№ 2’2021

НАУКА і ОБОРОНА

Щоквартальний науково-теоретичний та науково-практичний журнал

ISSN 2618-1614 (Print)
ISSN 2618-1622 (Online)

Видається з 1994 р.

Зміст

Contents

DOI 10.33099/2618-1614-2021-15-2-3-7
УДК 355.02(477)

В. М. Телелим,
доктор військових наук, професор, професор кафедри стратегії національної безпеки та оборони, Національний університет оборони України імені Івана Черняховського,

В. І. Єфіменко,
старший викладач кафедри стратегії національної безпеки та оборони, Національний університет оборони України імені Івана Черняховського,

П. А. Мінєєв,
провідний науковий співробітник кафедри стратегії національної безпеки та оборони, Національний університет оборони України імені Івана Черняховського

До питання розробки та імплементації плану оборони України

У статті розглянуто деякі історичні аспекти надання питанням планування у сфері оборони системного характеру. Проаналізовано проблеми планування оборони України, зокрема незабезпеченість нормативно-правової бази щодо державного регулювання питань стратегічного планування як на законодавчому, так і на виконавчому рівнях, відсутність у законодавчих документах деяких важливих визначень та наявність некоректних (помилкових) положень. Запропоновано шляхи вдосконалення системи державного стратегічного планування. Визначено пропозиції щодо приведення строків планування у відповідність до термінів каденції Президента України, надання розширених повноважень Міністерству оборони України, порядку затвердження документів плану оборони України.

Ключові слова: планування оборони, план оборони України, система державного стратегічного планування.

Постановка проблеми. У вересні 2019 р. Верховною Радою України були внесені зміни до Закону України «Про оборону України» [1], згідно з якими були визначені поняття «План оборони України» (далі – План оборони), а також відповідальні за визначення його структури та порядок розроблення. Упродовж 2020 р. Міністерство оборони України, яке Кабінетом Міністрів України було визначене відповідальним за розробку Плану оборони, здійснило комплекс заходів з організації виконання цього складного завдання. Зокрема, була створена Міжвідомча робоча група, розроблена структура Плану оборони, підготовлена і проведена стратегічна командно-штабна воєнна гра з метою відпрацювання найскладніших документів, організована низка нарад з фахівцями різних органів державної влади, відпрацьований графік розробки.

Однак практична реалізація розробки Плану оборони виявила певну неготовність окремих міністерств до виконання в установлені терміни визначених документів. Однією з причин такого стану розроблення Плану оборони сьогодні є відсутність цілісної системи державного стратегічного планування. Це, у свою чергу, зумовлює відсутність єдиного підходу до планування, неузгодженість різних планових документів, невизначеність статусу деяких стратегічних документів, відсутність відповідальності за прийняття неефективних управлінських рішень.

Аналіз останніх досліджень і публікацій. Наукову роботу в галузі теорії стратегічного планування та управління ведуть багато фахівців, при цьому не лише тісно пов'язані із сектором безпеки та оборони (В. М. Телелим [2], А. М. Сиротенко [3], О. Ф. Сальникова [4], В. К. Горовенко [5], Р. І. Тимошенко [6]), а й учені, дослідження яких більше спрямовані на державну економічну сферу.

Попри значну кількість наукових публікацій, пов'язаних з дослідженням стратегічного планування та управління, питання створення реально функціонуючої державної системи в цій галузі залишаються невирішеними.

Чинні в Україні документи планування в секторі безпеки та оборони, структури оборонного планування, планування застосування сил оборони сьогодні не складаються в єдину систему державного стратегічного планування, їхня ієрархія та хронологічна послідовність розроблення на законодавчому рівні не визначені.

Виклад основного матеріалу. Перші спроби надати питанням планування у сфері оборони системний характер були зроблені з упровадженням на початку 2000-х рр. у діяльність Збройних Сил України, інших військових формувань процедур оборонного планування. Зокрема, був розроблений і у 2004 р. набув чинності Закон України «Про організацію оборонного планування», у Міністерстві оборони України 21 грудня 2006 р. був виданий наказ № 749 «Про затвердження Положення про організацію стратегічного планування в Міністерстві оборони України».

У зазначеному Положенні наводилися визначення стратегічного планування, його сутність, складові, принципи, об'єкти, суб'єкти, терміни, організація та багато інших важливих дефініцій процесу планування.

Однак проблема полягала в тому, що питання стратегічного планування були сформульовані у відомчому документі (згаданому наказі Міністерства оборони України) та були обов'язковими для виконання лише в Міністерстві оборони і Збройних Силах України.

Водночас питання оборонного планування були законодавчо закріплені в Законі України «Про організацію оборонного планування», що спричинило певний дисбаланс в управлінській діяльності держави, коли лише одна складова загального процесу (оборонне планування) регламентувалася, а сам процес (стратегічне планування) залишався фактично некерованим.

Про це згадувалось у статті В. М. Телелима, Ю. В. Пунди, П. А. Мінєєва [2]. Зокрема, в ній підкреслювалася відсутність у питаннях планування у сфері оборони чіткої системи управлінській діяльності, збалансованого, синхронізованого процесу з дотриманням логічної послідовності розроблення документів, існування невідповідності в питаннях термінології, зверталась увага на випадки затвердження головою держави відомчих документів стосовно розвитку окремих силових структур ще до завершення оборонного огляду й видання Стратегічного оборонного бюлетеня.

Надання більшої системності процесам стратегічного планування в масштабах держави активно розпочалося з початком відбиття збройної агресії РФ та ведення проти України гібридної війни.

