а саме: зміцнення агресором системи державної влади у своїй країні, разом із посиленням контролю над усіма сферами її життєдіяльності; ідеологічне оброблення власного населення задля об'єднання довкола ідей націоналізму у формі завуальованого великодержавного шовінізму, захисту так званих "національних цінностей та інтересів", боротьби із "зовнішнім ворогом" в умовах "оточеної фортеці" тощо, а також максимального послаблення опозиції у всіх її проявах; захоплення інформаційного простору України та використання його у своїх інтересах для формування у суспільстві відповідних настроїв; руйнація державної влади Україні, у т.ч. підкуп впливових урядовців, політичних діячів та керівництва силових структур; просування агентів впливу на посади у державних органах влади; розпалювання протистояння між різними політичними силами та встановлення контролю над ними (насамперед із ідеологічно близьких і корумпованих партій та рухів); ідеологічне розколювання населення України шляхом стимулювання внутрішніх суперечностей політичного, міжнаціонального та міжрелігійного характеру (зокрема в рамках створення та підтримки різних партій, рухів та організацій відповідного, у т. ч. екстремістського спрямування); усебічне послаблення України, підрив довіри населення до влади, а також поширення протестних та сепаратистських настроїв у суспільстві, шляхом провокування соціально-економічних та інших проблем (у т. ч. шляхом застосування елементів торговельно-економічних та енергетичних

війн); дискредитація зовнішньої та внутрішньої політики України, нав'язування її керівництву та населенню певних ідей та цивілізаційних цінностей шляхом проведення активної інформаційної кампанії із застосуванням спеціальних методів "зомбування" суспільства, активно залучаючи як державні, так і неурядові організації.

На активному етапі проводилась прихована агресія проти України з метою безпосередньої реалізації поставлених завдань, таких як: створення на території України незаконних збройних формувань із представників місцевих антиурядових сил, співробітників спецслужб РФ, найманців та бойовиків; провокування на території України внутрішнього конфлікту на політичній, соціально-економічній, конфесійній та міжнаціональній основі, а також стимулювання процесів його переростання в масові виступи населення, акції громадської непокори, безлад та сутички демонстрантів з правоохоронними органами; позиціонування "лідерів" акцій протесту з числа завербованих представників опозиційних політичних сил загальнодержавного або місцевого рівнів, а також створення самопроголошених "органів влади"; захоплення з допомогою учасників акцій протесту, представників незаконних збройних формувань та спецслужб країни-агресора урядових будівель та важливих об'єктів транспортної і промислової інфраструктури, а також блокування діяльності силових структур, зокрема із використанням мирних жителів як "живих щитів" тощо; поступове введення на територію України регулярних збройних сил агресора під виглядом місцевих збройних формувань ("загонів самооборони", "ополченців" тощо) з метою допомоги опозиції та сепаратистам у захопленні влади в державі або в її окремих регіонах та створення системи управління всіма угрупованнями, які здійснюють гібридну агресію; прихована участь регулярних збройних сил РФ у бойових діях; проведення масштабної інформаційної операції з підтримки антидержавних сил в Україні, а також із дискредитації її керівництва та його дій із забезпечення конституційного ладу в державі.

У районах, де противник досягнув своїх цілей на перших двох етапах, він перейшов до третього – завершального етапу, в ході якого проводились заходи щодо закріплення своїх позицій на анексованих територіях, а саме: надання всебічної підтримки новій (в АР Крим) владі та сепаратистським режимам на території Донецької та Луганської областей (разом зі створенням органів влади та силових структур); надання допомоги в ініціюванні та проведенні "референдумів" про зміну спрямованості зовнішнього та внутрішнього курсу, статусу регіонів тощо, а також у проведенні "виборів" до центральних та місцевих органів влади в сепаратистських регіонах; легалізація самопроголошених квазідержавних утворень, гальмування процесів урегулювання ситуації на території України під виглядом посередницької участі у мирних переговорах (при цьому Російська Федерація жодним чином не визнає себе стороною конфлікту); створення умов для забезпечення військової присутності Росії на довготривалій (постійній) основі (під виглядом "миротворчих сил" або збройних формувань сепаратистів), а також для реалізації інших інтересів Росії, зокрема економічних; примушення України до

визнання легітимності анексії її території та нав'язування відновлення територіальної цілісності на умовах Російської Федерації.

У "гібридній війні", як формі вирішення міждержавних протиріч, роль воєнної сили та форми і способи її застосування суттєво відрізнялися від умов так званої класичної, або конвенційної війни.

Основною воєнною силою, на яку спирався агресор, приховуючи зв'язок із нею, є іррегулярні війська. Ці сили завчасно готувалися агресором, забезпечувались озброєнням і військовою технікою, а у багатьох випадках і командним складом вищої та середньої ланки. Діючи таким чином, агресор усіляко намагався трактувати конфлікт як внутрішній, заперечуючи свою причетність до нього.

У ситуаціях, коли виникала загроза розгрому іррегулярних сил ("внутрішньої армії") або їхні можливості виявлялися недостатніми для виконання певних бойових завдань (наприклад, в Іловайську та Дебальцевому), агресор вдавався до безпосереднього застосування у бойових діях військових підрозділів регулярних збройних сил.

Висновки

Аналіз агресивних дій РФ проти України протягом останнього десятиріччя засвідчив, що вони мали характерні ознаки поетапного ведення "гібридної війни". Усі етапи мали місце в АР Крим і, як результат, відбулась анексія. Причому з настанням третього етапу розпочався перший етап "гібридної війни" на сході України, а третій її етап триває і сьогодні.

"Гібридна війна" проти України є реалізацією комплексу "гібридних загроз", які можуть включати конвенційні військові сили (що, як правило, асоціюються з державою) – найсучасніше озброєння, системи управління і тактики загальновійськового бою з атрибутами, які зазвичай асоціюються з повстанськими або кримінальними організаціями (поєднанням регулярних та іррегулярних сил).

Список літератури

1. Голованов А. В., Починок С. М. Аналіз складу та характеру дій незаконних збройних формувань та диверсійно-розвідувальних сил під час проведення антитерористичної операції на сході України // Труди університету: зб. наук. пр. Київ: НУОУ, 2014. № 4 (125). С. 21–24.

2. Горбулин В. "Гибридная война" как ключевой инструмент российской геостратегии реванша: URL: http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html.

3. Курбан О. Сучасна гібридна війна: нові форми агресії. З дослідження "Інформаційні війни у соціальних онлайн-мережах" URL: http://ua.racurs.ua./1063-suchasna-gibrydna-viyna-ta-yiyi-vidobrajennya-u-virtualniy-realnosti-chastyna2.

4. Требін М. Феномен "гібридної" війни // Гілея (2014) Випуск 87 (8). С. 366–371.

5. McCuen J. Hybrid Wars // Military rewiew (March-April 2008) P. 107–113.

Забезпечення інформаційної безпеки України як головний чинник протидії гібридній агресії

Володимир Ткаченко, кандидат військових наук
Заступник начальника управління - начальник відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-9625-2434
Юрій Саричев, кандидат технічних наук, старший науковий співробітник
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-1380-4959
Віктор Зубков
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/ 0000-0003-1616-2795
Микола Підгородецький, кандидат військових наук
Заступник начальника кафедри оперативного та бойового забезпечення Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/ 0000-0003-4807-8635

Анотація. *Доповідь присвячена викладенню загального підходу щодо розуміння необхідності забезпечення інформаційної безпеки держави як важливого елементу протидії гібридній агресії. Наведено основні законодавчі аксіоми для забезпечення інформаційної сфери України в ході протидії під час гібридної агресії. Впровадження наведених положень дозволить найбільш адекватно реагувати на гібридні загрози інформаційного характеру, зокрема з точки зору протидії негативному інформаційному впливу на особовий склад військ (сил).*

Ключові слова: *гібридна агресія, воєнна сфера, інформаційна безпека держави, протидія негативному інформаційному впливу, стратегічні комунікації.*

Вступ

Постановка проблеми у загальному вигляді. Одним із головних висновків "гібридної" війни Росії з Україною є висновок про багаторазове зростання ролі її інформаційної складової. Наслідком зазначеного є потреба невідкладного та пріоритетного нарощення відповідних спроможностей сил оборони України для посилення інформаційної безпеки держави у воєнній сфері загалом.

Значна частина необхідних заходів для цього передбачена законодавством України, де зокрема на Міністерства оборони України покладено завдання щодо

протидії спеціальним інформаційним операціям, спрямованим проти ЗС України та інших військових формувань, а також проведення заходів щодо відсічі воєнної агресії у кіберпросторі, здійснення військової співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз.

Водночас, незважаючи на вжиті організаційні заходи, що проводяться, протидія агресивним інформаційним діям Росії, як невід'ємній частині ведення "гібридної" війни з Україною, має стати ефективнішою. Головною умовою цього має бути наявність розвинутої теоретичної бази щодо забезпечення інформаційної безпеки держави, зокрема у воєнній сфері. Проте сталої теорії щодо цього питання на сьогодні ще немає, незважаючи на численні національні та зарубіжні фахові публікації. Зазначене шкодить створенню адекватної нормативно-правової бази, що негативно позначається на практичних діях.

Аналіз останніх досліджень та публікацій. Сучасний стан проблеми забезпечення інформаційної безпеки, зокрема в Україні, характеризується активними спробами розвитку відповідних теоретичних засад, про що свідчать численні публікації в наукових виданнях. Серед вітчизняних вчених і фахівців цій проблемі приділено увагу в роботах О.Юдіна, В.Богуша, В.Горбуліна, В.Остроухова, М.Присяжнюка, В.Толубка, І.Руснака, В.Телелима, О.Левченка [1 – 8] та ін.

В той же час, незважаючи на значну кількість фахових публікацій за цією проблемою, в Україні на системному рівні й досі належним чином не опрацьоване питання інформаційної безпеки держави, в тому числі у воєнній сфері. Зокрема, відсутнє єдине розуміння базових термінологічних категорій цієї предметної сфери. Зазначене шкодить створенню адекватної нормативно-правової бази, що негативно позначається як на теоретичних узагальненнях, так і на практичних діях. Отже, першочерговим завданням щодо протидії інформаційній агресії, що сьогодні є базовим елементом "гібридності" агресії Росії проти України, є необхідність системного розуміння теоретичних основ забезпечення інформаційної безпеки держави, в тому числі її складових – кібербезпеки, зокрема кібероборони, стратегічних комунікацій тощо, зокрема у воєнній сфері.

Метою виступу є уточнення місця та ролі інформаційної безпеки України загалом (та її складових) як важливого чинника протидії гібридній агресії.

Викладення основного матеріалу

Для забезпечення інформаційної безпеки держави насамперед слід визначитися із фундаментальними положеннями, відповідно до яких має бути організовано та реалізовано цей процес і усі його складові. Таку фундаментальність забезпечує певна аксіоматична база цієї предметної сфери, якої необхідно неухильно дотримуватися. Для суспільного життя та державної діяльності окремої країни аксіоматичним базисом є національна Конституція та державні закони, положення яких мають значення окремих аксіом за певними напрямами упродовж деякого періоду аж до внесення відповідних конституційних або законодавчих змін.

У статті 17 Конституції України визначено, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу. Зауважимо, що зазначена вимога означає найвищий пріоритет діяльності держави. Отже, це положення для інформаційної сфери України слід розглядати та сприймати як першу і головну законодавчу аксіому.

Зважаючи на першу законодавчу аксіому для інформаційної сфери України, має бути законодавче розуміння сутності інформаційної безпеки держави. Слід підкреслити, що законодавство України вперше визначило сутність інформаційної безпеки в Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" [9] в редакції: "*інформаційна безпека* – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігають завдавання шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується;

негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій;

несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації".

Пізніше, у проєкті Стратегії інформаційної безпеки України, яка запропонована Кабінетом Міністрів України та підтримана Радою безпеки та оборони України [10], на наш погляд, це визначення було модифіковане не в кращу сторону (з точки зору формальної логіки та причинно-наслідкових зв'язків).

Нажаль, недосконаліть вітчизняного законодавства стосується й інших нормативно-правових актів держави. Так, як попередня, так і чинна Стратегії національної безпеки України [11] не дотримуються законодавчої спадковості і не акцентують наведених чинників шкоди та їх джерел (причин, природи). Зокрема, визначаються лише такі загрози інформаційній безпеці України, як "відсутність цілісної комунікативної політики держави" та "недостатній рівень медіакультури суспільства". Але це висвітлює лише окремі самостійні ознаки загроз, які доцільні для імплементації у визначення поняття "інформаційна безпека України". Їх не може вважати загрозою, а лише наслідком, тобто зазначене є шкодою, а загроза полягає в іншому та більш кореневому, системному – *внутрішньодержавній нездатності формування та реалізації відповідної галузі інформаційної політики*. Таку тезу підтверджує одне із узагальнених положень цієї Стратегії: "Джерелом загроз незалежності України, її суверенітету і демократії залишається недостатня ефективність державних органів, що ускладнює вироблення і реалізацію ефективної політики".

Тим не менш, первинне визначення [9] можна сприймати як другу законодавчу аксіому для інформаційної сфери України. Ця законодавча аксіома деталізує першу конституційну аксіому та відповідає принципу системного підходу. Таке законодавче формулювання сутності інформаційної безпеки може бути уточнене, але загалом формулювання є доволі чітким, узагальненим та збалансованим. Друга аксіома має принципові наслідки.

Наслідок перший із другої аксіоми. Кібернетична безпека (кібербезпека) – це інформаційна безпека в просторі електронних інформаційних ресурсів. Відповідно, кіберпростір (середовище електронних інформаційних ресурсів) є частиною загального (єдиного) інформаційного простору. В єдиному інформаційному просторі діють єдині загальні закони та методологічні підходи і принципи, тому сутність кібербезпеки України є ідентичною наведеному визначенню. Саме тому штучне (адміністративне) роз'єднання інформаційної безпеки та кібербезпеки суперечить Конституції України, а також логіці, за якою відбуваються всі інформаційні процеси, порушується принцип системності, отже, є недопустимим і для теорії, і для практики. На жаль, в міжнародних та національних нормативно-правових актах припустилися такої ж системної методологічної помилки, що має негативні наслідки, зокрема й для розвитку національного інформаційного законодавства з подальшим викривленням теорії та спотворенням практики щодо забезпечення кібербезпеки. Ця методологічна помилка має бути виправлена.

Наслідок другий із другої аксіоми. Очевидними стають загрози інформаційній безпеці України (незалежно від джерела їх походження та форми реалізації – інформаційна агресія, умисні маніпулятивно-злочинні інформаційні дії, механічне руйнування, інформаційна неспроможність, непрофесійна діяльність, службова бездіяльність), які, матеріалізуючись на практиці, можуть завдати шкоди людині, суспільству чи державі, а саме:

неповнота, невчасність та невірогідність інформації, що використовується;

негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій;

несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Зауважимо, що у чинній Стратегії національної безпеки України [11] наведені інші загрози інформаційній безпеці, які не в повній мірі корелюють з вищенаведеними. Таким чином, зазначене не відповідає вищенаведеному законодавчому визначенню сутності інформаційної безпеки, тобто другій аксіомі та другому наслідку із неї, чим порушується принцип системного підходу. Такий стратегічний наратив може лише доповнювати вищенаведений перелік загроз, за виключенням пункту щодо "інформаційної війни" як політизованого та неконкретного за власне інформаційною складовою.

Наслідок третій із другої аксіоми. Забезпечення інформаційної безпеки України (в тому числі у кіберпросторі, оскільки кіберпростір – невід'ємна складова частина усього інформаційного простору) також є цілком очевидним процесом як протидія збитковості і полягає в реалізації запобіжних заходів проти завдавання шкоди через вищезазначені чинники.

Ситуацію ускладнюють і додаткові чинники: відсутність комунікативної політики держави; недостатній рівень медіакультури суспільства.

На стратегічне спрямування таких запобіжних заходів вказано у [9], де визначено спосіб вирішення проблеми інформаційної безпеки. Ґрунтуючись на цьому положенні, визначимо *третю законодавчу аксіому*. Способом

забезпечити інформаційну безпеку в Україні (вирішити проблему інформаційної безпеки) має бути:

створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

підвищення рівня координації діяльності державних органів щодо виявлення, оцінювання і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії негативному інформаційному впливу та комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері.

До цих положень також слід додати: розвиток системи державних комунікацій – стратегічних, урядових, кризових (як умова запровадження механізму успішної реалізації цілісної комунікативної політики держави для нейтралізації однієї із нинішніх загроз інформаційній безпеці).

На погляд авторів, наведені законодавчі аксіоми та очевидні наслідки із них мають закласти певний фундамент у будь-яку діяльність, спрямовану на забезпечення інформаційної безпеки України. Насамперед, це стосується становлення теоретичних основ цього конституційного напряму діяльності як запоруки проведення адекватних практичних заходів та створення ефективної загальнодержавної системи, а також її складових, зокрема складової воєнної сфери. В умовах нинішнього спротиву агресивним намірам з боку Росії проти України, зокрема в інформаційній площині як базового чинника ведення "гібридної" війни, ця вимога є надзвичайно актуальною.

Висновки

1. Відсутність сталої теорії щодо забезпечення інформаційної безпеки держави, в тому числі у воєнній сфері, шкодить створенню адекватної нормативно-правової бази, що негативно позначається на практичних діях. Тому першочерговим завданням щодо протидії негативному впливу в інформаційному просторі держави постає необхідність системного розуміння теоретичних основ забезпечення інформаційної безпеки держави.

2. Законодавча аксіоматика, а також очевидні її наслідки, мають закласти фундаментальність у будь-яку діяльність, що спрямована на забезпечення інформаційної безпеки України, в тому числі у кіберпросторі, зокрема у воєнній сфері. У першу чергу, це стосується становлення теоретичних основ цього конституційного напряму діяльності як запоруки проведення адекватних практичних заходів.

3. Відповідно до положень законодавства України та розвинутої теорії вирішенням проблеми забезпечення інформаційної безпеки держави, що дозволить найбільш адекватно реагувати на "гібридні" загрози інформаційного характеру (в тому числі у кіберпросторі), має бути:

створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

підвищення рівня координації діяльності державних органів щодо виявлення, оцінювання і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії негативному інформаційному впливу та комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

розвиток системи державних комунікацій – стратегічних, урядових, кризових як умова реалізації цілісної комунікативної політики держави.

Список літератури

1. Розвиток форм і способів інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С.18-23.
2. Інформаційна безпека держави у контексті протидії інформаційним війнам. Навчальний посібник / [за ред. В.Б. Толубка]. – К.: НАОУ. – 2004. – 315 с.
3. Інформаційна безпека держави: навч. посібник / О.К.Юдін, В.М.Богуш. – Х.: Консум, 2005. – 576 с.
4. Проблеми захисту інформаційного простору України: Монографія / В.П.Горбулін, М.М.Биченок / Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.
5. Інформаційна безпека (соціально-правові аспекти): підруч. / В.М.Петрик, В.В.Остроухов, М.М.Присяжнюк та ін. – К.: КНТ, 2010. – 771 с.
6. Забезпечення інформаційної безпеки держави: підручник / В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін. // за заг. ред. О.А. Семченка. – К.: ПАТ «Віпол», 2015. – 672 с.
7. Інформаційна безпека: підручник / [В.В. Остроухов, М.М. Присяжнюк, О.І.Фармагей, М.М.Чеховська та ін.]; під ред. В.В.Остроухова. – К.: Ліра-К, 2021. – 412 с.
8. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія / О.В. Левченко. – Житомир: Видавець ПП «Євро-Волинь», 2021. – 172 с.
9. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" від 09.01.2007 р. № 537-V // Законодавство України [Електронний ресурс]. – Режим доступу: URL: https://zakon.rada.gov.ua.
10. Стратегія інформаційної безпеки України: Указ Президента України від 28.12.2021 № 685 Про рішення РНБО України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" // Законодавство України [Електронний ресурс]. – Режим доступу: URL: http://zakon.rada.gov.ua.
11. Стратегія національної безпеки України: Указ Президента України від 14.09.2020 № 392 Про рішення РНБО України від 14 вересня 2020 року "Про Стратегію інформаційної безпеки України" // Законодавство України [Електронний ресурс]. – Режим доступу: URL: http://president.gov.ua.

Деякі шляхи протидії російській гібридній агресії проти України

Федір Саганюк, кандидат юридичних наук, доцент
Старший науковий співробітник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000–0002–9516–0562
Юрій Мудрак
Начальник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000–0002–1159–5746
Юрій Піщанський
Старший науковий співробітник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-4392-3318

Анотація. Розглянуті сучасні гібридні дії Російської Федерації (далі – РФ) проти України з огляду чинного законодавства України та міжнародного гуманітарного права.

Ключові слова. Гібридні дії, агресія, тероризм, незаконні збройні формування, міжнародне гуманітарне право.

Вступ

Постановка проблеми. У відповідності до чинного законодавства України, збройна агресія – це застосування іншою державою або групою держав збройної сили проти України. Збройною агресією проти України вважається будь-яка з таких дій:

вторгнення або напад збройних сил іншої держави або групи держав на територію України, а також окупація або анексія частини території України;

блокада портів, узбережжя або повітряного простору, порушення комунікацій України збройними силами іншої держави або групи держав;

напад збройних сил іншої держави або групи держав на військові сухопутні, морські чи повітряні сили або цивільні морські чи повітряні флоти України;

засилання іншою державою або від її імені озброєних груп регулярних або нерегулярних сил, що вчиняють акти застосування збройної сили проти України, які мають настільки серйозний характер, що це рівнозначно переліченим в абзацах п’ятому - сьомому цієї статті діям, у тому числі значна участь третьої держави у таких діях;

дії іншої держави (держав), яка дозволяє, щоб її територія, яку вона надала в розпорядження третьої держави, використовувалася цією третьою державою (державами) для вчинення дій, зазначених в абзацах п'ятому - восьмому цієї статті;

застосування підрозділів збройних сил іншої держави або групи держав, які перебувають на території України відповідно до укладених з Україною міжнародних договорів, проти третьої держави або групи держав, інше порушення умов, передбачених такими договорами, або продовження перебування цих підрозділів на території України після припинення дії зазначених договорів [1].

Аналіз останніх досліджень та публікацій. За даними Управління верховного комісара ООН з прав людини, загальна кількість людських втрат внаслідок бойових дій на Сході України в результаті збройної агресії РФ за період з 14 квітня 2014 року до 30 червня 2021 року складає близько 42500-44500 осіб, а саме:

загиблих: 13200-13400 осіб (щонайменше 3901 цивільних осіб, близько 4200 військовослужбовців ЗС України та інших силових структур і приблизно 5800 членів незаконних збройних формувань);

поранених: 29600-33600 осіб (орієнтовно 7000-9000 цивільних осіб, приблизно 9800-10800 військовослужбовців ЗСУ та інших силових структур, а також близько 12800-13800 членів незаконних збройних формувань) [2].

Протягом восьми років на Сході України Росія веде неприпустимі агресивні гібридні дії, застосовуючи регулярні підрозділи власних збройних сил. Анексія Криму, вторгнення до східних областей України, створення там незаконних терористичних озброєних груп, вчинення ними терористичних актів, тортури, вбивства невинних людей та інші злочинні діяння. У відповідності до міжнародних норм, такі діяння, незалежно від оголошення війни, іменуються агресією [3].

Таким чином, на Сході України та в Криму здійснюється збройна агресія РФ, тобто масштабне протистояння з найбільшою інтенсивністю воєнних дій, неабиякою тривалістю, значними матеріальними збитками.

Метою доповіді є пошук ефективних підходів до належного оцінювання наявних агресивних гібридних збройних дій РФ проти України та інших суверенних держав світу для можливої їх нейтралізації відповідно до чинного законодавства України та міжнародного гуманітарного права.

Викладення основного матеріалу.

Суттєвими шляхами, які можуть сприяти вирішенню наявних безпекових проблем вбачаються:

1. Подальший розвиток військової освіти, воєнної науки, стримування і відбиття російської агресії та недопущення гібридної війни і міжнародного тероризму.

2. Удосконалення оборонного планування розвитку спроможностей сил оборони та інших процесів забезпечення всеохоплюючої оборони України, необхідних теоретичних напрацювань та їх впровадження, а також законодавчих

й інших нормативно-правових актів. У відповідності до чинного законодавства України.

3. Прийняття адекватних наявним безпековим умовам і викликам обґрунтованих стратегічних рішень на основі належних наукових досліджень та рекомендацій щодо переходу до нового формату протидії російській гібридної агресії і тероризму відповідно до наявних воєнних загроз та викликів.

Тероризм - суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей [4].

Гібридна агресія РФ проти України показала, що нинішня стратегія і тактика російської агресії проти України набули характерних ознак міжнародного тероризму. Вони здійснюються терористичними організаціями та угрупованнями, у тому числі за її активної підтримки, і пов'язані з викраденням, захопленням, вбивствами ні в чому не винних людей, руйнуванням важливих народногосподарських об'єктів, систем життєзабезпечення, комунікацій [4].

Російська окупаційна адміністрація та збройні формування РФ на окупованих територіях Автономної Республіки Крим та міста Севастополя, а також в окремих районах Донецької та Луганської областей України грубо порушують права та свободи людини і громадянина.

Спеціальні служби РФ здійснюють розвідувально-підривну діяльність проти України, намагаються підживлювати сепаратистські настрої та рухи, використовують організовані злочинні угруповання і корумпованих посадових осіб, прагнуть зміцнити інфраструктуру впливу.

Деструктивна пропаганда РФ як ззовні, так і всередині України, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність країни.

Відповідно до ст.1 Закону України "Про боротьбу з тероризмом" такі дії РФ мають бути визнані як Україною, так і міжнародною спільнотою, передусім, ООН, ОБСЄ, ЄС, НАТО, як міжнародний тероризм, тобто злочинна діяльність, що охоплює:

планування, організацію, підготовку та реалізацію терористичних актів;

підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів;

організацію незаконних злочинних збройних формувань і організацій для вчинення та участі в терористичних;

вербування, озброєння, підготовку та використання терористів;

пропаганду і поширення ідеології тероризму на кшталт "руського міру";

проведення навчання тероризму;

в'їзд в Україну громадян РФ та представників воєнізованих угруповань, зокрема "Вагнер", з терористичною метою;

фінансування в Криму та на Донбасі терористичних організацій з метою їх подальшого використання.

Україні та міжнародній спільноті потрібно офіційно на законодавчому рівні визнати, що Росія регулярно підтримує бойові дії створених нею

терористичних угруповань на Донбасі та в Криму як особовим складом, так і надсучасним озброєнням, спеціальною та військовою технікою. На Донбас РФ постачає вантажі військового призначення, продовжує незаконно безконтрольно перетинати державний кордон України залізничним транспортом (ешелонами) та колонами військової техніки, ніби "гуманітарними".

Вкрай небезпечною виявляється і розповсюдження керівництвом РФ так званої стратегії "руського міру" та "захисту російськомовного населення на теренах інших держав".

Для активнішої протидії зазначеним агресивно-терористичним гібридним діянням РФ доцільно:

По-перше, зосередити увагу усіх інституцій України та міжнародного співтовариства на ефективній реалізації міжнародно-правових норм та правил, передбачених, зокрема, Глобальною контртерористичною стратегією ООН (*UN Global Counter-Terrorism Strategy*), яка визначає загальні стратегічні підходи до боротьби з тероризмом у світовому масштабі. Цей міжнародно-правовий документ спрямований на зміцнення національних, регіональних та міжнародних зусиль по боротьбі з тероризмом. Держави-члени ООН погодилися не тільки чітко оголосити про те, що тероризм є неприйнятним у всіх його формах і проявах, але й висловили рішучість зробити практичні кроки на рівні окремих держав щодо запобігання тероризму і боротися з ним. Ці кроки включають широке коло заходів від зміцнення потенціалів окремих держав у боротьбі з терористичними загрозами до забезпечення координації контртерористичної діяльності в системі ООН.

Україна, як держава-член ООН, повинна скористатись цим міжнародним документом у повному обсязі і спонукати до його виконання інші країни ООН, у тому числі і Росію.

Глобальна контртерористична стратегія ООН передбачає чотири основні напрями дій щодо:

усунення умов, що сприяють поширенню тероризму;

запобігання тероризму і боротьбі з ним;

зміцнення потенціалу держав щодо запобігання тероризму і боротьбі з ним та зміцненню ролі системи ООН у цій сфері;

забезпечення загальної поваги прав людини і верховенства права в якості фундаментальної основи для боротьби з тероризмом.

Зазначена стратегія ООН є визнаним світовою спільнотою набором узгоджених принципів та збалансованих заходів з реагування на загрозу міжнародного тероризму, які повинні бути реалізовані як єдине ціле, об'єднуючи цілі безпеки, верховенства закону і загально світового розвитку. Її основою є резолюція Генеральної Асамблеї ООН (A/RES/60/288) та План дій (додаток до неї). За визначеними нею принципами всі форми і прояви тероризму представляють серйозну загрозу миру та безпеці, внаслідок чого визнаються злочинною поведінкою і підлягають рішучому осуду, незалежно від того, проти кого вони спрямовані, де відбуваються та які цілі переслідують.

У зв'язку з цим необхідно посилити міжнародне співробітництво з метою запобігання та протидії всім формам і проявам тероризму.

Боротьба проти міжнародного тероризму повинна вестися під керівництвом Генеральної Асамблеї ООН. Вона має найбільше представництво і є основним міжнародним органом, компетентним вирішувати питання міжнародного тероризму, що зумовлює необхідність посилення ролі ООН та Генеральної Асамблеї в цьому питанні.

По-друге. Відповідно до ст.45 Стратегії національної безпеки України, державний суверенітет, територіальна цілісність, демократичний конституційний лад та інші життєво важливі національні інтереси мають бути захищені також від невоєнних загроз з боку РФ та інших держав, зокрема, спроб спровокувати внутрішні конфлікти. Пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції є:

активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам;

запобігання, виявлення та припинення проявів сепаратизму, тероризму, екстремізму, припинення діяльності незаконних збройних формувань, політично мотивованого насильства та інших зазіхань на конституційний лад;

отримання повної і достовірної інформації про ситуацію в Україні та світі, протидія зовнішнім загрозам національній безпеці України [5].

Для розвитку потенціалу стримування гібридних агресивних дій РФ Україна має вибудувати всеохоплюючу оборонну за принципами і стандартами прийнятих у державах-членах НАТО.

По-третє. Україна має посилити боротьбу на дипломатичному рівні та міжнародній арені для захисту її суверенного права від нападу агресора, покликати міжнародні інституції спонукати РФ виконувати нормами міжнародного права, зокрема шляхом посилення санкцій щодо польотів військових літаків РФ у міжнародному просторі, походів її військових кораблів у міжнародних водах, особливо з так званими гуманітарними вантажами тощо.

Висновок

Враховуючи те, що протягом восьми років керівництвом РФ та її збройними формуваннями ведуться гібридні агресивні дії на території України, без оголошення війни і цинічним нехтуванням норм міжнародного гуманітарного права, пов’язані з вбивствами, захопленнями та викраденнями ні в чому не винних людей, масовими зруйнуваннями чисельних населених пунктів, важливих народногосподарських об’єктів, систем життєзабезпечення, комунікацій, Україною та міжнародним співтовариством належить розцінити їх як міжнародний тероризм і вжити ефективних заходів відповідно до Глобальної контртерористичної стратегії ООН (UN Global Counter-Terrorism Strategy), яка визначає загальні стратегічні підходи до боротьби з аналогічним тероризмом у світовому масштабі.

Список літератури

1. Закон України “Про оборону України” від 06.12.1991 № 1932-XII зі змінами.

2. Радіо Свобода, 2021 30 травня. URL:https://www.radiosvoboda.org/a/news-un-donbas-vtraty-gertvy/31359458.html.

3. Резолюція XXIX сесії Генеральної Асамблеї ООН від 14.12.1974 № 3314. Ст.1, 3.

4. Закон України “Про боротьбу з тероризмом” від 20.03.2003 № 638-IV зі змінами.

5. Стратегія національної безпеки України: затв. Указом Президента України від 14.09. 2020 №392/2020.

Забезпечення процесу виявлення і оцінювання рівня негативного інформаційного впливу на особовий склад Збройних Сил України в системі протидії такому впливу

Петро Сніцаренко, доктор технічних наук, старший науковий співробітник
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-6525-7064
Юрій Саричев, кандидат технічних наук, старший науковий співробітник
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-1380-4959
Віталій Грицюк
Ад'юнкт Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-3146-1956
Антон Ткаченко, кандидат технічних наук, старший науковий співробітник
Начальник наукового відділу Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-1620-4206

Анотація. *Доповідь присвячена викладенню основних положеннь щодо методичного підходу до створення підсистеми виявлення та оцінювання негативного інформаційного впливу на особовий склад ЗС України як необхідного елемента системи протидії такому впливу, зокрема під час "гібридної" агресії. Сутність методичного підходу полягає у впровадженні такого рішення, яке дозволить найбільш адекватно реагувати на "гібридні" загрози інформаційного характеру, зокрема з точки зору протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил).*

Ключові слова: *"гібридна" агресія, моніторинг інформаційного простору, виявлення та оцінювання негативного інформаційного впливу на особовий склад військ (сил), система протидії, лінгвістичний критерій.*

Вступ

Постановка проблеми у загальному вигляді. Невід'ємною складовою забезпечення інформаційної безпеки України, в тому числі у воєнній сфері, повинна бути протидія негативному інформаційному впливу. Особливої важливості для України ця обставина набула напередодні та в період агресії з боку Російської Федерації, коли гостро та відчутно проявилися наслідки негативного зовнішнього інформаційного впливу, зокрема на особовий склад

Збройних Сил України (ЗС України). В цьому складному узагальненому питанні особливим є процес виявлення та оцінювання негативного інформаційного впливу, що здійснюється в інтересах протидії.

Аналіз останніх досліджень та публікацій. Питання протидії негативному інформаційному впливу на особовий склад ЗС України протягом останніх десятиліть розглядалося в працях українських науковців В.Толубка, І.Руснака, В.Телелима, С.Жука, А.Рося, Т.Дзюби, Г.Пєвцова, О.Левченка [1–7] та інших. Аналіз показує, що на сьогодні теорія протидії такому впливу обмежена на рівні концептуально-декларативних положень, а тому для практики є недосконалою. У ній бракує чітких формальних методів і методик для кількісних оцінок певних аспектів цієї сфери, у тому числі щодо виявлення та оцінки рівня негативного інформаційного впливу на особовий склад ЗС України. З цієї причини його кількісна оцінка не проводиться, а оцінка морально-психологічного стану ЗС України здійснюється за якісними показниками на основі результатів моніторингу у військах вже після наслідків інформаційних впливів, що не дозволяє йому ефективно протидіяти.

Метою доповіді є висвітлення особливостей функціонування підсистеми виявлення та оцінювання з автоматизованою класифікацією інформаційних подій в системі управління протидією негативному інформаційному впливу на особовий склад ЗС України.

Виклад основного матеріалу

Військовим стандартом [8], який затверджує термінологію з питань інформаційної безпеки у воєнній сфері, визначається, що під *інформаційним впливом слід розуміти організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан цільової аудиторії та/або в процес функціонування технічних об'єктів інформаційної інфраструктури шляхом застосування інформаційних засобів і технологій*.

Відомо, що за характером дії інформаційний вплив може бути поділений на два види – інформаційно-технічний та інформаційно-психологічний. Розглядаючи у подальшому питання інформаційного впливу на цільову аудиторію, якою є особовий склад військ (сил) та органи військового управління, дотримуємося його розуміння в сенсі інформаційно-психологічного впливу. Негативний інформаційний вплив на таку цільову аудиторію спричиняє зниження рівня її морально-психологічного стану, що, відповідно, знижує загальну боєздатність військових формувань. Активна протидія негативному інформаційному впливу на особовий склад військ (сил) має розпочинатися у випадку загрози такого впливу або його здійснення з боку противника. Результат протидії досягається шляхом реалізації певних складових взаємопов'язаного процесу. Особливо відповідальними для якісної реалізації усього управлінського процесу протидії є перші дві фази – виявлення негативного інформаційного впливу та об'єктивна оцінка рівня такого впливу на армійську цільову аудиторію. При цьому необхідно розуміти, що будь-які інформаційні заходи (дії) обов'язково передбачають постійний моніторинг інформаційного простору та добування даних в інтересах оцінки поточної інформаційної ситуації.

Слід зауважити, що оцінка рівня негативного інформаційно-психологічного впливу до сьогодні на особовий склад ЗС України здійснюється фактично за його наслідками, тобто “постфактум” і опосередковано – через оцінку рівня морально-психологічного стану. Ця обставина дає підставу стверджувати про необхідність запровадження принципу реагування на прояви негативного інформаційного впливу на особовий склад ЗС України на основі кількісного оцінювання рівня такого впливу.

З цією метою розроблено методику побудови підсистеми виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад ЗС України, яка дозволяє визначити його рівень на основі кількісної міри інтенсивності прояву такого впливу [9–11] за певний період часу шляхом “вагового” накопичення. Це забезпечує можливість відносно об’єктивно прогнозувати динаміку цього процесу та можливі наслідки, щоб адекватно та на випередження реагувати (протидіяти) негативним процесам. Методика пропонується невід’ємним елементом у загальному контурі управління процесом протидії, який забезпечує підтримку морально-психологічного стану особового складу військ (сил). Це має бути головною метою та об’єктом управління в системі протидії негативному інформаційному впливу на особовий склад військ (сил), яка базується на кібернетичному принципі управління.

На практиці в МО України та ЗС України діяльність структурних підрозділів, задіяних в цьому процесі, розбалансована, вони діють поодиноко та не координовано. При цьому зазначена методика виявлення та оцінювання інформаційного впливу на особовий склад військ (сил) сьогодні може бути реалізована лише “ручним” методом, що є трудомістким та тривалим процесом. Це шкодить оперативності управлінського процесу протидії такому впливу та загалом ефективності здійснення випереджувальних стабілізаційних заходів, що потребує іншого підходу щодо реалізації розробленої методики. Це має бути автоматизація цієї методики в підсистемі виявлення та оцінювання інформаційного впливу.

Зазначене спричиняє потребу розв’язання задачі підвищення оперативності та зниження трудомісткості процесу виявлення та кількісної оцінки рівня негативного інформаційного впливу на особовий склад ЗС України в інтересах проактивної протидії такому впливу шляхом автоматизації процесу реалізації.

З цією метою запропоновано підхід спрощення базової методики, що дозволяє перейти від селекції інформаційних повідомлень багатьох класів до їх відбору за одним домінуючим (найбільш інформативним) класом. Це означає як скорочення числа критеріїв відбору (селекції) повідомлень до одного, так і спрощення задачі обґрунтування цього критерію з причини значного скорочення спектру лінгвістичних ознак, а відтак – полегшення реалізації відповідної процедури (алгоритму) автоматизації. На цьому ґрунті отримано удосконалену методику, яка, на відміну від відомої базової методики, побудована з використанням найбільш інформативного скороченого переліку лінгвістичних ознак інформаційних повідомлень негативного характеру для ЗС України. Тобто селекція та відбір релевантних інформаційних повідомлень має здійснюватися за спрощеним лінгвістичним критерієм.

Висновки

1. Невід'ємною складовою системи протидії негативному інформаційному впливу є підсистема виявлення та оцінювання такого впливу.

2. Аналіз існуючої системи протидії негативному інформаційному впливу на особовий склад військ (сил) ЗС України показує, що вона має ряд недоліків організаційного, технічного та методичного характеру, що є об'єктивною підставою для її суттєвого удосконалення в інтересах більш дієвого забезпечення виконання ЗС України завдань за призначенням.

3. Розроблена методика виявлення та кількісної оцінки рівня негативного інформаційного впливу на особовий склад ЗС України. Але її реалізація ускладнена із-за значної трудомісткості та складнощів розробки лінгвістичних критеріїв відбору для класів інформаційних повідомлень негативного характеру.

4. Підвищення оперативності вирішення завдання виявлення та оцінювання негативного інформаційного впливу на особовий склад ЗС України, як необхідної умови високої результативності випереджувальних заходів протидії такому впливу, вбачається у реалізації автоматизації та спрощення визначених процедур оцінювання та класифікації проявів впливу.

5. Удосконалення методики виявлення та кількісної оцінки рівня негативного інформаційного впливу на особовий склад ЗС України запропоновано реалізувати за рахунок звуження спектру лінгвістичних ознак такого впливу шляхом скорочення великого числа критеріїв відбору негативних повідомлень до одного (за ознаками домінуючого класу).

Наявність потреби вирішення цього завдання як проблемного визначає *напрямок подальших досліджень*, зокрема пов'язаних з розробкою лінгвістичного критерію відбору релевантних повідомлень домінуючого класу та моделі автоматизованої класифікації інформаційних подій в системі управління протидією негативному інформаційному впливу на особовий склад ЗС України.

Список літератури

1. Розвиток форм і способів інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С.18-23.

2. Толубко В.Б., Жук С.Я., Рось А.О. та ін. Інформаційна безпека держави у контексті протидії інформаційним війнам: навчальний посібник / За ред В.Б.Толубка. – К.: НАОУ, 2004. – 176 с.

3. Толубко В.Б. Концептуальні основи інформаційної безпеки України / В.Б.Толубко, С.Я.Жук, В.О.Косевцов // Наука і оборона. – 2004. – № 2. – С. 19-25.

4. Горбулін В.П. Проблеми захисту інформаційного простору України: Монографія / В.П. Горбулін, М.М. Биченок // Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.

5. Основи стратегії національної безпеки та оборони держави: підручник. / О.П. Дузь-Крятченко, Т.М. Дзюба, А.О. Рось. 2-ге вид., доп. і випр. – К.: НУОУ, 2010. – 591 с.

Обґрунтування інформаційних рішень щодо створення автоматизованої системи управління угруповання військ сил оборони для протидії гібридній агресії проти України

Олександр Головченко
Начальник науково-дослідного відділу центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-4444-0764

Анотація. *Переважна більшість провідних міжнародних і вітчизняних політологів, воєнно-політичних експертів, військових спеціалістів та аналітиків поділяють думку, що в рамках реалізації підступної неоімперської "гібридної політики" Росією була розв'язана і зараз продовжується проти України так звана "гібридна війна", тобто повноцінна війна – «гібридна» по формі та «асиметрична» за змістом. Її відмінність характеризується як веденням агресивних військових дій під прикриттям незаконних (неформальних) збройних формувань, так і одночасним використанням широкого спектра політичних, економічних (в т. ч. енергетичних і торговельно-економічних), а також інформаційно-пропагандистських заходів, з яких, як правило, і починається ця «гібридна війна», та які її супроводжують впродовж усього періоду військових дій. Ряд провідних експертів Заходу небезпідставно називають її ще як "війна нового покоління" або "війна нової генерації" [5]. Доповідь присвячена формуванню загальносистемних вимог до технологічних рішень щодо створення автоматизованої системи оперативного управління для протидії гібридній агресії проти України та обґрунтуванню шляхів її побудови.*

Ключові слова: *система оперативного управління, інтеграція систем, інформаційна сумісність, ситуаційна обізнаність, засоби спостереження та розвідки, геоінформаційна система.*

Вступ

Постановка проблеми. На початку проведення Антитерористичної операції на територіях Донецької та Луганської областей (далі – АТО) не передбачалося широке використання механізованих, артилерійських частин та підрозділів, тому питання автоматизації процесів управління військами і зброєю займали другорядні позиції. При переході АТО в гостру фазу із залученням механізованих, артилерійських частин та підрозділів, створенням в подальшому оперативного угруповання військ (сил), поряд з необхідністю побудови якісної системи зв'язку, постала гостра потреба у забезпеченні бойових підрозділів, що виконують завдання, багатофункціональною інформаційно-управляючою системою, яка б інтегрувала функції управління військами, зброєю, розвідкою, радіоелектронною боротьбою, а також зв'язку, навігації, орієнтування і розпізнання [1 – 2].

Однією з основних переваг створення зазначеної системи є можливість оперативного розв'язання в штабах різноманітних інформаційних і розрахункових задач. Засоби автоматизації системи бойового управління, в першу чергу, повинні забезпечити роботу офіцерів штабів і командних пунктів, на які покладається виконання наступних завдань: інформаційне забезпечення, обґрунтування оцінок поточної тактичної обстановки, розробка рекомендацій, підготовка бойової та довідкової документації, контроль і координація діяльності підпорядкованих, взаємодіючих і вищестоящих штабів і загальновійськових формувань. Нагальною потребою для побудови такої системи є впровадження системного підходу на основі формування обґрунтованих технологічних рішень щодо її створення.

Аналіз останніх досліджень і публікацій. З метою підвищення оперативності і якості управління військами та силами у багатьох країнах, зокрема в Україні, ведуться роботи, пов'язані з впровадженням у процеси управління інформаційних систем (автоматизованих систем управління – АСУ).

Основними складовими таких систем стають існуючі та перспективні (на цей час такі, що розробляються як військовими фахівцями, так і волонтерськими організаціями) інформаційні системи за відповідними напрямками. При цьому, в багатьох випадках, зазначені системи створюються спонтанно, в процесі виконання вузьких завдань окремими підрозділами і не відповідають вимогам ефективного бойового управління відповідного підрозділу, частини, угрупування в цілому. Незважаючи на це, існуюча вимога щодо прийняття ефективних управлінських рішень під час ведення бою, спричинила інтенсивний розвиток і активне впровадження саме цих систем, які наразі забезпечують виконання завдань в зоні проведення операції Об'єднаних сил бойовими підрозділами і можуть стати основою для створення перспективної автоматизованої системи оперативного (бойового) управління військами.

Мета доповіді. Доведення варіанту формування загальносистемних вимог до технологічних рішень щодо створення автоматизованої системи управління угрупування військ сил оборони для протидії гібридній агресії проти України.

Виклад основного матеріалу

Інформаційне забезпечення передбачає автоматизований збір, облік, класифікацію та систематизацію даних, аналіз і розподіл підготовленої інформації. Вважається, що найбільш важливі дані повинні залишатися в своєму первинному вигляді. Другорядні і непотрібні дані виключаються в ході їх аналізу на кожній дільниці з урахуванням специфіки роботи відповідного органу управління та його інформаційних потреб. При цьому обсяг та якість інформації, що надається командувачу (командиру), повинні бути оптимально достатніми для вироблення управлінських рішень. Особовий склад командних пунктів повинен мати простий доступ до інформації при дотриманні вимог безпеки її зберігання і розподілу. Пристрої відображення інформації повинні забезпечувати зручність в її зчитуванні і розумінні, швидкому виділенні із загального обсягу найбільш важливих відомостей, а також оперативному внесення необхідних змін в будь-які документи, що розробляються [3].

За оцінкою військових аналітиків, до 75% часу при підготовці рішення штабами (командними пунктами) витрачається на інформаційну та розрахункову роботу. Для безпосередньо аналітичної роботи командирів і офіцерів штабів залишається лише 25% від цього часу. При цьому 15-20% робочого часу витрачається на здійснення записів у книгах (журналах) і друкування документів за допомогою електронно-обчислювальних машин, що використовуються виключно у якості друкарських машинок. Стільки ж часу йде на пошук різних документів і довідкових матеріалів, зняття копій, прийом і передачу документів між інстанціями, їх реєстрацію, сортування і організацію зберігання. Таким чином, при ручному способі обробки даних при реалізації розглянутого обсягу завдань в умовах дефіциту часу в штабах ланки оперативного угрупування військ – бригада, батальйон, належним чином в середньому обробляється та аналізується не більш 30% інформації, що надходить, причому тільки до 10% оброблених матеріалів використовується при виробленні рішення командувача (командира). Впровадження засобів автоматизації в процес управління військами і зброєю дозволить скоротити час зазначеного циклу в 2,5-3 рази [4].

На підставі аналізу інформаційних систем, які використовуються у зоні проведення операції Об'єднаних сил на території Донецької та Луганської областей (програмно-апаратний комплекс "ГІС-Арта", комплекс засобів автоматизації "Кропива", система управління вогнем "СУВА", комплекс засобів автоматизації "АртОС") можна зробити висновок, що жодна з розглянутих систем, не в повній мірі, а тільки за окремими елементами, не задовольняє вимогам до інформаційної системи оперативного угрупування військ (сил). Широке розмаїття технологічних підходів та програмних продуктів, що використовуються, вимагає впорядкування і системного підходу, як до питання функціонального призначення таких систем, так визначення їх ролі та місця в єдиному інформаційному середовищі підтримки і прийняття управлінських рішень за напрямком застосування бойових систем.

На сьогодні широке розмаїття системних рішень, технологічних підходів та програмних продуктів, що використовувались під час їх створення, практично унеможливлює автоматизацію процесів збору і комплексної обробки інформації від різнорідних сенсорів розвідки (джерел інформації), а також видачі даних (інформації) споживачам у потрібному їм форматі. Зазначене не дозволяє об'єднати їх у єдину автоматизовану систему оперативного (бойового) управління оперативного угрупування військ (сил) без створення та впровадження єдиної інтеграційної складової (платформи).

Єдиним доцільним (можливим) на сьогодні шляхом створення прообразу інформаційної системи оперативного угрупування військ в обмежені строки є об'єднання різнорідних джерел (сенсорів) інформації, інформаційних та інших систем та комплексів, які наразі використовують у зоні проведення операції Об'єднаних сил на території Донецької та Луганської областей шляхом забезпечення їх інформаційної сумісності.

Для забезпечення інформаційної сумісності та взаємодії між автоматизованими (інформаційними, інформаційно-аналітичними) системами різного функціонального призначення, побудованими на різних програмно-

апаратних платформах із застосуванням сучасних інформаційних технологій, необхідно у переліку заходів із створення інформаційної системи оперативного угрупування військ (сил) передбачити розроблення відповідної інтеграційної складової.

Виходячи з матеріалів, проаналізованих вище, автоматизована система управління угрупування військ сектору оборони повинна стати інструментом координації дій всіх учасників які виконують завдання з метою протидії гібридній агресії проти України.

Функціонально інформаційна (автоматизована) система оперативного (бойового) управління повинна забезпечувати ситуаційну обізнаність про оперативно-тактичну (тактичну) обстановку, комплексне планування бойових операцій (дій) та їх моделювання, підвищення оперативності та якості управління з'єднаннями, частинами і підрозділами за рахунок [4]:

скорочення часу та підвищення якості збирання, оброблення та надання інформації на автоматизовані робочі місця посадових осіб органів військового управління;

скорочення часу та підвищення обґрунтованості вироблення замислу, прийняття рішень і розроблення планів на застосування військ, сил і засобів в операціях (бойових діях);

скорочення термінів та підвищення надійності обміну інформацією між органами військового управління оперативного і тактичного рівнів, а також взаємодіючих органів;

підвищення оперативності, стійкості, безперервності і прихованості управління військами (силами) і засобами в операціях (діях);

зменшення працевтрат та підвищення ефективності управлінської роботи посадових осіб органів управління.

Основними результатами створення інформаційної автоматизованої системи управління угрупування військ сил оборони повинні бути: технічні рішення на створення дослідного зразка зазначеної системи; дослідний зразок системи, як загальний результат, технічні рішення на створення функціональних і забезпечуючих підсистем та комплекси засобів автоматизації пунктів управління на оперативному та тактичному рівнях; комплексна система захисту інформації інформаційної системи оперативного угрупування військ (сил); система експлуатації, обслуговування та супроводження вказаної системи.

Висновки

Подальше ведення Росією гібридної війни проти України у масштабах і формах станом на сьогодні призводитиме до поступового виснаження України на фоні можливого припинення або послаблення міжнародних санкцій проти Росії. Тому використання інформаційних систем повинні стати інструментом координації дій всіх складових сил оборони з метою протидії гібридній агресії проти України та забезпечити зменшення періоду часу між моментом виявлення противника і моментом його ураження.

Функціонально інформаційна система оперативного угрупування військ (сил) повинна забезпечувати ситуаційну обізнаність про оперативно-тактичну

(тактичну) обстановку, комплексне планування операцій (бойових дій) та їх моделювання, підвищення оперативності та якості управління з'єднаннями, частинами і підрозділами

В умовах жорсткого дефіциту часу єдиним доцільним на сьогодні шляхом створення дослідного зразка інформаційної системи оперативного угрупування військ є об'єднання різнорідних джерел (сенсорів) інформації, інформаційних та інших систем і комплексів, побудованих на різних програмно-апаратних платформах, які наразі використовують у зоні проведення операції Об'єднаних сил, за рахунок забезпечення їх інформаційної сумісності шляхом розроблення відповідної інтеграційної складової.

Список використаної літератури

1. Szlachta B. Nato Architecture Framework. NATO Operational View. [Electronic Resource] / Bernard Szlachta // Noble Prog. – 2016. – Mode of access: http://trainingcoursematerial.com/index.phptitleNato_Architecture_Framework_(NAF)-_3.3_-_NATO_ Operational_V ew&printable=yes.

2. The DoDAF Architecture Framework Version 2.02 [Electronic Resource] // Chief Information Officer U.S. Department of Defense. – 2011. – Mode of access: http://cionii.defense.gov/sites/dodaf20/index.html.

3. Кірпічніков Ю. А. Аналіз рамкових архітектур побудови інформаційних систем НАТО та визначення особливостей архітектури C4ISR [Електронний ресурс] / Ю. А. Кірпічніков, В. А. Федорієнко, О. В. Головченко, О. В. Андрощук // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. - 2017. - № 1.- С.78-84.

4. Стужук П. І. Теоретичні основи і практичні рекомендації щодо обробки розвідувальних відомостей (даних) / П. І. Стужук // К: НАОУ, 1998. – 82 с.

5. [Електронний ресурс] https://www.ukrinform.ua/rubric-polytics/2107122-gibridna-vijna-rosii-proti-ukraini-uroki-ta-visnovki.html

Стан розвитку безпілотних розвідувальних комплексів та ракетно-артилерійських систем Збройних Сил Російської Федерації

Руслан Черевко, доктор філософії
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-0414-0695
Олександр Хімченко
Ад'юнкт Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-4227-0514
Іван Криворучко
Ад'юнкт Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-1038-3175
Андрій Романюк
Ад'юнкт Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-4268-0601
Ірина Загорка
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-0693-1434

Анотація. *У доповіді наведений стан удосконалених розвідувальних БпЛА та ракетно артилерійських систем Збройних Сил Російської Федерації, які можуть бути використані в безконтактних бойових діях проти України.*

Ключові слова: *розвідувальні БпЛА, ракетно-артилерійські системи, безконтактні бойові дії, гібридна війна.*

Вступ

Постановка проблеми. Воєнна реформа і переозброєння збройних сил Російської Федерації, нарощування військової присутності на тимчасово окупованому Кримському півострові, ОРДЛО та вздовж українсько-російського кордону, інтенсифікація заходів підготовки військ та органів військового управління потребують проведення детального аналізу щодо стану озброєння та військової техніки противника.

В контексті підготовки до відсічі можливої збройної агресії РФ залишається актуальним питанням дослідження пріоритетних напрямів розвитку

російських збройних сил, форм і способів їх застосування. Таке дослідження є невід'ємною умовою забезпечення ефективної реалізації власної політики щодо захисту державного суверенітету та відновлення територіальної цілісності.

Аналіз останніх досліджень і публікацій. Безпілотні авіаційні комплекси (БпАК) та ракетно-артилерійські системи не залишилась поза увагою науковців. До історії створення, розвитку, стану та бойового їх застосування звертались неодноразово; було досліджено і описано застосування БпАК у різних воєнних кампаніях [1–3].

У монографії [4] описано подальшу еволюцію безпілотних літальних апаратів, але не наведено характеристик сучасних БпАК провідних виробників, які позитивно себе зарекомендували у останніх конфліктах, мало уваги приділено висвітленню питань щодо застосування новітніх зразків розвідувальних БпАК Росії.

Вказані обставини не дозволяють у повній мірі врахувати досвід застосування розвідувальних БпАК та ракетно-артилерійськими систем в конфліктах і зробити висновки до чого слід бути готовими у протистоянні з противником.

Метою доповіді **є** висвітлення сучасного стану удосконалених зразків розвідувальних БпАК та ракетно-артилерійських систем збройних сил Російської Федерації, які можуть бути використані під час збройної агресії проти України.

Виклад основного матеріалу

Останіми роками, за поглядами військового керівництва збройних сил провідних країн світу та РФ, домінує тенденція щодо зниження власних втрат під час ведення бойових дій за рахунок підвищення вражаючих характеристик озброєння та військової техніки. Провідну роль у досягненні цієї мети відводиться БпАК.

В умовах ведення сучасних мережецентричних та гібридних війн БпАК є одним з основних засобів ведення розвідки (наряду з космічною розвідкою). Тому, країни, що ведуть сучасні війни, активно удосконалюють існуючі методи та способи застосування БпЛА.

Активна робота щодо оснащення збройних сил БпЛА проводиться в РФ. Так відчувши недоліки відсутності БпЛА в ході ведення бойових дій у Чечні та Грузії, у міністерстві оборони РФ, починаючи з 2009 року ведеться активна робота у цьому напрямку.

На теперішній час на озброєнні армії РФ знаходяться наступні основні безпілотні комплекси типу "Орлан-10", "Форпост", "Элерон-10, "Тахион", "Застава", які можуть передавати розвідувальні дані в режимі реального часу. Тим самим підрозділи ракетних військ та артилерії сухопутних військ, повітряно-десантних військ і морської піхоти ЗС РФ отримали надійне джерело цілевказівки. Станом на липень 2018 р., за офіційними російськими даними, у війська надійшло до 1,9 тис. розвідувальних БпЛА різних типів [5].

Ефективність поєднання сучасних розвідувальних БпЛА та систем ураження продемонстрували активні бойові дії на Донбасі впродовж 2014-2015 рр. За різними підрахунками, до 85% всіх бойових втрат українських підрозділів

є наслідком роботи ворожої артилерії у поєднанні з розвідувальними БпЛА [6]. Так, впродовж 2014 до першої половини 2016 рр. бойові пошкодження загалом отримали 2576 одиниць бронетехніки, з яких 391 – не підлягали відновленню. З цих втрат майже 45% є наслідками роботи ворожої артилерії [7]. У цей же період було пошкоджено 1278 одиниць артилерійського озброєння, з яких 201 – не підлягали відновленню [8].

На сьогодні загальновійськові з'єднання (військові частини) ЗС РФ достатньо насичені розвідувальними БпЛА тактичної і частково оперативно-тактичної ланок. Практично жодне тренування (навчання) підрозділів рівня батальйону і вище не відбувається без залучення БпЛА розвідки, цілевказівки та коректування вогню артилерії.

Російська Федерація прагне збільшення глибини виявлення сил противника. З цією метою йдуть роботи над такими БпЛА, як "Форпост-Р" і "Альтиус-У", які були вперше продемонстровані у серпні 2019 року. Порівняно з попередніми, у цих БпЛА збільшено радіус дії, тому їх можна віднести до безпілотних комплексів оперативного рівня. На сьогодні підписано перший контракт на постачання 10 систем "Форпост-Р" для потреб російської армії.

Паралельно з насиченням російських військ розвідувальними БпАК на озброєння надходять й інші системи виявлення. Так, на сьогоднішній день всі артилерійські бригади загальновійськових армій мають на озброєнні комплекси розвідки вогневих позицій та контролю стрільби артилерії "Зоопарк-1М" (контробатерейна РЛС), яка призначена для розвідки по пострілу (пуску) вогневих позицій стріляючих мінометів, артилерії, реактивних систем залпового вогню, стартових позицій тактичних ракет і забезпечення стрільби (пусків) своїх аналогічних засобів. "Зоопарк-1М" виконує розрахунок траєкторій ракет і снарядів, здатний коректувати вогонь своїх артилерійських засобів, стежити за повітрям і здійснювати контроль за БпЛА. Крім того, появились портативні комплекси артилерійської розвідки, такі як "Аистенок", "Кредо", "Фара", які дозволяють здійснювати розвідку місцевості, виявляти ворожі позиції та наносити по них удари артилерією [9].

Також розроблено оптико-електронний комплекс "Ирония", який призначений для ведення спостереження і збирання інформації про місцевість та виявлення різних предметів. Комплекс розвідки, управління та зв'язку "Стрелец-М", який дозволяє пришвидшити процес передачі розвідувальних даних до систем ураження [9].

Незважаючи на те, що основна увага в рамках переозброєння російської армії приділяється системам розвідки і спостереження, наразі у військах триває процес заміни радянських ракетно-артилерійських систем на більш сучасні, із наголосом на зменшення часу розгортання. Так, на озброєння сухопутних військ надходять РСЗВ "Торнадо-Г" і "Торнадо-С", які є еволюційним розвитком радянських систем "Град" та "Смерч" відповідно. На відміну від своїх попередників "Торнадо-Г", "Торнадо-С" мають системи автоматичної топоприв'язки, перезаряджання, а також збільшену дальність: до 40 км для "Торнадо-Г" та до 120 км – "Торнадо-С". У 2020 р. завершилося переозброєння 439-ї бригади реактивної артилерії Південного ВО на системи "Торнадо-С" [9].

Крім того, СВ ЗС РФ повністю відмовилися від гаубиці Д-30, яка має меншу мобільність і дальність та більший час на розгортання та згортання. Замість неї на озброєння мотострілецьких і танкових з'єднань надходять гаубиці "Мста-Б" та самохідні "Мста-С" [9]. Ці системи мають більшу вогневу міць, радіус ураження і темп стрільби порівняно із самохідними артилерійськими установками "Гвоздика" та "Акація", які перебувають на озброєнні ЗС України. Таким чином, останніми роками в сухопутних військах РФ триває робота відразу за декількома напрямками, спрямована на збільшення дальності й мобільності відповідних систем ураження.

Окремо слід згадати ОТРК "Искандер-М". На сьогодні у ЗС РФ кожна загальновійськова армія має у своєму складі ракетну бригаду, озброєну зазначеними комплексами [9].

Припинення дії Договору про ліквідацію ракет середньої та малої дальності (РСМД) дозволяє РФ перейти до відкритого нарощування спроможностей окремих ракетних бригад загальновійськових армій за рахунок озброєння новими крилатими ракетами середньої дальності із радіусом дії 1,5-2 тисячі км. Мова може йти про щонайменше 4 самохідні пускові установки для кожної ракетної бригади. Також наявні пускові установки ОТРК "Искандер-М" можуть бути модернізовані для використання різнотипних ракет. Усі ці заходи в комплексі посилюють здатність ЗС РФ проводити вогневе ураження на всю глибину території нашої держави з різних напрямів.

Досі залишається відкритим питання щодо готовності РФ до масованого застосовування РВіА у разі можливого збройного конфлікту з Україною.

За результатами навчань "Кавказ – 2020" та "Захід – 2021", можна зробити висновок щодо практичного відпрацювання питань ЗС РФ з підготовки та проведення масованих ракетних ударів. Так в ході навчань "Кавказ – 2020" на Астраханьському полігоні відпрацьовувались питання нанесення масованих ракетних ударів з застосуванням комплексів "Искандер-М" та "Торнадо-С", при чому цілевказання здійснювалось за допомогою БпАК "Орлан-10". Тому не слід виключати можливість використання високоточної зброї для ураження важливих об'єктів бойового потенціалу ЗС України і воєнної інфракструктури нашої держави.

Висновки

Таким чином, можна зробити висновок, що РФ дедалі більше прагне до безконтактного бою на тактичному, оперативно-тактичному та оперативному рівнях за допомогою ефективного поєднання засобів вогневого ураження та систем розвідки і спостереження, про що свідчать заходи підготовки військових частин та органів військового управління.

Як наслідок, можна говорити про значні успіхи РФ з нарощування потенціалу для безконтактного бою з можливістю нанесення вогневого ураження на всю глибину нашої держави. Цього їм вдалося досягнути, перш за все, за рахунок насичення підрозділів удосконаленеми системами розвідки, спостереження і передачі даних на ураження в режимі реального часу.

Список літератури

1. Варакута В.П. Історія війн та воєнного мистецтва / В.П. Варакута, І.М. Кириленко. – Х.: НТУ “ХПІ”, 2019. – 274 с.
2. Кучеренко Ю. Ф., Науменко М. В., Кузнєцова М. Ю. Аналіз застосування безпілотних літальних апаратів та визначення напрямку їх подальшого розвитку при веденні мережецентричних операцій. Системи озброєння і військова техніка. 2018. № 1(53). С. 25-30. https://doi.org/10.30748/soivt.2018.53.03.
3. Корсунов С. І., Левагін Г. А., Коротій В. О. Застосування засобів повітряного нападу провідних країн світу у збройних конфліктах і локальних війнах. Збірник наукових праць Харківського університету Повітряних Сил. 2016. №3 (140). С. 131-135.
4. Беспілотна авіація у військовій справі: колективна монографія / Мосов С. П., Погорецький М. В., Салій С. М., Сєлюков О. В., Фещенко А. Л. Київ : Інтерсервіс, 2019. 324 с.
5. В Минобороны назвали число беспилотников в российской армии. Российская газета, 7 июля 2018. – [Електронний ресурс]. – Режим доступу: https://rg.ru/2018/07/06/reg-cfo/v-minoborony-nazvali-chislobespilotnikov-v-rossijskoj-armii.html.
6. Preserving Ukraine’s Independence, Resisting Russian Aggression: Page 4, February 2015. – [Електронний ресурс]. – Режим доступу: https://www.brookings.edu/wpcontent/uploads/2016/06/UkraineReport_February2015_FINAL.pdf.
7. Втрати Збройних Сил у бронетехніці під час АТО у 2014-2016 роках: Вперше оприлюднена детальна офіційна інформація статистика. – [Електронний ресурс]. – Режим доступу:https:// defence-ua. com/home-page/9497.
8. Втрати артилерії за час АТО: Вперше оприлюднена детальна офіційна інформація статистика втрат ЗСУ. – [Електронний ресурс]. – Режим доступу: https://defenceua.com/index.php/home-page/9605.
9. Сучасне озброєння і військова техніка Збройних Сил Російської Федерації. Довідник учасника ООС / С.П. Корнійчук, О.В. Турінський, Г.В. Пєвцов, та ін.; за заг. ред. С.П. Корнійчука. Х.: ДІСА ПЛЮС, 2020. 1220 с.

Завдання спільних бойових порядків пілотованої та безпілотної авіації в операціях

Ярослав Ярошенко
Ад'юнкт кафедри авіації Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-8651-4920
Володимир Герасименко, кандидат військових наук
Докторант кафедри авіації Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-2014-7408
Олександр Блискун
Ад'юнкт кафедри авіації Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7751-8313
Анатолій Ткаченко
Старший викладач кафедри авіації Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-7316-5437
Олександр Титаренко
Доцент кафедри авіації Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-3523-9519

Анотація. *В умовах загрози вторгнення військ Російської Федерації на територію України актуальною проблемою залишається питання стримування противника, в тому числі й за участі авіації Збройних Сил України. У даній статті розглянуті сучасні погляди на застосування пілотованої та безпілотної авіації в майбутніх військових операціях. Проведено порівняння завдань, які може виконувати пілотована та безпілотна авіація. Здійснено класифікацію завдань для спільних авіаційних груп пілотованої та безпілотної авіації. За допомогою метода аналізу ієрархій визначено завдання, які за поглядами експертів найбільш доцільно виконувати у спільному бойовому порядку. Проведено короткий огляд щодо можливого економічного ефекту від застосування спільних авіаційних груп. Надано рекомендації щодо подальших досліджень у даній області.*

Ключові слова: *пілотована та безпілотна авіація; спільний бойовий порядок; бойове застосування.*

Вступ

Постановка проблеми. Розвиток сучасних технологій у галузі авіації та інформаційних технологій передбачає постійні зміни в мистецтві ведення операцій. У [1] визначено основні риси збройної боротьби в майбутньому і кожна з цих рис притаманна безпілотній авіації. Так, зокрема поява безпілотних літальних апаратів (БпЛА) призвела до необхідності спільного застосування пілотованої та безпілотної авіації в ході бойових дій. Першим важливим завданням, яке покладалося на безпілотну авіацію стала розвідка. По мірі розвитку технологій розвідка в операціях переросла в систему безпілотних розвідувальних засобів, яка включає в себе різні рівні застосування від тактичного до стратегічного. Якщо у війнах XX ст. переважну більшість розвідувальних завдань виконувала пілотована авіація, то вже з початку XXI ст. ця функція поступово перейшла до безпілотних авіаційних комплексів (БпАК). Безпілотники стали складовою системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR), а також без них неможливе впровадження концепції мережецентричних війн [2]. Також, з початку XXI ст. у США успішно проведена робота щодо створення ударних БпЛА, що започаткувало новий етап у їхнього розвитку та спровокувало зміни у мистецтві ведення сучасних війн. Крім того продовжують з'являтися нові типи БпЛА, наприклад дозаправники в повітрі, які вже успішно проходять льотні випробування [3-5], продовжуються роботи щодо розроблення безпілотних винищувачів [6-10]. Тому, враховуючи складну військово-політичну обстановку довкола України та високу ймовірність вторгнення Російської Федерації на територію України, актуальними питаннями на сьогодні залишаються завдання, які зможуть виконувати спільні авіаційні групи пілотованих та безпілотних літальних апаратів Збройних Сил України?

Аналіз останніх досліджень та публікацій. Сучасна пілотована авіація призначена для виконання значної кількості завдань [11-14], проте розвиток засобів протиповітряної оборони, які можуть виявляти та знищувати повітряні цілі на великих дальностях привів науковців та військових провідних країн світу до висновку, що необхідність збереження пілота є пріоритетною у майбутніх війнах. Саме тому, наприкінці XX ст. провідні країни світу задля збереження життя льотного складу та високовартісної авіаційної техніки почали застосовувати безпілотні літальні апарати для виконання у повітряних операціях завдань, які не передбачали застосування зброї. Саме тоді почалась ера безпілотної авіації, на теперішній час жоден збройний конфлікт не обходиться без безпілотників. Виникає питання як ефективно поєднати пілотовану та безпілотну авіацію у сучасних збройних конфліктах та які функції вони повинні виконувати, щоб у повній мірі реалізувати бойовий потенціал і перших, і других?

На даний час можна з впевненістю сказати, що на безпілотну авіацію покладаються значна кількість завдань, які виконує пілотована авіація [15-16], крім найбільш складної та перспективної у майбутньому місії – це повітряний бій з пілотованими та безпілотними літаками противника. Для вирішення цієї проблеми у США, наприклад, розроблено перспективні концепції Manned and

Unmanned aircraft teaming (MuM-T)[17], Loyal Wingman [18-20], Next Generation Aircraft Dominance [21-22]. Також, ще не освоєний напрям повітряних перевезень особового складу безпілотниками, оскільки людина в психологічному плані ще не готова довірити себе роботизованій системі й для вирішення даного питання необхідно провести ще низку досліджень та випробувань.

Класифікація даних завдань за групами важливості дозволить науковій спільноті зосередити увагу на перевагах та проблемах такого застосування у майбутніх операціях.

Мета дослідження – класифікація завдань, які може виконувати пілотована та безпілотна авіація Збройних Сил України.

Виклад основного матеріалу

Розподілимо завдання, які може виконувати спільна авіаційна група пілотованих та безпілотних літальних апаратів (Спільна авіаційна група) в операціях на завдання вищого рівня (оперативні та стратегічні), оперативно-тактичні завдання та завдання тактичного рівня (Рис.1).

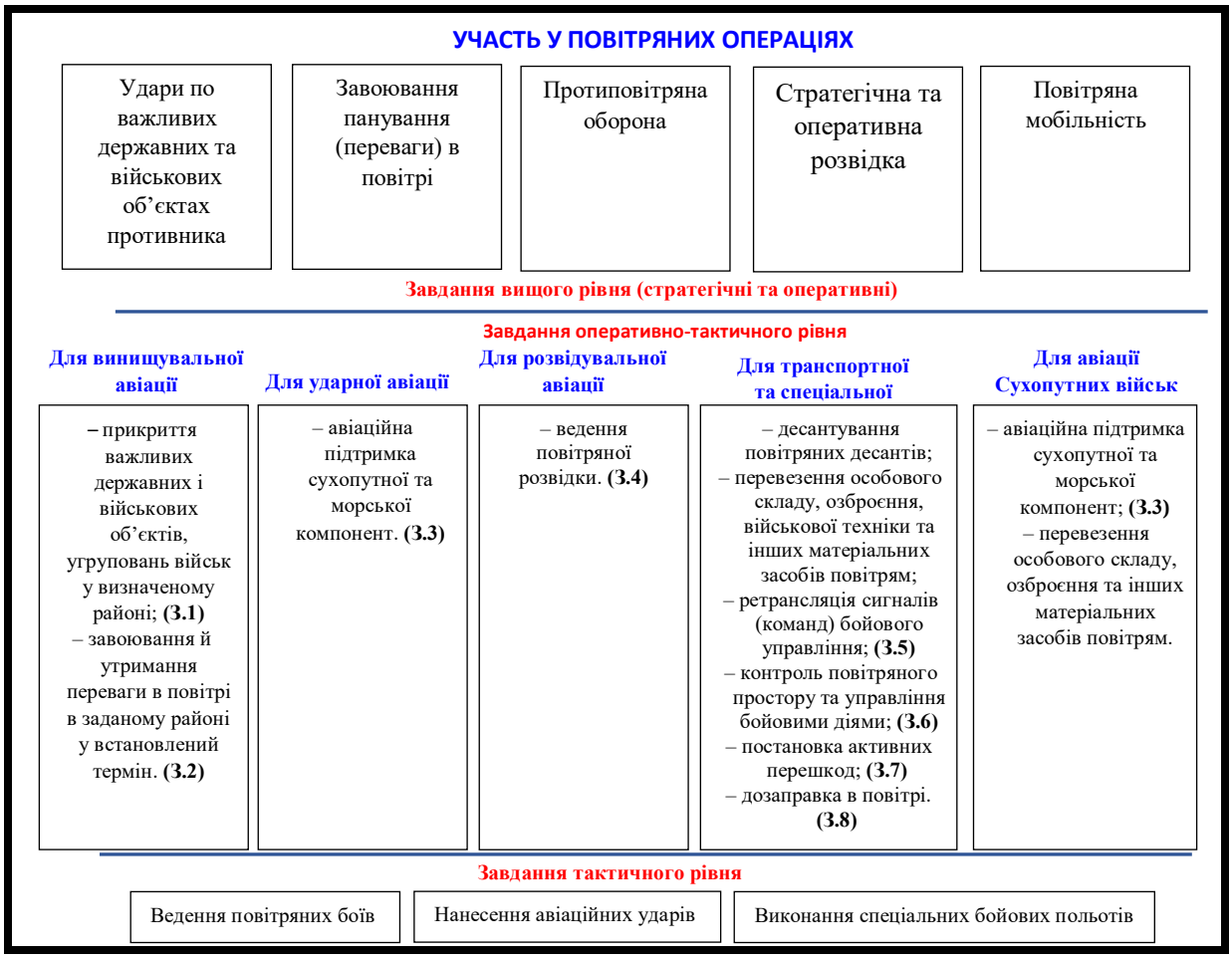

Рисунок 1. Класифікація завдань спільного бойового порядку пілотованої та безпілотної авіації в операціях

Розглянемо більш докладно завдання оперативно-тактичного рівня в наступальній операції, оскільки спільна авіаційна група – це різнорідне угруповання і їх завдання значно ширші за тактичні.

Умовно позначимо завдання, які може вирішувати авіація в наступальній операції присвоївши їм порядковий номер (див. рис. 1). Завдання, які притаманні транспортній авіації (десантування повітряних десантів та перевезення особового складу, озброєння, військової техніки та інших матеріальних засобів повітрям) винесемо в обмеження та під час дослідження розглядати не будемо.

За 9-ти бальною шкалою порівнянь завдань [23, с.102] побудуємо матрицю пріоритету завдань (Табл.1).

Таблиця 1

Матриця пріоритету завдань

	1	2	3	4	5	6	7	8	9	10	11
Завдання	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	$\sum_{\text{рядків}}$	$K_{\text{важл.}}$	λ
3.1	1	0,33	0,2	3	5	1	3	7	2,9	0,21561	2,37175
3.2	3	1	1	3	9	7	5	7	3,44	0,25576	0,83123
3.3	5	1	1	5	9	7	7	7	4,08	0,30335	0,8888
3.4	0,33	0,33	0,2	1	9	1	3	3	1,07	0,07955	1,09546
3.5	0,2	0,11	0,11	0,11	1	0,33	0,33	1	0,27	0,02007	0,80297
3.6	1	0,14	0,14	1	3	1	1	1	0,7	0,05204	1,00602
3.7	0,33	0,2	0,14	0,33	3	1	1	3	0,63	0,04684	0,96772
3.8	0,14	0,14	0,14	0,33	1	1	0,33	1	0,36	0,02677	0,80297
$\sum_{\text{стовпчиків}}$	11	3,25	2,93	13,77	40	19,33	20,66	30	13,45	1	8,76692

Як видно з розрахунків найбільший пріоритет у виконанні завдань спільною авіаційною групою пілотованої та безпілотної авіації мають: авіаційна підтримка військ; завоювання й утримання переваги в повітрі в заданому районі у встановлений термін; прикриття важливих державних і військових об'єктів, угруповань військ у визначеному районі. Найменший пріоритет має задання щодо ретрансляції сигналів (команд) бойового управління (Рис. 2).

Рисунок 2. Діаграма пріоритетів завдань, які може виконувати спільна авіаційна група пілотованої та безпілотної авіації

За допомогою метода аналізу ієрархій виділено завдання, які вже на даний час можуть виконуватися спільними авіаційними групами пілотованої та безпілотної авіації з більшою ефективністю, за рахунок зменшення числа втрат високовартісної техніки та льотного складу.

Висновки.

У даному дослідженні проведено об’єднання завдань, що покладаються на пілотовану та безпілотну авіацію та викладено погляди на їх спільне застосування. Їх можна застосовувати під час проведення досліджень сучасних військових операцій, особливо в частині, що стосується їх повітряних складових. Практично дані питання можливо застосовувати в ході майбутніх військових навчань та операцій, що дозволить значно розширити варіанти бойового застосування авіації Збройних Сил України.