Упродовж 2015–2016 рр. у державі вперше в логічній послідовності були розроблені й уведені в дію Стратегія національної безпеки, Воєнна доктрина України, Концепція розвитку сектору безпеки і оборони, Стратегічний оборонний бюлетень, у 2017 р. була затверджена Державна програма розвитку Збройних Сил України.

Вагомим кроком уперед у площині вдосконалення питань стратегічного планування стали Закони України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях» [7], «Про національну безпеку України» [8], зміни до Закону України «Про оборону України» [1], згідно з якими Росія визнається агресором (що необхідно Україні для обґрунтування міжнародно-правових наслідків російської агресії), війна нарешті названа війною, встановлено, що сектор безпеки та оборони України складається не лише із сил безпеки та сил оборони, а й охоплює ще оборонно-промисловий комплекс, а також громадян та громадські об'єднання, котрі добровільно беруть участь у забезпеченні національної безпеки, з'ясоване поняття План оборони та порядок його розроблення.

Окремим розділом у Законі України «Про національну безпеку України» визначені питання планування у сферах національної безпеки та оборони. Зокрема, сформульована мета планування в зазначених сферах, принципи, строки, документи планування та відповідальні за їх розроблення, вперше на законодавчому рівні встановлено, що Стратегія національної безпеки України опрацьовується протягом шести місяців після вступу на пост Президента України, розкрито питання державного оборонного замовлення, фінансового забезпечення сектору безпеки та оборони.

У Збройних Силах України наприкінці 2020 р. введено в дію Доктрину «Об'єднане планування» [9], яка повинна сприяти координації та узгодженню заходів усіх видів планування, створенню в органах військового управління Збройних Сил України всіх рівнів єдиних підходів до процедур об'єднаного планування в загальній системі застосування сил оборони держави.

Утім, попри проведені заходи, слід визнати, що нормативно-правова база з питань державного стратегічного планування не повною мірою забезпечує врегулювання питань як на законодавчому, так і на виконавчому рівнях. Наприклад, згадана Доктрина «Об'єднане планування» призначена для використання в діяльності лише службових осіб Міністерства оборони України, Апарату Головнокомандувача Збройних Сил України, Генерального штабу Збройних Сил України, органів військового управління Збройних Сил України стратегічного та оперативного рівнів. Що стосується органів управління інших складових сил оборони, то застосування положень цього документа не є обов'язковим, ця Доктрина є лише «прийнятною як посилання», та аж ніяк не зобов'язує органи державної влади, які не входять до сил оборони і взагалі до сектору безпеки та оборони, дотримуватися положень Доктрини.

Аналіз головних законодавчих документів державного рівня в зазначеній галузі (Законів України «Про оборону України», «Про національну безпеку України») показує, що, наприклад, такі поняття, як «планування у сфері національної безпеки», «державне стратегічне планування», «об'єднане планування», між собою практично не пов'язуються, хоча за змістом дуже тісно перетинаються, що призводить до неоднозначного тлумачення.

Так, у Законі України «Про оборону України» визначено: «**План оборони України** – складова частина оборонного планування, що містить сукупність документів, які визначають зміст, обсяги, виконавців, порядок і строки здійснення політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту» [1].

Між тим, саме оборонне планування (головною метою якого є визначення пріоритетів і напрямів розвитку сил оборони) відповідно до положень Закону України «Про національну безпеку України» є складовою системи державного стратегічного планування [8].

У Доктрині «Об'єднане планування» наголошується, що планування оборони держави є складовою системи державного стратегічного планування: «**Планування оборони держави** – складова частина системи державного

стратегічного планування, що визначає мету, завдання та порядок дій суб'єктів забезпечення оборони держави, а також розподіл відповідних ресурсів при загрозі застосування воєнної сили, у разі збройної агресії або збройного конфлікту» [9].

Таким чином, виявляється, що двома складовими системи державного стратегічного планування є оборонне планування (Закон України «Про національну безпеку України») та планування оборони держави (Доктрина «Об'єднане планування»), при цьому в обох має бути План оборони, що з погляду коректності зазначеного викликає величезний сумнів (хоча Доктрина «Об'єднане планування» чомусь прямо і не вказує, що План оборони мусить бути складовою планування оборони) (*рис. 1*).

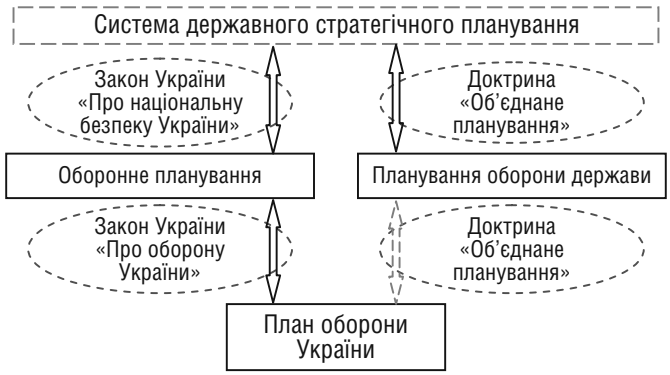


Рис. 1. Некоректності визначень стосовно Плану оборони України

Відповідно, некоректність чинного на сьогодні визначення в Законі України «Про оборону України», в якому план оборони України визначається як складова оборонного планування, стає очевидною.

Водночас, на нашу думку, заради справедливості варто зазначити, що на сьогодні визначення **системи державного стратегічного планування** в законодавчій базі України немає, тож які ще складові входять або можуть входити до цієї системи, не зрозуміло, у зв'язку із чим можна робити лише припущення.

Крім того, в Доктрині «Об'єднане планування» формулювання планування оборони держави як таке, що «визначає … завдання та порядок дій суб'єктів забезпечення оборони держави», можна тлумачити так, що до них (суб'єктів) належать лише ті, які **забезпечують** оборону [9], а не безпосередньо її здійснюють, що звужує зміст плану оборони до комплексу планів підтримки та забезпечення, фактично виключаючи із цього комплексу плани саме воєнних заходів. І це підтверджується, якщо проаналізувати існуючий склад комплексу планів, котрі входять до плану оборони України: серед них немає жодного, який би регламентував заходи безпосередньо відсічі збройній агресії.

Зазначене викликає, на наш погляд, помилкове (чи принаймні дискусійне) визначення планування оборони як окремої складової стратегічного планування у сфері оборони, рівнозначної таким видам планування, як планування відсічі збройній агресії, оборонне планування, мобілізаційне планування [3].

Між тим, аналіз визначень **«оборона України»** та **«план оборони України»** показує, що категорія «планування оборони» за змістом набагато ширша порівняно з переліченими вище видам планування і якраз вона складається з багатьох видів планування, серед яких, зокрема, планування відсічі збройній агресії, оборонне планування, мобілізаційне планування.

Це досить легко з'ясувати, якщо проаналізувати, які ж документи повинні визначати зміст, обсяги, виконавців, порядок і строки виконання **воєнних заходів** щодо підготовки до збройного захисту й захист країни в разі збройної агресії чи збройного конфлікту. Очевидно, що передусім це документи стратегічного планування застосування сил оборони (завчасного та безпосереднього), оборонного планування (розвиток і набуття спроможностей сил оборони), мобілізаційного планування (в частині підготовки сил оборони та їх переведення на організацію та штати воєнного часу).

Проте на сьогодні в переліку документів [9], що входять до комплексу плану оборони України, взагалі відсутні навіть згадки про плани, які регламентують саме воєнні заходи. Тож виходить, що планування оборони представляється як окремий вид планування разом з іншими, серед яких є планування відсічі збройній агресії, оборонне плануванням. При цьому План оборони виглядає лише як комплекс планів забезпечення та підтримки.

На думку авторів статті, загальна система планування оборони (*рис. 2*) повинна не лише об'єднувати всі види планувань підготовки держави до відсічі збройній агресії та безпосередньо її відбиття, а й установлювати зв'язок між документами, а також принципову хронологічну послідовність їх відпрацювання.

Можна стверджувати, що в такому разі система планування оборони означатиме систему державного стратегічного планування у сфері оборони або систему об'єднаного планування, що й залишається лише закріпити на законодавчому рівні.

У принципі до аналогічної думки схиляються автори статті «Актуальні проблеми планування оборони України: комплексний підхід» у журналі «Наука і оборона» (2020, № 1): «Як показує проведене дослідження, План оборони є документом, що має об'єднати за цілями, завданнями і заходами інші види планування в системі стратегічного планування у сфері оборони держави» [3].

На наш погляд, перше, що треба зробити у плані вдосконалення законодавчої бази, – це підготувати Закон України «Про організацію державного стратегічного планування», в якому визначити сутність цього планування, його складові, зв'язок між ними, об'єкти та суб'єкти планування, види планування за строками, документи планування та терміни їх розробки.