Список використаних джерел

1. Об’єднана оперативна концепція сил оборони 2030. Київ, ГШ ЗСУ. – 2021. 34 с.
2. Теоретичні основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби: монографія / [О.М. Загорка, А.А. Корецький, А.К. Павліковський, І.О.Загорка]; за заг. Ред. І.С. Руснака. – К. НУОУ ім. Івана Черняховського, 2020. – 248 с.
3. Close Air Support. Joint Publication 3-09.3. – 361 p.
4. Stefano D'urso. MQ-25 Stingray Tests Move Forward With First F-35C Lightning II Air-To-Air Refueling, 2021 https://theaviationist.com/2021/09/17/mq-25-refuels-f-35/.
5. David Cenciotti. Boeing MQ-25 Stingray Tanker Drone Achieves Another First: Air-to-Air Refueling With An E-2D, 2021 https://theaviationist.com/ 2021/ 08/ 19/mq-25-aar-e-2d/.
6. Безпілотний стелс Ace One: як екс-очільник ДП “Антонов” створює британсько-український ударний БПЛА, 2021 https://defence-ua.com/weapon _and tech/bezpilotnij_stels_ace_one_jak_eks_ochilnik_dp_antonov_stvorjuje_britansko_ukrajinskij_udarnij_bpla-4031.html
7. В Україні вперше показали розроблений спільно з Туреччиною безпілотний винищувач, 2020. https://www.unian.ua/weapons/10818008-v-ukrajini-vpershe-pokazali-rozrobleniy-spilno-z-turechchinoyu-bezpilotniy-vinishchuvach-foto-video.html
8. Безпілотні винищувачі в Японії планують взяти на озброєння в 2035 році, 2021. https://portaltele.com.ua/news/technology/bezpilotni-vynyshhuvachi-v-yaponiyi-planuyut-vzyaty-na-ozbroyennya-v-2035-rotsi.html
9. У Туреччині анонсували безпілотний літак-«убивцю» винищувачів, 2021. https://texty.org.ua/fragments/104162/u-turechchyni-anonsuvaly-bezpilotnyj-litak-ubyvcyu-vynyshuvachiv/.
10. Винищувач шостого покоління, 2021. https://uk.wikipedia.org/wiki/ Винищувач_шостого_покоління.
11. Герасименко О.І. Тактика авіації Повітряних Сил. Навчальний посібник. К.: НАУ, 2006. – 134 с. https://studfile.net/preview/5376215/.
12. Збройна боротьба у повітрі та космосі: підручник / М. О. Єрмошин, С. П. Ярош, Є. І. Ряполов та ін.; за заг. ред. М. О. Єрмошина. ХНУПС, 2019. – 496 с.

13. Доктрина Повітряні Сили Збройних Сил України. Вінниця, КПС ЗС України, 2020. – 40 с.

14. NATO STANDARD AJP-3.3. Allied Joint Doctrine For Air And Space Operations. Edition B Version 1. - April 2016. - 100 p.

15. Радецький В. Г., Руснак І. С., Даник Ю. Г. Безпілотна авіація в сучасній збройній боротьбі: Монографія. - К.: НАОУ, 2008. -224 с.

16. Безпілотна авіація у військовій справі: кол. Монографія / С.П. Мосов, М.В. Погорецький, С.М. Салій, О.В. Сєлюков, А.Л. Фещенко; за ред. проф. С.П. Мосова. - Київ: Інтерсервіс, 2019. - 324 с.

17. Livio Rossetti, 2020. Manned-Unmanned Teaming. https://www.japcc.org/manned-unmanned-teaming/.

18. Beth Stevenson. Loyal Wingman Part of the Future of Air Combat, 2019. https://www.ainonline.com/aviation-news/defense/2019-06-13/loyal-wingman-part-future-air-combat

19. Jamie Freed, 2019. Boeing unveils unmanned combat jet developed in Australia. https://www.reuters.com/article/us-australia-airshow-boeing-unmanned/boeing-unveils-unmanned-combat-jet-developed-in-australia-idUSKCN1QF2XT.

20. Garrett Reim, 2021. Northrop Grumman unveils Model 437 loyal wingman concept https://www.flightglobal.com/military-uavs/northrop-grumman-unveils-model-437-loyal-wingman-concept/145407.article.

21. John A. Tirpak, 2009. The Sixth Generation Fighter https://www.airforcemag.com/article/1009fighter/.

22. Air Force Next-Generation Air Dominance Program: An Introduction https://crsreports.congress.gov/product/pdf/IF/IF11659.

23. Т. Саати. Принятие решений. Метод анализа иерархий. – М. Радио и связь, 1993. 278 с.

Гібридна агресія Російської Федерації: основи стійкості України

Віктор Павленко, кандидат військових наук
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-4313-3079
Ніна Андріянова, кандидат політичних наук
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7115-2445
Микола Шпура, кандидат військових наук, старший науковий співробітник
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-3350-6003
Дмитро Федянович, кандидат військових наук, старший науковий співробітник
Начальник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-9896-8655

Анотація. *Доповідь "Гібридна агресія Російської Федерації: основи стійкості України" присвячена аналізу умов та факторів щодо забезпечення стійкості України у протидії гібридній агресії Російської Федерації після 2014 року. Визначені основні чинники, що впливають на стан реформування сектору безпеки і оборони України щодо підвищення здатності системи управління державою, силами оборони відновлюватися та адаптуватися до змін у безпековому середовищі.*

Ключові слова: *всеохоплююча оборона, гібридна агресія, збройні сили, реформи, стійкість, сектор безпеки та оборони.*

Вступ

Постановка проблеми. В Україні з 2014 року триває збройний конфлікт на Сході України. За останні два десятиліття цей конфлікт є одним із найбільш масштабних конфліктів у Європі. За підрахунками ООН, загальна кількість людських втрат, пов'язаних з конфліктом в Україні з 14 квітня 2014 року по 31 січня 2021 року, становить близько 13,5 тис. загиблих (щонайменше 3,4 тис. цивільних осіб, близько 4,2 тис українських військових та приблизно 5,7 тис. осіб зі складу незаконно створених збройних формувань [1].

Нажаль, конфлікт на Сході ще продовжується. Тому екзистенційно важливим є забезпечення стійкості держави до нових викликів та загроз та відновити державний суверенітет та територіальну цілісність України.

Аналіз останніх досліджень та публікацій. Сучасні дослідження спираються на положення основних нормативно-правових документів у зовнішньополітичній сфері та у сфері державної оборонної політики [2-7]. Різним аспектам протистояння гібридній агресії з боку Російської Федерації присвячені також достатньо багато публікацій вітчизняних дослідників [8-11]. Разом з цим питання забезпечення стійкості нашої держави щодо протидії агресору висвітлені недостатньо.

Мета доповіді. Визначити основні чинники, що впливають на стан реформування сектору безпеки і оборони України щодо підвищення здатності системи управління державою, силами оборони відновлюватися та адаптуватися до змін у безпековому середовищі, як основних складових забезпечення стійкості держави.

Виклад основного матеріалу

Головною метою Стратегії воєнної безпеки України є завчасно підготовлена та всебічно забезпечена всеохоплююча оборона України на засадах стримування, стійкості та взаємодії, що забезпечує воєнну безпеку, суверенітет і територіальну цілісність держави [6]. При цьому Стратегією воєнної безпеки України визначається, що стійкість у ході всеохоплюючої оборони України досягається здатністю системи управління державою, сил оборони, національної економіки, інфраструктури та суспільства швидко відновлюватися та адаптуватися до змін у безпековому середовищі й до тривалого протистояння в наданні відсічі і стримування збройної агресії проти України, підтриманням спроможностей до здійснення стратегічного розгортання, територіальної оборони України, руху опору, ведення операцій (бойових, спеціальних, стабілізаційних дій), налагодженням надійних каналів комунікації з населенням та підтриманням його життєдіяльності.

Зважаючи на наявність багатьох складових забезпечення стійкості, як основи забезпечення всеохоплюючої оборони успішність системи заходів, що вживає держава для протидії гібридній агресії з боку Російської Федерації оцінити вкрай складно. Однією з причин цього є те, що Росія постійно нарощує зусилля з реалізації власних агресивних намірів, спрямованих на поступове зниження ресурсних та економічних можливостей України щодо забезпечення стійкості, які одночасно супроводжуються ретельно спланованими заходами з дестабілізації суспільно-політичної обстановки у нашій державі.

Сьогодні складно визначити перебіг конфлікту на сході України без підтримки західних партнерів, світової спільноти або, як би діяла Росія та які наслідки мала Україна, у разі якщо б воєнно-політичне керівництво держави не задіяло Збройні Сили України та інші військові формування у тому числі добровольчі для протидії російській агресії на Донбасі у 2014 році.

З сучасних досліджень [8-10] відомо, що гібридні війни більш ефективні у країнах, де державні інститути слабкі, а політична та військова еліти

корумповані. На думку західних експертів головною перешкодою до приєднання України до ЄС та НАТО є недостатні зусилля останньої щодо викорінення корупції та забезпечення верховенства права та реформування сектора безпеки і оборони. Отже, можна констатувати, що реформи в державних органах виконавчої влади, секторі безпеки і оборони сьогодні є основним фактором та ключем до забезпечення стійкості України у протистоянні зовнішній агресії.

Тому невипадково, що Уряд України узяв курс на першочергове реформування саме тих сфер національної та воєнної безпеки, які можуть безпосередньо вплинути на підвищення стійкості у протистоянні російській агресії, а саме військової (оборони та безпеки) сфери, економічної, політико-дипломатичної сферах, у яких головне місце належить боротьбі з корупцією.

Важливим підґрунтям для здійснення заходів реформування, особливо сектору безпеки і оборони стали зміни в доктринальній базі України. Це законодавче закріплення європейських та євроатлантичних намірів України [2], зміни до Закону України "Про засади зовнішньої і внутрішньої політики України" [3] прийняття Закону України "Про національну безпеку України" [4], прийняття Стратегії національної безпеки України [5] та Стратегії воєнної безпеки України [6], та ін.

Сучасні дослідники та політичні і військові експерти зазначають, що Україна змушена вести дві війни одночасно: одну на східному фронті, щодо стримування агресивних намірів Російської федерації, та іншу – на національному рівні, з метою ефективного впровадження реформ, перешкоджання яким здійснює корумпована бюрократична влада та олігархи. Джерелом загроз незалежності України, її суверенітету і демократії залишається також недостатня ефективність державних органів, що ускладнює вироблення і реалізацію ефективної політики держави.

Незважаючи на вищезазначені перешкоди згідно з незалежними оцінками, Україна значно покращила свій оборонний потенціал. Збройні Сили України та інші військові формування здійснюють заходи щодо забезпечення оперативної сумісності з арміями країн-членів НАТО та продовжують набувати цінного бойового досвіду на Сході України.

Важливим чинником, що покращує реформування політико-дипломатичної сфери в інтересах підвищення стійкості держави є інтенсивність та продуктивність політико-дипломатичних відносин. Так, контакти між українськими та західними політиками та дипломатами відіграли важливу роль у стримуванні агресії Росії. Залучення західних партнерів, насамперед Німеччини, Франція та США до посередництва та притягнення Росії до відповідальності було одним із найбільших досягнень України у врегулюванні конфлікту (при цьому вкрай важливо, щоб вони вели переговори з Росією в рамках нормандського формату). Ці та інші країни-члени НАТО та ЄС підтримали Україну з ключових питань, наприклад, наполягаючи на демілітаризації східної України до того, як можуть бути досягнуті будь-які нові політичні домовленості чи "особливий статус" для територій, що непідконтрольні уряду України.

Ще один важливий момент у тому, що санкції ЄС та США проти Росії чітко сигналізують, хто є агресором, навіть якщо сам агресор заперечує свою причетність.

Іншою менш відомою для суспільства, але важливою опорою України була підтримка її міжнародних трибуналах, включаючи Міжнародний Суд та Міжнародний трибунал з морського права. Проміжний успіх для України настав у листопаді 2019 року, коли Міжнародний Суд ухвалив, що її претензії до Росії є обґрунтованими та підпадають під юрисдикцію суду. Україна подала позов ще у 2017 році, звинувативши Росію у порушенні міжнародних угод про боротьбу з расовою дискримінацією та фінансування тероризму. Українській стороні знадобилося три роки, щоб підготувати 29 томів та понад 17, 5 тис. сторінок доказової бази проти Росії.

Важливим фактором підвищення стійкості України є громадянське суспільство, особливо ветерани війни, оскільки вони володіють унікальним досвідом та знаннями, що можуть сприяти розвитку українського суспільства. Реалізація потенціалу ветеранів війни можлива шляхом створення експертного середовища ветеранів війни, залучення до роботи в органах державної влади та органах місцевого самоврядування, участь у громадських об'єднаннях [11].

Незважаючи на вищезазначені здобутки, історія реформ в Україні неоднозначна. Саме по собі це не применшує досягнень України у намаганні підвищити стійкість до зовнішній агресії у всіх сферах національної безпеки. Однак кожна незавершена реформа або слабке місце в її інститутах – це те, на чому противник може отримати вигоду, особливо в таких сферах, як безпека та оборона. Зусилля щодо реформування, які мають вирішальне значення для стійкості країни, іноді розглядаються як два кроки уперед та крок назад.

Наприклад, у спробі викорінити хабарництво українська влада створила антикорупційну інфраструктуру, до якої входять Вищий антикорупційний суд, Національне антикорупційне бюро України (НАБУ), Спеціалізована антикорупційна прокуратура та Національне агентство із запобігання корупції. Проте досі не було "великих" справ щодо притягнення до відповідальності та покарання корумпованих чиновників. Вищезгадана конституційна криза, яка завдала удару як по антикорупційній інфраструктурі, так і по судовій системі, є ще одним прикладом гальмування процесів реформування в державі.

Реформа СБУ, що давно назріла, все ще триває, незважаючи на амбітне законодавство, значний суспільний тиск і безпрецедентну підтримку Заходу. Тим часом, хоча українська армія 2021 року порівняно з армією 2014 року справді схожа на фенікса, що відродився з попелу, деякі її стандарти все ж таки мають бути покращені. У 2018-2020 роках з армії пішли 77 тис. офіцерів-контрактників, майже третина Збройних Сил України. Це говорить про те, що держава має докласти більше зусиль, щоб зробити Збройні Сили України дієвим інститутом, що забезпечує стійкість держави у протидії зовнішнім викликам і загрозам [12].

Водночас, всі ці недоліки процесів реформування на шляху набуття стійкості, безумовно, можна пояснити. Жодний процес державного будівництва не може працювати ідеально, особливо в державі, яка є жертвою гібридної

агресії. Однак важливо пам'ятати, що будь-яка помилка офіційних осіб може не лише нашкодити країні, а й бути використаною агресором.

Висновки

Вищезазначені фактори сприяють підвищенню стійкості держави в контексті всеохоплюючої оборони, що у першу чергу забезпечує готовність сил оборони України, національної економіки, населення та всієї держави до надання відсічі збройній агресії проти України, вжиття превентивних заходів щодо протидії воєнним загрозам, досягнення та підтримання спроможностей завдати противнику неприйнятних політичних, економічних, воєнних та інших втрат, за яких він буде змушений відмовитися від подальших дій.

Можна стверджувати, що позитивні зміни у розвитку сектора безпеки і оборони відбулися, це в першу чергу законодавче закріплення євроатлантичних намірів, прийняття нормативно-правових документів адекватним сучасним викликам і загрозам, відповідним зовнішньополітичним реаліям. Окрім цього, важливою є адаптація структури Збройних Сил до їх реальних потреб.

Безцінною є й зовнішня підтримка України міжнародним товариством, як фактор підвищення її стійкості, як центральної складової.

Перед державою Україна стає непросте завдання щодо продовження реформ з метою підвищення стійкості у протистоянні сучасним викликам та загрозам.

Список літератури

1. ООН підрахувала кількість жертв бойових дій на Донбасі. https://www.radiosvoboda.org/a/news-oon-kst-gertv-boyovyh-donbas/31110937.html (дата звернення: 23.11.2021).

2. Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору) : Закон України від 7 лютого 2019 року № 2680-VIII. URL: https://zakon.rada.gov.ua/laws/show/2680-19#Text (дата звернення: 23.11.2021).

3. Про засади внутрішньої і зовнішньої політики: Закон України від 1 липня 2010 року № 2411-VI зі змінами 08.07.2018. https://zakon.rada.gov.ua/laws/show/2411-17#Text (дата звернення: 23.11.2021).

4. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 23.11.2021).

5. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 23.11.2021).

6. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 25 березня 2021 року № 121/2021. URL:

https://www.president.gov.ua/documents/1212021-37661 (дата звернення: 23.11.2021).

7. Послання Президента України Володимира Зеленського до Верховної Ради про внутрішнє та зовнішнє становище України від20 жовтня 2020 року URL: https://www.president.gov.ua/news/poslannya-prezidenta-ukrayini-volodimira-zelenskogo-do-verho-64717 (дата звернення: 23.11.2021).

8. Воєнні аспекти протидії гібридній агресії: досвід України: монографія /за загальною редакцією А.М. Сиротенка. Київ: НУОУ ім. Івана Черняховського, 2020. 176 с.

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

10. Парахонський Б.О., Яворська Г.М. Онтологія війни і миру: безпека, стратегія, смисл: монографія. Київ: НІСД, 2019. 560 с.

11. Фрідріх Ю., Люткефенд Т. Реінтеграція ветеранів та зміцнення суспільної єдності в Україні. Довга тінь Донбасу. URL: https://www.gppi.net/media/ GPPi_2021_Friedrich_Luetkefend_Long-Shadow-of-Donbas_ukr.pdf (дата звернення: 23.11.2021).

12. За три роки з ЗСУ звільнилось 77 тисяч контрактників. Ukrainian Military Pages. URL:https://www.ukrmilitary.com/2020/10/77.html (дата звернення: 23.11.2021).

Необхідність розвитку нормативно-правової бази цивільно-військового співробітництва в Україні

Ігор Ушаков, аспірант Інституту державного управління та наукових досліджень з цивільного захисту

Старший науковий співробітник відділу аналізу та узагальнення інформації навчально-наукового центру підготовки офіцерів для багатонаціональних штабів Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0002-0231-085X

Анотація. *Доповідь присвячена аналізу нормативно-правових документів з цивільно-військового співробітництва в Україні. Використаний порівняльний та контент-аналізи нормативно-правових документів України з метою формування теоретичної основи для удосконалення нормативно-правової бази України в згаданій сфері.*

Ключові слова: *цивільно-військове співробітництво, Україна.*

Вступ

Постановка проблеми. Скориставшись зарубіжним досвідом, отриманим під час участі в міжнародних операціях з підтримання миру і безпеки, в ЗС України в травні 2014 року було започатковано створення структур цивільно-військового співробітництва (ЦВС) [1].

Але цей досвід був притаманний лише для міжнародних операцій з підтримання миру і безпеки. Випадків застосування структур ЦВС на території всередині держави для військових або антитерористичних операцій з відбиття збройної агресії зафіксовано не було.

Методичні основи організації ЦВС ООН, НАТО та ЄС ще не повністю адаптовані до нормативно-правової бази України, що вимагає розробки конкретних механізмів реалізації цивільно-військового співробітництва в Україні.

Дослідження з даної тематики зумовлено потребами подальшого удосконалення та розвитку нормативно-правової та методичної бази ЦВС в Україні в умовах протидії агресії Російської Федерації шляхом узагальнення нормативно-правової бази діяльності ЦВС ООН, НАТО та провідних країн світу при їх застосуванні у міжнародних операціях з підтримання миру і безпеки, у ліквідації надзвичайних ситуацій техногенного та природного характеру, гуманітарних операціях та визначенні рекомендацій щодо його застосування при розвитку вітчизняного нормативно-правового забезпечення, формування політики та діяльності ЦВС ЗС України.

Аналіз останніх досліджень та публікацій. Доповідь базується переважно на аналізі керівних документів ЦВС та праць дослідників цивільно-військового співробітництва в Україні, таких, як І.М. Коропатнік; О.О.

Ноздрачев; В.В. Попов; О.В. Минько; Ю.А. Калагін; О.Ф. Сальнікова; Н.В. Васюкова тощо. Однак актуальність та проблематика теми статті потребують подальшого дослідження у даній сфері.

Мета доповіді. Проаналізувати нормативно-правове регулювання реалізації цивільно-військового співробітництва в Україні з метою подальшого удосконалення його механізмів.

Виклад основного матеріалу

Досвід ЦВС США в рамках Північноатлантичного альянсу та його переосмислення в 90-ті роки XX ст. стали головним надбанням в області кризового реагування НАТО. Виділявся окремий блок з системи багатонаціональних оперативних сил НАТО, в обов'язки якого входили виключно функції взаємодії з цивільними організаціями. Функцією такого блока мало стати налагодження контактів та надання місцевій владі та міжнародним і неурядовим організаціям технічної, координаційної, інформаційної та іншої підтримки.

Україна долучилася до миротворчої діяльності в 1992 році. За цей період набула значний досвід у сфері підготовки національних контингентів та персоналу, участі у міжнародних операціях з підтримання миру і безпеки, організації та виконання заходів ЦВС на тактичному рівні, використовуючи при цьому методологічну та нормативно-правову базу ЦВС ООН, НАТО, ЄС та найбільш розвинутих країн світу.

При створенні структур цивільно-військового співробітництва в Збройних Силах України, ще у 2014 році, метою ЦВС було визначено створення сприятливих умов для виконання покладених на ЗС України, ДСНС України та ІВФ держави завдань за рахунок співробітництва військового командування з цивільним населенням.

Пакет цільових нормативних документів, що використовується для правового регулювання застосування ЦВС включає три основні блоки документів: концептуально-установчі, доктринальні і процедурно-процесні акти.

Законом України "Про боротьбу з тероризмом" [2] визначено умови залучення ЗС України до вирішення питань внутрішньої безпеки в разі виникнення терористичних загроз безпеці держави із-за меж України, що дозволяє застосовувати ЦВС в антитерористичній операції (АТО) (а пізніше, після 30 квітня 2018 року, в Операції об'єднаних сил (ООС).

Мету, основні принципи організації, функції, сутність та складові системи ЦВС, основні методи та складові оцінки цивільного середовища, завдання, порядок організації та здійснення ЦВС ЗС України визначено у відповідних керівних документах. Базовими документами для використання на цей час є: доктрина "Цивільно-військове співробітництво" від 02.07.2020 р. [3]; наказ Генерального штабу Збройних Сил України "Про затвердження Тимчасової настанови з цивільно-військового співробітництва у ході підготовки та застосування Збройних Сил України" від 02.04.2019 р. № 131 [4]; наказ Генерального штабу Збройних Сил України "Про затвердження Тимчасової настанови з оцінки цивільного середовища" від 24.04.2019 р. № 159 [5];

“Методичний посібник для військ (сил) з питань цивільно-військового співробітництва” [6] та навчальний посібник НУОУ “Цивільно-військове співробітництво за стандартами НАТО” [7].

Зокрема у Доктрині ЦВС розглянуто особливості організації ЦВС у різних формах застосування ЗСУ; розкрито сутність та основні шляхи розв’язання комплексних міжвідомчих питань (супутніх завдань); окреслено роль та місце ЦВС під час повсякденної діяльності та у ході застосування ЗС України та інших складових сил оборони у разі збройної агресії в будь-яких її формах і проявах, зокрема у формі гібридної війни, або збройного конфлікту [3].

Проте методичні основи організації ЦВС ООН, НАТО та ЄС ще не повністю адаптовані до нормативно-правової бази України, що окреслює необхідність розвитку нормативно-правової бази цивільно-військового співробітництва в Україні.

Висновки

Проведений аналіз засвідчує результативність роботи щодо розбудови та розвитку нормативно-правової бази ЦВС в умовах протидії агресії РФ у 2014–2021 роках, а також необхідність продовження формування політики організованих дій у зазначеному напрямі й удосконалення цієї діяльності згідно з вимогами та викликами часу. Окрім цього, пропонується продовження вивчення та імплементації досвіду відповідних структур ЦВС ООН, НАТО, ЄС та провідних країн світу з метою формування сучасної вітчизняної моделі інституції ЦВС.

Список літератури

1. В зоні АТО розпочали роботу оперативні групи військово-цивільного співробітництва Збройних Сил України. URL: http://old.kmu.gov.ua/kmu/control/uk/publish/article?art_id=247494968&cat_id=248446171.

2. Закон України “Про боротьбу з тероризмом”. Відомості Верховної Ради України від 20.06.2003 – 2003 р., № 25, ст. 180.

3. Доктрина “Цивільно-військове співробітництво”: затв. наказом Головнокомандувача Збройних Сил України від 02.07.2020 р.

4. Наказ Генерального штабу Збройних Сил України “Про затвердження Тимчасової настанови з цивільно-військового співробітництва у ході підготовки та застосування Збройних Сил України” від 02.04.2019 р. № 131.

5. Наказ Генерального штабу Збройних Сил України “Про затвердження Тимчасової настанови з оцінки цивільного середовища” від 24.04.2019 р. № 159.

6. Методичний посібник для військ (сил) з питань цивільно-військового співробітництва: затверджений Заступником начальника Генерального штабу Збройних Сил України від 03.09.2019 /Під заг. керівництвом О. Ноздрачова. Київ: Управління цивільно-військового співробітництва Збройних Сил України, 2019. 167 с.

7. Цивільно-військове співробітництво за стандартами НАТО: навчальний посібник. – К.: НУОУ ім. Івана Черняховського, 2015. – 87 с.

Основні складові воєнно-економічного забезпечення обороноздатності держави в умовах гібридної війни

Руслан Бойко, кандидат технічних наук, старший науковий співробітник
Провідний науковий співробітник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-7240-4299
Володимир Бойко, кандидат економічних наук, старший науковий співробітник
Провідний науковий співробітник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-3264-7111
Микола Бутенко
Старший науковий співробітник науково-дослідного відділу Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-7272-5826

Анотація. *Доповідь "Основні складові воєнно-економічного забезпечення обороноздатності держави в умовах гібридної війни" присвячена аналізу стану питання воєнно-економічного забезпечення обороноздатності держави, розуміння терміну обороноздатність держави та визначення основних її складових. Ситуація, що склалася в країні показує, що воєнно-економічні складові обороноздатності держави є одними з ключових елементів її формування.*

Ключові слова: *обороноздатність держави, гібридна війна, воєнно-економічне забезпечення обороноздатності держави, воєнно-економічний потенціал, науково-технічний потенціал, соціальний потенціал, моральний потенціал.*

Вступ

Постановка проблеми. Порушення недоторканості України завдало значних втрат її економіці, добробуту населення та акцентувало увагу керівництва держави до проблем підвищення рівня обороноздатності країни [1–4]. Україна, сьогодні змушена активно шукати раціональні рішення протидії новим ризикам та загрозам. Сучасні, складні умови розвитку Збройних Сил України, достатньо напружена зовнішньополітична обстановка в світі та навколо України вимагають від керівництва держави постійного прийняття складних та відповідальних рішень щодо реалізації заходів зміцнення обороноздатності

України з метою збереження її недоторканості та накопичення такого потенціалу, який би дозволив дати адекватну відсіч противнику.

Нестабільність обстановки у світі показує, що навіть за достатнього розвитку системи колективної безпеки, жодна з країн не захищена повною мірою. Наявність постійних загроз безпеці будь-якій країні, незалежно від її статусу у світі, значно підвищує необхідність завчасної підготовки економіки країни та її армії до стійкого функціонування в умовах сучасної війни [1-6]. Витрачені на Збройні Сили України мільйони сьогодні, це збережені мільярди в найближчому майбутньому [4]. Однак, витрачанню коштів має передувати дослідження щодо їх раціонального розподілу за складовими воєнно-економічного забезпечення.

Аналіз останніх досліджень та публікацій. Широке застосування способів та методів воєнно-політичних конфліктів гібридного типу для вирішення міждержавних проблем на сучасному етапі розвитку людства, спонукали вітчизняних науковців до поглибленого їх аналізу. Так, останнім часом дослідженню питань економічного впливу, як складової "гібридної війни" присвячені праці Горбуліна В.П., Магди Е.В., Лещенка О.Я., Ткача І.М. Аналіз їх досліджень дозволяє стверджувати, що виклики та загрози, які несе "гібридна війна", особливо на економічну складову, постійно трансформуються, змінюють свою форму, характер та ознаки. Одним із головних напрямків досліджень щодо формування та забезпечення необхідного рівня обороноздатності держави є дослідження раціонального розподілу коштів за складовими воєнно-економічного забезпечення з урахуванням досвіду попередніх досліджень, але й з адаптацією їх до сучасних умов розвитку України.

Мета доповіді. Проаналізувати сучасний стан воєнно-економічного забезпечення обороноздатності держави та визначити її основні складові.

Виклад основного матеріалу

Матеріальною основою оборони та ведення війни є економіка. Вона впливає на масштаби і тривалість бойових дій, адже відомо, що при однакових стратегіях протиборства перемога буде у тої сторони, яка має більше ресурсів. Для ведення збройної боротьби необхідні Збройні Сили, а для їх утримання значні людські, матеріальні та фінансові ресурси, обсяги яких залежать від рівня економічного розвитку країни. Існуючі умови розвитку України загострили проблеми економічного забезпечення власних Збройних Сил, але завдали поштовх щодо розуміння необхідності їх наявності в достатній чисельності та з відповідним рівнем готовності виконувати завдання щодо оборони держави.

Відповідно до ст.35 Закону України "Про національну безпеку України" [7] "обсяг видатків на фінансування сектору безпеки і оборони має становити не менше 5% запланованого обсягу внутрішнього валового продукту (ВВП), з яких не менше 3% відсотків - на фінансування сил оборони". У 2018 році на оборону було виділено 2,74 % від ВВП [9], недофінансування 0,26 % ВВП, що склало у натуральному виразі 925 млн. грн. У 2019 році на оборону виділено 2,58% від ВВП [10]. Оборонний сектор у 2019 році недоотримав 0,42 % або у натуральному виразі приблизно 1,5 млрд. грн. щоб вийти на мінімальні

нормативні показники – 3 % від ВВП. В 2020 році фінансування власних Збройних Сил склало 2,25% від ВВП, тобто бюджет Міністерства оборони України у порівнянні із 2019 роком менший на - 0,32% від суми номінального ВВП, що відповідно складає – 14,7 млрд. грн. [10]. Це говорить про те, що ослаблена національна економіка не в змозі забезпечити мінімально необхідні потреби національної оборони (рис.1).

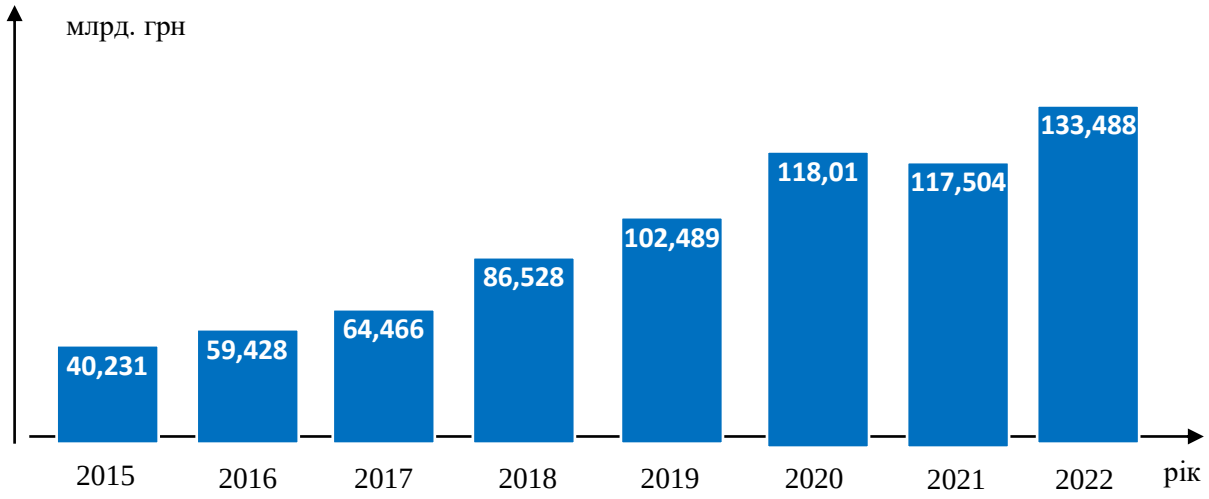

Рисунок 1. Бюджет Міністерства оборони України у 2015-2022 рр.

Сьогодні функціонування Збройних Сил України супроводжуються різким зростанням воєнних потреб та наявністю ризиків втрати чи знешкодження економічних об'єктів держави (захоплення території, завдання шкоди підприємствам, вивезення із захоплених територій корисних копалин, підприємств, матеріальних цінностей тощо). Тобто стає зрозуміло, що ступінь готовності держави до війни (конфлікту) визначається не тільки рівнем розвитку озброєння та військової техніки, кількістю матеріально-технічних засобів, рівнем забезпеченості фінансовими ресурсами, а й тим, чи готова економіка в цілому, тобто чи здатна швидко зорганізуватись та стійко функціонувати за умов сучасних викликів та загроз. Успішне виконання основних воєнно-економічних завдань, які постають перед державою, більш за все залежить від якості організації воєнно-економічної діяльності на усіх рівнях розвитку збройних сил та високої ефективності управління економікою держави як у мирний, так і воєнний час. Ефективне вирішення сучасних політичних цілей держави, які постають перед Україною сьогодні неможливе без підтримання обороноздатності України на рівні достатньому для ефективної протидії існуючим та ймовірним загрозам.

Однією з головних складових обороноздатності держави є її економічний потенціал. Економічний потенціал характеризує національну економіку України з боку наявних можливостей для виробництва необхідних державі матеріальних ресурсів. Основними елементами економічного потенціалу є: населення країни як джерело трудових та мобілізаційних ресурсів (чисельність, професійність, культурно-технічний рівень, розташування); національні багатства – накопичені

матеріальні цінності (запаси матеріальних засобів, майно, ресурси тощо); промисловість та її галузі (рівень техніки та технологій, потужності галузей виробництва тощо); сільське господарство (матеріально-виробнича база, джерела продовольства для збройних сил та населення, розвиток агропромислового комплексу тощо); інфраструктура як сукупність матеріальних об'єктів національної економіки (шляхи сполучення, транспортні засоби, зв'язок та інформаційні засоби, торгівля тощо); технічна база управління економікою.

Частина економічного потенціалу держави, яка може використовуватися для задоволення воєнних потреб за умов максимального напруження матеріальних, людських та фінансових ресурсів держави складає його воєнно-економічний потенціал (ВЕП). ВЕП характеризує воєнно-економічні можливості держави, які безпосередньо можуть бути використані для зміцнення обороноздатності та ведення війни. Один із найсильніших впливів на створення та зміцнення обороноздатності держави здійснює науково-технічний потенціал (НТП). Під НТП держави розуміють здатність та готовність науки та техніки ефективно вирішувати наявні та перспективні завдання, які постають перед суспільством. Сучасні реалії показують, що нестабільність ситуації в країні протягом останнього десятиріччя, низький рівень забезпеченості негативно вплинули на рівень НТП країни. Щорічно 3-5% найталановитіших спеціалістів різних галузей досліджень залишають країну в пошуках забезпеченості та захищеності. У порівнянні з початком років незалежності існуючий науково-технічний потенціал України знизився практично в 2-3 рази, що негативно відбивається і на процесах розвитку ЗС України та зміцнення її обороноздатності. Сьогодні вкрай необхідно створити умови ефективного нарощування рівня НТП країни. Україна є одним з лідерів з outsource. Наші програмісти, які працюють у приватних компаніях, забезпечують промислову електроніку для світових гігантів, таких, як General Motors та BMW. Тому необхідно створити відповідні програми для розвитку вітчизняного науково-технічного потенціалу.

Для розвитку НТП України слід приділити увагу досвіду США з розвитку власного науково-технічного потенціалу. На нашу думку, першість в цьому напрямку належить Агентству передових оборонних дослідницьких проектів Міністерства оборони США (Defense Advanced Research Projects Agency (DARPA)) [11]. У процесі відбору проектів DARPA зазвичай надають перевагу тим проектам, які мають одночасно високі ризики і високу віддачу у виконанні. Найбільш відомими проектами DARPA є: технологія STEALTH, GPS, Інтернет (прототипом якого була мережа ARPANET) тощо. В організаційному плані DARPA є незалежною структурою, яка визначає перспективний напрямок та формулює цілі, завдання програм, підбирає колектив виконавців (на основі конкурсного відбору), фінансує, управляє та контролює хід робіт. Фінансування DARPA здійснюється з бюджету Міністерства оборони США. Річний бюджет DARPA складає більше 3 млрд. дол. або 0,4 % від загального оборонного бюджету на рік, що дозволяє здійснювати відбір найкращих фахівців для відповідних проектів.

Обороноздатність держави має не тільки матеріально-технічну, а й соціальну складову. Сутність та тенденції розвитку суспільства безпосередньо впливають на розвиток держави в цілому. Соціальний потенціал – це можливості та готовність суспільства держави розвивати власну країни та задовольняти її потреби щодо зміцнення її обороноздатності. Одними з головних складових соціального потенціалу є: національні відносини; можливості населення; стан забезпеченості населення; стан та доступність освіти тощо. З історичного досвіду відомо, що якою б не була високо розвинута економіка країни, але перемога у війнах дуже часто залежала від моральної готовності населення захищати свою країну, тобто від духовних можливостей та готовності населення до сумісних дій, які підпорядковані досягненню певної цілі. Ці можливості населення характеризуються наступною складовою – моральним потенціалом, який являє собою у воєнному відношенні – ступінь духовної готовності та здатності населення та армії витримувати випробування сучасної війни та мобілізовуватися для досягання перемоги в ній. Важливим джерелом морального духа населення та армії є суспільно-політичний лад, який знаходить своє практичне відображення в політиці, яка проводиться державою. Відома фраза Карла Густава Маннергейма: “Перш ніж витрачати великі гроші на оборону, треба створити людям життя, яке варто було б захищати” не втрачає своєї актуальності і сьогодні [12].

Сукупність елементів, які складають матеріальні та духовні можливості держави, визначають його воєнний потенціал, який характеризує можливості держави утримувати та удосконалювати збройні сили, підвищувати їх боєздатність, поповнювати навченими кадрами, забезпечувати сучасним озброєнням, матеріальними засобами у мирний час і воєнний період. Основними складовими воєнного потенціалу є: кількість та якість ОВТ; забезпеченість військ матеріальними та фінансовими ресурсами відповідно до потреб; кількість особового складу; морально-психологічна готовність особового складу; підготовленість особового складу до вирішення завдань за призначенням (навички); наявність навчених та готових до мобілізації резервів; структура ЗС з погляду співвідношення військової техніки та особового складу в них, відповідність організаційних форм вимогам сучасної війни; рівень розвитку воєнного мистецтва та розроблення воєнної доктрини держави, ступінь їх відповідності реальній дійсності та вимогам воєнної практики; ступінь підготовленості командних кадрів, та їх вміння управляти військами; рівень бойової готовності ЗС і мобілізаційні можливості держави.

Дослідження [13], показують, що воєнний потенціал держави здійснює найбільший вплив на показник рівня обороноздатності держави, та знаходиться в тісному взаємозв’язку із економічним, науково-технічним, соціальним та моральним (духовним) потенціалами держави.

Висновки

У доповіді сформовані основні методологічні аспекти досліджень обороноздатності держави, а також визначені головні пріоритети її зміцнення. Головна увага матеріалу доповіді акцентована на дослідженнях питань воєнно-

економічного забезпечення обороноздатності держави, визначена роль воєнного та економічного потенціалу держави в загальному показнику оцінювання її обороноздатності, а також розкрито взаємозв'язок цих потенціалів між собою та з іншими потенціалами країни.

Список літератури:

1. Три роки АТО. Висновки та перспектив станом на 14.04.2017 року / [Електрон. ресурс]. – Режим доступу:https:// espreso.tv./2017./try_roky_ato_yak_ pochynalosya.
2. Гібридна війна Росії проти України: уроки та висновки – 24.10.2016 / [Електронний ресурс]. – Режим доступу:https://www.ukrinform.ua/2107122-gibridna-vijna-rosii-p.
3. Пасічко В. Обороноздатність держави теоретичні основи системного дослідження [Текст] / В. Пасічко / Політичний менеджмент. – К., 2008. – № 2. – С. 136-142.
3. Романченко І.С. Теорія відверненого збитку: моногр. / І.С. Романченко, В.О. Шуєнкін, В.М. Можаровський //Центральний науково-дослідний інститут Збройних Сил України. – Львів: Національна академія Сухопутних військ України, 2017. – 244 с.
4. Магда Е. В. Гибридная война: выжить и победить. Харьков: Виват. 2015.
5. Лещенко О.Я. «Гібридна війна» як науковий конструкт: проблеми пошуку термінологічної та концептуальної сутності. Епістемологічні дослідження в філософії, соціальних і політичних науках, (6), 60-71. (2016). URL: https://visnukpfs.dp.ua/index.php/PFS/article/view/853.
6. Світова гібридна війна: український фронт: монографія / За заг. ред. В.П. Горбуліна.
7. Закон України "Про національну безпеку України" – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19 Закон України "Про національну безпеку" Text.
8. Про Державний бюджет України на 2018 рік: Закон України від 07.12.2017 р. № 2246-VIII. Законодавство України. 2017.
9. Про Державний бюджет України на 2019 рік: Закон України від 23.11.2018 р. № 2629-VIII. Законодавство України. 2018.
10. Збройним Силам розвиток не передбачено. http://opk.com.ua/2020.
11. Defense Advanced Research Projects Agency URL: https://www.darpa.mil.
12. Карл Густав Маннергейм "Мемуари" у 2-х томах https://socratify.net/ quotes/karl-gustav-mannergeim/260063.
13. Основні методологічні аспекти воєнно-економічного забезпечення обороноздатності держави: теорія та практика [Текст]. О.М. Семененко, Р.В. Бойко, О.Г. Водчиць, Ю.Б. Добровольський, Д.В. Бердочник // Зб. наук. пр. Системи озброєння і військова техніка. – К., 2017. – № 3 (51). – С. 165-175.