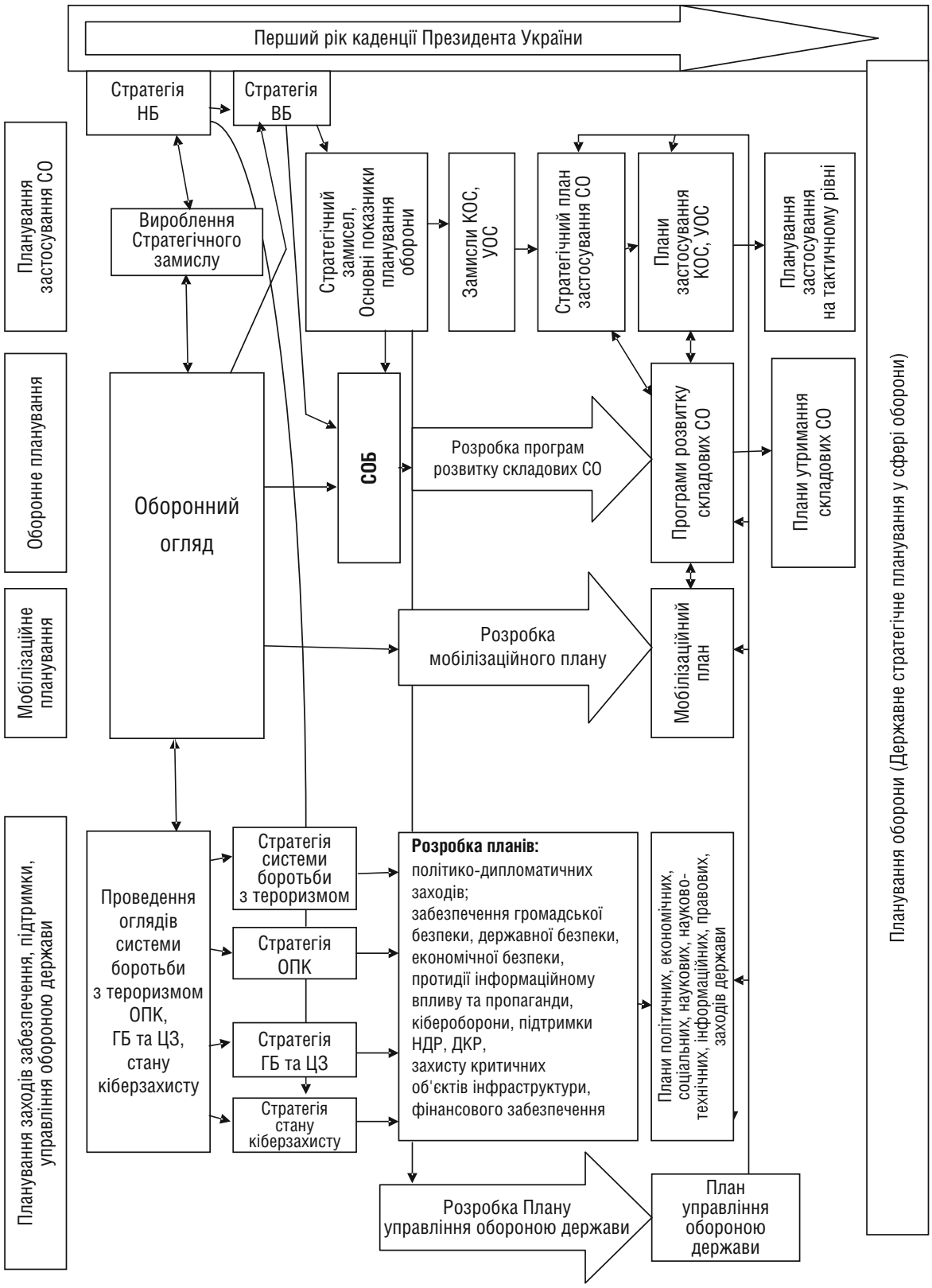


Рис. 2. Загальна система планування оборони

При цьому воєнні заходи планування оборони, особливо заходи стратегічного планування застосування сил оборони, повинні бути визначальними серед інших, оскільки саме вони вирішують долю країни в процесі збройного протистояння з ворогом. Саме на основі стратегічного замислу застосування сил оборони готуються стрижневі дані для Основних показників планування оборони держави: висновки з оцінки воєнно-політичної обстановки довкола України; сценарії застосування сил оборони в кризових ситуаціях воєнного характеру, збройному конфлікті та під час відсічі збройній агресії із зазначенням держав – потенційних противників; загальні кількісні показники чисельності військ (сил); показники розрахункових потреб тощо.

Дуже важливою видається також остаточна прив'язка строків планування до термінів каденції Президента України з огляду на те, що він за статусом є Верховним Головнокомандувачем Збройних Сил України.

На сьогодні строки опрацювання регламентуються лише для Стратегії національної безпеки України, яка розробляється протягом шести місяців після вступу на пост Президента України. Вважаємо за доцільне визначити загальну тривалість відпрацювання всіх документів Плану оборони терміном не більше одного року з тим, щоб більша частина припадала на виконавчу фазу, яка тривала би протягом чотирьох років. Із цього випливає, що термін розроблення Стратегії національної безпеки України було б раціонально скоротити до двохтрьох місяців, зменшити (й офіційно визначити) також тривалість розроблення інших концептуальних документів, передбачити їх опрацювання в режимі паралельної роботи, відвести основну частину на розробку відомчих програм і планів і ретельне узгодження.

З метою впорядкування процесу планування оборони держави варто **поширити повноваження Міністерства оборони України**. Наприклад, у статті 10 Закону України «Про оборону України» доцільно зазначити, що Міністерство оборони України є **головним органом** з планування оборони держави (залишаючи при цьому Генеральний штаб Збройних Сил України **головним військовим органом** з планування оборони держави). Природним кроком виглядатиме факт надання Міністерству оборони України відповідних повноважень, згідно з якими інші центральні органи виконавчої влади будуть зобов'язані виконувати завдання головного органу з планування оборони держави. З метою впорядкування процесу зазначеного планування доцільним виглядає **розроблення документа на кшталт Табеля термінових донесень**, що дасть можливість Міністерству оборони України чіткіше відстежувати й контролювати стан справ у всіх сферах оборони держави.

Треба чітко усвідомити, що розроблення планувальних документів – це лише частка величезної роботи з усього процесу планування оборони держави, яка повинна здійснюватися постійно. Дуже велике значення мають організація постійного контролю за виконанням усього комплексу відомчих планів, регулярне їх узгодження та перевірка відповідності завданням усебічного забезпечення застосування сил оборони України, систематичне їх уточнення й оновлення за необхідності, підготовка відповідних фахівців, які працюють із цих питань, на постійній основі.

Постає ще одне запитання: якщо План оборони – це комплекс документів, то, власне кажучи, яким чином він має затверджуватися Президентом України – Верховним Головнокомандувачем Збройних Сил України? Як вводитись у дію?

На наш погляд, кращим варіантом виглядає затвердження Президентом України – Верховним Головнокомандувачем Збройних Сил України Плану управління обороною держави – документа, який регламентує всі питання керівництва найскладнішими процесами підготовки та відсічі збройній агресії, а також символізує закінчення фази планування оборони. Введення в дію Плану оборони доцільно здійснювати шляхом затвердження його Указом Президента України.

Перелік літератури

1. Про внесення змін до Закону України «Про оборону України» щодо організації оборони держави [Електронний ресурс] : Закон України № 133-IX від 20 вересня 2019 р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/133-20#n2.

2. *Телелим В. М.* До питання організації стратегічного планування у сфері оборони / В. М. Телелим, Ю. В. Пунда, П. А. Мінєєв // Наука і оборона. – 2015. – № 3–4. – С. 40–44.

3. Актуальні проблеми планування оборони: комплексний підхід [Електронний ресурс] / А. М. Сиротенко, П. В. Щипанський, А. К. Павліковський, М. М. Лобко // Наука і оборона. – 2020. – № 1. – С. 3–12. – Режим доступу : https://doi.org/10.33099/2618-1614-2020-10-1-3-12.

4. Аналіз військових аспектів гібридної війни: їх зміст та уроки протидії [Електронний ресурс] / О. Ф. Сальникова, В. С. Корендович, С. І. Антоненко, П. А. Мінєєв // Сучасні інформаційні технології у сфері безпеки та оборони. – 2018. – № 2 (32). – С. 111–118. – Режим доступу : https://doi.org/10.33099/2311-7249/2018-32-2-111-118.

5. *Горовенко В. К.* План оборони України: у зоні особливої уваги [Електронний ресурс] / В. К. Горовенко // Центр досліджень армії, конверсії та роззброєння. – Режим доступу : https://cacds.org.ua/?p=8121.

6. *Тимошенко Р. І.* Проблеми вдосконалення планування оборони України [Електронний ресурс] / Р. І. Тимошенко, М. М. Лобко // Наука і оборона. – 2018. – № 1. – С. 11–17. – Режим доступу : https://doi.org/10.33099/2618-1614-2018-2-1-11-17.

7. Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях : Закон України № 2268-VIII від 18 січня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2268-19#Text.

8. Про національну безпеку України [Електронний ресурс] : Закон України № 2469-VIII від 21 червня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19.

9. Про затвердження доктрини «Об'єднане планування» : наказ Головнокомандувача збройних Сил України № 225 від 22 грудня 2020 р.

DOI 10.33099/2618-1614-2021-15-2-8-16
УДК 355.45.02

В. С. Фролов,
кандидат військових наук, старший науковий співробітник, провідний науковий співробітник центру воєнно-стратегічних досліджень, Національний університет оборони України імені Івана Черняховського,

В. М. Семененко,
кандидат технічних наук, старший науковий співробітник, заступник начальника центру воєнно-стратегічних досліджень, Національний університет оборони України імені Івана Черняховського, полковник

Організація територіальної оборони України в умовах гібридної війни з Росією

В умовах можливого широкомасштабного вторгнення збройних сил Російської Федерації на територію України гостро постає питання організації територіальної оборони в умовах гібридних загроз. Реальну сутність сучасної агресивної політики Росії відображають описані в статті чотири основні напрями загроз національним інтересам України та наведена послідовність основних заходів гібридної агресії Російської Федерації проти України. Організація системи територіальної оборони як складової системи оборони України є недостатньо вивченим елементом організації оборони України. Основні проблеми організації системи територіальної оборони в Україні, закордонний досвід, можливі завдання та варіант структури територіальної оборони України наведені в даній статті. Актуальність статті підтверджує поданий 25 травня 2021 р. Президентом України до Верховної Ради України проєкт Закону «Про основи національного спротиву».

Ключові слова: територіальна оборона, гібридна війна, організація оборони України, агресія Російської Федерації.

Початок XXI століття характеризується активізацією імперських амбіцій Російської Федерації (РФ). Її національні інтереси мають глибоке історичне коріння, яке зароджувалось у ранні часи формування *«Московії»*, потім набуло розвитку за часів Російської імперії та Радянського Союзу.

Лідерам Кремля у відносно короткі строки вдалося побудувати в пострадянській Росії імперіалізм, котрий за своєю сутністю відповідає зразку, яким його малювали ідеологи комунізму, – безмежна влада капіталу, нещадна експлуатація робочого класу, мілітаризація економіки та гонка озброєнь, прагнення до світового панування тощо.

Для відновлення імперії Російська Федерація вибрала найнебезпечніший та найагресивніший спосіб – пряму військову агресію проти держав колишнього СРСР, окупація частини їхніх територій. Основною метою таких дій є примусити народи цих держав перейти під юрисдикцію Росії.

Створення «Придністровської республіки», захоплення Абхазії та Південної Осетії, окупація Криму та сходу України підтверджують імперські амбіції Кремля. Російська Федерація розгорнула воєнні дії в Сирії з метою не допустити енергоресурси Близького Сходу на європейський ринок у збиток «Газпрому» та заявити світовому суспільству про свої амбіції в геополітичному просторі як одного зі світових лідерів.

На наш погляд, сучасна політика кремлівської влади російської імперії XXI ст. базується на:

- неофашистській ідеології «русского мира»;
- найагресивніших рисах зовнішньої політики держав IX–XX ст.;
- сталінській, репресивній системі державного управління.

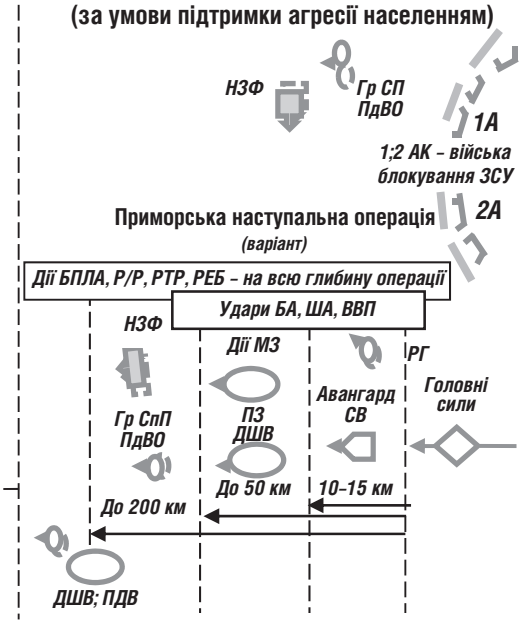
Підготовка та ведення гібридної війни проти України відображає реальну сутність сучасної агресивної політики Росії. Основні напрями загроз національним інтересам України з боку Російської Федерації в умовах ведення гібридної війни, проаналізовані авторами в попередній статті [1], показані на *рисунку 1*.