Логістичне забезпеченя сил оборони у ході протидії агресору у гібридній війні

Петро Закусило, доктор військових наук, старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-0421-7736
В'ячеслав Козачук, кандидат технічних наук, старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0002-0207-7461
Григорій Хаврич
Центральний науково-дослідний інститут Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-1984-5946

Анотація. *У доповіді розглядаються погляди на організацію логістичного забезпечення у ході протидії агресії противника у гібридній війні, які базуються на результатах аналізу існуючих світових тенденцій розвитку гібридної війни, досвіду України як держави та досвіду її сил оборони під час протидій агресії РФ.*

Логістичне забезпечення сил оборони у ході протидії агресору у гібридній війні має низку суттєвих відмінностей, які слід обов'язково враховувати під час підготовки та відбиття збройної агресії. Результати досліджень можуть бути використані у ході удосконалення системи логістичного забезпечення Збройних Сил України.

Ключові слова: *гібридна війна, логістичне забезпечення, збройна агресія, протидія в гібридній війні, конвенціальна війна.*

Вступ

Постановка проблеми. Сучасна агресія Російської Федерації проти України здійснюється у формі гібридної війни. Це твердження вже не викликає жодних сумнівів. Однією з особливостей цієї війни стало зміщення акценту у використанні методів боротьби у напрямку комплексного застосування політичних, інформаційних, економічних та інших невоєнних засобів з опорою на військову силу [1]. Непідготовленість України в цілому, її Збройних Сил до такої війни призвели до того, що її початковий етап став програним. Разом з тим, досягнути мети агресії противнику не вдалось, тому, як ми зараз бачимо, агресор продовжує неконвенціальну частину гібридної війни.

Досвід воєнних протистоянь, які відбувались на першому етапі гібридної війни у 2014-2015 роках, підтвердив непідготовленість до такого виду війн не лише бойових частин і підрозділів, а й частин логістичного забезпечення. Тому напрошується висновок, що питання визначення особливостей логістичного

забезпечення у ході гібридної війни, яка на сьогодні перебуває у неактивній воєнній фазі, є актуальним.

Аналіз останніх досліджень і публікацій. Проведений аналіз останніх публікацій у відкритих джерелах свідчить про те, що таке явище, як гібридна війна вже добре відоме. Цій темі присвячено багато публікацій, серед яких слід відмітити [2–6]. Але у своїй більшості ці публікації мають або загальноосвітній характер, або украй фрагментарний характер, що висвітлюють окремі аспекти гібридної війни, або закритий характер, і тому не виносяться на обговорення науковою громадськістю.

Мета доповіді. Мета доповіді полягає у викладенні поглядів на особливості організації логістичного забезпечення у ході протидії агресії противника у гібридній війні.

Виклад основного матеріалу

В останні роки з'явилось декілька визначень такого поняття, як гібридна війна. Але за своєю суттю всі або майже всі дефініції зводяться до наступного: це комплекс заходів з використанням, передусім, політичних, економічних, інформаційно-психологічних та інших невоєнних дій, застосування терористичних, диверсійних, кримінальних груп, а також (можливо) воєнних дій, які виконуються, як правило, наприкінці конфлікту, тобто для завершення агресії та досягнення поставленої мети. Слід відмітити, що деякі дослідники до невоєнних засобів гібридної війни також відносять традиційну дипломатію, правові, ідеологічні та деякі інші інструменти впливу на країну – жертву агресії [2].

Гібридна війна може складатися з декількох умовних етапів:

формування комплексу гібридних загроз з урахуванням специфіки впливу на країну – жертву агресії;

послідовно-паралельний руйнівний вплив на ключові сфери управління країни-жертви з зосередженням основних зусиль на найбільш критичних напрямках, які забезпечують безпеку держави, – економіка, фінанси, морально-психологічний стан армії та цивільного населення тощо;

розгортання неоголошених воєнних дій, у ході яких країна-агресор атакує державні структури й регулярну армію противника за допомогою місцевих заколотників і сепаратистів, підтримуваних зброєю та фінансами з-за кордону. Важливе місце приділяється діям екстремістського характеру, насамперед так званої п'ятої колони, яка використовується для нанесення таранних ударів по владі;

висування державі-жертві ультимативних вимог щодо пріоритетів її внутрішньої і зовнішньої політики та, в кінцевому рахунку, капітуляції.

Деякі дослідники виділяють два умовних етапи гібридної війни [3]: прихованого протиборства та відкритого воєнного протистояння. Але така диференціація, на наш погляд, призводить до створення та використання занадто спрощених моделей гібридної боротьби, що безумовно призведе до помилок під час прийняття рішення на протидію противнику у такій війні.

Важливою особливістю гібридної війни є відсутність її детального, синхронізованого плану. Розробляється лише загальна цільова установка на

руйнування держави – жертви гібридної агресії, виконання якої здійснюють урядові та неурядові органи.

Держава-агресор протягом певного часу не розкриває себе, не проводить масштабних мобілізаційних заходів, прагне вести війну з використанням найманців, приватних військових компаній, створює на території держави-жертви іррегулярні формування, активізує їх дії, а також так звану «п'яту колону» і агентів впливу. Зокрема, плани дій по дестабілізації адміністративно-політичної, соціально-економічної й культурно-світоглядної сфер передбачають створення на території країни – жертви розподілених мережних структур з високим ступенем самостійності й здатністю до самосинхронізації. Заздалегідь відпрацьовуються канали їх фінансового, матеріально-технічного, інформаційного, кадрового забезпечення, створюються склади зброї, боєприпасів, засобів зв'язку, підбираються місця для підготовки бойовиків.

На цьому етапі протидія має складатися передусім із заходів поліцейського характеру, у яких беруть участь правоохоронні органи, у тому числі й спеціальні.

На етапі переходу держави-агресора до більш активних дій, але все ще не воєнних, коли стає зрозумілим, хто ініціює конфлікт, протидія має переходити у площину політичну, дипломатичну, інформаційну. Передусім це мають бути демарші в міжнародних установах (організаціях), економічні санкції, запити по допомогу до країн-партнерів, міжнародних судів тощо. Але це не виключає необхідності протидії заходами поліцейського характеру, більш того, активність протидії має наростати.

Крім того, необхідно здійснювати активну інформаційно-психологічну обробку скупчених для навчання в спеціалізованих таборах на території агресора, особливо в його прикордонних районах, польових командирів і бойовиків для здійснення силових акцій.

На цьому етапі мають бути активізовані дії усіх видів розвідки, насамперед космічної, технічної тощо для своєчасного попередження про можливий перехід держави-агресора до воєнних дій.

На етапі активних дій воєнного характеру, звичайно, крім дій регулярних військових формувань в рамках конвенціальної війни, одним з напрямків протидії може бути застосування сил спеціальних операцій проти стратегічно важливих об'єктів на окупованій території, викрадення та ліквідація (ізоляція) лідерів сепаратистських формувань, а також надання підтримки іррегулярним формуванням, які діють на окупованій території.

Під час протидії противнику у гібридній війні мають виконуватись заходи логістичного забезпечення. Звичайно, логістичне забезпечення матиме деякі особливості.

Функції логістичного забезпечення у гібридній війні, особливо на завершальній її стадії, такі ж самі, як й у ході конвенціональної війни:

забезпечення МтЗ;

забезпечення ОВТ, технічне обслуговування та відновлення (ремонт) ОВТ, їх використання (технічне забезпечення);

переміщення та перевезення (транспортування);

інфраструктурне забезпечення.

Також у керівних документах з логістичного забезпечення наведено перелік основних завдань логістики:

визначення потреб ЗС України, інших складових сил оборони, які залучаються до виконання завдань оборони держави, а також для участі в міжнародних операціях, в ОВТ, МтЗ, об'єктах інфраструктури, роботах та послугах;

планування та управління логістичним забезпеченням застосування сил оборони в стратегічних діях та операціях сил оборони;

планування розвитку спроможностей об'єднаної логістики в рамках середньострокового та короткострокового оборонного планування для досягнення гарантованого рівня виконання завдань оборони держави;

визначення пріоритетів розвитку ОВТ складових сил оборони;

планування забезпечення мобілізаційних потреб сил оборони на особливий період в ОВТ, спеціальній техніці та інших МтЗ (ресурсах) за рахунок можливостей національної економіки;

проектування, розроблення (модернізація, модифікація) ОВТ, МтЗ, їх закупівля, постачання, зберігання, технічне обслуговування та відновлення, вилучення та реалізація непридатних для використання ОВТ і матеріально-технічних засобів;

забезпечення військ (сил) ОВТ, МтЗ, об'єктами інфраструктури, організація їх експлуатації, використання;

створення запасів ОВТ, МтЗ, їх накопичення, відновлення замість витрачених (втрачених), ешелонування, утримання у стані, який забезпечить своєчасне приведення сил оборони в готовність до застосування (використання за призначенням) та розосередження відповідно до завдань, які виконуються в ході оборони держави;

планування та здійснення військових перевезень усіма видами транспорту;

розквартирування військ (сил);

організація харчування, лазне-прального та торговельно-побутового обслуговування особового складу.

Для визначення особливостей логістичного забезпечення під час ведення гібридної війни, слід проаналізувати функції та завдання логістичного забезпечення застосування відповідних сил і засобів з протидії противнику в гібридній війні на кожному умовному етапі.

Так, на першому етапі, коли протидія противнику має складатися передусім із заходів поліцейського характеру, у яких беруть участь правоохоронні органи, у тому числі спеціальні, мають виконуватися усі заходи логістичного забезпечення (тобто усі функції та завдання), які притаманні мирному часу.

На другому етапі, який передує фазі активних бойових дій, мають бути активізовані логістичні операції, направлені, серед іншого, на забезпечення руху опору, зокрема створення запасів матеріально-технічних засобів, передусім стрілецького озброєння та боєприпасів, продовольства та деяких інших видів військового майна, забезпечення їх надійного зберігання та швидкої видачі за призначенням.

При цьому заходи інфраструктурного забезпечення мають бути спрямовані, передусім, на створення необхідної кількості спеціально обладнаних споруд з місцями для прихованого зберігання визначених запасів МтЗ. Такі заходи мають бути завершені заздалегідь до початку відкритого протистояння.

Другий етап характеризується також активізацією усіх видів розвідки, насамперед космічної, технічної. З цієї причини логістичне забезпечення при цьому має бути орієнтоване, передусім, на підтримку заходів повсякденної діяльності та бойового чергування відповідних частин та підрозділів.

Особлива увага повинна приділятись відновленню та підтриманню надійного функціонування транспортних комунікацій та об'єктів інфраструктури, особливо на бар'єрних рубежах, що забезпечує стабільне та безперервне постачання матеріально-технічних засобів їх користувачам.

Висновки

У доповіді викладено погляди на організацію логістичного забезпечення у ході протидії агресії противника у гібридній війні, які базуються на результатах аналізу існуючих світових тенденцій розвитку гібридної війни, досвіду України як держави та досвіду її сил оборони під час протидій агресії Ерефії.

У подальшому передбачається більш детальне визначення особливостей заходів логістичного забезпечення у ході відсічі діям держави-агресора.

Список літератури

1. Протидія гібридній війні: досвід України: аналітична доповідь / Київ: Національний інститут стратегічних досліджень, 2016. 70 с.

2. Бартош А. А. Стратегия и контрстратегия гибридной войны / Военная мысль, 2018, №10. С. 6–19.

3. Сержантов А. В., Смоловый А. В., Долгополов А. В. Трансформация содержания войны: от прошлого к настоящему – технологии «гибридных» войн / Военная мысль, 2021, №2. С. 20–27.

4. Бартош А. А. «Трение» и «износ» гибридной войны / Военная мысль, 2018, № 1. С. 5–13.

5. Бартош А. А. «Серые зоны» как ключевой элемент современного операционного пространства гибридной войны / Военная мысль, 2021, №2. С. 6–19.

6. Зарудницкий В. Б. Характер и содержание военных конфликтов в современных условиях и обозримой перспективе / Военная мысль, 2021, №1. С. 34–44.

Теоретичні особливості використання центру обробки даних в приватних хмарах в умовах гібридного конфлікту: види, переваги та недоліки

Ольга Андрощук, кандидат психологічних наук
Старший науковий співробітник науково-дослідної лабораторії Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-1032-7459
Максим Голобородько, кандидат технічних наук, старший науковий співробітник
Начальник науково-дослідного управління Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-2381-7219
Андрій Фатальчук
Науковий співробітник науково-дослідної лабораторії Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-8944-4051
Олег Розумний
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-3225-8375

Анотація. *Доповідь присвячена аналізу можливості (доцільності) використання центрів оброблення даних (ЦОД) як елементів цифрової інформаційної інфраструктури органів державної влади сектору безпеки і оборони України в умовах гібридної війни. Визначено поняття ЦОД, недоліки і переваги існуючих ЦОД порівняно з локальними аналогами. Також розглянуто питання інформаційної безпеки ЦОД з використанням "хмарних" технологій. Особливу увагу приділено особливостям застосування даної технології для подальшого розвитку інформаційної інфраструктури. Проаналізовано приклади зарубіжного досвіду успішного використання ЦОД у "приватних хмарах".*

Ключові слова: *центр обробки даних, приватна хмара, інформаційний сервіс, хмарні технології.*

Вступ

Постановка проблеми. Бурхливий розвиток світового суспільства супроводжується масовим впровадженням інформаційних технологій у різні сфери життя, зокрема у сферу безпеки і оборони держави. Зазначене створило

передумови для позиціонування інформаційної зброї в парадигмі гібридної війни як зброї першого удару. В якості основних цілей інформаційних та кібер-атак розглядається перш за все інформаційний простір сектору безпеки і оборони.

В даному випадку йдеться про інформаційну інфраструктуру органів державної влади сектору безпеки і оборони України (далі – ІІ) та забезпечення ії кібернетичної (інформаційної) безпеки. Існуюча ІІ включає в себе засоби інформаційних технологій, такі як засоби оброблення та зберігання даних, хмарні послуги, операційні системи, програми, різні мережеві технології, служби резервного копіювання, моніторинг і механізми безпеки, а також засоби автентифікації, авторизації та аудиту. Фізична інфраструктура включає пристрої та датчики всіх форм, а також системи управління, які забезпечують належне функціонування зазначених елементів. Забезпечення кібернетичної (інформаційної) безпеки ІІ вимагає комплексного підходу, починаючи від вибору певних фізичних пристроїв до визначення порядку надання інформаційних послуг у хмарі.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень показав, що вимоги до інформаційної безпеки діяльності органів державної влади сектору безпеки і оборони України постійно посилюються [1-2]. Про актуальність проблеми свідчать дослідження В. Домарева, І. Конеєва, А. Беляєва, А. Савченко, В. Василенко, О. Колісника, Т. Халявкіної, Б. Корнієнко, Л. Галати та ін. [1-5]. Зокрема у праці А. Савченко, В. Василенко, О. Колісника, Т. Халявкіної [3] розглядаються методи моніторингу та управління інфраструктурою ЦОД, для забезпечення високої надійності та інформаційної безпеки. Вчені Б. Корнієнко та Л. Галата у своїх роботах [4] запропонували метод дослідження математичної моделі системи інформаційної безпеки в комп'ютерній мережі, в тому числі ЦОД. В ній вони оцінили пропускну здатність мережі та її компонентів, визначили "вузькі" місця в структурі обчислювальної системи; порівняно різні варіанти організації мережі, здійснили перспективний прогноз розвитку системи та передбачили майбутні вимоги відносно пропускної здатності мережі.

Однак, у розглянутих дослідженнях невисвітленим лишилось питання забезпечення надійності та оптимізації інфраструктури ЦОД.

Мета доповіді. Аналіз та систематизація теоретичних та практичних аспектів використання ЦОД як елементів цифрової інформаційної інфраструктури органів державної влади сектору безпеки і оборони України (далі – "приватна" хмара СБОУ) в умовах гібридної війни. Відповідно до поставленої мети, завданнями статті було визначення загальних принципів побудови ЦОД, аналіз недоліків і переваг існуючих ЦОД у "приватних хмарах" порівняно з їх локальними аналогами. Питання кібернетичної (інформаційної) безпеки ЦОД та захисту даних у "приватній" хмарі СБОУ.

Виклад основного матеріалу

За останні кілька років роль інформаційних систем і технологій суттєво зросла. Впровадження інформаційних систем стало необхідною умовою

підвищення мобільності, гнучкості та ефективності системи управління обороною держави.

Хмарні обчислення (англ. Cloudcomputing) – технологія розподіленої обробки даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс. Розвиток сфери хостингу було обумовлено виниклою потребою в програмному забезпеченні і цифрових послугах, якими можна було б управляти зсередини, але які були б при цьому більш економічними і ефективними [6].

Одним з основних підходів в основі хмарних технологій стоїть сервіс, до назв варіантів надання послуг прийнято додавати словосполучення "as a service", що в перекладі означає "у вигляді сервісу" SaaS (Software as a service), або програми у вигляді сервісів – варіант, при якому пропонується використовувати конкретне ПО, наприклад, корпоративну систему, у вигляді сервісу з підпискою [6]. Одним з варіантів використання SaaS э "приватна хмара".

Приватна хмара – це пул комп'ютерних ресурсів, що надаються як стандартний набір служб, який визначається, проектується і контролюється конкретним підприємством. Існують такі різновиди "приватних хмар":

– самостійно розміщена приватна хмара забезпечує контроль над архітектурою і операціями, використовуючи наявні інвестиції в персонал і устаткування, забезпечує виділене локальне середовище, яке проектується, розміщується і управляється всередині компанії;

– розміщена приватна хмара – це виділене середовище, яке проєктується всередині компанії, а розміщується і управляється за її межами. У ній поєднуються переваги управління службою та архітектурним проєктом з перевагами аутсорсингу;

– приватна хмара на основі пристрою – це виділене середовище, яке закуповується у постачальника та проєктується їм з орієнтиром на постачальника послуг і ринок функцій і контролем над архітектурою. Це середовище розміщується всередині організації і має внутрішнє або зовнішнє управління. В ньому поєднуються переваги використання попередньо налаштованої архітектури і низькими ризиками при розгортанні, з перевагами внутрішньої системи безпеки і контролю [7].

В наш час проєктування і побудова дата-центрів суворо регламентована стандартами, які встановлюють вимоги для проектування дата-центрів. Серед вимог до Центру обробки даних (ЦОД) можна виділити цілодобовий режим роботи та моніторингу, високу відмовостійкість, надмірність (резервування), безпеку, контроль параметрів середовища, пожежну безпеку, можливість швидкого розгортання та зміни конфігурації, підключення до територіальних, глобальних мереж або Internet [8–9].

Дата-центр (від англ. *data center*), або центр (зберігання і) обробки даних (ЦОД/ЦХОД) – це спеціалізована будівля для розміщення (хостингу) серверного і мережевого устаткування і підключення абонентів до каналів мережі Інтернет.

Центр обробки даних (ЦОД) – це комплекс потужних серверів, дискових сховищ і технічних рішень, призначених для автоматизації та безперебійної роботи комерційних процесів.

Якість і надійність – два основних критерії при виборі дата-центру. Якісний ЦОД повинен відповідати наступним вимогам: розміщення обладнання повинно бути надійно захищене від впливу навколишнього середовища; безперебійне постачання електроенергії; якісна система вентилювання повітря і відведення тепла; розвинена і багаторівнева система охорони: обгороджена територія, контрольно-пропускна система з доглядом, відеоспостереження, управління доступом; обізнані співробітники, які обслуговують інфраструктуру ЦОД і клієнтське обладнання.

Типи ЦОД:

- корпоративні (основні та резервні). Використовуються звичайними та інтернет-компаніями для зберігання власної актуальної інформації, а також забезпечуються функціонуванням віртуальних сервісів;
- комерційні (хостингові). Орієнтовані на зберігання і обробку даних сторонніх користувачів (клієнтів) з метою підвищення ефективності повсякденної економічної діяльності;
- використовуючі технологію Web 2.0.

Принципи роботи ЦОД: віртуалізація; кластеризація; масштабування; резервування.

Першочерговим завданням дата-центрів є створення сприятливих і захищених умов для доступу конкретної компанії до власних даних і їх закриття від сторонніх користувачів.

Унікальні можливості ЦОД гарантують ефективність і безперебійність роботи будь-якої організації, допомагаючи вирішувати більшість проблем, властивих будь-якому виду бізнесу.

Основний показник роботи ЦОД – відмовостійкість; також важлива вартість експлуатації, показники енергоспоживання і регулювання температурного режиму.

Склад ЦОД: технічні компоненти (серверний комплекс, системи зберігання та резервного копіювання даних, мережева інфраструктура, системи інженерної експлуатації та безпеки дата-центру), програмне забезпечення (операційні системи серверів, робочих станцій, програмне забезпечення баз даних, засоби адміністрування серверів і робочих станцій, резервного копіювання, кластеризації і інвентаризації, програми пристроїв зберігання даних, браузери та клієнти електронної пошти), організаційне середовище, що забезпечує функціональність процесів, пов’язаних з наданням IT-послуг.

Основні етапи створення ЦОД: планування (розробка технічного завдання та плану реалізації); узгодження обраної концепції і її адаптація до реальних умов експлуатації дата-центру; безпосередня реалізація проекту; експлуатація центру обробки даних; модернізація дата-центру.

Будівництво безпечного і надійного ЦОД можливо тільки при дотриманні вимог і нормативів, які стосуються характеристик приміщення, де буде розташовуватися обладнання. Від фактичного стану майданчика залежить не тільки належне функціонування ЦОД, а й вартість його облаштування.

Висновки

З метою забезпечення надійного функціонування інформаційної інфраструктури органів державної влади сектору безпеки і оборони України та забезпечення ії кібернетичної (інформаційної) безпеки в умовах гібридної війни доцільно застосовувати сучасні "хмарні" технології.

Використання "хмарних" технологій може значно знизити витрати на побудову центрів обробки даних та забезпечення їх функціонування. Крім того хмарні технології забезпечують можливість практично миттєво реагувати на виникаючі потреби користувачів в інформаційних сервісах. Закладені у технологію можливості щодо автоматизації операцій із забезпечення кібербезпеки інформаційної інфраструктури і завдань управління інформаційною безпекою, зокрема швидкого усунення відомих або нових загроз інформаційної безпеки, дозволять надати ефективної відсічі гібридним атакам країни-агресора.

Список літератури

1. Домарев В. В. Безопасность информационных технологий. Системный подход. Киев, 2004. 992 с.
2. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. СПб, 2003. 354 с.
3. Savchenko A. S., Vasylenko V. A., Kolisnyk O. V., Holiavkina T. V. Computer networks monitoring and management methods. *Наукоємні технології.* 2018. Т. 39. №3. С. 281–288. DOI: 10.18372/2310-5461.39.13075.
4. Korniyenko B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. Наукоємні технології. 2017. Т. 34. №2. С. 114–118. DOI:10.18372/2310-5461.34.11608.
5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2016. 960 с.10.
6. Cloud Computing: Global (2010 - 2015) URL: http: // www. marketsandmarkets.com/Market-Reports/cloud-computing-234.html.
7. Монахов Д. Н., Монахов Н. В., Прончев Г. Б., Кузьменков Д. А. Облачные Технологии. Теория и практика книга, МАКС Пресс Москва, МГУ, 2013 г. – С. 128.
8. ANSI/TIA-942 STANDART Telecommunications Infrastructure Standard for Data Centers. URL: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.
9. Сюзанн Найлз. Стандартизация и модульность в Адаптивной Инженерной Инфраструктуре Центра обработки данных. Информационная статья №116. *APC*. URL: https://www.apc.com/salestools/VAVR-626VPD/VAVR-626VPD_R0_RU.pdf.

Хмарні технології в умовах гібридного конфлікту: види, категорії, переваги та недоліки

Ольга Андрощук, кандидат психологічних наук
Старший науковий співробітник науково-дослідної лабораторії центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-1032-7459
Юрій Кірпічніков
Начальник науково-дослідного відділу центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0003-4444-0764
Ганна Литовченко
Науковий співробітник науково-дослідного відділу центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-8625-1438
Микола Петрушен
Старший науковий співробітник науково-дослідного відділу центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7448-2765

Анотація. *Доповідь присвячена аналізу та визначенню загальних принципів хмарних технологій та сервісів, хмарних обчислень. Розглянуті питання застосування хмарних технологій в сфері оборони в умовах конфліктів гібридного типу. Проаналізовано недоліки і переваги існуючих хмарних моделей порівняно з локальними аналогами.*

Ключові слова: *хмара, сервіс, хмарні технології, хмарні сервіси, хмарна платформа, хмарна інфраструктура, обчислювальні ресурси.*

Вступ

Постановка проблеми. Останні політичні та воєнні події змусили Україну жити в новій реальності і приймати блискавичні рішення у відповідь на гібридні загрози XXI століття. В сучасних умовах Збройним Силам України, належить виробити і застосувати нові сучасні підходи до розвитку власного інформаційного простору, забезпечення його стійкості та безпеки.

У Концепції Національної програми інформатизації [1] визначено, що інформатизація Збройних Сил України є складовою частиною інформатизації

держави і включає процеси створення, впровадження і застосування у мирний та воєнний час сучасних методів, систем і засобів одержання, оброблення, зберігання, передавання та використання інформації.

Протягом тривалого часу у Збройних Сил України створювались та розвивались окремі автоматизовані, інформаційні, інформаційно-аналітичні та інші програмні системи, що не зв'язані між собою. На даний час інформаційне середовище в сфері оборони реалізовано у вигляді "вертикальних замкнутих контурів" з відсутністю обміну даними між інформаційними системами. Існуючий стан інформаційного середовища є більше статичним, ніж динамічним, який не дозволяє швидко адаптуватись під потреби споживачів інформації в умовах гібридного конфлікту та в повній мірі використовувати інформаційну перевагу над ворогом. Даний підхід унеможливлює ефективне використання інформації для забезпечення оперативної потреби "потрібна інформація в потрібному місці в потрібний час".

Розуміння необхідності об'єднання усіх існуючих інформаційних систем сил оборони у цілісну взаємозв'язану інформаційну інфраструктуру призвело до потреби застосування хмарних технологій, що має збільшити швидкість та якість процесів інформаційного обміну для прийняття стратегічних рішень та успіху операцій і бойових дій в умовах гібридного конфлікту.

Аналіз останніх досліджень і публікацій. У науковій літературі інформаційних технологій розглядаються в рамках теорії інформаційного суспільства. Засновниками і головними розробниками цієї теорії вважаються такі вчені: Д. Белл, Ю. Хаяші, Ж. Бодрійяр, М. Постер, М. Кастельс, М. Пайор, Ч. Сейбл, Л. Хіршхорна.

Такі вчені, як В.Ю. Биков, О.Г. Кузьмінська, Ю.Г. Носенко, М.П. Шишкіна, та ін. у своїх дослідженнях наголошують на важливості застосування хмарних технологій і сервісів, для використання у державних відомствах. Оскільки інформаційні технології постійно вдосконалюються, виникає потреба подальшого дослідження різних аспектів застосування хмарних технологій і сервісів у підготовці майбутніх докторів філософії

Мета доповіді. Визначення загальних принципів застосування хмарних технологій в сфері оборони в умовах гібридного конфлікту, аналіз недоліків і переваг існуючих хмарних моделей порівняно з локальними аналогами.

Виклад основного матеріалу

За останні кілька років роль інформаційних систем і технологій суттєво зросла. Впровадження інформаційних систем стало необхідною умовою підвищення мобільності, гнучкості та ефективності інформаційних систем та автоматизованих систем управління Збройних Сил України. На сьогодні хмарні технології знаходять активне застосування у сфері оборони всіх розвинених країн, забезпечуючи принципово нові та ефективні можливості.

Хмарні технології (англ. Cloud computing) – це модель забезпечення зручного мережевого доступу на вимогу до загального пулу (pool) обчислювальних ресурсів, які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними витратами. Термін "хмара" (cloud)

використовується як метафора, заснована на зображенні мережі Інтернет на діаграмі комп'ютерних мереж, або як образ складної інфраструктури, за якою приховано всі технічні деталі.

Парадигма хмарних технологій передбачає віддалену обробку та зберігання даних. Ця технологія надає користувачам доступ до комп'ютерних ресурсів віддалених серверів і використання програмного забезпечення як онлайн-сервісу [2]. Хмарні сервіси, що надають ті чи інші види послуг, в свою чергу діляться на три категорії: публічні, приватні та гібридні [3].

Публічна "хмара" – IT-інфраструктура, яку використовують багато різних користувачів і організаційних структур. Користувачі при цьому не можуть управляти і обслуговувати "хмару", вся відповідальність за це лежить на власнику "хмари".

Приватна "хмара" – безпечна IT-інфраструктура, контрольована і експлуатована однією організаційною структурою, яка може керувати "хмарою" самостійно або доручити це зовнішньому підряднику.

Гібридна "хмара" – IT-інфраструктура, яка використовується, коли частина потужностей приватної "хмари" перекидається на публічну "хмару", якщо вона не справляється з поточними завданнями.

На даний момент розрізняють три основні моделі хмарних сервісів:

1. Інфраструктура як сервіс (Infrastructure as a Service або IaaS).

IaaS – інфраструктура як сервіс. Даний підхід полягає в тому, що виділяється інфраструктура на вимогу, наприклад, кілька віртуальних машин, на які можна встановити будь-які операційні системи. Замовник сам налаштовує маршрутизацію, балансування навантаження, бази даних і т.д.

IaaS заснована на технології віртуалізації, що дозволяє користувачеві обладнання ділити його на частини, які відповідають поточним потребам, тим самим збільшуючи ефективність використання наявних обчислювальних потужностей, дискового простору, мережевої пропускної здатності і інших ресурсів. Крім того, IaaS надає в розпорядження користувача весь набір функцій управління в одній інтегрованій платформі [4].

Однією з головних цінностей моделі IaaS є процес вивантаження обчислювальних завдань в "хмару" в період необхідності максимальної кількості обчислювальних ресурсів. У цьому випадку досягається економія за рахунок того, що не потрібно вкладати кошти в придбання додаткових серверів під час пікових навантажень, які в решту часу працюють з невеликим навантаженням.

2. Платформа як сервіс (Platform as a Service або PaaS).

PaaS – платформа як сервіс. Суть PaaS рішень полягає в тому, що виділяється не набір віртуальних машин, а ціла платформа. Це дозволяє не визначати який сервер використовувати, а просто розробити і розгорнути інформаційну систему або спеціальне програмне забезпечення (СПЗ) в "хмарі". Унікальність PaaS полягає в тому, що вона дозволяє створювати і розгортати інформаційні системи та СПЗ на заздалегідь існуючій обчислювальній платформі. Обчислювальна платформа являє собою місце, де може функціонувати СПЗ, якщо воно відповідає стандартам цієї платформи [5].

3. Програмне забезпечення як сервіс (Software as a Service або SaaS).

SaaS – програмне забезпечення як сервіс. Сервіс за запитом, коли користувач взагалі нічого не виконує в плані налаштувань СПЗ, а тільки його споживає. Таке СПЗ безпосередньо доступне кінцевому користувачеві, і цим SaaS принципово відрізняються від рішень класу IaaS і PaaS, які спрямовані не на користувачів, а на розробників і власників ІТ-систем [6].

Незважаючи на збільшення кількості державних проєктів, пов'язаних з хмарними сервісами, все ще існують чинники, які досі пір стримують активне впровадження хмарних технологій в сфері оборони. Як і у будь-яких технологіях, хмарні технології мають як свої переваги, так і недоліки. До основних переваг можна віднести наступні:

1. Доступність. Доступ до інформації, що зберігається у хмарі, може отримати кожен, хто має комп'ютер, планшет, будь-який мобільний пристрій, підключений до мережі Інтернет.

2. Час. Хмара дозволяє попрацювати над залученням клієнтів і підвищенням їх задоволеності.

3. Мобільність. Використання хмар дозволяє користувачеві підключитися до необхідного серверу з будь-якого пристрою не прив'язуючи його до конкретного робочого місця.

4. Економічність. Хмари доступні з будь-кого пристрою який під'єднано до мережі Інтернет та у якому є Веб-браузер.

5. Простота у використанні. Більшість хмарних платформ мають інтуїтивно зрозумілу консоль управління, за допомогою якої можна підключати необхідні ресурси, коли це потрібно.

6. Вибір. Існує безліч готових рішень, які працюють за принципом зареєструвався і користуєшся – SaaS. Є моделі PaaS, які дозволяють розгортати власні рішення в "хмарі". Цілий ряд постачальників пропонує послуги IaaS.

7. Гнучкість. Всі необхідні ресурси надаються провайдером автоматично.

8. Висока технологічність. Великі обчислювальні потужності, які надаються в розпорядження користувача та які можна використовувати для зберігання, аналізу і обробки даних.

10. Надійність. Надійність, яку забезпечують сучасні хмарні обчислення, набагато вище, ніж надійність локальних ресурсів.

Є й ряд недоліків:

хмарна послуга надається завжди провайдером, відповідно, збереження даних користувача залежить від провайдера;

поява хмарних монополістів;

необхідність завжди бути в мережі для роботи;

небезпека хакерських атак (при зберіганні даних на локальному комп'ютері можна в будь-який час відключитися від мережі і очистити систему за допомогою антивірусу).

Висновки

Застосування хмарних технологій в сфері оборони та, зокрема, в Збройних Силах України в умовах гібридного конфлікту дозволить в повній мірі використовувати переваги обміну потрібною інформацією через всі домени інформаційного простору – від стратегічної до тактичної ланки (до кожного

солдата на полі бою), усунути принцип “ізольованості” існуючих інформаційних систем та забезпечити задоволення потреб в інформації, яка необхідна для швидкого прийняття рішень. Хмарні технології мають надати можливості користувачам в сфері оборони знаходити та обмінюватись інформацією, яка потрібна, в час коли вона потрібна, у вигляді, який дозволить ефективне її використання.

В рамках створення інформаційної інфраструктури Міністерства оборони України та Збройних Сил України без розвитку галузі інформаційних технологій з залученням хмарних моделей слід приділити значну увагу.

Список літератури

1. Про Концепцію Національної програми інформатизації: закон України [прийнято Верхов. Радою 04 лютого 1998 р. №75/98-ВР (Зі змінами та доповненнями)]. URL: http://zakon2.rada.gov.ua/ laws/show/75/98-вр.

2. Бондар Є.С., Гороховський С.С. Хмарні обчислення та їх застосування. Вісник КНУ ім. Т. Шевченка, Вип. № 1, К.: КНУ, 2011. – 74–82 с.

3. Дайновський Ю.А., Гліненко Л.К. Бізнес-моделі хмарного надання ІТ-послуг. Маркетинг і цифрові технології. 2019. Т. 3. № 2. С. 18–44.

4. Mell P., Grance T. The NIST Definition of Cloud Computing: Recommendation of the National Institute of Standards and Technology. Gaitherburg : National Institute of Standards and Technology, September 2011. III, 3 p. (Special Publication 800-415). [Electronic Resource].– Mode of access: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

5. Лозинський А.П. Синтез технологій платформ хмарних обчислень. Control Systems and Computers. 2019. № 6. С. 35–45.

6. Seethamraju R. Adoption of software as a service (SaaS) enterprise resource planning (ERP) systems in small and medium sized enterprises (SMEs). Information systems frontiers. 2015. Vol. 17 (3). P. 475–492. doi: 10.1007/s10796-014-9506-5.

Стратегічна повітряна операція, як один з можливих механізмів гібридної війни Російської Федерації проти України

Володимир Горбенко, кандидат військових наук, доцент
Професор кафедри авіації інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7030-0995
Олена Коршець, кандидат технічних наук, доцент
Заступник начальника кафедри Повітряних Сил інституту авіації та протиповітряної оборони Національний університет оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7225-0848

Анотація *В доповіді розглянуті існуючі погляди щодо можливих механізмів досягнення політичних цілей гібридної війни Російської Федерації проти України. Визначені можливі політичні цілі, сфери впливу та ймовірні сценарії для досягнення Російською Федерацією своєї мети. Проведено аналіз основних концепцій, які можуть бути теоретичною основою дисфункції державної системи. Визначені можливі варіанти впливу Російської Федерації в різних сферах. Обґрунтовано загрозу проведення комбінованої інформаційної та стратегічної повітряної операції, як дієвого механізму досягнення політичних цілей Російської Федерації в Україні. На підставі аналізу досвіду проведених повітряних операцій "Буря Пустелі" проти Іраку та "Союзницька Сила" в Югославії визначені можливі характер, масштаб, ресурси та кількісні показники виконання основних оперативних завдань стратегічної повітряної операції проти України.*

Зважаючи на розглянуті механізми досягнення РФ політичних цілей в Україні на основі концепцій "стратегічного паралічу", "центрів ваги" та "операції на основі ефектів", слід далі посилювати обороноздатність країни в усіх сферах, в першу чергу, в інформаційні та повітряній.

Ключові слова: *гібридна війна, дисфункція державної системи, інформаційна операція, стратегічна повітряна операція, стратегічний параліч, операція на основі ефектів*

Вступ

Постановка проблеми. Для побудови власної стратегії та вироблення варіантів врегулювання конфлікту на Сході, насамперед, потрібні комплексна оцінка ситуації та формування можливих сценаріїв досягнення політичних цілей РФ в Україні. Логіка дій агресора залежить від великої кількості факторів і обставин, що виходять далеко за межі проблеми Донбасу та українсько-російських відносин.

Можливими сценаріями досягнення політичних цілей РФ в Україні є:

1) залишення України у сфері впливу РФ невійськовими засобами;

2) використання РФ силового сценарію, за умов неспроможності досягнення політичних цілей невійськовими засобами: масований комплексний удар по Україні одночасно з кількох напрямків (Донбас, Крим, Чорноморське узбережжя, Придністров'я, Білорусь) із застосуванням регулярних військ з метою утворення підконтрольній РФ дуги, що з'єднує Придністров'я і Крим з власною територією.

Проте, реалізація даних сценаріїв вимагатиме значних ресурсів. Дедалі більш критичною стає суперечність між станом економіки РФ та її зовнішньополітичними амбіціями. Навіть за умов локальних успіхів, РФ надалі буде складно їх досягати, утримувати, і тим більше розвивати, – якщо цей тягар не перекласти на суб'єкти-жертви.

Аналіз останніх досліджень та публікацій. Слід зазначити, що концепція створення "керованого хаосу" (підриву противника зсередини) була апробована та активно використовується РФ на пострадянському просторі. Події на Сході України подібні діям РФ в Південній Осетії, Абхазії, Нагірному Карабасі, Придністров'ї і, певною мірою, в анексованому Криму.