У процесі підготовки й ведення гібридної війни проти Грузії та України Російська Федерація застосовує новітні способи тиску на національні інтереси на *чотирьох основних напрямах*:

Напрям перший. Дискримінація України в економічній, енергетичній, дипломатичній, транспортній та інших сферах міжнародного співробітництва, порушення міжнародного права та договорів у двосторонніх відносинах тощо. Ведення так званої «м'якої» війни з боку Росії проти України та інших пострадянських республік не припинялось із часів розпаду колишнього СРСР.

Напрям другий. Розгортання та ведення агресивної *інформаційної та кібернетичної боротьби*.

Інформаційна війна ведеться Російською Федерацією в геополітичному просторі постійно та охоплює всі сфери

Перший напрям	Другий напрям	Третій напрям	Четвертий напрям
«М'яка» війна	**Інформаційна боротьба**	**Втручання у внутрішні справи**	**Воєнні дії (за умови підтримки агресії населенням)**
Використання ООН, ОБСЄ, інших організацій для дискримінації України; використання фінансово-економічного та енергетичного впливу на Україну; блокування співробітництва України з ЄС, НАТО ; застосування дипломатичних заходів тощо	Організація інформаційної війни з метою: дискредитації влади України; формування проросійських поглядів серед населення; посилення антиукраїнських настроїв у РФ; активізація системних кібератак тощо	Дестабілізація внутріполітичної обстановки: активізація антидержавних політичних сил; засилання кримінальних елементів; формування НЗФ; диверсії на арсеналах, складах мітинги, протести та блокування роботи влади тощо	
1. Державна Дума 2. Президент РФ 3. Рада Міністрів РФ 4. Дипломатичний корпус РФ	1. Державна Дума 2. Президент РФ 3.ФСБ; МО; ГРУ ГШ РФ; Сили СО 4. Проросійські політичні партії	1. Президент РФ 2. ФСБ; ГУР ГШ; «приватні» НЗФ 3. Козацькі в/формування РФ 4. РГ ВО «Південь» РФ	

5. Зовнішня розвідка РФ

ПдВО – Південний військовий округ РФ;
ПЗ ДШВ – передовий загін у складі ДШВ;
МЗ – мобільні загони (ДШВ, СВ);
НЗФ – незаконні збройні формування.

Рис. 1. Напрями ведення гібридної війни РФ проти України

діяльності. Вона провадиться незалежно від рівня і стану взаємовідносин між державами (групами держав). Основна мета інформаційних операцій – поширення і захист націоналістичних ідей «русского мира», виправдання військової агресії проти сусідніх держав та застосування збройних формувань на інших континентах [2].

А. Ілларіонов, колишній радник В. Путіна, науковий співробітник інституту Катона (Вашингтон, США) вважає сучасну інформаційну боротьбу Четвертою світовою війною та стверджує: «Інформаційна війна – перша тотальна світова війна. І в Першій світовій, і в Другій світовій, і в так званій Третій світовій (Холодній) війнах були чітко окреслені театри воєнних дій, фронти, фланги, тили. ...Через свої іманентні якості інформація володіє властивістю поширюватися, не зважаючи на кордони і визначені обмеження. Тому інформаційна війна не має ні тилу, ні флангів. Фронти інформаційної війни можуть пролягати будь-де» [3].

Напрям третій. Втручання у *внутрішні справи* інших держав. На світовому рівні – втручання у вибори керівних органів, підтримка екстремістських політичних партій і рухів, забезпечення озброєнням та військовими фахівцями антидержавних терористичних організацій.

У постградянських державах втручання РФ у внутрішні страви є більш масштабним та охоплює:

- формування та фінансову підтримку політичних партій, сепаратистських рухів та проросійських ЗМІ;
- усебічну підтримку проросійських сил для виборів (призначення) до органів державної влади;
- проведення комплексних заходів з дискредитації політичного керівництва держав;
- формування агентури та ескалацію криміногенної обстановки тощо.

Російська Федерація завжди активно застосовує комплекс «асиметричних» засобів дестабілізації внутрішньополітичної ситуації та, використовуючи результати першого та другого напрямів загроз національним інтересам, намагається максимально ускладнити діяльність урядових структур держави-суперника та обмежити їхній вплив на соціальні, економічні й інші внутрішньополітичні процеси.

Напрям четвертий. *Військова агресія*. Збройна агресія, як правило, є силовим продовженням досягнення зовнішньополітичної мети, не досягнутої застосуванням «м'якої війни» – силами, засобами та методами трьох попередніх напрямів.

Однією з основних умов вторгнення збройних сил (ЗС) Росії на територію сусідніх держав є підтримка агресії значною кількістю місцевого населення. Відсутність такої підтримки ускладнює обґрунтування окупації

з погляду міжнародного права, ускладнює можливості формування органів місцевого самоврядування, які б діяли в інтересах держави-агресора, та потребує значних затрат на застосування надзвичайних заходів для підтримання функціонування окупаційного режиму на окупованих територіях. Аналіз підтримки населення від початку агресії до сьогодні в загрозливих регіонах України наведений у дослідженнях Національного інституту стратегічних досліджень «Український фронтир» [4–6].

Аналіз розгортання гібридної агресії Росії проти України показаний на *рисунку 2*.

Планування, організацію, забезпечення та управління військовою **агресією РФ проти України** можна поділити на *чотири рівні*:

Перший рівень. Розробку стратегічної ідеї збройної агресії здійснювало політичне керівництво РФ під безпосереднім керівництвом Президента В. Путіна як Верховного Головнокомандувача ЗС РФ. Безпосереднє планування, організацію та всебічне забезпечення здійснювали Федеральна служба безпеки (ФСБ), Міністерство оборони (МО), Генеральний штаб ЗС РФ, штаби видів ЗС, повітряно-десантних військ і штаб Південного військового округу.

Другий рівень. Політичну платформу гібридної агресії РФ в Україні складали «Партія регіонів», Комуністичні партії України та Автономної Республіки Крим, проросійські партії та рухи Криму[1].

Основними виконавцями рішень сепаратистських політичних сил були:

- проросійськи налаштована частина населення східних регіонів;
- пенсіонери «радянської» орієнтації;
- представники кримінального бізнесу, яким загрожувала кримінальна відповідальність за незаконно придбаний бізнес;
- керівний склад органів місцевого самоврядування, правоохоронних органів та Збройних Сил України (ЗСУ), які перейшли на бік агресора тощо.

Сепаратистські політичні партії та рухи формували органи окупаційної влади, організовували адміністративне управління окупованими територіями, жорстко переслідували і знищували українські патріотичні організації та їхніх лідерів під виглядом наведення окупаційного «порядку», організовували мітинги, збори тощо з метою підтримання агресії Росії та протидії державній владі.

Третій рівень. Застосування ЗС РФ, інших військових формувань у гібридній агресії. Загальне керівництво військовою складовою агресії проти України, управління планом стратегічної ізоляції воєнного конфлікту здійснювалися МО, Генеральним штабом ЗС та ФСБ Російської Федерації.

Безпосереднє управління військовою агресією проти України здійснювалось оперативними групами Міністерства оборони, Генерального штабу (ГШ) та ФСБ РФ з об'єднаних командних пунктів Південного військового округу та Чорноморського флоту в м. Севастополь.

Основу військових формувань РФ в агресії проти України складали угруповання військ (сил) сухопутних військ; повітрянодесантні війська; морська піхота Чорноморського, Балтійського та Північного флотів; агентура Головного розвідувального управління (ГРУ) ГШ та ФСБ в Україні; війська спеціального та особливого призначення ЗС РФ; воєнізовані загони «Кубанського козацтва» та незаконні військові формування, які створювалися на окупованих територіях, що комплектувалися проросійським, антидержавним населенням України та «патріотами» «русского мира» Російської Федерації.

Військові частини регулярних військ ЗС РФ застосовувалися для блокування військових містечок Збройних Сил України та Внутрішніх військ Міністерства внутрішніх справ, аеродромів, морських портів, позицій протиповітряної оборони, систем управління повітряною та морською навігацією тощо. На території Донбасу регулярні війська РФ складали основу ведення воєнних дій проти Збройних Сил України.

«Козацькі» підрозділи на першому етапі брали участь у захопленні органів місцевого самоврядування та виконували поліцейські функції на окупованій території. Надалі вони використовувалися для охорони та оборони штабів, артилерійських частин, засобів розвідки та радіоелектронної боротьби, сухопутних комунікацій тощо.

Четвертий рівень. Стихійні дії кримінальних елементів на окупованій території та в інших регіонах України.

Стихійні погроми здійснювалися кримінальними елементами з Росії, України, інших республік колишнього СРСР; правопорушниками, котрі перебували під слідством українських правоохоронних органів тощо.

Основною метою дій таких груп було захоплення архівних документів та кримінальних справ в органах (архівах) МВС, СБУ, судах. Частина з них знищувалася на місці або продавалася зацікавленим злочинцям; важливіші відбирались агентурою ФСБ (в основному документи з архіву СБУ).

Стихійні дії полягали в погромах банків, торговельних закладів з метою наживи. Основними об'єктами для злочинних елементів були склади зі зброєю, боєприпасами та наркотичними речовинами.

Однією з особливостей гібридної агресії проти України є те, що військові формування Російської Федерації вводилися тільки в регіони, в яких місцевим населенням підтримка «русского мира» перевищували 50%[2].

Так, у Дніпропетровській, Запорізькій, Херсонській, Харківській та інших південно-східних областях України агресивні плани керівництва РФ були провалені через незначну підтримку агресії місцевим населенням та високу активність українських патріотичних сил.

[1] За матеріалами інтерв'ю Л. Грача 21 березня 2017 р.; джерело: https://meduza.io/feature/2017/03/21/esli-by-nas-ne-podderzhal-patrushev-v-krymu-stoyal-by-amerikanskiy-flot.

[2] За інформацією офіційного сайту ЦВК України: https://www.cvk.gov.ua.