В жодному зі створених РФ конфліктів не досягнуто стратегічної мети. Кількість та тривалість конфліктів постійно зростає, зростають витрати на їх підтримання, проте це не дає очікуваних результатів. Тому, застосування РФ воєнної сили з метою пришвидшення отримання ефекту від "керованого хаосу" цілком вірогідне. Для цього, РФ постійно збільшує кількість своїх військ поблизу українських кордонів і на окупованих територіях, модернізує та створює нові ударні оперативні сили, перевіряє на практиці концепції їх застосування в умовах операцій нової генерації. Ці сили мають наступальну спрямованість та є інструментом агресії [1-8, 22, 23].

Мета доповіді. Загроза повномасштабного вторгнення російських військ залишається цілком реальною і може прогнозуватися як один з можливих наступних етапів гібридної війни проти України. За даних умов, питання визначення можливих дієвих механізмів гібридної війни Російської Федерації проти України є актуальним. Стратегічна повітряна операція може розглядатися, як одна з оптимальних форм дій агресора для ураження з повітря основних стратегічних об'єктів на всій території країни, насамперед, об'єктів структури держави, економіки, а не військ (сил). Це дозволяє мінімізувати втрати, а за певних умов, уникнути безпосереднього зіткнення військ, досягнути політичної мети без наземного вторгнення та окупації, мінімізувати витрати та ризики.

Викладення основного матеріалу

В діях РФ можна відстежити певні тенденції, які спрямовані на поетапне впровадження концепцій: стратегії непрямих дій, "м'якої сили", технології "керованого хаосу" ("кольорових революцій") тощо. Дані підходи базуються на поглядах Сун Цзи та Клаузевіца, які надавали першочергове значення політичним аспектам війни та маніпулюванню керівництвом держави, а не знищенню військової сили. В сучасній війні, перемога над противником,

насамперед, досягається дисфункцією його державної системи без повного руйнування її критичних складових: політичне керівництво країни, життєво необхідні ресурси, інфраструктура, населення, розгорнуті угруповання військ (сил). Згідно теорії Дж. Уордена, необхідно вирахувати та уразити тільки критичні вузли, так звані, "центри ваги", якими є зв'язки та взаємні відношення між "складовими державної системи (рис. 1). На основі даної теорії, бажаним результатом є добровільна або примусова зміна політичного курсу держави шляхом часткового або повного паралічу свідомості та волі керівництва країни [9-23].

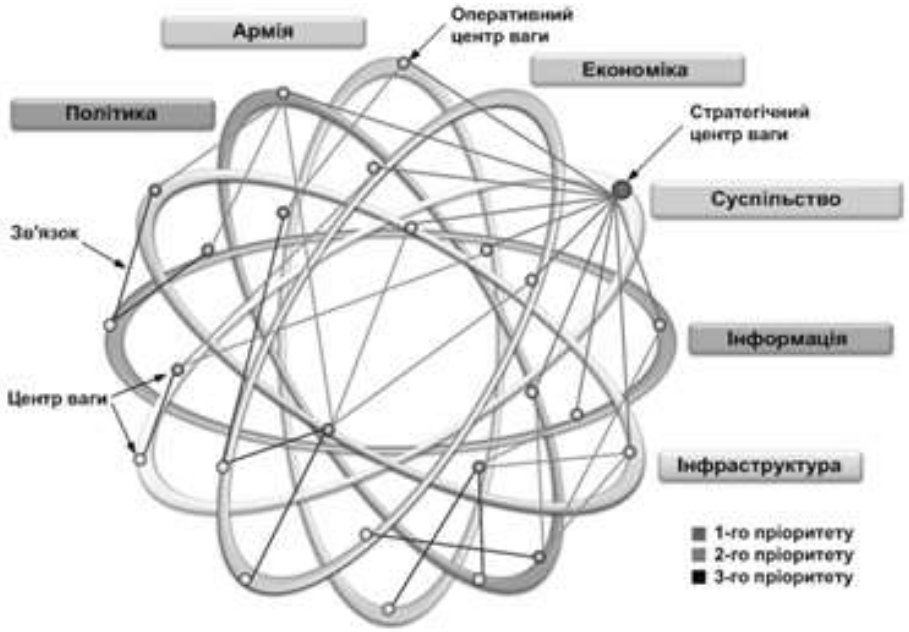

Рис. 1. Удосконалена модель сучасного операційного середовища для операцій на основі ефектів

З огляду на окреслені тенденції, цілком ймовірно, що РФ для реалізації силового сценарію, може обрати концепцію "стратегічного паралічу". Дана концепція, неодноразово апробована західними країнами в різних конфліктах та упродовж тривалого часу активно досліджується військовими експертами РФ.

Оптимальними діями для реалізації цієї концепції є удари з повітря по основним стратегічним цілям на всій території країни, насамперед, по об'єктам структури держави противника, економіки, а не його військам (силам). Це дозволяє мінімізувати втрати, а за певних умов, уникнути безпосереднього зіткнення військ, досягнути політичної мети без наземного вторгнення та окупації, мінімізувати витрати та ризики.

Згідно цієї моделі повітряні сили завдають удари не тільки по воєнним об'єктам та військам, але і по об'єктам критичної інфраструктури: залізничним шляхам, мостам, телевізійним і радіостанціям, промисловим підприємствам та іншим об'єктам, відповідальним за забезпечення життєдіяльності населення. У поєднанні з потужною інформаційною кампанією, досягається комбінований ефект – прискорення виснаження національних ресурсів, виникнення у населення відчуття незахищенності, розчарування та невдоволення керівництвом

країни, подавлення волі до супротиву. Результатом такої операції є досягнутий фізичний, функціональний або психологічний ефект (операції на основі ефектів).

Досвід агресії РФ в Україні із застосуванням регулярних військових формувань, засвідчив зростання втрат і збільшення опору по мірі просування вглиб території України. Подальше вторгнення неминуче призвело б до збільшення угруповання військ (сил) та зростання тривалості операції, а отже і витрат ресурсів на її проведення. За активної фази конфлікту, РФ вдалося досягти тільки тактичних успіхів на окремих напрямках. Досягнення оперативних успіхів вимагало збільшення масштабу агресії, що не було реалізовано.

Наразі, через відмову розв'язати конфлікт воєнним шляхом, відбувається його замороження. У будь-якому варіанті, це призведе до збільшення його тривалості та постійного зростання ресурсних витрат РФ. Як свідчать результати президентських та парламентських виборів в Україні, навіть за умови зміни правлячої еліти, швидкі зміни не настають. А відсутність швидкого результату не є прийнятним для РФ.

За таких умов, кардинальним варіантом є прискорення руйнівних процесів всередині самої країни. Каталізатором таких процесів можуть бути внутрішні протести населення та розрив зв'язків між ним та політикумом. На сьогодні існує тільки два дієвих інструменти реалізації наведених концепцій. Це вплив в інформаційній сфері силами та засобами інформаційної боротьби, та вплив у фізичній сфері засобами повітряного нападу. Вплив в інформаційній сфері, як свідчить досвід, досягається відповідною інформаційною кампанією. Проте, такий варіант також не дає швидкого результату. Саме тому, тільки комплексний цілеспрямований інформаційний та фізичний вплив на критичні "центри ваги", які визначають життєвоважливі ресурси для населення, їх руйнування, здатний створити хаос, протест, який буде направлений на керівництво країни.

Джуліо Дуе вже в 1921 році визначив, що саме повітряні сили відіграватимуть найважливішу роль у війнах майбутнього. Адже тільки вони можуть забезпечити досягнення ефектів, уражаючи ключові "центри ваги" на всій території країни противника одночасно.

Військово-повітряні сили (ВПС) повітряно-космічних сил (ВКС) РФ за сукупністю кількісно-якісних показників спроможні провести стратегічну повітряну операцію під час якої, у взаємодії із засобами дальнього вогневого ураження інших видів збройних сил, завдати вибіркових високоточних ударів по усьому спектру об'єктів критичної інфраструктури на усю глибину території України. Станом на 2021 рік у складі авіації ВПС ПКС РФ очікується до 1 500 літаків, більшість з яких є модернізованими та сучасними. Значна кількість льотного і технічного складу ВПС отримала бойовий досвід у Сирійській кампанії.

Оцінити можливість проведення стратегічної повітряної операції ВПС ПКС РФ на території України можна на прикладі порівняння з подібною за масштабом операцією "Буря пустелі" на території Іраку.

Результати порівняльного аналізу свідчать, що проведення на першому етапі повітряно-наступальної операції з метою завоювання переваги у повітрі,

дозволить за 3–5 діб (до 450 літако-вильотів) зруйнувати систему протиповітряної оборони за рахунок ураження виключно аеродромів, літаків на них, засобів зенітних ракетних військ та радіотехнічних військ Повітряних Сил ЗС України.

Завоювання переваги у повітрі створить сприятливі умови для проведення стратегічної повітряної операції метою якої буде – руйнування стратегічної та регіональних систем життєвоважливих для населення: електропостачання, забезпечення паливно-мастильними матеріалами тощо (рис. 2). За таких умов, упродовж 7–10 діб противник виконає основні завдання операції, витративши до 1200–1500 літако-вильотів.

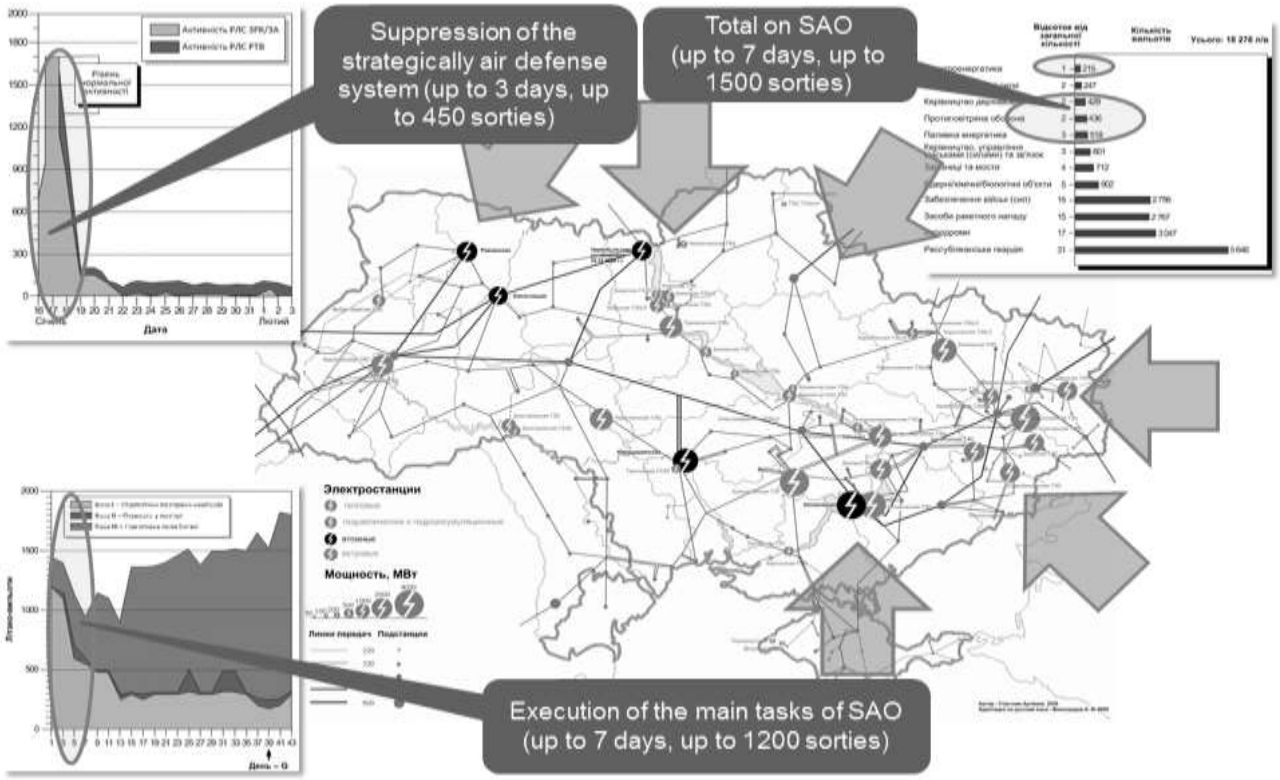

Рис. 2. Варіант проведення стратегічної повітряної операції за досвідом сучасних операцій

Слід зазначити, що для швидкого досягнення прийнятного результату, цілком достатньо зосередити зусилля лише на одному місті – столиці держави.

Обраний механізм досягнення політичних цілей шляхом проведення стратегічної повітряної операції із нанесенням повітряних ударів по обраним об’єктам на значній відстані від стратегічного “центру ваги” та великих міст, може створити у суспільній свідомості уявлення про “відсутність війни” та непричетності РФ до цих подій. Стратегічна повітряна операція в сукупності з інформаційною операцією, яка спрямована на насадження наративу: “уряд та президент нездатні знайти дієві механізми поліпшення ситуації”, із подальшим виведенням правлячої влади “з гри” призведуть до наростання невдоволення населення, та, як результат – до чергової революції із прогнозованою та керованою для РФ зміною влади. А за умови жорсткого подавлення протесту

суспільства, будуть створені умови для введення “миротворчого” контингенту РФ.

Висновки

Зважаючи на наведені механізми досягнення РФ політичних цілей в Україні на основі концепцій “стратегічного паралічу”, “центрів ваги” та “операції на основі ефектів”, слід далі посилювати обороноздатність країни в усіх сферах, в першу чергу, в інформаційні та повітряній.

Необхідно послідовно проводити єдину гнучку державну політику, інтеграцію усіх складових сил оборони, створювати та впроваджувати в життя єдину систему взаємоузгоджених і всебічно зважених заходів економічного, політичного, інформаційного та воєнного характеру, адекватних викликам та загрозам.

За умови модернізації економіки, соціальної сфери, системи управління, сил оборони, насамперед Повітряних Сил, Україна буде здатна протистояти агресії РФ і зможе реалізувати прийнятну модель врегулювання конфлікту на Донбасі.

Список літератури

1. Пашков М. Війна на Донбасі: реалії і перспективи врегулювання: аналітична доповідь / М. Пашков. – К.: ЦентрРазумкова, 2019. – 144 с
2. Мартинюк В. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і східного партнерства / В. Мартинюк. –К.: Центр глобалістики “Стратегія ХХІ”, 2018. – 105 с.
3. Полумієнко С.К. Гібридна війна, її окремі передумови, стратегії та наслідки / С.К. Полумієнко // Вісник Націо-нальної академії наук України. – 2017. – № 8. – С. 72-82.
4. Левченко О.В. Еволюція гібридної війни Російської Федерації проти України / О.В. Левченко // Наука і оборона. – 2017. – № 2. – С. 11-16.
5. Князєв Д. Деструктивні чинники гібридної війни / Д. Князєв, С. Князєв // Бизнес и безопасность. – 2017. – № 4.–С. 2-6.
6. Киричок А.П. Гібридна війна як феномен військово-інформаційної думки ХХІ ст. / А.П. Киричок // Держава тарегіони. – 2017. – № 2. – С. 26-30.
7. Сенченко О. Новий виклик людству – гібридна війна / О. Сенченко // Вісник Книжкової палати. – 2017. – № 5.–С. 41-45.
8. Майбутнє безпекове середовище 2030: стратегічне передбачення (попередній опис) – К.: МОУ, 2019. – 53 с\.
9. Савин Л.В. Пять стратегических колец Уордена и петля Бойда НОРД / Л.В. Савин. – Режим доступу: https://www.academia.edu/39347264/ Пять_стратегических_колец_Уордена_и_петля_Бойда_НОРД.
10. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию: монография / Л.В. Савин. – М.: МОД “Евразийское движение”, 2011. – 130 с.
11. Попов И.М. Война будущего: взгляд из-за океана. Военные теории и концепции современных США / И.М. По-пов. – М.: АСТ-Астрель, 2004. – 444 с.
12. Савин Л.В. Новые способы ведения войны. Как Америка строит империю / Л.В. Савин. – Санкт-Петербург:Питер, 2016. – 352 с.

13. Ralph D.Th. Chasing the Centre of Gravity in the Age of Accelerations [Electronic resource] / D.Th. Ralph // ISPSWStrategy Series: Focus on Defense and International Security. – 2018. – No. 550. – P. 1-6. – Available at: https://www.ispsw.com/wp-content/uploads/2018/05/550_Thiele.pdf.

14. John A.W. The Enemy Asa System / A.W. John // Air Power Journal. – 1995. No. 1(9). – P. 40-55. – Available at:https: //www.airuniversity.af.edu/Portals/10/ ASPJ/ journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf.

15. David S.F. John Boyd and John Warden. Air Power's Quest for Strategic Paralysis. School of Advanced AirpowerStudies // S.F. David. – Alabama: Air Universiti Press, 1995. – 59 p. – Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a 291621.pdf.

16. Rich G. Personal Theories of Power: Air Power – Annihilation, Attrition, and Temporal Paralysis [Electronic resource]/ Security Policy – Armed Forces – Media // G. Rich. – 2015. – Available at: https://www.offiziere.ch/?p=23022.

17. David R.M. The Air Campaign: John Warden and the Classical Airpower Theorists / R.M. David. – Alabama: Air Uni-versity Press, 1999. – 96 p.

18 Joint Battle Damage Assessment Course Syllabus. Joint Targeting School Joint Staff, Virginia Beach: Joint Staff J-7,2015. – P. 1-13. – Available at: https://ru.scribd.com/document/359515469/Battle-Damage-Course-Syllabus.

19. John A.W. The Air Campaign: Planning for Combat / A.W. John. – USA: Books Express Publishing, 2011. – 224 p.

20. Скорик А.Б. Аналіз операції "Союзницька Сила" і оцінка її впливу на зміну стратегії оборони США / А.Б. Скорик, В.В. Воронин, О.М. Доска // Збірник наукових праць Харківського університету Повітряних Сил. – 2009. – № 3(21). – С. 19-22.

21. Дуэ Д. Господство в воздухе / Д. Дуэ. – М.: АСТ, 2003. – 608 с.

22. Дроздов С.С. Аналіз операційного середовища та ймовірні сценарії застосування Повітряних Сил Збройних Сил України /С.С. Дроздов, В.В. Тюрін, О.А. Коршець, В.М. Горбенко // Наука і оборона. – 2019. – № 3. – С. 25-30.

23. Горбенко В.М. Оцінювання можливих механізмів досягнення Російською Федерацією політичних цілей в Україні з використанням концепцій стратегічного паралічу та операцій на основі ефектів / В.М. Горбенко, О.А. Коршець, Н.О. Королюк // Збірник наукових праць Харківського національного університету Повітряних Сил, 2020, 1(63) – С. 113-123.

Аналіз впливу розгортання систем зон заборони достопу та блокування району (A2/AD – ANTI-ACCESS/AREA-DENIAL) Російською Федерацією на застосування Збройних Сил України

Андрій Луцишин, доктор філософії
Старший викладач кафедри Повітряних Сил інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7733-7109
Григорій Степанов, кандидат військових наук, доцент
Доцент кафедри Повітряних Сил інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-9190-2821
Ігорь Костюк, доктор філософії
Начальник науково-інноваційної лабораторії наукового відділу організації досліджень науково-методичного центру організації наукової та науково-технічної діяльності Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7185-3671
Олександр Титаренко, кандидат військових наук, доцент
Доцент кафедри Повітряних Сил інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-3992-9314

Анотація. *Предметом доповіді є зони заборони доступу та блокування району (A2/AD – anti-access/area-denial) збройними силами Російської Федерації (ЗС РФ), що створені на кордонах з Україною та країнами членами НАТО. Метою доповіді є аналіз їх впливу на застосування Збройних Сил України та визначення напрямків подальших досліджень щодо пошуку способів ефективної боротьби з ним.*

Ключові слова: *A2/AD, anti-access/area-denial, зони заборони доступу, блокування району, застосування збройних сил, Східноєвропейського ТВД.*

Вступ

Постановка проблеми. На сучасному етапі розвитку розбудови Збройних Сил України в умовах збройної агресії РФ актуальними є завдання щодо забезпечення спроможності максимальної реалізації бойового потенціалу військ (сил) в умовах комплексного впливу противника. ЗС РФ протягом останніх 10

років за рахунок прийняття на озброєння зенітних ракетних комплексів С-400, ракетних комплексів “Іскандер” впровадили комплексне застосування різновидових сил під надійним прикриттям від ударів з повітря, що забезпечує максимальну реалізацію бойового потенціалу наземного компонента. При цьому, здійснено акцент на “блокуванні” зони проведення операції у повітряному просторі. Головна особливість зон A2/AD у тому, що ешелонована побудова системи ППО за рахунок залучення всіх рівнів засобів зенітних ракетних засобів (дальньої, середньої, малої дальності та ближньої дії), засоби РЕБ, засоби кібернетичного впливу, застосування космічного угруповання створюють умовну “сферу”, яка унеможливлює завоювання панування авіацією противника у повітрі на потрібний час у визначеному районі. У той же час під прикриттям “захисної сфери” тактичні ракетні системи, системи протикорабельного захисту, системи РСЗВ здійснюють вогневий вплив по наземному та морському компоненту угруповання противника. У комплексі ці фактори створюють сприятливі умови для застосування оперативно-тактичних, тактичних угруповань в умовах вогневої підтримки артилерії, РСЗО.

Для дослідження та вибору раціональних способів дій військ (сил) в умовах комплексного впливу угруповання військ противника, що створює зону заборони доступу та блокування району є необхідність провести аналіз A2/AD, визначити її вплив на ЗС України.

Аналіз останніх досліджень та публікацій. Аналіз джерел [1-6] свідчить, що проблема визначення раціональних способів та форм застосування сил та засобів угруповань військ під час виконання завдань в межах зони A2/AD є актуальною. В [3-5] розглянуто вплив створених зон A2/AD на потенційні можливості сил та засобів НАТО на Східноєвропейському ТВД. Аналіз впливу зон A2/AD на застосування Збройних Сил України було розглянуто частково. Питанню впливу системи зон заборони доступу та блокування району, що розгорнута навколо території України на бойову спроможність ЗС приділено уваги недостатньо. Саме тому існує потреба у дослідження зазначеного питання.

Мета доповіді. Тому метою даної статті є:

по-перше, проаналізувати вплив створених та перспективних зон A2/AD РФ на застосування ЗС України на Східноєвропейському ТВД;

по-друге, визначити перспективні напрямки дослідження з метою визначення форм та способів застосування сил та засобів угруповань військ сил оборони України.

Виклад основного матеріалу

Що під собою розуміють термін “A2/AD” – anti-access/area-denial, що перекладається як зона заборони доступу та блокування району [1].

Використання зазначеного терміну воєнними експертами у сучасній наукових виданнях почалося з прийняття на озброєння Росією та Китаєм удосконалених оперативно-тактичних ракетних систем, зенітних ракетних комплексів великої дальності та протикорабельних ракетних комплексів та залучення їх у єдину бойову систему, що забезпечує їх комплексне застосування. Це дозволило створювати “захисну сферу”, у якій війська імовірного противника

не будуть мати можливість проникнути без ризику отримання критичного збитку.

У відкритих джерелах A2/AD, (anti-access and area denial – зона обмеження доступу та заборона маневру) визначається як – концепція стримування противника (звичайним комплексом озброєння) шляхом створення підвищеної небезпеки для дислокування або переміщення сил та засобів противника у район, що знаходиться під захистом системи A2/AD [1-5]. Вона включає в себе сили та засоби: протиповітряної та берегової оборони, наступального озброєння першого удару (ракети малої та середньої дальності) крилаті ракети і інше високоточне озброєння.

Впровадження зазначеної концепції застосування сил та засобів ЗС РФ є відповіддю на форми і способи ведення бойових дій, що використовують коаліційні сили НАТО у останніх збройних конфліктах [4-5].

Відповідно до існуючих сценаріїв завоювання панування в повітрі та подавлення ППО, авіаційні удари повинні вивести з ладу командні пункти і системи військового та державного управління, критичні елементи інфраструктури паралізувавши процес управління військами, наступною ціллю повинні стати артилерійські і тактичні ракетні частини та підрозділи, а силам армійської авіації залишається зачистити осередки організованого спротиву збройних сил, знищівши механізовані, танкові частини, підрозділи потенційного противника [3-5].

Роз’єднані і дезінтегровані сили, що залишилися без управління, стануть вже легкою здобиччю для наземної складової наступаючого угруповання, які безперешкодно маневрують в умовах панування в повітрі своєї авіації а також в інформаційному і розвідувальному просторі.

Запропонована концепція є значною загрозою для проведення вищезазначеного сценарію. Основна небезпека зон A2/AD якраз в тому, що розвинені, ешелоновані системи ППО всіх рівнів (великої, середньої, малої дальності та ближньої дії), просунуті системи РЕБ і кібератаки створюють своєрідну “сферу” яка гарантує прикриття визначеного району проведення операції від “панування” ВПС НАТО (а також, можливо, супутникового угрупування) на визначеній час [2-3].

У свою чергу, під прикриттям захисної “сфери” у повітряному просторі, системи протикорабельного захисту, тактичні ракетні системи і РСЗО “сковують” або знищують наземний і морський компонент, а також наземні елементи авіаційного угруповання противника у межах досяжності РВіА.

Зазначені фактори створюють ідеальні умови для застосування оперативно-тактичних, тактичних угруповань, для яких основою є стрімки удари танкових і механізованих частин в умовах масштабної підтримки артилерії і РСЗО.

Подібна ситуація створює настільки серйозні ризики для дії ЗС держав, що країни НАТО вже зараз проводять ряд державних програм, з метою усунення зазначені критичні уразливості.

На даний час військові аналітики визначають наступні зони A2/AD [1,3,5]: Калінінград; Мурманськ, Полярний; Санкт-Петербург; Москва;

Севастополь; Новоросійськ; Новосибірськ; Владивосток; Находка; Петропавлівськ-Камчатський; Нова Земля; Тіксі; Авіабаза “Хемеймим” в Латакії (Сирія).

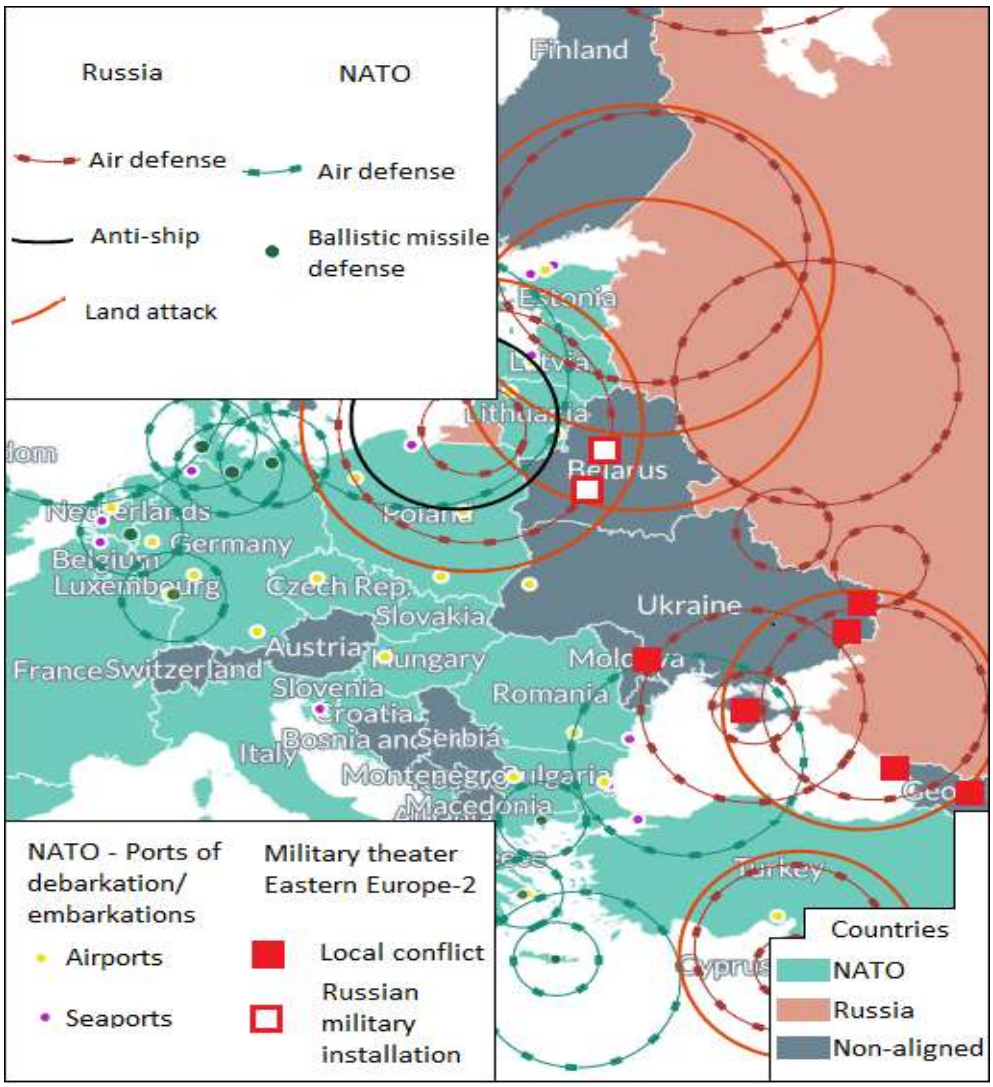

Рис. 1 Середня і Східна Європа: A2/AD системи НАТО і Росії. (Джерело: карта складена на підставі відкритих ресурсів Центру стратегічних міжнародних досліджень, Вашингтон, США)[6].

На підставі проведеного аналізу наявних джерел інформації, аналітичних оглядів експертів, можливо визначити основні особливості впливу впровадження РФ концепції A2/AD на умови, в яких ЗС України доведеться виконувати завдання оборони держави з урахуванням можливості допомоги країн НАТО, а саме [1-6]:

Російські A2/AD заходять в простори восьми країн НАТО: Естонії, Латвії, Литви, Польщі, Румунії, Туреччини, Норвегії, Німеччини.

Збройні конфлікти (Україна, Грузія) знаходяться як би “під сферами” протиповітряних і наземних A2/AD систем РФ.

Російські системи A2/AD зі сходу, півдня щільно охоплюють Україну. Можливо спрогнозувати створення такої зони і на території Білорусії. Це дозволить завершити охоплення території України і з півночі та накрити

оперативний напрямок зі сторони Польщі. Наслідком чого стане проблематичне використання аеропортів у Кракові і Львові для перекидання спорядження, а можливо і військ НАТО до України. У цьому може виникнути необхідність у разі ескалації.

Встановлені на окупованому півострові Крим російські системи A2/AD спроможні блокувати доступ по морю в українські морські порти (Одеса, Миколаїв, Херсон) і до Молдови через гирла Дністра і Дунаю. У разі кризи використання морських портів і аеропортів – Естонії, Латвії, Литви, Польщі і Туреччини може бути ускладнено. Нарощування сил та засобів НАТО для безпосередньої підтримки ЗС України можуть зіграти критичну роль у разі ескалації збройного конфлікту з РФ.

Висновки

На підставі вище зазначеного та враховуючи наявні сили та засоби, які знаходяться на озброєнні ЗС України, пропонуються напрямки розвитку форм та способів застосування для спроможності максимально реалізувати свій бойовий потенціал, а саме:

застосування здійснювати на базі міжвидових оперативних угруповань, що надає можливість підібрати раціональний комплект сил та засобів у відповідності до противника та створити свої локальні зони A2/AD на загрозливих напрямках;

використання звичайних боєприпасів та безпілотні системи на тактичному та оперативних рівнях для розвідки та вогневого впливу, що дозволить скувати систему та перейняти ініціативу;

високоманеврений бій на всіх рівнях. Кожний підрозділ, пункт управління, яке виявлене та знаходиться на місті протягом певного часу буде виведено з ладу. Маневр значно ускладнює націлювання і являється простим засобом нейтралізувати загрозу виявлення та знищення;

розробка та впровадження заходів безпеки операції, бойових дій – пасивний захист. Скритність та введення противнику в оману – зазначені процеси в умовах сучасної боротьби займають одне з важливих місць у досягнені поставлених цілей.

створення розвідувально-ударних систем. Основним принципом ведення бойових дій повинно стати процес виявлення противника та його знищення в най коротший термін.

Як підсумок, потрібно зазначити, що проблема успішного ведення бойових дій в умовах впливу зони A2/AD для ЗС України є актуальною та потребує подальшого ретельного дослідження.

Список літератури

1. A2/AD, wikipedia (електронний ресурс) URL: https://uk.wikipedia.org/wiki (дата звернення 14.11.2021).

2. Kazianis, Harry. Anti-Access Goes Globa (електронний ресурс) URL: http://the-diplomat.com/flashpoints-blog/2011/12/02/anti-access-goes-global/ дата звернення 14.11.2021).

3. Glen E. Howard, Lithuania’s key role in countering Russian A2/AD challenge to Baltics The Jamestown Foundation Wednesday, March 2, 2016 (електронний ресурс) URL: https://www.delfi.lt/en/politics/lithuanias-key-role-in-countering-russian-a2ad-challenge-to-baltics.d?id=70576206/ дата звернення 10.11.2021).

4. Admiral John Richardson is the 31st Chief of Naval Operations Chief of Naval Operations Adm. John Richardson: Deconstructing A2AD. October 3, 2016 (електронний ресурс) URL: https://www.delfi.lt/en/politics/lithuanias-key-role-in-countering-russian-a2ad-challenge-to-baltics.did70576206/ дата звернення 27.10.21).

5. Алексей Леонков. Вне зоны доступа: система A2/AD стала камнем преткновения для НАТО. Арсенал Отечества, 08.10.2019, (електронний ресурс) URL: https://rg.ru /2019/10/08/vne-zony-dostupa-sistema-a2ad-stala-kamnem-pretknoveniia-dlia-nato.html.

6. Kathleen Weinberger. Russian A2AD systems deployment – August 2016 Chart. Institute for the Study of War, (електронний ресурс) http://iswresearch.blogspot.com/2016/08/russian-anti-access-and-area-denial.html.

Передумови та чинники впливу на розвиток так званого “військово-патріотичного виховання” на тимчасово окупованих територіях України

Ігор Підопригора, доктор філософії
Викладач кафедри суспільних наук Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-7764-3675

Анотація. *Розкрито передумови, що сприяли розгортанню так званого "військово-патріотичного виховання" на тимчасово окупованих територіях Донецької та Луганської областей, та чинники впливу на нього після 2014 року.*

Ключові слова: *гібридна агресія Російської Федерації проти України, тимчасово окуповані території Донецької та Луганської областей, військово-патріотичне виховання.*

Вступ

Постановка проблеми. Одним із аспектів гібридної агресії Російської Федерації (РФ) проти України є зміна ідентичності населення тимчасово окупованих територій для його ширшого залучення до збройної боротьби та створення ілюзії громадянської війни в Україні. Тому доцільність розгляду передумов і чинників впливу на розвиток так званого “військово-патріотичного виховання” населення на тимчасово окупованих територіях викликана необхідністю прогнозування її можливих наслідків у майбутньому та вироблення пропозицій щодо їх нейтралізації.

Аналіз останніх досліджень та публікацій [1-2, 7-8] засвідчив, що попри наявність в Україні значного масиву наукових досліджень та публіцистичних матеріалів про гібридну війну та збройну агресію РФ проти України, їх автори не зосереджують достатньої уваги на питаннях зміни ідентичності населення тимчасово окупованих територій України шляхом організації так званого “військово-патріотичного виховання”.

Мета доповіді полягає у висвітленні передумов виникнення та виявленні чинників впливу на розвиток так званого “військово-патріотичного виховання” на тимчасово окупованих територіях України, що, на нашу думку, в подальшому сприятиме обранню дієвих шляхів протидії діяльності противника щодо зміни ідентичності населення тимчасово окупованих територій.

Виклад основного матеріалу

Опираючись на аналіз розвитку суспільно-політичних процесів у регіонах [1, 7, 12], передумовами, які сприяли виникненню так званого “військово-патріотичного виховання”, були наступні.

1. Особливості “радянського” періоду розвитку до 1991 року, що сприяли формуванню особливої регіональної ідентичності населення Донецької та Луганської областей, коли особливе місце Донбасу як важливого індустріального центру країни сформувало особливе бачення населенням своєї ролі. Наслідком цього періоду є почуття ностальгії за радянським минулим, соціальними стандартами того періоду, які давали впевненість у завтрашньому дні [1, с. 9-10; 2, с. 13]. Також у той час система виховання населення носила наднаціональний характер, уніфікуючи представників різних народів [3, с. 120].

2. Наявність ідеологічного підґрунтя і просування ідей для розвитку сепаратистських настроїв і відокремлення від України, зокрема просування ідей сепаратизму та федералізму, створення та забезпечення діяльності громадських і політичних організацій для реалізації зазначених ідей; фальсифікація історії України з метою ідеологічного обґрунтування проросійського сепаратизму в Автономній Республіці Крим, Донецькій і Луганській областях; активне апелювання до православної ідентичності населення та протистояння чужим західним цінностям з боку представників домінуючої у регіоні релігійної конфесії (Української православної церкви Московського патріархату). Це сприяло різнополярній ідентичності населення на Сході України - радянській, російській, релігійній, невизначеній. Крім того, впровадженню і функціонуванню на тимчасово окупованих територіях видозміненої копії чинної в РФ владної моделі (що ґрунтується на тотально корумпованих політико-суспільних відносинах) сприяло культивування серед населення регіону кримінальної свідомості. Тому тимчасово окуповані території й надалі будуть маргіналізуватися [1, с. 7, 19; 2, с. 13-22; 3, с. 35; 4].

3. Наявність груп населення, потенційно готових сприймати проросійські ідеї. Зокрема у регіоні до 2014 року проживала значна кількість етнічних росіян (38,2 % у Донецькій області та 39 % у Луганській) і російськомовного населення, більшість якого була зорієнтована на російські традиції та радянські цінності [2, с. 18].

4. Особливості політики РФ на пострадянському просторі та безпосередньо стосовно України, як ключового елементу антиросійської політики США/НАТО щодо Росії; намагання всіляко утримати Україну поза зоною європейської/євроатлантичної безпеки та у сфері російського впливу; намагання Росії за допомогою успіхів у локальних конфліктах на пострадянському просторі підтвердити претензії на глобальне лідерство; збереження права втручатися у внутрішні справи суверенних держав і здійснювати силові дії на пострадянському просторі у довгостроковій перспективі; усталена російська практика щодо заморожування конфліктів на пострадянському просторі з метою збереження своєї присутності у ключових регіонах чи продовженні здійснення впливу на новостворені держави. Усе це у поєднанні з небажанням Росії нести відповідальність за агресію перед світовою спільнотою в подальшому сприяло заморожуванню конфлікту та перетворенню тимчасово окупованих територій Донецької та Луганської областей на інструмент дестабілізації внутрішньої ситуації в Україні [1, с. 15; 2, с. 11; 5-6; 7, с. 22].

5. Завдяки домінуванню РФ в інформаційному просторі регіону були успішно здійснені: інформаційна кампанія з дискредитації українського Євромайдану і Революції гідності в кінці 2013 на початку 2014 років, дискредитація ідеї української державності та стимулювання сепаратизму на Сході України, проведення інформаційних і психологічних операцій проти Збройних Сил України [1, с. 15; 2, с. 14-15].

6. Збройна агресія РФ проти України, окупація нею Автономної Республіки Крим, окремих районів Донецької та Луганської областей.

Також важливими передумовами були наявність у регіоні розгалуженої мережі навчальних закладів і функціонування в радянський період Донецького вищого військово-політичного училища, що в подальшому стало матеріальною базою так званого "військово-патріотичного виховання".

Окремо слід враховувати цілеспрямований прихований вплив з боку РФ на військово-патріотичне виховання у Збройних Силах України у період до 2014 року [3, с. 154]. Це, у поєднанні з доволі низьким рівнем матеріального та соціального забезпечення військовослужбовців, сформувало негативне ставлення у певної частини жителів регіону, які пройшли службу у Збройних Силах України, до збройного захисту держави.

Чинниками впливу на розвиток так званого "військово-патріотичного виховання" на тимчасово окупованих територіях доцільно вважати наступні.

1. Необхідність прикриття агресії проти РФ проти України шляхом спотворення реальності та створення ілюзії громадянської війни в самій Україні [2, с. 25]. У зв'язку з чим виникла необхідність широкого залучення населення регіону до збройної боротьби проти України. Тому одразу ж після встановлення контролю над тимчасово окупованими територіями, РФ почала створювати відповідні умови для залучення місцевого населення до бойових дій у складі терористичних організацій "ЛНР" та "ДНР" задля формування хибних оцінок і негативного ставлення інших держав і міжнародних інституцій та населення самої РФ до подій в Україні.

2. Створення незаконних збройних формувань на тимчасово окупованих територіях і необхідність їх комплектування місцевим населенням [5, с. 7, 11-12, 27; 8, с. 33-37]. З огляду на недостатню підтримку дій РФ місцевим населенням весною 2014 року вона була змушена застосовувати підрозділи сил спеціальних операцій, а влітку 2014 року вводити регулярні збройні сили для зупинки наступу Збройних Сил України. Разом із тим потенційно недостатня чисельність збройних сил РФ для забезпечення окупації значних територій України, брак підготовлених мобілізаційних ресурсів та великі втрати російських військ стимулювали використання Росією матеріальних та ідеологічних засобів для вирішити проблеми комплектування збройних формувань терористичних організацій "ЛНР" та "ДНР".

3. Економічна криза на тимчасово окупованих територіях (зниження рівня життя населення, занурення населення в процес перманентного забезпечення базових потреб, відсутність перспектив економічного розвитку, зниження рівня науки і освіти до мінімально необхідного для забезпечення діяльності терористичних організацій "ЛНР" та "ДНР"), неспроможність РФ забезпечити

економічний розвиток тимчасово окупованих територій і гідний рівень життя населення. Тому краще, у порівнянні з іншими верствами населення, матеріальне становище учасників незаконних збройних формувань терористичних організацій “ЛНР” та “ДНР” стало економічною передумовою їх комплектування місцевим населенням [9, с. 218-222].

4. Створення на тимчасово окупованих територіях засобів масової інформації підконтрольних РФ терористичних організацій (телебачення, радіо, друкованої пропаганди), символічне наповнення інформаційного поля тимчасово окупованих територій (заміна символіки, створення ідеалу “захисника”, створення пантеону “героїв”, створення орієнтирів - формування образу ворога, образу союзників та образу жертви), використання ефекту інформаційного вакууму стало підґрунтям для інформаційного супроводження збройної агресії проти України і маніпулювання настроями та поведінкою місцевого населення [1, с. 15; 3, с. 179-180; 9, с. 218-222; 10].

5. Відсутність в української влади достатніх ресурсів для переселення великої кількості громадян з тимчасово окупованих територій в інші регіони держави та забезпечення для них кращих умов життя.

Також, з огляду на проведене раніше теоретичне осмислення військово-патріотичного виховання [11, с. 225-230] та характер діяльності РФ на тимчасово окупованих територіях України [2, с. 32-33; 12, с. 115-128, 449-450, 475-488] є всі підстави стверджувати, що так зване “військово-патріотичне виховання” є частиною інформаційних і психологічних операцій щодо зміни ідентичності населення тимчасово окупованих територій спочатку на місцеву регіональну, а в подальшому на російську.

Висновки

Таким чином, можна констатувати, що станом на початок 2014 року було створено ідеологічні, соціально-політичні та інформаційні передумови, а з квітня 2014 року – реальні умови для здійснення так званого “військово-патріотичного виховання” населення тимчасово окупованих територій Донецької та Луганської областей.

З’ясування сутності військово-патріотичного виховання, врахування особливостей військово-патріотичного виховання у Збройних Силах України, аналіз характеру діяльності РФ на тимчасово окупованих територіях України дозволяють стверджувати, що так зване “військово-патріотичне виховання” на тимчасово окупованих територіях є частиною інформаційних і психологічних операцій РФ проти України. Кінцевою метою цих операцій є зміна ідентичності населення тимчасово окупованих територій (за період з 2014 року на тимчасово окупованих територіях України з’явилося нове покоління громадян, яке, включаючись у соціальне життя через місцеві заклади освіти, виховується в умовах антиукраїнської пропаганди й інтеграційних процесів із Російською Федерацією).

Список літератури

1. Березовець Т., Кравченко В., Каракуц А., Доброєр О. (2016), Два роки з початку АТО та гібридної війни РФ проти України : Провал путінського бліц-кригу. Частина 2. Київ, 75 с.
2. Біла книга антитерористичної операції на Сході України 2014–2016 (2017). Київ, 250 с.
3. Пашкова О.О. (2021), Військово-патріотичне виховання курсантів вищих військових навчальних закладів України (1991–2019). Київ, 312 с.
4. В'ячеслав Яремчук (2017), Україна у протидії новітній релігійно-інформаційній експансії з боку РПЦ. Наукові записки ІПіЕНД ім. І.Ф. Кураса НАН України, випуск 5-6 (79-80), С. 127-145.
5. Бєлєсков М. М. (2021), Сучасний російський спосіб ведення війни: теоретичні основи і практичне наповнення. Київ, 29 с.
6. Горєлов В., Клименко В., Дерікот О., Кидонь В. (2021), «Заморожені» конфлікти в геополітиці РФ: історія та реальність для України (1991–2020 рр.). Воєнно-історичний вісник, № 2(40), С. 99-110.
7. Біла книга 2021. Служба зовнішньої розвідки України (2021). Київ, 74 с.
8. Илья Яшин, Ольга Шорина (2015), Независимый экспертный доклад «Путин. Война». Москва, 66 с. www.putin-itogi.ru.
9. Гірник А.М. (2018), Життя на тимчасово окупованих територіях: як його бачать мешканці Донецької та Луганської областей. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення. Маріуполь, 331 с.
10. Ігор Підопригора (2018), Ефект інформаційного вакууму як чинник впливу на організацію інформаційно-пропагандистського забезпечення Військово-Морських Сил Збройних Сил України у лютому–березні 2014 року. Військово-історичний меридіан, № 1 (19), С. 64–78.
11. Ihor Pidopryhora, Olha Pashkova (2021), Theoretical foundations of military-patriotic education. Філософсько-соціологічні та психолого-педагогічні проблеми підготовки військового професіонала у глобалізованому світі. Київ, 380 с.
12. Підопригора І.І. (2020), Інформаційно-пропагандистське забезпечення у Військово-Морських Силах Збройних Сил України у 1992–2014 роках. К.; 615 с.

Моделювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері

Віталій Кацалап, кандидат військових наук, доцент

Доцент кафедри застосування інформаційних технологій та інформаційної безпеки, інституту забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0003-4804-8022

Андрій Прима, доктор філософії

Начальник науково-дослідного відділу науково-дослідного управління Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0002-0776-6864

Микола Прима

Науковий співробітник науково-дослідного відділу науково-дослідного управління Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,

Київ, Україна

https://orcid.org/0000-0002-8363-1929

Анотація. *Запропоновано методичний підхід щодо визначення змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері, який на відміну від існуючих враховує характеристику можливої загрози за рахунок функціонального зрізу ієрархічної структури органу управління.*

Предмет дослідження – моделювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері.

Мета доповіді – викладення підходу щодо моделювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері який, на відміну від існуючих, враховує інформаційну можливість складових сил оборони України на основі передових інформаційних технологій.

Методи досліджень – для вирішення завдань моделювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері застосовувалися методи системного аналізу, синтезу, узагальнення.

Основні результати досліджень:

визначено характеристики змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері;

наведено порядок моделювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері;

формалізовано послідовність оцінювання зовнішнього інформаційного середовища.

Результати тез доповіді можуть бути використані у якості практичних рекомендацій щодо вибору методологічних рішень для оцінювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері.

Ключові слова: *загрози інформаційній безпеці, виклики, інформаційні загрози, модель оцінки, воєнна сфера, інформаційна сфера.*

Вступ.

Постановка проблеми. Забезпечення ефективного управління силами оборони України вимагає своєчасного реагування на виклики інформаційних загроз національній безпеці держави у воєнній сфері. Аналіз загроз та викликів інформаційній безпеці наведений у Стратегії інформаційної безпеки України [1].

На сьогоднішній день відповідно до Стратегії інформаційної безпеки України в інформаційні сфері розглядають такі виклики та загрози: збільшення кількості глобальних дезінформаційних кампаній; інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав; соціальні мережі як суб'єкти впливу в інформаційному просторі; недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій; інформаційний вплив Російської Федерації як держави-агресора на населення України; інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України; обмежені можливості реагувати на дезінформаційні кампанії.

Зазначене впливає на спроможності держави щодо забезпечення її національній безпеки у воєнній сфері.

Аналіз останніх досліджень та публікацій [2-4] показав, що зміст викликів інформаційних загроз національній безпеці держави у воєнній сфері здебільшого характеризується такими діями над інформацією, як зберігання, використання та її поширення.

Тому використання Російською Федерацією технології інформаційного втручання в будь-яке повідомлення може стати змістом виклику інформаційній загрозі національній безпеці держави у воєнній сфері.

В такому випадку під змістом виклику інформаційних загроз національній безпеці держави у воєнній сфері будемо розуміти поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації.

Мета доповіді полягає у викладенні підходу щодо моделювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері який, на відміну враховує характеристику можливої загрози за рахунок функціонального зрізу ієрархічної структури органу управління.

Викладення основного матеріалу.

Аналіз викликів та загроз в інформаційні сфері табл.1 свідчить про наявність у кожному джерелі воєнної складової, яка формує джерело загрози інформаційній безпеці у воєнній сфері.

Таблиця 1

Аналіз викликів та загроз в інформаційні сфері

Виклики в інформаційній сфері	Загрози в інформаційній сфері
Вплив технічних засобів іноземної розвідки на політичні, економічні, військові структури	Пропаганда ворожих державі національних ідей через поширення науково-популярних і художніх фільмів, публіцистичних матеріалів, літератури, текстових музичних творів та творів образотворчого мистецтва
Концепції окремих держав щодо інформаційної та психологічної війни	Розповсюдження агітаційних матеріалів на користь протиборчої сторони в місцях дислокації частин і підрозділів військових формувань держави
Міжнародні терористичні організації та комп'ютерна злочинність	Наявність у вітчизняному інформаційному просторі продукції для впливу на індивідуальну та масову свідомість особового складу національних військових формувань з боку іноземних ЗМІ

Наведений аналіз табл.1 свідчить, що зміст викликів інформаційних загроз національній безпеці держави у воєнній сфері можуть мати деструктивний або відверто ворожий характер та спричиняють появу загроз в інформаційній сфері. Кожен виклик має свій відповідний зміст який потребує аналізу та постійного порівняння такого виклику опираючись на ефективну систему моніторингу зовнішніх і внутрішніх інформаційних загроз, завдання якої є оцінювання рівня показників цих загроз для прийняття адекватних рішень щодо підвищення рівня інформаційної безпеки держави у воєнній сфері.

Враховуючи зазначене виникає необхідність розглядати оцінювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері через рівнем виклику під яким розуміємо – кількість та змістовність інформаційних процесів (дій, фактів) за певний проміжок часу, виявлених в інформаційному просторі держави, які потенційно (за певних умов) можуть створити інформаційно-психологічну загрозу особовому складу військ (сил) [3].

Тому формалізація та оцінювання змісту виклику за допомогою точних математичних моделей і методів суттєво обмежені через:

різнорідність, розподіленість, багатозв'язність і динамічність джерел і об'єктів інформаційних загроз, що його породжують;

надто велику кількість параметрів, що відображають суспільні інформаційні відносини і характеризують відповідні інформаційні загрози;

відсутність необхідних статистичних даних внаслідок неповноти, неоперативності і недостовірності практично доступної інформації.

Саме ця аргументація свідчить на користь застосування графоаналітичних методів оцінювання змісту виклику на основі використання професійного досвіду та інтелектуальних можливостей фахівців інформаційної сфери, що дає можливість відносно адекватно "вимірювати" інформаційні процеси, які проявляються безпосередньо в певному інформаційному просторі. Цей підхід може стати основою методичної бази для створення системи моніторингу інформаційних загроз у воєнній сфері.

Таким чином, раціональним шляхом вирішення проблеми оцінювання

зміст викликів інформаційних загроз національній безпеці держави у воєнній сфері може бути застосування графоаналітичного методу оцінювання, сутність якого відома із джерела [2].

Для практичного застосування графоаналітичного методу при розробці методики потрібно мати відповідний набір процедур з метою отримання необхідних формальних методичних елементів. Для визначення таких процедур першочергово важливо структурувати ескалацію загального негативного (деструктивного) інформаційного процесу по відношенню до об'єктів впливу (від його зародження до набуття агресивних форм), що слід вважати головною передумовою для розробки моделі.

Запропонована модель оцінювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері становить теоретико-множинну форму взаємозв'язків між чинниками зовнішнього середовища і внутрішніми можливостями всіх складових сил оборони України. Врахування зазначених взаємозв'язків дозволяє окреслити правила формування логічних виразів, які надалі стануть основою методології забезпечення інформаційної безпеки у воєнній сфері.

Наведена методель описує взаємозв'язки між ієрархією інформаційного середовища та індифікаторами у вигляді графів з вершинами P_{f_1} та P_{f_2}. Значення цих вершин будуть характеризувати мету якою є виявлення на ранніх стадіях загроз інформаційній безпеці у воєнній сфері.

Використання наведених дискретних шкал дозволяє побудувати модель оцінювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері $h_{джер}$ рис. 1.

Рис. 1. Модель оцінювання змісту викликів інформаційних загроз національній безпеці держави у воєнній сфері

Для формування загроз інформаційній безпеці у воєнній сфері в наведеній методології використовуються як кількісні, так і якісні показники значення яких можна подати виразом:

$$G = \langle \{f\}, \{m\}, \{b\}, \{\square_{джер}\} \rangle$$

деf - оцінка загроз національній безпеці;

m - оцінка загроз інформаційній безпеці;

b - оцінка загроз інформаційній безпеці у воєнній сфері;

$\square_{джер}$ - оцінка джерел загроз інформаційній безпеці у воєнній сфері на основі запропонованої моделі рис.1.

Висновки

Таким, чином на відміну від існуючих підходів до моделювання зміст викликів інформаційних загроз національній безпеці держави у воєнній сфері, запропонований підхід дозволяє:

дати розгорнуту характеристику можливої загрози за рахунок функціонального зрізу ієрархічної структури;

врахувати більше число зовнішніх і внутрішніх чинників, що роблять істотний вплив у наближенні реальних процесів, що модулюються.

Врахування інформаційного протиборства з одного боку та застосуванням заходів захисту своїх систем (добування, оброблення, розповсюдження та зберігання інформації) з іншого є одним із умов підвищення ефективності управління силами оборони України.

Список літератури

1. Стратегія інформаційної безпеки. Затв. Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.

2. Макаров И.М. Теория выбора и принятия решений: Учебное пособие / И.М. Макаров, Т.М. Виноградская, А.А. Рубчинский, В.Б. Соколов. – М.: Наука, 1982. – 328 с.

3. Науково-дослідна робота шифр “Система-Р” “Удосконалення системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) та органи військового управління” 130 с.

4. Сніцаренко П.М. Методичний підхід до визначення критеріїв оцінки рівня інформаційного впливу на елементи інформаційної інфраструктури воєнної організації держави. / Ю.О Саричев, П.М. Сніцаренко, В.О. Кацалап // Збірник наукових праць військової частини А1906, № 31. – К.: Міністерство оборони України, 2011. - С. 126 – 139.

5. Кацалап В.О. Методика оцінки деструктивного інформаційно-психологічного впливу / В.О. Кацалап, П.М. Сніцаренко, Ю.О Саричев // Збірник матеріалів науково-практичної конференції Національної академії Служби безпеки України “Інформаційна безпека: виклики і загрози сучасності”. – К.: НА СБУ, 2013. – С. 338-340.

Інформаційна боротьба як невід'ємна складова гібридної війни

Максим Кіріакіді
Начальник Інституту Військово-Морських Сил Національного університету "Одеська морська академія",
Одеса, Україна
https://orcid.org/0000-0003-4050-3377
Едуард Сарафанюк, кандидат педагогічних наук, доцент
Професор кафедри гуманітарних та соціально-економічних дисциплін Військової академії (м. Одеса),
Одеса, Україна
https://orcid.org/0000-0001-9805-3474
Геннадій Білоус
Науковий співробітник НДЦ ЗСУ «Державний океанаріум» ІВМС Національного університету «Одеська морська академія»,
Одеса, Україна
https://orcid.org/0000-0002-1321-0520

Анотація: *Авторами розглянуто питання інформаційної боротьби Російської Федерації проти України та країн Заходу. Запропоновано при цьому системний підхід щодо державної інформаційної політики та забезпечення інформаційної безпеки під час гібридної війни для захисту національних інтересів та нейтралізації загроз в інформаційному просторі нашої країни.*

Ключові слова: *гібридна війна, інформаційна боротьба, інформаційна безпека, інформаційний простір.*

Вступ

Постановка проблеми. В сучасних умовах посилення збройної агресії з боку Російської Федерації (РФ) проти України значну роль у гібридній війні відіграє інформаційна складова. Україна відчула важливість інформаційного чинника після негативних наслідків проведених противником інформаційно-психологічних операцій і реалізації інформаційних загроз, що призвели до певної шкоди інформаційній інфраструктурі держави. По суті, інформаційна загроза – наміри, дії або явища, які шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси можуть ускладнити (унеможливити) реалізацію національних інтересів держави (функцій її структурних органів) [1]. Метою гібридної війни з боку агресора є подальша ескалації конфлікту та ліквідація України як самостійної держави. Сьогодні, чи то в Україні, чи у великих країнах світу, триває процес розуміння цієї нової реальності, переоцінка існуючої концепції інформаційної безпеки держави та формулювання нових механізмів боротьби з негативним інформаційним впливом. Проте аналіз діяльності РФ в інформаційному просторі показує [2–4], що заходи протидії негативному інформаційному впливу агресора не були ефективно

реалізовані в Україні та подальшому вдосконалені. На даний час забезпечення інформаційної безпеки України вимагає не лише розробки окремого механізму інформаційної протидії противнику, а й реалізації системного підходу, що включає комплекс взаємопов'язаних заходів, які випливають з проведення інформаційних операцій Росією.

Аналіз останніх досліджень та публікацій. Серед дослідників забезпечення інформаційної безпеки держави та ведення інформаційної війни заслуговують на увагу дослідження В. Божка [2], Д. Уітера [3], Я. Малик [4], В. Горбуліна [5], В. Толубка [6], А. Бедрицкого [7] та ін.

В той же час, незважаючи на значну кількість публікацій за цією тематикою, проблематика цього питання потребує подальшого розгляду. При цьому слід зазначити, загрози інформаційній безпеці держави у воєнній сфері залишаються на високому рівні, а тому, враховуючи сучасний досвід боротьби з гібридною агресією на сході України, актуальність цих зусиль потребує подальшого розгляду.

Мета доповіді полягає у розгляді стратегії російського інформаційного протиборства проти України та країн Заходу, особливостей її впровадження в українському інформаційному просторі, а також визначенні ролі та місця інформаційної зброї при реалізації противником інформаційних загроз.

Основна частина

Після вторгнення РФ на територію України, анексії нею Криму гібридна війна перестала бути предметом дослідження лише військових науковців, а увійшла до воєнно-політичної сфери як серйозний виклик національній безпеці України та західних країн. Гібридна війна – це особливий тип збройного конфлікту, в якому бойовим діям відведена другорядна роль. Задача агресора під час гібридної війни полягає у нав'язуванні противнику своєї волі шляхом застосування різних видів сили. При цьому бойові дії відіграють в ослабленні противника допоміжну роль, будучи лише каталізатором дестабілізуючих процесів, попередньо запущених за допомогою економічних, політичних, інформаційних та інших методів [2].

Одною зі складових гібридної війни стала інформаційна боротьба, під час якої, перш за все, державні і недержавні суб'єкти агресора через інформаційний простір спрямовують свої дії проти політичних керівників і громадськості іншої країни. Перетворення інформації на зброю є найбільш відмінною рисою російської компанії 2014 року, та недавніх зусиль РФ по розділенню і дестабілізації західних країн в умовах еміграційної кризи [3]. При цьому під інформаційною зброєю розуміється сукупність способів, прийомів, засобів і технологій інформаційного впливу, призначених для нанесення збитку (ураження) елементам інформаційної інфраструктури противника в ході ведення інформаційної боротьби [1].

Російський підхід до інформаційної боротьби поєднує інформаційно-психологічні і інформаційно-технічні (кібернетичні) акції (операції), які є ключовими елементом того, що російські аналітики називають "війною нового покоління". У війні нового покоління ставка робиться на використання

некінетичних методів, які провокують суспільну незадоволеність і створюють атмосферу колапсу, де застосовується зовсім невелика кількість військової сили. Розвиток інформаційних технологій передачі і обробки інформації в значній мірі дозволили РФ на повну силу використовувати пропаганду і дезінформацію як методи досягнення своїх цілей. Розуміння наслідків російської інформаційної боротьби дає можливість керівництву західних країн, суспільству і, що саме головне, медійним компаніям бути менш схильними до дезінформації, обману і маніпуляцій.

Основною метою інформаційної боротьби є здобуття психологічних або фізичних переваг перед противником. Найбільш вдалим, на наш погляд, визначенням інформаційної боротьби стало таке: "це вид конфлікту, при якому завданнями протиборчих сторін є захист власної інформації та інформаційних систем, маніпулювання інформацією противника або її спотворення, а також обмеження можливостей протиборчої сторони в доступі і обробці інформації" [7].

Абсолютно очевидно, що РФ усвідомлює цінність володіння інформаційним простором, особливо в період, коли будь-які новини легко доступні через офіційні і неофіційні канали розповсюдження інформації. Взявши за основу інформаційну спецоперацію, проведену під час анексії Криму, РФ активніше, ніж її противники (опоненти), і далі системно використовує інформаційний простір для розширення можливостей поширення дезінформації та ворожої пропаганди з метою досягнення своїх агресивних геополітичних цілей. При цьому РФ, як агресор, розглядає інформаційні операції швидше, як спосіб цілеспрямованого впливу, чим руйнівні дії (хоча ці обидва процеси не є взаємовиключними). Інформаційна зброя (засоби і технології інформаційного впливу) сьогодні дозволяє російському агресору здійснювати ураження елементів державної інформаційної інфраструктури України.

Стратегія російського інформаційного протиборства продовжує еволюціонувати, що свідчить про її динамічний характер та здатність працювати на випередження. Використання терміну "інформаційна боротьба" є визнанням критичності домінування в інформаційній сфері, яка залежить лише від контенту інформаційних ресурсів та ефективності інформаційних технологій, які застосовуються, у той час, коли використання військової та цивільної компонент багато в чому обмежено. РФ застосовує комплекс зовнішніх агресивних заходів, зокрема інформаційних, для того, щоб збільшити збентеження і невпевненість у об'єкта впливу (населення та ЗСУ). Проте, допоміжна і підтримуюча роль інформаційного протиборства, зокрема в умовах України, передбачає, що його краще використовувати не окремо, а у поєднанні з іншими конвенційними і неконвенційними діями, для досягнення максимальної ефективності масштабних дестабілізуючих інформаційних компаній (інформаційних операцій).

В той же час, постійне збільшення інформаційних потоків унеможливлює сталий контроль за ними з боку будь-якої держави. Тому провідним завданням під час протистояння в інформаційній сфері є не контроль за такими потоками, а контроль алгоритму руху інформації. Зростання ефективності заходів безпосереднього інформаційного впливу в межах загальної інформаційної

боротьби досягається шляхом встановлення контролю над інформаційним простором іншої країни, а також точності та цілеспрямованості таких інформаційних акцій (операцій). При цьому акцент робиться на визначенні необхідного обсягу і рівня негативного інформаційного впливу, а також особливостей цільових аудиторій (ступеня диференціації населення за системами матеріальних і духовних цінностей, здатності адекватно сприймати відомості та реагувати на них, а також політичної, економічної, етнорелігійної та іншої ситуації в державі й регіоні) [4].

В сучасних умовах російські фахівці взяли на озброєння весь пропагандистський арсенал колишнього Радянського Союзу. Вони вважають, що мистецтво інформаційного протиборства необхідно постійно відточувати, передивлятися час від часу і підлаштовуватися під конкретну цільову аудиторію. Тому РФ активно удосконалює свої методи інформаційної боротьби, які використовуються на даний час, оскільки вона застосовує інформаційну зброю і впроваджує її в арсенал невоєнних засобів для досягнення власних геополітичних цілей. Найбільша цінність інформаційної зброї полягає в тому, що вона може грати провідну роль залежно від конкретних завдань та умов проведення інформаційної боротьби. Ця обставина має особливе значення, оскільки для досягнення геополітичних цілей в умовах збройного конфлікту сьогодні значно зростає роль невоєнних засобів.

Висновки

1. Метою інформаційної боротьби є управління процесом зміни свідомості людей, їх світогляду, ставлення до суспільства і держави; при цьому небезпекою для людей є втрата ними власної волі, для суспільства – наявність громадської дезорієнтації, а для держави – її суверенітету.

2. В інформаційних операціях сучасності успіх буде забезпечуватися за рахунок все більшого вдосконалення інформаційної зброї.

3. Як показує практика, недостатня увага до інформаційних загроз може завдати значної шкоди політичній системі будь-якої держави аж до руйнування самої держави.

Список використаних джерел

1. Військовий стандарт ВСТ 01.004.004 – 2014 (01) “Інформаційна безпека держави у воєнній сфері. Терміни та визначення”. – [Чинний від 2014 – 02 – 27]. К.: МОУ, 2014. – 22 с.

2. Божко В. Особливості та уроки “гібридної” війни Росії проти України // [Електронний ресурс]. – Режим доступу: URL: https://bintel.org.ua/nukma/ gibridnaja_vojna (дата звернення 16.11.2021).

3. Уітер Д. Даючи визначення “гібридної” війни // [Електронний ресурс]. – Режим доступу: URL: https://perconcordiam. com (дата звернення 16.11.2021).

4. Малик Я. Інформаційна війна і Україна // [Електронний ресурс]. – Режим доступу: URL: http://www.lvivacademy.com (дата звернення 16.11.2021).

5. Проблеми захисту інформаційного простору України: Монографія / В.П. Горбулін, М.М. Биченок // Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.

6. Інформаційна безпека держави у контексті протидії інформаційним війнам. Навчальний посібник / [за ред. В.Б. Толубка]. К.: НАОУ.–2004. –315 с.

7. Бедрицький А.В. Еволюція американської концепції інформаційної війни // Аналітичні огляди: РІСІ. – 2003. № 3. – С.3.

Розповсюдження інформації в соціальних мережах – головний інструмент реалізації державного наративу

Володимир Рахімов
Ад'юнкт кафедри застосування інформаційних технологій та інформаційної безпеки Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-9868-986X

Анотація. *Соціальне середовище в якому ми безпосередньо перебуваємо, містить чималу кількість соціальних груп, які впливають на нашу поведінку, емоціональний та психічний стан. Особливу місце в процесі впливу займають процеси отримання та розповсюдження інформації. Стрімкий розвиток інформаційних технологій та поява нових форм комунікацій дали змогу збільшити кількість джерел інформації. Вивчення та дослідження процесів розповсюдження та модифікації інформації, що циркулює в соціальних медіа залишається перспективним напрямом, як для аналітиків, маркетологів так і для проведення спеціальних інформаційних та психологічних дій в інтересах застосування військ (сил).*

Ключові слова*: інформація, інформаційний вплив, медіа, стратегічні комунікації, наратив, соціальні мережі.*

Вступ

Постановка проблеми. Російські та проросійські засоби масової інформації постійно здійснюють розповсюдження викривленої інформації стосовно подій в Україні та світі в цілому. Більшість матеріалів спрямовані на дискредитацію воєнно-політичного керівництва, водночас головною метою є дестабілізація воєнно-стратегічної, воєнно-політичної та суспільно-політичної обстановки. Одним із найголовніших завдань агресора є відмова України від вступу до Європейського союзу та Організації Північноатлантичного договору.

У публікаціях Войтка О. В. та Солоннікова В. Г. вирішувалося завдання щодо наукового обґрунтування вступу до ЄС, НАТО на підставі аналізу статистичних даних громадської думки та прогнозування сценаріїв її розвитку [1–2].

Отримані прогнозні дані дозволили визначити особливості впровадження загальнодержавного наративу системою стратегічних комунікацій та реалізувати інтереси держави у вигляді підтримки населенням її стратегічного курсу для набуття повноправного членства України в Європейському союзі та Організації Північноатлантичного договору.

Аналіз останніх досліджень та публікацій. Збройну агресію Російської Федерації проти України прийнято називати "гібридною війною", яка здійснює впливи за різними напрямами на всі сфери життєдіяльності нашої держави. Дослідження "гібридних дій" залишається пріоритетним напрям, яким займається низка вітчизняних та закордонних вчених. В роботах Ланде Д.В.,

Даника Ю.Г., Сальнікової О.Ф., Сніцаренка П.М., Войтка О.В. та багато інших, висвітлено матеріали щодо форм і способів, які може використовувати агресор для досягнення своїх цілей та водночас розкривають теоретичні та практичні основи для протидії цим викликам та загрозам. Дослідження процесів розповсюдження інформації, аналіз якісних характеристик інформації відіграють важливу роль під час оцінювання цільових аудиторій та ступеня сприйняття даної інформації з різних джерел інформації.

Інтернет-сервіси дають змогу змоделювати процеси розповсюдження інформації. Автором за допомогою одного із таких сервісів (Melting Asphalt) запропоновано варіант візуалізації моделі розповсюдження інформації серед цільової аудиторії та запропоновані показники, які впливають на розповсюдження інформації у соціальній мережі [3].

Мета доповіді. Опис та візуалізація моделі розповсюдження інформації серед цільової аудиторі для реалізації державного наративу з використанням сучасних програмних сервісів.

Виклад основного матеріалу

Процес розповсюдження інформації складається з безпосереднього розповсюдження інформації з різних джерел в мережі та зміни думок агентів (користувачів) мережі про висвітлену інформацію. Водночас процес розповсюдження інформації в соціальній мережі крізь вузли зв'язків опосередковано можна порівняти з процесом розповсюдження вірусів (епідемій). Враховуючи новизну, час подачі та актуальність інформації швидкість її розповсюдження набирає великої інтенсивності, так починаючи з невеликих груп розповсюдження інформації охоплює більші соціальні групи та після набуття свого максимуму поступово або швидко йде на спад [4–5].

Базову модель розповсюдження інформації в медіа можна представити як сукупність комунікаційних вузлів (кількість користувачів соціальної мережі), ребер (зв'язки між користувачами та іншими медіа) та активних вузлів (агенти впливу або розповсюдження інформації) (рис.1).

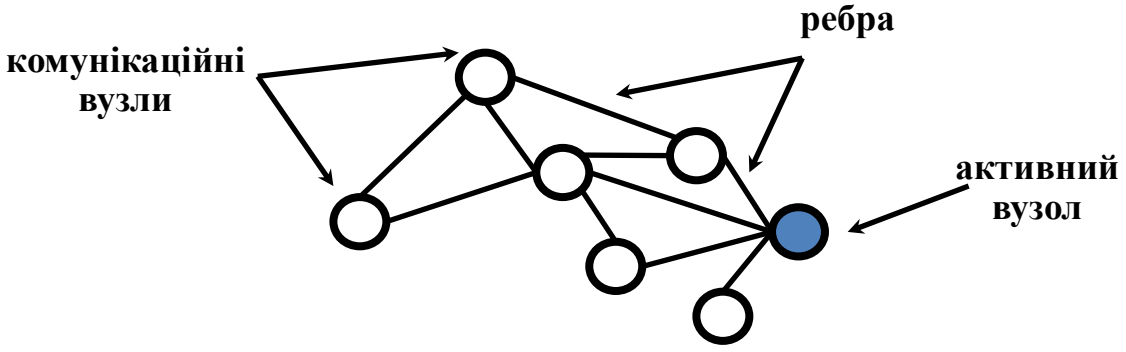

Рис.1 Базова модель розповсюдження інформації

Аналіз використання медіа в інформаційному просторі України дав змогу визначити, що отримання інформації (новин) з традиційних джерел (телебачення, радіо, друковані видання) систематично зменшується з кожним роком. Це об'єктивний перерозподіл структури споживання, пов'язаний з

розповсюдженням Інтернету та підвищенням його доступності для потенційної аудиторії, а саме користувачів соціальних мереж. Так користувачі Інтернету, які використовують соціальні мережі кожен день, у 2021 році в нашій державі склало 82%, а серед молодих людей у віці 18-35 років 97%. Останні кілька років спостерігається не тільки зростання частки споживачів, які дізнаються новини із Інтернету, та зменшення долі тих, хто використовує для цього телебачення, а і зменшення частки тих, хто використовує обидва джерела одночасно.

Так, у 2021 році споживачі новин в онлайн-медіа та соціальних мережах, які не дивляться новини на ТБ, склали 29% цільової аудиторії (рис.2) [6].

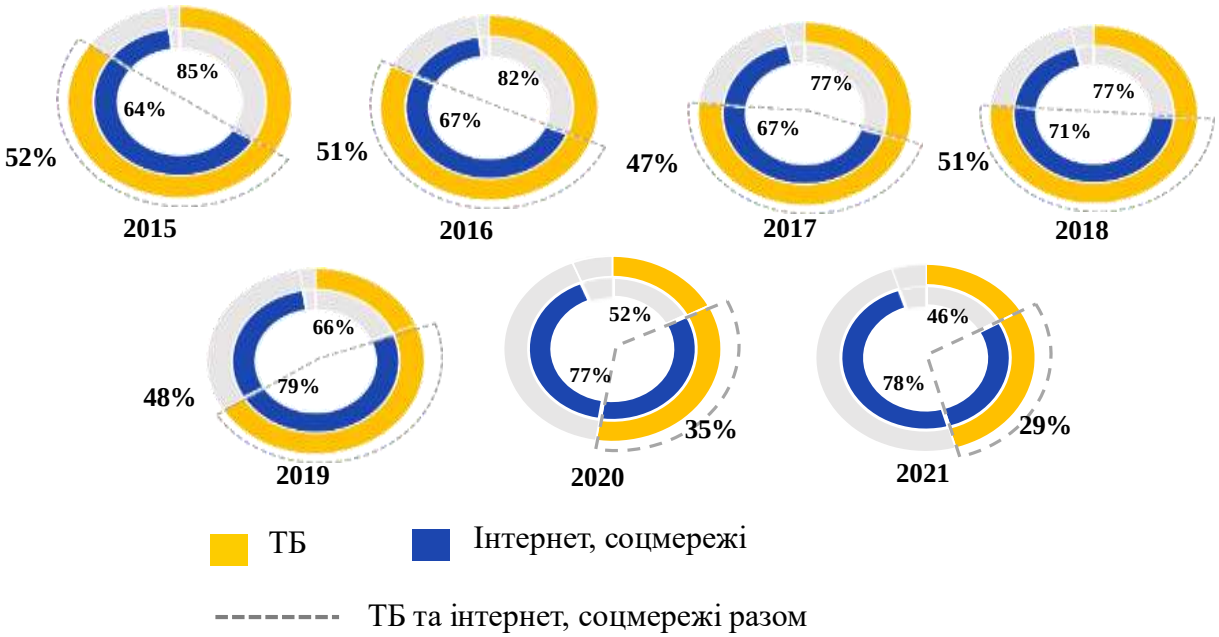

Рис.2 Використання медіа для отримання інформації (новин) протягом 2015-2021 років в інформаційному просторі України

Статті, коментарі, “репости”, аудіо, відео та інше інформаційне наповнення є основою сучасних соціальних мереж. Різноманітність інформації, можливість створення, модифікації та просування свого контенту все більш приваблює певну категорію користувачів, які в подальшому виступають в ролі блогерів (агентів впливу) та ставлять перед собою завдання осягнути як можна більшу цільову аудиторію (залучення нових користувачів та утримання старої аудиторії).

Отже, використання моделі розповсюдження епідемії дає можливість представити інформаційну одиницю як вірус, який у часі інфікує все більшу частку людей та певних цільових аудиторій, завдяки їхньої комунікації один з одним. Водночас необхідно врахувати, що вірус має деякий життєвий строк та деяка цільова аудиторія має імунітет, тобто мають стійкість до певного типу інформації.

В основі моделі розглядаються три основні групи людей, на які розбивається загальна кількість людей в соціальній мережі. Наприклад, кількість користувачів в певній соціальній мережі можна визначити як:

$$N(t) = S(t) + I(t) + R(t),$$

де: N(t) – загальна кількість користувачів;
S(t) – кількість користувачів, які сприймають інформацію але не здійснюють ніякої діяльності в соціальній мережі (репост, коментар);
I(t) – кількість користувачів, які отримали інформацію, і її розповсюджують;
R(t) – кількість користувачів, які мають психологічний бар'єр до інформації та не сприймають інформацію.

Водночас для візуалізації та побудови відповідних графіків щодо розповсюдження інформації необхідно розглянути низьку коефіцієнтів, які будуть безпосередньо впливати та модель розповсюдження інформації, а саме [7]:

β – параметр, який відображає швидкість передачі інформації новим агентам, або ймовірність передачі інформації при комунікації між агентами серед цільової аудиторії;

γ – параметр, який відображає швидкість втрати цікавості до інформації за час розповсюдження інформації , тобто інформація стає не цікавою для цільової аудиторії оскільки втратила свою цінність та актуальність.

λ – інтенсивність підписування на новинного агента;

μ – інтенсивність відписування від новинного агента;

ξ – інтенсивність прочитування новини.

Для візуалізації моделі розповсюдження інформації обрано сервіс програмного забезпечення Melting Asphalt який в 2020 році був використаний для проведення досліджень моделі розповсюдження COVID-19. Враховуючи базову систему рівнянь моделі розповсюдження інформації та систему критеріїв та показників дає змогу отримати мінімальні та максимальні значення для ефективного розповсюдження визначеної інформації [3]. Візуалізація процес розповсюдження інформації серед цільових аудиторій відображена рисунку 3 (параметри, які впливають на розповсюдження інформації обрано випадково).

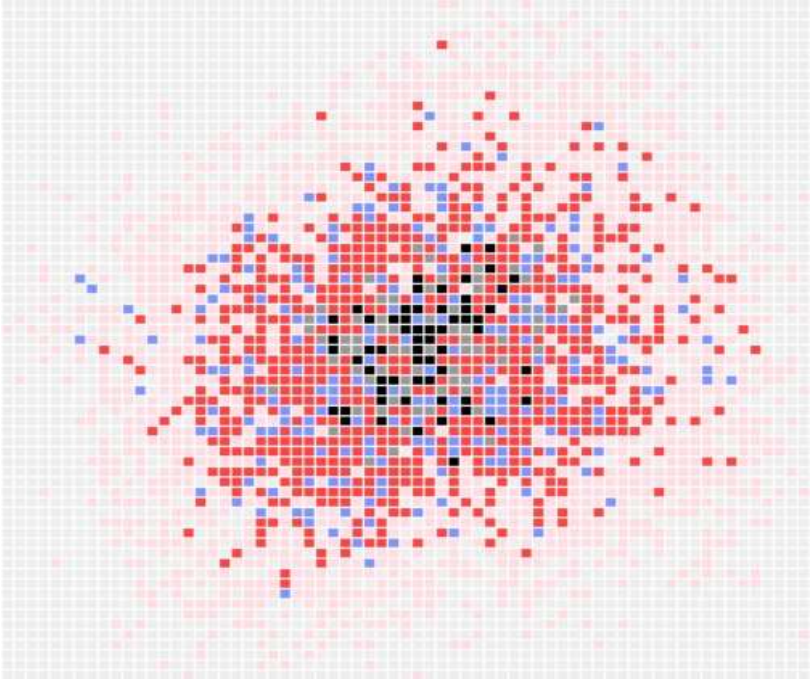

Рис. 3а. Дискретна візуалізація розповсюдження інформації

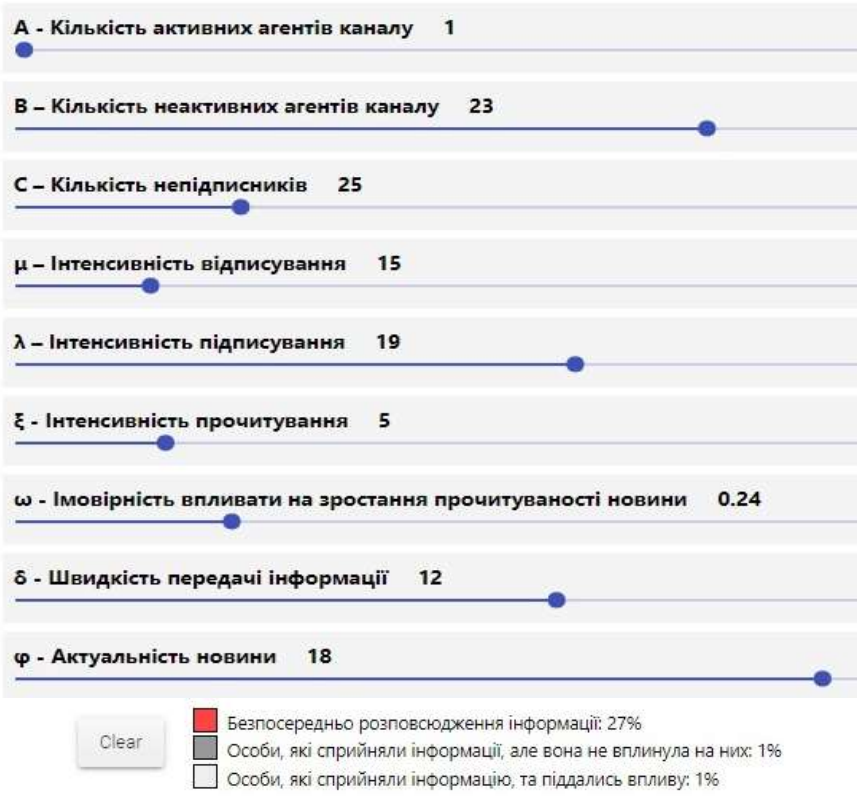

Рис. 3б. Показники та критерії які впливають на розповсюдження інформації
Рис. 3. Візуалізація моделі розповсюдження інформації

Висновки

Подальше дослідження моделі розповсюдження інформації надасть можливість визначити додаткові критерії та показник, які будуть впливати на ефективність заходів щодо реалізації стратегічного наративу держави. Водночас в подальшому досліджені необхідно враховувати той факт, що відсутність тривалого аналізу інформації та короткочасний емоційний сплеск дає змогу привернути увагу різним категоріям суспільства та викликати стрімке зростання коментарів та інших видів діяльності, але така інформація може також швидко втратити свою актуальність, що буде враховано під час її оновлення (підсилення), або заміни загалом, аналогом можуть бути фейкові новини. Реакції користувачів на отриману інформацію та інші фактори, які впливають на її розповсюдження дають змогу визначити найбільш вигідний час на її висвітлення, що безпосередньо буде впливати на розповсюдження інформації.

Отже, враховуючи на стратегічний курс держави щодо вступу до ЄС та НАТО, використовуючи інструментарій та враховуючи зазначені показники моделі розповсюдження інформації серед цільової аудиторії, ми можемо змоделювати процес розповсюдження інформації та прогнозувати варіанти реалізації стратегічного наративу державного. Водночас це дає змогу визначити загальні підходи в системі планування Збройних Сил України .

Список літератури

1. Войтко О. В., Солонніков В. Г., Полякова О. В. Особливості застосування методу фрактального аналізу сталості процесу розвитку громадської думки при реалізації стратегічного наративу держави. Сучасні інформаційні технології у сфері безпеки та оборони. 2020. №2(38). С. 145-150.
2. Солонніков В. Г., Войтко О. В., Пащенко Т. П. Обґрунтування реалізації стратегічного наративу держави. Сучасні інформаційні технології у сфері безпеки та оборони. 2020. №1 (37). С. 203-212.
3. About Melting Asphalt. URL: https://meltingasphalt.com.
4. Болотин А. В. Разработка модели распространения новостей в социальных сетях на основе SIR – модели эпидемии. М.: Московский институт электроники и математики, 2018.
5. Gubanov D. A, Novikov D. A, Chkhartishvili A. G "Social networks: models of information influence, management and confrontation", 2010. 228 pages.
6. Опитування USAID-Internews щодо споживання меді. https://detector.media/doc/images/news/archive/2021/193866/usaid_internews_media_report_2021_ukr.pdf?fbclid=IwAR0Enf-DL6hGTYpZXSA6SMBYL1NLQR-lbcjr 2f1 jD7yQbdHYGQIWRi-h_mQ.
7. Voitko V. O "Model of dissemination of information in the implementation of the strategic narrative of the state" Modern Information Technologies in the Sphere of Security and Defence № 2 (41)/2021.
8. Візуалізація моделі розповсюдження інформації. URL:https://xexq6.csb. app.

Аналіз системи зенітно ракетного прикриття та вимоги до неї в сучасних умовах

Сергій Базіло
Ад'юнкт кафедри зенітних ракетних військ інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-1597-3724

Анотація. *В сучасних умовах значної актуальності набувають питання, що пов'язані з підвищенням ефективності функціонування системи зенітного ракетного прикриття за рахунок побудови нестандартних бойових порядків військових частин (підрозділів) зенітних ракетних військ та створення раціональних систем їх зенітного ракетного вогню. В доповіді викладений підхід, який дає змогу за допомогою комплексного врахування факторів, які здійснюють суттєвий вплив на ефективність функціонування системи зенітного ракетного прикриття, обґрунтувати вимоги до неї та розробити рекомендації щодо підвищення ефективності функціонування системи зенітного ракетного прикриття в сучасних умовах.*

Ключові слова*: засоби повітряного нападу, зенітний ракетний підрозділ, зенітні ракетні війська, зенітне ракетне прикриття, система зенітного ракетного вогню, система зенітного ракетного прикриття, сегмент зони ураження, повітряний противник.*

Вступ

Постановка проблеми. Однією з основних тенденцій розвитку збройної боротьби на сьогоднішній день є розширення просторового розмаху воєнних дій та зміщення центру бойових дій у повітряний простір. Боротьба за панування в повітряній сфері увійшла до розряду найбільш пріоритетних завдань збройного протиборства. Необхідно зазначити, що поряд із завданням щодо прикриття важливих державних об'єктів від ударів повітряного противника на зенітні ракетні війська покладені завдання щодо прикриття угруповань військ (сил) під час ведення ними операцій (бойових дій). Зростання обсягу і складності завдань обєднаних операцій спонукає до підвищення вимог до захисту військ і об'єктів від ударів засобів повітряного нападу противника.

Аналіз останніх досліджень та публікацій. Питанням підвищення ефективності зенітного ракетного прикриття військ в операціях присвячені теоретичні роботи таких дослідників [1–3]. Розглянуті підходи задовольняють вимогам до них та забезпечують проведення досліджень, але поглиблений аналіз та сучасні умови, у яких буде здійснюватись зенітне ракетне прикриття в дають змогу стверджувати, що вони потребують певного удосконалення для забезпечення можливості оцінювання з урахуванням факторів, які в сучасних умовах набувають першочергового значення.

Мета доповіді. На основі аналізу існуючих підходів щодо зенітного ракетного прикриття військ в операціях було з'ясовано, що в них комплексно не враховано низку факторів, які в сучасних умовах функціонування системи зенітного ракетного прикриття в операціях набувають першочергового значення. З цією метою в доповіді проаналізовано фактори, що значно впливають на систему зенітного ракетного прикриття та обґрунтовані вимоги до неї в сучасних умовах.

Виклад основного матеріалу

Для обґрунтування вимог до системи зенітного ракетного прикриття та рекомендацій щодо підвищення ефективності її функціонування необхідно проаналізувати фактори, які в сучасних умовах можуть суттєво на неї впливати. При цьому завдання аналізу полягає у винайденні саме тих факторів, що несуть в собі чітко визначений зміст і формують конкретні умови обстановки, в яких виконуються завдання зенітного ракетного прикриття та визначають форми і способи бойового застосування сил та засобів зенітних ракетних військ.

До зовнішніх факторів, що значно впливають на ефективність функціонування системи зенітного ракетного прикриття можна віднести: сучасні особливості операцій; об'єкти зенітного ракетного прикриття (їх розміри, завдання та характер дій); повітряний і наземний противник; взаємодіючі сили та засоби; умови операційної зони; радіаційна, хімічна і біологічна обстановка та інші. Зважаючи на те, що зовнішні фактори є об'єктивно існуючими і практично не можуть бути керованими, їх необхідно всебічно враховувати [1].

До внутрішніх факторів можна віднести: просторові характеристики системи зенітного ракетного прикриття; тактико-технічні характеристики зенітних ракетних комплексів; рівень підготовки бойових обслуг; ступінь забезпеченості озброєнням та військовою технікою; можливості з радіоелектронної протидії; ступінь централізації і автоматизації управління; якість організації і здійснення взаємодії; можливості з раптовості дій та введення противника в оману; способи та тактичні прийоми ведення протиповітряних боїв; бойові можливості військових частин (підрозділів) зенітних ракетних військ, що залучені для виконання завдань зенітного ракетного прикриття в операціях [2].

Досягнення підвищення ефективності функціонування системи зенітного ракетного прикриття можливе, головним чином, за допомогою досконалого аналізу та врахуванні зовнішніх факторів та за рахунок впливу на внутрішні фактори. Таким чином, цільову функцію ефективності функціонування системи зенітного ракетного прикриття в операціях можна представити у вигляді виразу:

$$E = f(\alpha_к, \beta_y, t) \to \max;\ k = 1....w;\ y = 1.....v, \qquad (1)$$

де E – ефективність функціонування системи зенітного ракетного прикриття;

$\alpha_к$ – зовнішні фактори;

β_y – внутрішні фактори;

t – часові параметри.

Виходячи із аналізу елементів оперативної побудови угруповань військ

(об'єднаних сил), як об'єктів зенітного ракетного прикриття можна зазначити, що для успішного досягнення мети операції, необхідно забезпечити ефективне та стійке зенітне ракетне прикриття різних за складом, характером участі в операції, розмірами та ступенем рухомості елементів оперативної побудови під час виконання ними оперативних завдань.

Результати аналізу можливого масштабу та характеру дій повітряного противника свідчать про наявність основних, сучасних тенденцій бойового застосування засобів повітряного нападу противника: непередбаченість ударів повітряного противника (можливі удари з різних напрямків, без прив'язки до напрямків зосередження зусиль); зменшення підльотного часу до об'єктів прикриття; зменшення нарядів (застосування засобів повітряного нападу противника невеликими групами, поодинокими літаками) за рахунок збільшення частки високоточної зброї; збільшення частки засобів повітряного нападу, які будуть діяти на малих та гранично малих висотах; збільшення кількості безпілотних літальних апаратів, які діятимуть у зонах вогню військових частин (підрозділів) зенітних ракетних військ [4].

При аналізі системи зенітного ракетного прикриття в операціях було з'ясовано, що при її створенні не враховуються фактори, що здійснюють значний вплив на ефективність її функціонування та вимоги до неї в сучасних умовах, тому вона створюється інтуітивно, за застарілими підходами.

За результатами аналізу зовнішніх та внутрішніх факторів було виявлено ряд невідповідностей в практиці військ при створенні системи зенітного ракетного прикриття, які дають змогу висунути вимоги до системи зенітного ракетного прикриття в сучасних умовах: невідповідність структури системи завданням операції, замислу командувача на операцію; прикриття з необхідною ефективністю угруповань військ, боєздатність яких в найбільшій мірі визначає успіх операції на різних її етапах; урахування множини можливих рубежів виконання завдань повітряним противником; максимальна реалізація можливостей щодо створення системи вогню до рубежів виконання завдань повітряним противником, у тому числі на малих та гранично малих висотах, з урахуванням впливу рельєфу місцевості; суцільність (рівноефективність за кількістю стрільб до рубежу виконання завдань повітряним противником) при прикритті тих чи інших елементів оперативної побудови; всевисотність системи зенітного ракетного вогню; первинність системи вогню на малих та гранично малих висотах під час побудови бойових порядків [3]; забезпечення перекриття зон ураження зенітних ракетних комплексів різного типу для реалізації безперервного вогневого впливу; можливість зосередження зусиль на найважливіших елементах оперативної побудови, найімовірніших напрямках та висотах дій повітряного противника; потрібна щільність вогню на визначених напрямках; параметри бойового порядку повинні забезпечувати взаємне вогневе прикриття зенітних ракетних підрозділів, найкраще використання вигідних умов місцевості, потрібну щільність вогню на визначених напрямках, збереження зенітних ракетних підрозділів.

Для підвищення ефективності відбиття ударів повітряного противника по елементам оперативної побудови угруповання військ в операціях пропонується

формувати та залучати до виконання таких завдань перспективну зенітну ракетну бригаду змішаного складу, на озброєнні якої знаходяться зенітні ракетні комплекси середньої та малої дальності.

При побудові бойового порядку такої бригади необхідно корегування існуючих нормативних параметрів бойових порядків зенітних ракетних підрозділів, що будуть входити до її складу. Рекомендується визначати віддалення бойових позицій зенітних ракетних підрозділів від переднього краю з урахуванням ступеня їх збереження та ступеня реалізації сегментів їх зон ураження. Це дасть змогу реалізувати вогневі та можливості з прикриття зенітних ракетних підрозділів з одного боку та зберегти зенітні ракетні комплекси для їх подальшого застосування, з іншого.

При визначенні відстаней між бойовими позиціями зенітних ракетних підрозділів, в умовах невизначеності напрямків ударів повітряного противника, пропонується створювати рубіж суцільного прикриття з рівними можливостями за кількістю стрільб з урахуванням конфігурації зон ураження зенітних ракетних комплексів. Створення зазначеного рубежу дасть змогу здійснювати, суцільне (рівноефективне за кількістю стрільб до рубежу виконання завдань повітряним противником) зенітне ракетне прикриття визначених елементів оперативної побудови та надасть можливість проводити однакову кількість стрільб до рубежу виконання завдань повітряним противником в будь-якій частині зони вогню зенітної ракетної бригади змішаного складу за рахунок компенсації недостатньої кількості стрільб одного підрозділу, іншим.

При виборі місць бойових позицій вогневих одиниць пропонується врахувати ступінь реалізації їх зон ураження на малих та гранично малих висотах з урахуванням впливу рельєфу місцевості. Для підвищення ступеню збереження зенітних ракетних підрозділів та створення “прихованої” для противника системи зенітного ракетного вогню пропонується біля кожної бойової позиції обладнувати місця очікування до бойового застосування з необхідним ступенем інженерного обладнання. Це надасть можливість мінімізувати час перебування вогневих одиниць на бойових позиціях та зменшить імовірність їх знищення засобами ураження повітряного противника.

Зважаючи на вищезазначене, в сучасних умовах система зенітного ракетного прикриття повинна володіти таким рівнем досконалості, який дозволяв би із заданою імовірністю забезпечувати вирішення завдань боротьби як з засобами повітряного нападу різних типів, забезпечуючи при цьому власну стійкість та ефективне прикриття елементів оперативної побудови від ударів з повітря, для успішного виконання ними оперативних завдань операції.

Висновки

Таким чином, врахування додаткових вимог до системи зенітного ракетного прикриття та практична реалізація запропонованих рекомендацій дасть змогу, на думку автора, урахувати низку факторів, що значно впливають на систему зенітного ракетного прикриття в операціях та підвищити її ефективність до рівня, при якому війська будуть спроможні виконати оперативні завдання операцій для успішного досягнення їх мети. Зважаючи на

вищезазначене, постає питання пошуку нових, нестандартних підходів до створення системи зенітного ракетного прикриття в операціях з метою підвищення ефективності її функціонування в сучасних умовах.

Список літератури

1. Синтез адаптивних структур системи зенітного ракетно-артилерійського прикриття об'єктів і військ та оцінка її ефективності / [Кириченко І.О., Єрмошин М.О., Дробаха Г.А., Доліна М.П.]. Х.: ХВУ, 2006. – 348 с.

2. Неупокоев Ф.К. Противовоздушний бой / Ф.К. Неупокоев // М.: Воениздат, 1989.– 262с.

3. Торопчин А.Я. Довідник з протиповітряної оборони / Торопчин А.Я Романенко І.О., Даник Ю.Г. та ін. – Х.: Вид-во "Харків", 2003. – 366 с.

4. Єрмошин М. О., Федай В. М. Аеродинамічні цілі зенітних ракетних військ : навч. посіб. Х.: ХВУ, 2004.– 285 с.

Розвиток роботехнічних системи озброєння для вирішення завдань в сучасних умовах ведення збройної боротьби

Володимир Комаров, доктор військових наук, професор
Начальник науково-дослідного управління в/ч А1906,
Київ, Україна
https://orcid.org/0000-0003-2873-8261
Вадим Олексіюк, кандидат військових наук
Начальник науково-дослідного відділу в/ч А1906,
Київ, Україна
https://orcid.org/0000-0002-9577-4257
Ігор Даценко
Заступник командира військової частини А0418,
Київ, Україна
https://orcid.org/0000-0002-4537-1297

Анотація. *Сучасний етап проведення операції Об'єднаних сил на Сході нашої держави характеризується необхідністю виконання широкого спектра завдань, зокрема й розвідувальних, у так званій "сірій зоні". Аналіз виконання завдань силами і засобами розвідки Збройних Сил України в "сірій зоні" свідчить про значні втрати особового складу, техніки та спеціального озброєння.*

Вирішити питання зменшення втрат особового складу розвідувальних підрозділів можна шляхом розроблення та постановки на озброєння сучасних наземних роботизованих (робототехнічних) комплексів (систем).

З проведеного аналізу випливає, що в Україні на сьогодні робляться лише перші кроки за напрямами створення та впровадження наземних роботизованих комплексів, тому спостерігається значне відставання від рівня оснащеності збройних сил провідних країн світу.

Ключові слова: *роботехнічні комплекси, воєнна безпека.*

Вступ.

Постановка проблеми. Сучасний етап проведення операції Об'єднаних сил (ООС) на Сході нашої держави характеризується необхідністю виконання широкого спектра завдань, зокрема й розвідувальних, у так званій "сірій зоні". Аналіз виконання завдань силами і засобами розвідки ЗС України в "сірій зоні" свідчить про значні втрати особового складу, техніки та спеціального озброєння.

Зменшити ці втрати можна шляхом розроблення та постановки на озброєння сучасних наземних роботизованих (робототехнічних) комплексів (систем) (НРК), які за своїм призначенням здатні виконувати розвідувальні завдання. Тому питання розроблення основ їх бойового застосування та оснащення Збройних Сил (ЗС) України, зокрема частин (підрозділів) розвідки, сучасними НРК набуває особливої актуальності.

Метою доповіді є аналіз тенденцій розвитку НРК у світі, а також вироблення пропозицій щодо напрямів створення та оснащення ними частин та підрозділів ЗС України.

Виклад основного матеріалу

Розроблення та виробництво НРК здійснюється у 37 країнах світу. Концепції створення та застосування НРК для вирішення завдань в сучасних збройних конфліктах визначають основну мету (ціль) їх створення, а саме [1–2]:

підвищення рівня бойових (розвідувальних) можливостей частин (підрозділів);

зниження рівня бойових втрат особового складу;

досягнення безперервності виконання завдань в умовах обмеженості фізіологічних можливостей людей.

У провідних країнах світу існує така класифікація НРК [2]:

розвідувальні та розвідувально-бойові (носимі (до 12 кг), носимо-возимі (12–200 кг), самохідні (200–2500 кг));

бойові та підтримки військ (важкі, середні, легкі);

забезпечення дій військ.

Досвід застосування НРК в операціях в Іраку, Афганістані, Сирії, в останньому Азербайджано-Вірменському конфлікті та на Сході нашої країни дав змогу визначити завдання, які на них можуть покладатись [1–2]:

розвідувальні та розвідувально-бойові:

розвідка (оптико-електронна, тепловізійна, радіотехнічна, радіолокаційна) та висвітлення поточної обстановки;

розвідка, цілевказання і ураження виявлених або спланованих цілей (розвідувальний пошук, засідка) в повітрі, на суші, на морі і під водою та інспектування цілей (дорозвідка після вогневого ураження);

встановлення розвідувально-сигналізаційної апаратури (сенсорів);

викриття позицій снайперів, вогневих засобів, засад і систем спостереження противника;

розвідка будівель та споруд і окремих об’єктів;

проведення інженерної розвідки;

бойові та підтримки військ:

ведення вогню;

дистанційне мінування і розмінування;

підтримка проведення спеціальних, психологічних та інформаційних операцій;

захист військ і техніки;

постановка радіозавад;

забезпечення дій військ:

ретрансляція зв’язку та навігація;

доставлення боєприпасів та вантажів;

медична евакуація з поля бою.

Наразі провідні країни світу проводять дослідження за такими основними напрямами:

теоретичне обґрунтування та апробація на практиці форм застосування та способів дій НРК;

розроблення перспективної структури частин (підрозділів) видів та родів військ;

створення нових поколінь НРК, які здатні формувати бойові групи;

підвищення завадозахищеності каналів управління та передачі даних, а також їх пропускної здатності;

розроблення автоматизованої системи розпізнавання “свій–чужий”;

досягнення універсальності та можливості спряження із системами озброєння видів та родів військ.

Результати аналізу цього питання в Україні свідчать, що нині робляться лише перші кроки за напрямами створення та впровадження НРК, тому спостерігається значне відставання від рівня оснащеності збройних сил провідних країн світу.

Термінове переозброєння ЗС України на засадах максимального використання новітніх НРК є нагальним завдання. Певне розуміння цього імперативу частково викладено в стратегічних документах з питань воєнної безпеки та розвитку ЗС України. Так, відповідно до Стратегічного оборонного бюлетеня України [3], передбачено впровадження безпілотних платформ (систем) повітряного, наземного та морського базування у структурі ЗС України, а також створення нових спроможностей військових частин та підрозділів розвідки, зокрема шляхом формування розвідувальних підрозділів НРК.

Разом з тим, питання розвитку НРК, їх структури, завдань, складу, оперативно-технічних вимог до них потребує подальшого наукового вивчення та обґрунтування.

Для подолання відставання доцільною є інтенсифікація розробок відповідних НРК. У контексті зазначеного перспективними напрямами їх створення можуть бути носимі та носимо-возимі НРК. Це обумовлено їх вартістю та наявністю відповідних технологій, а також можливістю виробництва національним оборонно-промисловим комплексом.

Висновок

Отже, в умовах “гібридної” війни з Росією, створення (розроблення) та використання НРК є одним з найважливіших завдань бойового (оперативного) забезпечення, розв’язавши яке, ЗС України зможуть успішно протистояти російській агресії та наблизитись до рівня розвитку збройних сил провідних країн світу.

Список літератури

1. А.В. Лопата,А.Б. Николаев. Современные робототехнические комплексы военного и специального назначения. Государственный научный центр РФ. ЦНИИ робототехники и технической кибернетики. С. 3–29.

2. С.И. Макаренко. Робототехнические комплексы военного назначения – современное состояние и перспективы развития. Системы управления, связи и безопасности. 2016. – № 2. С. 73–172.

3. Указ Президента України від 17.09.2021 № 473/2021 “Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року”.

Проблемні питання моніторингу зон воєнних конфліктів в місіях Організації Об'єднаних Націй в умовах гібридної агресії

Віталій Федорієнко
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-0921-3390
Олександр Кульчицький
Старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-4901-0192
Сергій Терещенко
Начальник науково-дослідної лабораторії Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-0988-4119
Вадим Капілевич
Провідний науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-9025-7608

Анотація. *Доповідь присвячена дефінітивному аналізу місця "моніторингу зон воєнних конфліктів та застосування гібридних методів впливу в зоні конфлікту" в нормативно-правових документах та організаційній структурі Організації Об'єднаних Націй (далі – ООН). Також наводиться сучасний стан моніторингу зон конфліктів персоналом ООН з точки зору наявних програмно-технічних систем. У доповіді пропонується дослідити деякі проблемні питання процесу моніторингу в зоні відповідальності миротворчих місій, що включає збір, обробку та аналіз сповіщення про наявні інциденти порушення безпеки із урахуванням сучасних гібридних методів впливу на ситуацію в зоні конфлікту. В основу роботи покладений практичний досвід моніторингу в місіях ООН, який може бути корисним для роботи Спільного центру контролю та координації питань припинення вогню в зоні проведення Операції об'єднаних сил на Південному Сході України [1].*

Ключові слова: *моніторинг зон воєнних конфліктів, місія ООН, збір та аналіз попереджень, сповіщення про наявні інциденти*.

Вступ

Постановка проблеми. На теперішній час у світі існує значна кількість конфліктів, які вимагають втручання міжнародних безпекових організацій, зокрема, ООН, Організація з безпеки і співробітництва в Європі, ОБСЄ та інші.

Конфлікти у зоні відповідальності миротворчих місій у світі можуть бути спричинені різними факторами. Зокрема, у зоні відповідальності стабілізаційної місії ООН у Демократичній Республіці Конго (United Nations Organization Stabilization Mission in the Democratic Republic of Congo, MONUSCO) постійно спостерігається протиправна діяльність елементів різних протиборчих сил. У більшості випадків ними можуть виступати, як армійські групи банд-формувань, з одного боку, так і підрозділи національних збройних сил чи місцевої поліції з іншого. Для визначення ступеню напруженості у такій зоні міжнародні миротворчі організації використовують різноманітні способи отримання інформації задіявши різні сили та засоби. Одним із них є *моніторинг зони конфлікту* силами національного персоналу ООН.

Більшість існуючих систем моніторингу для збору та аналізу інформації про інциденти не відповідають сучасним вимогам збору інформації через їх розосередженість та різноманітність методів, що застосовуються для досягнення своєї мети протиборчими силами. Наприклад, Місії ООН у Південному Судані (UN Missions in South Sudan, UNMISS) та MONUSCO працюють над удосконаленням своїх процесів управління даними, але досі не мають належних систем для збору та зберігання даних про загрози з усіх розділів для створення інтегрованого аналізу загроз, інформування про планування та впливу на рішення із урахуванням гібридних методів [5].

За відсутності систематичного використання даних, миротворчі місії не можуть враховувати у аналізі стійке, тривале насильство, яке, наприклад, при використанні простого способу аналізу чисельності, завдає більшої шкоди, ніж дуже помітні масові вбивства [5]. Це свідчить про те, що об’єм інформації раннього попередження – далеко не єдиний фактор, який визначає наскільки активно місія реагує на загрози захисту.

Тому питання дослідження проблемних питань систем моніторингу зон конфлікту є актуальним.

Аналіз останніх досліджень та публікацій. З точки зору моніторингу зон конфлікту, у нормативно-правових та звітних документах ООН [1-6], досить чітко відображена важливість задачі такого моніторингу та передбачені можливості щодо оснащення миротворців [4]. Питання щодо висвітлення слабких місць організації та програмно-технічного забезпечення для моніторингу зон воєнних конфліктів із застосуванням гібридних методів на оперативному та тактичному рівнях висвітлені в [1-7] вибірково.

Мета доповіді. Визначити підходи та надати пропозиції щодо моніторингу зон воєнних конфліктів з метою протидії агресивним гібридним методам що застосовуються у зоні конфлікту.

Виклад основного матеріалу

Моніторинг та нагляд є критично важливими функціями для виконання мандатів місії. Наприклад, вони необхідні для: перевірки дотримання режиму припинення вогню та мирних угод; захисту цивільного населення та регіонів; контролю виборів; підтримки права людини; підтримки санкцій; безпечних кордонів; та зменшення нелегальної торгівлі експлуатованих ресурсів. Коли небезпечні збройні угруповання та порушники мирних процесів знаходяться в активній фазі, життєво важливо знати їхній рух та рівень підготовки, особливо для досягнення раннього попередження та вжиття запобіжних заходів.

Тактичний рівень. Моніторинг та оцінка конфліктів з точки зору їх ситуативності та нестійкості є сферою практики роботи в полі, яка постійно розвивається [2].

Для ефективної та достовірної роботи проти порушень прав людини офіцери спостерігачі повинні вміти збирати та оцінювати відповідні факти. Ситуації з озброєними конфліктами можуть перешкоджати роботі з моніторингу і тим самим погіршувати здатність офіцерів реагувати на порушення прав людини в періоди збройних конфліктів. Особливо, коли її мандат вказує на те, що польова діяльність з прав людини повинна проводитися шляхом моніторингу активності збройних опозиційних груп [3].

На *оперативному рівні* надзвичайно важливо, щоб керівники місій використовували та організовували цикл інформації для врахування загроз у своїх системах стратегічного та оперативного планування, а персонал вживав рішучих та активних дій на основі інформації про раннє попередження. Коли цикл інформації, який включає збір, зберігання, аналіз, планування та прийняття рішень функціонує добре, миротворці можуть визначити проблеми захисту, зосередити сили та засоби на найбільш загрозливих ділянках, запобігти насильству або відреагувати на нього. Якщо цикл функціонує не вдало, елементи місії вражаються атаками незаконних збройних формувань і не ефективно захищають цивільне населення. Функції раннього попередження можуть бути реалізовані з урахуванням аналітичної складової, яка є характерною для оперативного рівня.

На с*тратегічному рівні* Департамент операцій з підтримання миру (Department of Peacekeeping Operations, DPKO) у Секретаріаті ООН, Департамент польової підтримки (DFS) та польові місії мають окремі потреби в моніторингу, що базується на даних, і аналітиці: DPKO потребує наскрізних та інтегрованих звітів щодо сукупності прогресу мандату зі стратегічної точки зору, включаючи важко вимірювані показники, такі як динаміка конфліктів. DFS, у свою чергу, потребує інтегровані стратегічні та оперативні дані, характерні для його основної функціональності. Місіям потрібні не лише наскрізні повноваження та бізнес-аналітика, але також дані оперативного та тактичного рівня на більш детальному рівні та більш швидкими темпами, щоб забезпечити оперативну та цілеспрямовану реакцію на місцях.

У MONUSCO обмін інформацією та інтегрований аналіз на рівні польових офісів, є найслабшими через відсутність координаційного персоналу.

За результатами проведеного аналізу з’ясовано, що на цьому рівні відсутні будь-які механізми, які б дозволяли проводити інтегрований аналіз, щодо виявлення загроз на “*гібридному*” рівні. У той же час, з доповіді Групи експертів ООН з технологій та інновацій в миротворчій діяльності ООН лунає, що окремі миротворці – військові, поліцейські та цивільні – можуть бути оснащені технологіями та підключені до телекомунікаційних мереж. У цій доповіді згадується опис “цифрового миротворця” [5], який базується на концепції “Цифрового миротворця” запропонованою Звітом групи експертів з питань технологій та інновацій у миротворчій діяльності ООН.

Існує ряд підходів до збору даних з метою подальшого моніторингу. Миротворчі операції традиційно покладаються на інформацію з відкритих джерел та інформацію, зібрану безпосередньо особами, які розгортаються в оперативній зоні шляхом спостереження та взаємодії з іншими зацікавленими сторонами. Зовсім недавно миротворчі операції почали використовувати обладнання з використанням розвідувальної сигналізації, що включає перехоплення радіозв'язку, а також геопросторової розвідки - включаючи інформацію з безпілотованих літальних апаратів, супутників, аерофотозйомки, з повітряних куль (аеростата) та інших засобів збору інформації.

На даний час ООН потрібні сучасні структури для збору та обміну інформацією [4]. Для цього Місія повинна мати достатню кількість персоналу та інституційні структури для збору, перевірки, обробки, аналізу та розповсюдження даних. Командири повинні вказати свої пріоритетні інформаційні вимоги, щоб забезпечити прийняття рішень, що базуються на фактичних даних та керуються інформацією. У сучасних операціях важливу інформацію потрібно збирати не лише від місцевого населення, а й вибірково ділитись з місцевим населенням. При цьому відсутність процесів і технологій для зберігання, оцінки та аналізу інформації про загрози підриває ситуаційну обізнаність.

Коли в травні 2019 року Центр захисту цивільного населення проводив свої дослідження в Південному Судані, у своєму звіті вони повідомили, що офіційними особами UNMISS не використовувалася універсальна база даних для відстеження інцидентів порушення безпеки. А деякі співробітники з власної ініціативи вели електронні таблиці інформації про інциденти та повідомляли про погрози. Це свідчить про відсутність цілісної системи моніторингу зони конфлікту та слабку організацію інформаційного циклу.

Досить часто миротворці ООН не можуть зупинити масові вбивства, запобігти жорстокості, контрабанді, встановити осіб агресорів та помітити порушників прав людини. У багатьох випадках місії ООН не мали належних інструментів, щоб передбачити або діяти, навіть коли була політична воля. Далі наведемо приклад неправильного використання наявності аналітичного програмного забезпечення. У Південному Судані, у 2016 році був проведений внутрішній аналіз можливих та найгірших сценаріїв насильства, UNMISS виявилася не готовою через не належну підготовку даних та перевантаженість системи.

У навчальному посібнику з прав людини [7] можна знайти таке твердження: “ООН повинна запровадити настроювану інформаційну систему управління та контролю, що підтримує геоінформаційні системи, для забезпечення більш узгодженої оперативної взаємодії від патруля до сектору місії та вищого штабу, що підтримується постійною та надійною передачею голосу, даних та відео”.

При спробі створити карти гарячих точок, зібрати статистичні дані або розглянути тенденції насильства, більшість співробітників покладалися на працезатратний процес перегляду окремих текстових файлів щоденних, тижневих та щомісячних звітів, що створюються персоналом, щоб генерувати цю інформацію вручну [4-5]. Разом з тим, незважаючи на різницю в навичках персоналу та їх підходів щодо аналізу ризиків, керівники обох місій UNMISS і MONUSCO, значною мірою покладаються на карти раннього попередження та карти активних дій (гарячих точок) для прийняття рішень. Ці документи базуються на інформації, повідомленій Центру аналізу спільних місій (Joint Mission Analysis Centres, JMAC) через їхні мережі, та визначають зони, де насильство чи напруга зростають.

Миротворчі місії стикаються із серйозними проблемами щодо створення інтегрованого аналізу загроз на кожному етапі інформаційного циклу, включаючи забезпечення того, щоб керівники місій ефективно використовували розвідку для встановлення пріоритетів місій та прийняття рішень. Вони також намагаються забезпечити, щоб інформація з усіх підрозділів місій входила в загальну оперативну картину та інформувала про прийняття рішень. Наприклад, хоча місії мають багато потоків інформації про загрози цивільному населенню та деякі інструменти для аналізу цих загроз, інформація часто не збирається разом і не зберігається в одному місці.

У минулому ООН не була добре технологічно оснащена. Утрата таких можливостей означає втрату шансів на мир, як це траплялося досить часто у минулому, коли Організація Об'єднаних Націй була недостатньо підготовлена до складних мандатів. Щоб бути ефективною у двадцять першому столітті, світова організація повинна не лише нарощувати власні технологічні можливості, але й знати про посилення щодо використання сучасних технологій конфліктуючими сторонами та цивільним населенням в районах, охоплених війною.

Висновки

У даній роботі були висвітлені в узагальненому виді потреби до моніторингу зон воєнних конфліктів та наведені проблемні питання у підходах до системи збору, зберігання та аналізу ранніх попереджень щодо загроз безпеки в Місіях ООН.

У той же час, технології не замінять слабкий процес або неправильний синтез зібраних даних для попередження небезпеки. Це пов’язане з тим, що вони можуть не лише надати величезну кількість інформації у розпорядження будь-якій особі відповідальній за прийняття рішення, але й сприяти, з одного боку, неможливості прийняття рішення через перевантаження інформацією а, з іншого

– прийняттю невірних рішень, якщо не застосовано належних програмних інструментів аналізу через їх відсутність чи низьку навченість персоналу.

Список літератури

1. Тимошенко Р. І. Аспекти практичної реалізації макету інформаційно-аналітичної системи фіксації обстрілів для Української сторони СЦКК / Р. І. Тимошенко, В. А. Федорієнко, О. С. Прокопенко // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. - 2017. № 3. С. 84-88. Режим доступу: http://nbuv.gov.ua/UJRN/Znpcvsd_2017_3_17.
2. Chapter XVI. Monitoring During Periods of Armed Conflict. [Електронний ресурс] // Training Manual on Human Rights Monitoring, 2018. C. 327–362. – Режим доступу до ресурсу: https://www.ohchr.org/Documents/ Publications/ training7 part 1618en.pdf.
3. Weissbrodt V. The Role of International Organizations in the Implementation of Human Rights and Humanitarian Law in Situations of Armed Conflict / Vid Weissbrodt. // Vanderbilt Journal of Transnational Law. – 1988. №21. C. 313.
4. Dorn A. Smart Peacekeeping: Toward Tech-Enabled UN Operations [Електронний ресурс] / A. Walter Dorn // New York International Peace Institute. – 2016. – Режим доступу до ресурсу: https://papers.ssrn.com/sol3/papers.cfm? abstract_id=2893246.
5. Data-Driven Protection. Linking Threat Analysis to Planning in UN Peacekeeping Operations [Електронний ресурс] // Center for Civilians in Conflict. – 2018. – Режим доступу до ресурсу: https://civiliansinconflict.org/wp-content/uploads /2018/11/CIVIC_PeaceKeeping_PRINT_Digital.pdf.].
6. Final Report: Expert Panel on Technology and Innovation in UN Peacekeeping [Електронний ресурс] // United Nations Peacekeeping. – 2015. Режим доступу до ресурсу: https://peacekeeping.un.org/sites/default/files/ performance-peacekeeping expert-panel-on-technology-and-innovation_report_ 2015. pdf.]
7. Monitoring During Periods of Armed Conflict. [Електронний ресурс] // Training Manual on Human Rights Monitoring / , 2018. – (OHCR). C. 327–362. – Режим доступу до ресурсу: https://www.ohchr.org/Documents/Publications/ training7part1618en.pdf

Методичний підхід до оцінювання рівнів небезпеки гібридних загроз у визначальних сферах національної безпеки держави

Володимир Богданович, доктор технічних наук, професор
Головний науковий співробітник Центрального науково-дослідного інституту Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-0481-9454
Вадим Олексіюк, кандидат військових наук
Начальник відділу в/ч А 1906,
Київ, Україна
https://orcid.org/0000-0002-9577-4257

Анотація. *Доповідь присвячена проблемі забезпечення національної безпеки в умовах створюваних недружніми державами гібридних загроз. Запропоновано методичний підхід до оцінювання рівнів небезпеки гібридних загроз у визначальних сферах національної безпеки держави.*

Урахування впливу наслідків гібридної загрози в визначальних сферах національної безпеки саме на воєнну безпеку через показники воєнної небезпеки, що генеруються гібридною загрозою в іншу сферу національної безпеки, становить новизну запропонованого методичного підходу.

Представлений методичний підхід дає змогу кількісно оцінювати рівень воєнної небезпеки від гібридної загрози завдяки врахуванню її деструктивного впливу на інші сфери національної безпеки.

Ключові слова: *гібридна війна, гібридна загроза, національна безпека, воєнна безпека, воєнна загроза, оцінювання рівня загрози.*

Вступ

Постановка проблеми. Доповідь присвячено проблемі забезпечення національної безпеки в умовах створюваних недружніми державами гібридних загроз. У XXI столітті збройні конфлікти та війни все частіше ведуться в «сірій зоні» [1], тобто поза межами міжнародного права, як у фізичному просторі, так і в інших вимірах – інформаційному, кібернетичному, культурному, когнітивному, – переважно невійськовими способами і з залученням іррегулярних формувань. До останнього часу в теорії забезпечення національної безпеки, у тому числі й військової безпеки, розглядалися загрози, які були спрямовані на одну зі сфер національної безпеки. Тобто взаємозв'язок воєної загрози з іншими сферами національної безпеки не розглядався взагалі, або недостатньо глибоко, що унеможливлювало застосування системного підходу до визначення заходів щодо нейтралізації, або зменшення впливу гібридної загрози. У результаті ефективність таких заходів знижувалася.

Успішне розв'язання даної проблеми потребує кількісно-якісного оцінювання гібридних загроз з метою недопущення повномасштабного застосування військової сили проти України.

Аналіз останніх досліджень і публікацій. У роботі [2] гібридна війна розглядається як інтеграція різних реальних і віртуальних загроз (дипломатичних, військових, економічних, інформаційних тощо) з метою психологічного впливу на державу-жертву, занурення її в ситуацію невизначеності, послаблення і руйнування без оголошення війни, а також створення навколо неї відповідного інформаційного поля, покликаного сформувати у світової спільноти такий образ цієї держави, який виправдовував би будь-які недружні і навіть агресивні дії на її адресу. Але питанням оцінювання рівня гібридних загроз автор не приділяє уваги.

У монографії [3] розглянуто методологічний апарат організації комплексної, у тому числі асиметричної протидії загрозам воєнного характеру. Протидію гібридним загрозам розглянуто лише в постановочному плані.

У публікаціях [4–6] наводиться загальна характеристика гібридних загроз, аналізується їх вплив на забезпечення національної безпеки, але методичні підходи до оцінювання їх рівня не розглядаються.

У Стратегії воєнної безпеки України зазначається, що всеохоплююча оборона України передбачає підтримання певного балансу та синергії воєнних і невоєнних засобів для забезпечення воєнної безпеки України, але яким чином досягається така синергія – у документі не визначено.

У зазначених та інших публікаціях не наводиться методичний апарат оцінювання рівня воєних загроз та їх деструктивного впливу, у разі їх реалізації у повному обсязі, на визначальні сфери національної безпеки держави.

Мета доповіді. Метою доповіді є запропонувати до застосування методичний підхід до оцінювання рівнів небезпеки гібридної загрози для національної і воєнної безпеки та обгрунтування заходів щодо зниження її впливу.

Виклад основного матеріалу

Запропонований методичний підхід до оцінювання рівнів небезпеки гібридних загроз у визначальних сферах національної безпеки держави базується на відомих технологіях експертного оцінювання, математичного моделювання та аналізу ієрархій.

Суть методичного підходу полягає у проведенні декомпозиції гібридної загрози, яка була встановлена під час моніторингу безпекового середовища, на предмет її деструктивного впливу на різні сфери національної безпеки. Визначаються, згідно з Паспортом загроз, характеристики гібридної загрози (характер, масштаб та просторові межі впливу, джерело походження тощо) та здійснюється їх проектування на воєнну безпеку держави для відповідного реагування системою забезпечення воєнної безпеки (СЗВБ).

Схему методичного підходу, який має вісім основних етапів, наведено на рис. 1. На кожному з етапів виконуються певні процедури, сутність яких зводиться до такого.

Першим і другим етапом передбачається проведення моніторингу безпекового середовища на предмет виявлення гібридних загроз $\{Z_G\}$ національної безпеки держави.

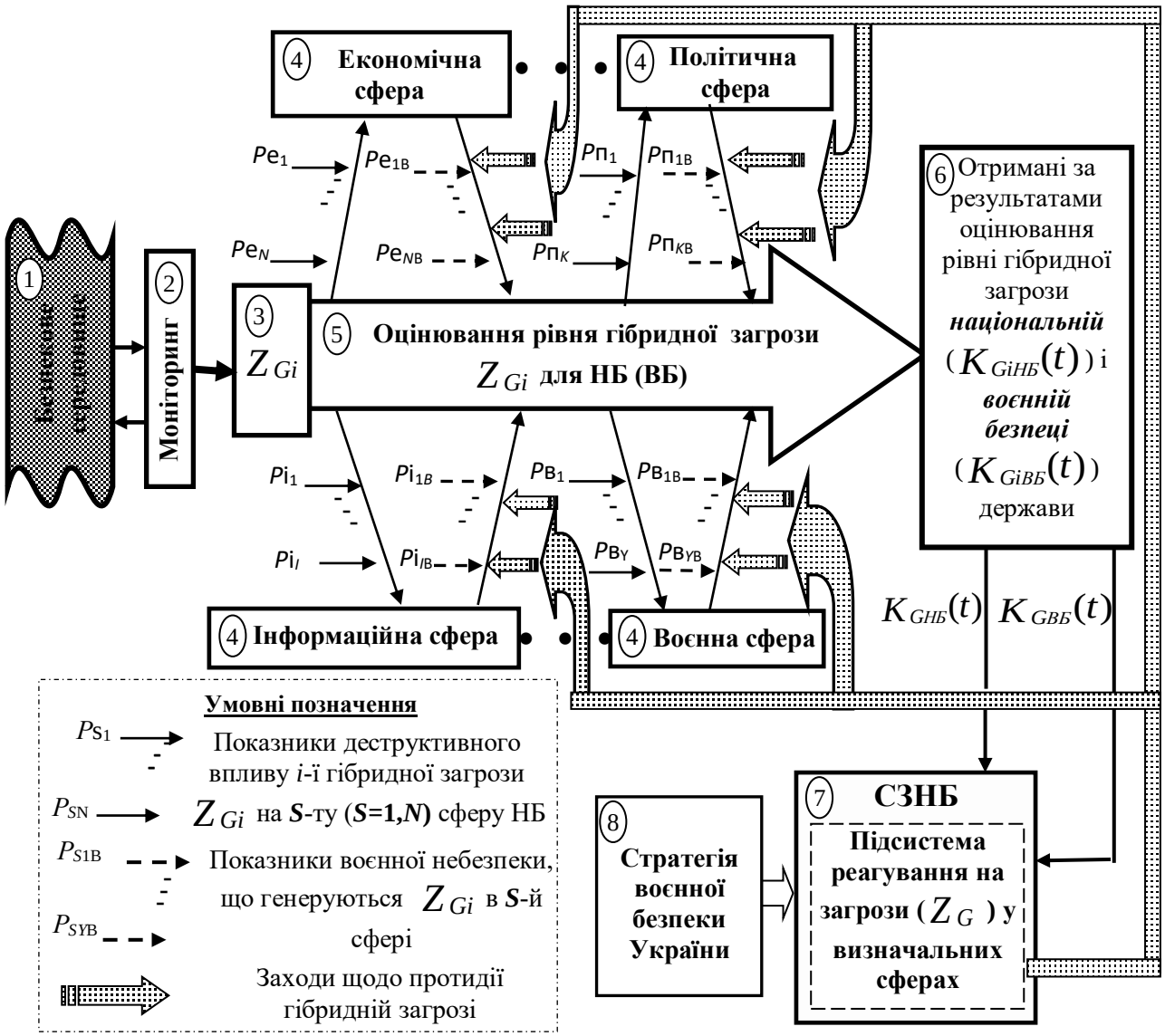

Рисунок 1 – Схема методичного підходу до оцінювання рівнів небезпеки гібридних загроз у визначальних сферах національної безпеки (НБ)

Під **безпековим середовищем** розумітимемо геополітичну, політико-дипломатичну, воєнну, економічну, інформаційну та інші сфери, де зароджуються, існують, накопичуються або проявляються сприятливі умови або небезпечні явища, потенційні та реальні загрози реалізації національних інтересів, у яких держава реалізує свою політику НБ, взаємодіє з міжнародними структурами безпеки, стратегічними партнерами, союзниками, військово-політичними та іншими інститутами й організаціями в інтересах забезпечення свого сталого розвитку на певному часовому інтервалі [3].

Організацію моніторингу розкрито в інших публікаціях [9], тому це не деталізується у даній роботі. Результатом моніторингу є гібридна загроза Z_{Gi}, вплив якої на воєнну безпеку держави потрібно дослідити.

На **третьому етапі** здійснюється опис гібридної загрози Z_{Gi} відповідно до Паспорта загроз. За результатами опису експерти проводять декомпозицію загрози та оцінюють її вплив на визначальні сфери НБ (***S***). Кількість сфер може бути різна, залежно від характеру гібридної загрози. На рис. 1, як приклад, їх показано чотири – політичну, економічну, інформаційну та воєнну сфери НБ.

На **четвертому етапі** експертами визначаються показники небезпеки для кожної сфери ($\{P_{SN}\}$) та показники впливу кожної зі сфер на зростання воєнної небезпеки ($\{P_{SYB}\}$).

Оцінювання рівня гібридної загрози Z_{Gi} для НБ, а також для воєнної безпеки здійснюється на **п'ятому етапі** із застосуванням "діаграми Ісікави" та удосконаленого методу аналізу ієрархій [8]. Оцінювання здійснюється за визначеними показниками деструктивного впливу *i*-ї гібридної загрози Z_{Gi} на ***S***-ту сферу ($\{P_{SN}\}$). Таке оцінювання є вже усталеною процедурою під час аналізу безпекового середовища. Але ця процедура, стосовно оцінювання воєнної безпеки, має суттєвій недолік через неврахування впливу наслідків гібридної загрози в інших сферах національної безпеки саме на воєнну безпеку. Урахування такого впливу під час оцінювання рівня воєнної небезпеки через показники воєнної небезпеки ($\{P_{SYB}\}$), що генеруються Z_{Gi} в ***S***-й сфері, і становить новизну запропонованого методичного підходу.

Отриманий на п'ятому етапі результат оцінювання рівня гібридної загрози Z_{Gi} для НБ (ВБ) формалізується на **шостому етапі** для обгрунтування заходів щодо зниження її впливу. Таке обґрунтування заходів здійснюється в СЗНБ у підсистемі реагування на загрози (Z_G) у визначальних сферах (**сьомий етап**) [7]. Розроблені з урахуванням Стратегії воєнної безпеки (**восьмий етап**) заходи щодо зниження впливу гібридної загрози Z_{Gi} спрямовуються для їхньої реалізації у відповідних сферах НБ.

Висновки

Таким чином, запропонований методичний підхід дає змогу кількісно оцінювати рівень воєнної небезпеки від гібридної загрози завдяки врахуванню її деструктивного впливу на інші сфери національної безпеки. Подальші дослідження планується спрямувати на підвищення точності кількісного оцінювання рівнів воєнної небезпеки від гібридних загроз.

Список літератури

1. Останков, В. (2019), Войны будущего начинаются сегодня, Военно-промышленный курьер, № 40 (803). С. 5–12.

2. Коданева, С.И. (2020), "Гибридные угрозы" безопасности России:

выявление и противодействие, Контуры глобальных трансформаций: политика, экономика, право, № 13 (2). С. 44–71. https: //doi.org/10.23932/2542-0240-2020-3.

3. Богданович, В.Ю., Свида, І.Ю., Романченко, І.С., Сиротенко, А.М., Дублян, О.В. (2021), Методологія комплексного використання військових і невійськових сил та засобів сектору безпеки і оборони для протидії сучасним загрозам воєнній безпеці України: моногр.; вид.2-ге, розширене та доповнене. НУОУ ім. Івана Черняховського, Київ, 364 с.

4. Бартош, А. (2019), Какой будет стратегия противостояния в XXI веке. Государства стали более уязвимы перед гибридными угрозами. http://nvo.ng.ru/concepts/2019-01-11/1_1029_strategy.html.

5. Магда Є.В. (2016), Загрози гібридної війни для європейської інтеграції України, Стратегічна панорама, № 1. С. 61–65.

6. Приміренко, В.М., Грицай, М.П. (2016). Способи ведення гібридної війни та роль збройної боротьби у ній. Труди ун-ту: зб. наук. пр. НУО України. Київ, № 5 (138). С. 104–109.

7. Сиротенко, А.М. (2018). Шляхи превентивної підготовки сил сектору безпеки і оборони до протидії загрозам воєнного та гібридного характеру в конфліктах XXI-го століття Труди ун-ту: зб. наук. пр. НУО України. Київ, № 1 (146). С. 5–12.

8. Богданович, В.Ю., Свида, І.Ю., Скулиш, Є. Д. (2012). Теоретико-методологічні основи забезпечення національної безпеки України: моногр.: у 7 т. Т.4, Воєнна безпека держави і шляхи її забезпечення; за заг. ред. Є.Д. Скулиша. Київ: Наук.-вид. відділ НА СБ України, 464 с.

Аналіз поняття гібридної війни, її визначення

Микола Павлунько, кандидат військових наук, доцент
Доцент кафедри Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0001-8255-6245
Олег Посмітюх, кандидат військових наук, доцент
Доцент кафедри Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-4467-9532
Сергій Тищук, кандидат технічних наук, доцент
Старший викладач кафедри Національного університету оборони України імені Івана Черняховського,
Київ, Україна
https://orcid.org/0000-0002-9661-5493

Анотація. *В доповіді розглянуті наукові публікації з досвіду протистояння проти гібридних загроз держав світу та на основі даних матеріалів визначені цілі, зміст, методи та способи ведення "гібридної війни" та сформульовано її визначення.*

Ключові слова: *гібридна війна, держава, національна безпека, збройний конфлікт, стратегічні дії.*

Вступ

Постановка проблеми. В сьогоднішніх війнах та збройних конфліктах, як на теренах України, так і в інших регіонах світу проявляються домінуючі важливі риси та характеристики війн майбутнього. Вони все більш набувають гібридного (комбінованого) характеру. Так сучасні воєнні конфлікти характеризуються появою нових форм і методів збройної боротьби. На даний час збройна агресія Російської Федерації, яка мала прихований характер свого початку і проводиться в переважній більшості в політичній, економічній, соціальній, інформаційних сферах і перейшла в "гібридну війну" проти України із прихованим залученням регулярних підрозділів збройних сил РФ.

Аналіз останніх досліджень та публікацій. Вивченню питань ведення "гібридних війн" присвячена велика кількість наукових праць іноземних авторів, а також й українських. Українські автори в основу своїх праць поклали оборонну направленість [1, 5-9]. В той же час, у роботі російських фахівців І. Попова і М. Хамзатова "Война будущего. Концептуальные основы и практические выводы. Очерки стратегической мысли" приділяється значна увага щодо змісту, типології майбутніх війн, стратегії і тактики дій, форм і способів застосування збройних сил на практиці.

Мета доповіді. Метою доповіді є проаналізувати цілі, зміст, поняття, методи та способи ведення "гібридної війни" та сформулювати її визначення.

Виклад основного матеріалу

Поява і розвиток нових стратегічних факторів породило концепт гібридної війни як стратегії протистояння між державами, який неможливо в чистому вигляді віднести ні до війни, ні до миру. Термін "гібридна війна" вперше надано в воєнних документах США и Великобританії на початку XXI сторіччя [3–4].

В англомовних джерелах мова йде о "Hybrid Warfare", у нас же отримав широко ходження термін "гібридна війна". В англійській мові терміну війна відповідають два слова "war" і "warfare" але вони ні є синонімами. Термін "war" за своїм змістом близький до слова "війна", а термін "warfare" – "воєнні дії", "збройна боротьба".

Але таке розуміння термінів не входить в протиріччя з понятійним апаратом вітчизняної воєнної теорії.

У роботах вітчизняних авторів надані різні визначення терміну "гібридна війна".

Курбан А. у роботі "Інформаційні війни в соціальних онлайн-мережах" [5] визначив гібридну війну як комбіноване, інтегроване воєнно-політичне і економічне протистояння у вигляді безстатусного, частіше скритого конфлікту. Звернув увагу на підвищення ролі невійськового впливу на противника за допомогою політичних (дипломатичних), економічних і гуманітарних елементів та зазначив, що інформаційна складова є основою діяльності на усіх етапах конфлікту від підготовки до пост-конфліктного періоду. Етапи гібридної війни: інноваційна агресія (кібернетична війна, економічний тиск, інформаційно-психологічні атаки і інше); застосування нерегулярних збройних формувань або приватних армій (повстанческий, партизанській рух, тероризм); офіційні воєнні дії або демонстрація сили (ідентифікована уніформа, зброя, офіційне визнання участі у конфлікті).

Радковець Ю. у роботі "Уроки дворічної "гібридної війни" Росії проти України" [6] надав наступне визначення - гібридна війна характеризується веденням воєнних дій з одночасним використанням широкого спектру політичних, економічних та інформаційно-пропагандистських заходів.

Левченко О. у роботі "Еволюція гібридної війни Російської Федерації проти України" [7] зазначив, що у гібридній війні комплексно застосовуються: дипломатичні; інформаційні, ідеологічні, економічні та частково військові засоби. Військова складова полягає у використанні комбінації збройних сил, нерегулярних формувань та невійськових сил у сполучені з діями сил спецоперацій. Об'єкти впливу: населення, органи державної влади, збройні сили і інші силові структури, економіка й фінансова система. Гібридна війна ведеться за певним планом, виконанням низки послідовних і взаємозалежних етапів. Етапи можна поділити на три фази: перша - підготовча фаза; друга - активна фаза; третя - закріплююча фаза.

Ліпкан В. у роботі "Сутність гібридної війни проти України" [8] зазначив, що гібридна війна це цілеспрямований процес встановлення зовнішнього управління альфа суб'єктом над об'єктом управління, встановлення тотального контролю над його сферою державного управління, в якому вирішальну роль відіграють інформаційні засоби (одна домінантна група управління підкорила

іншу соціальну групу при цьому не встановлюючи повного та тотального контролю над суверенітетом та територією, іншими важливими, але не життєво необхідними атрибутами, супроводжується капітуляцією збройних сил).

Рижков І. у роботі "Композитна стратегія протидії мережевим та гібридним викликам сучасного тероризму" [10] дав визначення гібридної (компаундної) війни, як військової стратегії, яка передбачає використання різних дій воєнного, дипломатичного, інформаційного характеру, спрямованих на досягнення стратегічних цілей. Зміна пріоритетів у бік використання нерегулярних збройних формувань пов'язана задля ускладнення кваліфікації дій агресора з позиції міжнародного права.

У посібнику [1] під редакцією Агаєва Н. "гібридна війна", в найзагальнішій формі за думкою авторів, визначена як агресія однієї держави проти іншої, зовні замаскована під внутрішньополітичний конфлікт в державі – жертви агресії. Ключовою особливістю – "гібридної війни" є поєднання двох здавалося б взаємовиключних чинників: прямого ведення війни агресором (від ухвалення усіх політичних і навіть оперативних військових рішень до прямої участі в бойових діях регулярних частин збройних сил) і категоричного публічного невизнання агресором своєї участі в конфлікті.

З аналізу досліджень українських авторів, щодо визначення терміну "гібридної війни", можна зауважити: по-перше дослідження стосуються в основному протистоянню України з Росією (гібридних дій Росії проти України), по-друге мають оборонну направленість, по-третє розкривають зміст терміну "гібридна війна" тільки з огляду на питання, які розглядаються автором у роботі.

Для більш змістовного розкриття терміну необхідно відповісти на наступні питання: масштаб, мета, стратегія, сторони, які протистоять, об'єкти впливу, методи, способи дій, хто керує процесом.

І так можна визначити, "гібридна війна" – є сучасна версія війни, як боротьби держави за своє минуле, сучасне і майбутнє, це війна нового покоління. Вона являє собою геополітичне явище. У геополітичному просторі кожна держава вибудовує свій проект, якій визначає місце держави в світі, її національні інтереси. Виходячи з національних інтересів будуються взаємовідношення з іншими державами (визначення їх місця і ролі в забезпеченні національних інтересів держави).

З огляду на вищезазначене за своїм масштабом "гібридна війна" відноситься до стратегічних дій. Вона є перманентною (безперервною) та всеосяжною. Підтвердження цього ми знаходимо в одній з публікацій "NATO Review magazine" де зазначається: "Термін "гібридна війна" був прийнятий усіма державами і став базисом сучасної воєнної стратегії" [2]. На сьогоднішній час вислів "бажаєш миру – готуйся до війни" воєнними теоретиками, з огляду на сучасну парадигму, замінений на "бажаєш миру – воюй".

За мету можна визначити просування та захист національних інтересів держави. Через категорію інтересу досягається взаємозв'язок між політикою, війною і економікою. Британській прем'єр-міністр XIX ст. лорд Генрі Пальмерстон висловив знамениту думку про те, що держава не може мати ні постійних друзів, ні постійних ворогів, але одні лише постійні інтереси. Тому

війна ведеться не за абстрактні ідеї, а за конкретну вигоду. Отже будівництво в державі в цілому повинно виходити з необхідності просування національних інтересів.

Стратегією "гібридної війни" є використання воєнних і невоєнних методів в ході війни спрямованих на досягнення військових, цивільних, політичних, економічних цілей в інтересах держави. Кінцева мета стратегії – стримування, хаотизація і деструкція держави противника.

Класичні стратегії виражені в китайської стратагемі. Стратагема – це "хитромудрий план, оригінальний шлях до досягнення військових, цивільних, політичних, економічних або особистих цілей". Стратагема являє собою сплав стратегії з умінням розставляти приховані від противника пастки.

Традиційними принципами китайської стратагеми є:

- керувати варварами з допомогою варварів;
- атакувати варварів за допомогою варварів;
- стримувати варварів за допомогою варварів.

Сторонами "гібридної війни" можна визнати держави, коаліції держав, глобальні та транснаціональні корпорації, наднаціональні утворення (типу "deep state").

Об'єктами впливу можна вважати: систему державного управління, інфраструктуру, система життєзабезпечення, суспільство, силові структури.

Методи за якими здійснюється вплив можна поділити на: методологічний, хронологічний, фактологічний, економічний, геноциду, силовий.

Основні способи які будуть використовуватися це:

силові – війни, в тому числі громадянська війна, розв'язана в середині держави, збройні конфлікти, "кольорові революції", тероризм, кримінал;

геноциду – наркотики, алкоголь, тютюн, медичні препарати та продукти харчування (які визивають онкологічні захворювання, безпліддя і інші пагубні наслідки для здоров'я людини та її нащадків), антисоціальні програми (скасування соціальних програм);

економічні – кредити під відсотки, санкції проти всіх або окремих секторів економіки, закриття ринків, блокування визначених технологій, санкції проти ключових персоналій, недопущення програмного продукту и кібернетичних технологій держави, хакерські атаки проти економічних інститутів держави;

фактологічні – заміщення традиційних цінностей, ідеологічних конструктів, десакралізація пророків, основних постулатів базових релігій, імплантація та привітання децивілізуючих соціальних практик, хакерські атаки проти політичних інститутів держави;

хронологічні – фальсифікація історії держави (нав'язування своєї точки зору на історичні події), порушення психології народу, соціальних зв'язків, почуття патріотизму;

методологічні – нав'язування хибної філософії, хибного світобачення, порушення зв'язків в суспільстві.

Висновки

Виходячи з розглянутого вище можна визначити що:

“Гібридна війна” – це спосіб дій однієї сторони проти іншої, яка представляє собою сукупність узгоджених і взаємопов’язаних за метою, завданнями, місцем, і часом одночасних або послідовних стратегічних та тактичних дій збройних сил, інших міністерств та відомств держави (коаліції держав), структурних підрозділів транснаціональних корпорацій, транснаціональних банків (наднаціональних утворень), які проводяться за єдиним замислом і планом під єдиним керівництвом з залученням визначених сил та засобів метою якої є просування своїх національних (транснаціональних) інтересів за рахунок національних ресурсів та територіальної цілісності інших держав.

“Гібридна війна” являє собою одну з найбільш актуальних загроз національній безпеці сучасної України. В цій війні адекватною відповіддю України повинні бути гібридні дії, які можна визначити як сукупність узгоджених і взаємопов’язаних за метою, завданнями, місцем, і часом одночасних або послідовних стратегічних та тактичних дій Збройних Сил України, інших міністерств та відомств, які проводяться за єдиним замислом і планом під керівництвом Верховного Головнокомандувача з залученням визначених сил та засобів держави метою яких є протистояння агресивним діям, захист національних інтересів, населення, системи державного управління, територіальній цілісності, традиційних цінностей, історії та забезпечення сприятливих умов для розвитку людини та держави. Гібридні дії повинні здійснюватися як у відповідь на дії агресора так і їх упереджуючи.

Список літератури

1. Агаєв Н. А., Герасименко М. В., Дикун В. Г., Стасюк В. В. Гібридна війна Росії проти України: Інформаційний вимір // навчальний посібник. К.; ТОВ ”7БЦ“, С. – 189.

2. Hybrid war – does it even exist? URL: NATO Review magazine [Електронний ресурс] – Режим доступу: http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/.

3. McGregor Knox and Williamson Murray, Eds. The dynamics of Military Revolution 1300-2050. Cambridge, Cambridge University Press, 2001.

4. Frank G. Hoffman. Conflict in the 21-th Century: the Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, December 2007 [Електронний ресурс] – Режим доступу: www.potomacinstitute.org /images/stories/publications/potomac_hybridwar_0108.pdf.

5. Курбан А “Інформаційні війни в соціальних онлайн-мережах” (Новые формы агрессии. Форум “Современные гибридные войны”. Телеком, военная связь. 2017).

6. Радковець Ю. Уроки дворічної “гібридної війни” Росії проти України. БІНТЕЛ. Журнал геополітичної аналітики. - №2.- 2016.- К. ТОВ “Друкарня Бізнес поліграф”, 2016.- 128с.

7. Левченко О.В. Еволюція гібридної війни Російської Федерації проти України. Наука і оборона №2 2017.
8. Ліпкан В.А. Сутність гібридної війни проти України. Імперативи розвитку цивілізації №2 2015.
9. Компанцева Л.Ф. Інформаційні та організаційні війни. Імперативи розвитку цивілізації №2 2015.
10. Рижков І.М. Композитна стратегія протидії мережевим та гібридним викликам сучасного тероризму. Імперативи розвитку цивілізації №2 2015.

Експлуатація радянських плакатних образів Другої світової війни в конструюванні інформаційного простору тимчасово окупованих територій України

Олександр Лисенко, доктор історичних наук, професор
Завідувач відділу історії України періоду Другої світової війни Інституту історії України НАН України,
Київ, Україна
https://orcid.org/0000-0002-4003-6433
Олександр Маєвський, кандидат історичних наук
Старший науковий співробітник відділу історії України періоду Другої світової війни Інституту історії України НАН України,
Київ, Україна
https://orcid.org/0000-0001-9926-3270
Людмила Хойнацька, кандидат історичних наук, доцент
Професор спеціальної кафедри № 2 Інституту Управління державної охорони України КНУ імені Тараса Шевченка,
Київ, Україна
https://orcid.org/0000-0001-7324-5461

Анотація. *Маніпулятивні пропагандистські підходи в експлуатації пам'яті про Другу світову війну формують на території так званих "республік" специфічний інформаційний простір, який забезпечує незаконним збройним формуванням необхідний рівень підтримки серед місцевого населення, а також виховує ціле покоління молоді з деформованим уявленням як про події Другої світової війни, так і вороже ставлення до України та усієї Західної цивілізації. Відвертий хейтспітч активно увійшов до інформаційного поля через теле- та радіоефіри, періодичні видання, виступи "лідерів" "республік" на мітингах та масових зібраннях. У проведеному авторами дослідженні проаналізована експлуатація російською пропагандою радянських плакатних образів Другої світової війни в конструюванні інформаційного простору псевдодержавних утворень на окупованих РФ територіях України.*

Ключові слова: *агресія, окупація, русский мир, пропаганда, плакат, інформаційний простір, креолізований текст, Друга світова війна.*

Вступ

Постановка проблеми. Одним з інструментів гібридної війни Російської Федерації проти України стали інформаційні технології. Враховуючи специфічні риси ментальності і національний склад значної частини населення Донбасу, російська пропагандистська машина генерувала особливі підходи до обробки масової свідомості у відповідному руслі. Значну частину ідеологічного продукту, зокрема у візуальному інформаційному просторі окупованого Донбасу, становлять креолізовані форми, що експлуатують тематику і стилістику плакатів періоду німецько-радянської війни 1941-1945 рр. Такий формат впливу

на процес колективної самоідентифікації мешканців “ДНР/ЛНР” має на меті зробити їх органічною частиною “русского мира” і налаштувати проти Української держави.

Аналіз останніх досліджень і публікацій. Проблема використання креолізованої продукції періоду Другої світової війни, а також експлуатація візуальних та вербальних образів в агітаційно-пропагандистських акціях на тимчасово окупованій території України допоки залишається поза увагою істориків. В окремих випадках до цього феномену спорадично звертаються публіцисти та політологи. Однак системний аналіз того, як функціонує наочна пропаганда у цьому тематичному сегменті, ще не здійснений.

Методологічні засади дослідження становлять напрацювання провідних фахівців, які займаються студіюванням проблем ідеологічного протистояння в умовах гібридної війни РФ проти України, а також полідисциплінарні прийоми наукового пізнання, що поєднують методики історії, політології, мистецтвознавства, психології та інших наукових напрямів.

Мета доповіді полягає у з’ясуванні особливостей політтехнологій, заснованих на експлуатації радянського ідеологічного продукту часів Другої світової війни в умовах агресії РФ проти України і тимчасової окупації її території.

Виклад основного матеріалу

Після захоплення частини українського Донбасу військами РФ формування інформаційного простору фейкових республік “ДНР/ЛНР” розпочалося з агресивної інформаційно-психологічної кампанії. Ідеологи “русского мира” одразу звернулися до використання креолізованої (тексти, що поєднують лінгвістичну й зображувальну складові) продукції періоду Другої світової війни. Візуальна кампанія розпочалася з актуалізації та ретрансляції емоційно-мотиваційних візуальних кластерів, які були створені радянськими художниками-плакатистами для формування образу ворога, “свого” і “чужого”, батьківщини. Саме ця символіка та цінності, якими вона позначалася, найкраще резонувала з ментальними маркерами значної частини мешканців цього регіону України.

Ідеологи “русского мира” на окупованій території України в Донецькій та Луганській областях активно використовують у своїх кампаніях термінологію та символіку періоду Другої світової війни, формуючи викривлений інформаційний простір за рахунок привласнення Росією вирішальної ролі у розгромі нацизму та конструюванню ворожого, демонічного образу Збройних Сил України. Радянський плакат періоду Другої світової війни став основою пропагандистських акцій і найбільш популярним каналом масової візуальної комунікації.

Серед перших радянських плакатних реплік на біг-бордах 6 на 3 метри у Донецьку з’явилися копії плакатів І. Тоїдзе “Батьківщина-мати кличе!” (1941 р.) (до плакатного аркушу додали лише підтекстівку-заклик – “Вступайте в ряды народного ополчения Донбасса!” (2014 р.); плакат В. Корецького “Воин Красной

Армии, спаси!" (1942 р.), підтекстівка якого була видозмінена на: "Воин русской армии, спаси!" та інші [1].

Другу групу становлять плакати, що цитують чи адаптують візуальні і вербальні складові радянських плакатів та апелюють до радянської мілітарної історії: "Судьбу русского народа повторять подвиги отцов, защищая родную землю. Вступай в народную армию Донецкой республики!" (2014 р.). На банері "Защити республику!", образ шахтаря, створений радянськими художниками-плакатистами, перенесений на фон з триколору "ДНР" та доповнений автоматом замість інструменту. На одному з банерів використано популярне в цьому регіоні побутове звернення: "Мужики! Все на защиту родной земли! Не допустим фильтрационные лагеря нацистов в Донбассе!". Забезпеченням візуальним контентом займалась одіозна структура – "ОПА" (Отдел пропаганды и агитации).

Російська пропаганда культивує радянське минуле, особливо пов'язане з перемогою у Другій світовій війні. При цьому проводиться паралель між нинішніми бойовиками та бійцями, які захищали цю територію у 40-х роках XX століття. На величезних плакатах, що іноді займають цілі висотні будівлі, височіють фотографії радянських солдатів, які обіймають своїх дружин. І тут же, трохи нижче, такий самий сюжет, але вже з місцевими бойовиками. І підпис: "Перемогли тоді – переможемо і зараз".

Окрім банерів на вулицях тимчасово окупованих територій України використовується і малоформатна візуальна продукція та пересувні виставки. Копії плакатів та листівок періоду Другої світової війни розклеюються на інформаційних дошках та фасадах будівель. Проводилися спеціальні конкурси плакатів. Так, 14 квітня 2017 р. у центрі Донецька активісти пропагандистського проекту "АртТаран" розмістили агітаційну виставку плакатів, створену молодими художниками з Донецька, Луганська, Ясинуватої, Єнакієво і Докучаєвська. Виставку умовно було поділено на 4 блоки: 1) день Перемоги; 2) день "Республіки"; 3) день захисника Батьківщини; 4) гуманітарна допомога братніх народів [2]. Серед представлених плакатів значна частина була виконана в радянській стилістиці, з високим індексом цитування, або ж відвертим плагіатом на зразок плаката, ідея і композиційне рішення якого запозичена з автолітографії В. Сєрова "Били, бьем и будем бить!" (1941 р.) з однойменною назвою.

До створення агітаційно-пропагандистської продукції залучаються не лише професійні художники, а й студенти та школярі, яких в директивному порядку змушують брати участь в оформленні виставок до ювілейних дат. Серед конкурсів плакату, в яких брали участь школярі і студенти – "Безопасность Республики – забота общая" (2021 р.) [3].

У рамках діяльності Інтеграційного комітету "Россия – Донбасс" 5 вересня 2017 р. у Донецькому краєзнавчому музеї відкрилася виставка "Плакати Великої Вітчизняної війни", де експонувалися креолізовані тексти з фондів Державного меморіального музею Олександра Суворова (Санкт-Петербург) Ця ж пересувна виставка демонструвала свої експонати і в інших містах на тимчасово окупованій території українського Донбасу. Серед представлених 51-ї копії

творів із зібрань петербурзького музею, які нав'язували асоціативний ряд з подіями на Сході України, були представлені плакати Кукриніксів "Нещадно розгромимо і знищимо ворога", "Смерть німецько-фашистським загарбникам", "Убий фашиста-нелюда", "Воїн Червоної Армії – помстися ворогові за кров і сльози радянських людей!", "Смерть дітовбивцям!" [4]. Подекуди, пропагандисти навіть не змінювали підтекстівки, а додавали лише триколори самопроголошених «республік».

"Велика перемога" в окупованих містах презентується ідеологами-пропагандистами як ідеал мужності і героїзму, притаманний винятково "радянському народу" і його правонаступникам і прямим спадкоємцям, тобто росіянам. Пропагандисти на місцевому рівні усіма доступними методами нав'язують населенню Донбасу особливу самоідентифікацію, називаючи тамтешніх мешканців "людьми великого русского мира", "радянським народом", "народом російським", "русским", "народом Донбасса".

За браком ресурсів і креативності в підходах "міністерство інформації ДНР" та "міністерство освіти і науки ДНР" проводять різноманітні конкурси на кшталт конкурсу мемів і демотиваторів "Языком плаката" [5]. Організатори конкурсу в інформаційному ставили перед учасниками завдання "підготувати свої варіанти демотиваторів чи мемів, присвячених спотворенню правди про Велику Вітчизняну Війну чи сучасному протистоянню з українським нацизмом. Аналогічну функцію мав виконати конкурс плакатів "Жива пам'ять в плакатній графіці" (2019р.). У такий спосіб здійснюється "патріотичне виховання" молоді на традиціях радянського культу "Великої Вітчизняної війни", а також принципового несприйняття сучасних цивілізаційних цінностей та всього українського.

Стандартною практикою російських окупаційних пропагандистських структур є залучення місцевих музейних та бібліотечних фондів, до яких, як правило, звертаються напередодні пам'ятних дат. Одним з чисельних прикладів, може слугувати виставка робіт художників-фронтовиків періоду Другої світової війни "Обпалені війною", яку провели 2017 р. в Донецькому художньому музеї присвячену з нагоди 74-ї річниці визволення Донбасу від німецьких загарбників [6]. Куратори виставки відібрали 54 малюнки з колекцій художників Р. Єфіменка, І. Кириченка, Є. Хмелькова. Більшість робіт ретранслюють нелюдські умови життя в'язнів Бухенвальду, звірства нацистів та героїзм учасників спротиву.

Висновки

Переважно увесь масив тематичних (сконцентрованих на подіях Другої світової війни) креолізованих текстів, які залучаються ідеологами так званих "республік", транслюють у масову свідомість агресивні наративи, культивують ненависть, закликають боротися, нищити та вбивати. На противагу доблесті радянських героїв і героїв "ополчення" наводиться нікчемність "ворогів-фашистів", та "банд укро-фашистів/нацистів". На тимчасово окупованих Росією територіях України головним "об'єктом виховання" є діти та молодь. Затяжна війна дає можливість ідеологам "русского мира" підкріплювати політичну

риторику “ЛДНР-івських пропагандистів”, які наполегливо і послідовно репрезентують тамтешньому населенню російську агресію як “визвольну боротьбу” обложеної “київськими фашистами народної республіки”. Це здійснюється за допомогою проекції історичної пам’яті про минулу війну на сучасний конфлікт, формування єдиного дискурсивного поля з високим мобілізуючим потенціалом, який забезпечує незаконним збройним формуванням необхідний рівень підтримки серед місцевого населення, а також виховує ціле покоління молоді з деформованим уявленням як про історичні події, так і вороже ставлення до України та усієї Західної цивілізації. Пропагандисти конструюють пам’ять про жертви масового насильства Другої світової війни для виправдання сучасного і майбутнього кровопролиття, формуючи підґрунтя для ескалації конфлікту.

Список літератури

1. Маєвський О. (2020), Формування інформаційного простору в так званих «ДНР» та «ЛНР» методами експлуатації візуальних образів Другої світової війни, Інформація і право, № 2 (33), С. 132–140.
2. Молодые художники и дизайнеры ДНР под открытым небом в Донецке организовали выставку агитплакатов [Електронний ресурс]. – Режим доступу: https://dan-news.info/obschestvo/molodye-xudozhniki-i-dizajnery-dnr-pod-otkrytym-nebom-v-donecke-organizovali-vystavku-agitplakatov.
3. Республиканский конкурс видеороликов и научных статей студентов «Безопасность Республики – забота общая!» [Електронний ресурс]. – Режим доступу: http://science.donnu.ru/respublikanskij-konkurs-videorolikov-i-nauchnyh -statej-studentov-bezopasnost-respubliki-zabota-obshhaya.
4. В Донецке открылась выставка «Плакаты Великой Отечественной войны» из фондов Государственного мемориального музея Александра Суворова (г. Санкт-Петербург) – (Министерство культуры ДНР). [Електронний ресурс]. – Режим доступу: http://mincult.govdnr.ru/news/v-donecke-otkrylas-vystavka-plakaty-velikoy-ot echestvennoy-voyny-iz-fondov-gosudarstvennogo.
5. Министерства образования и науки ДНР объявляет конкурс мемов и демотиваторов «Языком плаката». [Електронний ресурс]. – Режим доступу: https://mininfodnr.ru/v-respublike-startoval-konkurs-yazykom-plakata.
6. В Донецке открылась выставка работ художников-фронтовиков «Опаленные войной» [Електронний ресурс]. – Режим доступу: https://mincult. govdnr.ru/tegi/opalennye-voynoy.