Організація та керівництво	Виконавці	Основні заходи «гібридної» агресії
1. Формування замислу «гібридної» агресії РФ проти України		
Політичне керівництво РФ, ФСБ, МО	1. Генеральний штаб ЗС. 2. Департаменти ФСБ. 3. Штаби військових округів, флотів, ПДВ, видів ЗС РФ	1. Визначення політичної мети агресії. 2. Розробка планів операцій, методів та способів їх виконання. 3. Організація всебічного забезпечення
2. Політична платформа «гібридної» агресії РФ в Україні		
1. «Партія регіонів» та її союзники. 2. Комуністична партія України. 3. Російські політичні партії в АРК	1. Проросійська частина населення. 2. Пенсіонери та населення «радянської» орієнтації. 3. Представники кримінального бізнесу. 4. Дезертири МВС, ЗСУ, СБУ, прокуратури, судів	1. Формування органів окупаційної влади. 2. Організація адміністративного управління на анексованих територіях. 3. Переслідування патріотичних сил під виглядом наведення порядку. 4. Інформаційно-пропагандистська антиукраїнська діяльність. 5. Організація мітингів на підтримку «русской весны»
3. Застосування ЗС, інших військових формувань РФ у «гібридній» агресії		
1. Оперативні групи ГШ ЗС, ПДВ та ФСБ РФ. 2. Командування Південного ВО та ЧФ РФ	1. Агентура ГРУ ГШ, ФСБ РФ в Україні. 2. Групи СпП ПДВ, ГРУ ЗС та ФСБ РФ; Південного ВО. 3. Військові частини СВ,ПДВ, МП ЧФ, БФ, ПФ, ПКС, РЕБ. 4. «Дивізія» Кубанського козацтва РФ	1. Захоплення органів місцевого самоврядування, правоохоронних органів. 2. Захоплення об'єктів критичної інфраструктури (систем управління навігацією, основних сухопутних магістралей). 3. Блокування військових містечок, позицій ППО, баз ВМСУ, аеродромів, установлення контролю на кордоні з РФ. 4. Введення регулярних військ для блокування ППД та боротьби зі ЗСУ, НГУ
4. Стихійні дії кримінальних елементів		
1. Кримінальні авторитети України та РФ. 2. Стихійні дії кримінальних елементів з метою наживи	1. Криміналітет РФ та інших республік колишнього СРСР. 2. Підслідчі РФ, направлені правоохоронними органами РФ до України. 3. Проросійські кримінальні елементи України. 4. Правопорушники, які на час агресії перебували під слідством	1. Погроми архівів правоохоронних органів (МВС, СБУ, прокуратур). 2. Мародерство, пограбування банків та об'єктів приватної власності. 3. Участь у бойових діях у складі інших бандформувань. 4. Захоплення зброї, боєприпасів та наркотичних засобів

Рис. 2. Послідовність основних заходів гібридної агресії РФ проти України

Підсумовуючи викладене, слід зазначити, що в умовах можливого широкомасштабного вторгнення збройних сил Російської Федерації на територію України гостро постає питання щодо організації системи оборони України в умовах гібридних загроз та особливо її складової – територіальної оборони (ТрО).

Організація системи оборони України з початком відкритої військової агресії РФ проти України у 2014 р. недостатньо вивчена і потребує глибокого аналізу. У процесі такого аналізу пропонується враховувати наведені чотири основні напрями загроз національним інтересам України та послідовність основних заходів гібридної агресії Російської Федерації проти України.

Територіальна оборона як складова системи оборони України також потребує окремих досліджень з метою організації ефективної протидії можливому вторгненню збройних сил РФ.

Частково аналіз існуючої системи протидії загрозам національним інтересам України та шляхи її вдосконалення були розглянуті авторами в [1].

Водночас слід виокремити заходи, які стихійно проводилися патріотами на території більшості областей України від початку російської агресії. Основними з них були:

• по-перше, особовий склад мобілізаційного резерву масово та самостійно прибував до військових комісаріатів для направлення його до складу ЗСУ;

• по-друге, представники найактивнішої частини військовослужбовців запасу формували добровольчі батальйони, які самостійно перекидалися до Донецької та Луганської областей для відбиття вторгнення російських військ на територію України;

• по-третє, з виявленням значних проблем у забезпеченні військ у найкоротші строки сформувався волонтерський рух, який відіграв значну роль у підтриманні боєздатності військових частин ЗСУ та «добробатів» під час ведення бойових дій протягом 2014–2016 рр.;

• по-четверте, в населених пунктах практично всіх регіонів України самостійно розгорталися блокпости, які брали під свій контроль переміщення транспорту і населення, посилювали охорону об'єктів критичної інфраструктури держави тощо.

Отже, з початком російської гібридної агресії проти України стихійно формувалася **система всенародного спротиву**. Водночас у регіонах, де проросійські партії та рухи мали підтримку населення, створювались антиукраїнські воєнізовані організації та незаконні збройні формування під керівництвом сил спеціального призначення ГРУ Генерального штабу та ФСБ РФ.

Таким чином, під час стихійних дій самозахисту населення формувалися деякі елементи **організації територіальної оборони**, які необхідно врахувати командуванню ЗСУ для розробки основ нової системи протидії сучасним методам ведення гібридної війни Російською Федерацією проти України.

Саме тому останніми роками активізувалася законотворча робота щодо організації територіальної оборони України. Були розроблені та подані до Верховної Ради України декілька законопроєктів. На виконання положень Закону України «Про національну безпеку України» та відповідно до положень Стратегії воєнної безпеки, затвердженої Указом Президента України № 121 від 25 березня 2021 р., у державі запроваджений принцип всеохоплюючої оборони, ключовими елементами якої є стійкий опір агресору і використання для відсічі агресії всього потенціалу держави та суспільства. Наразі актуальним є проєкт Закону «Про основи національного спротиву» (№ 5557, зареєстрований 25 травня 2021 р.)[3], поданим Президентом України та прийнятим за основу зі скороченим строком підготовки [7]. Цей проєкт Закону повинен урегулювати питання розвитку територіальної оборони, організації руху опору та відповідної підготовки громадян України до національного спротиву, що є невід'ємною складової всеохоплюючої оборони держави на всій території України.

Одним з лідерів створення системи територіальної оборони за кордоном на сьогодні є Польща [8–10]. Війська територіальної оборони (пол. Wojska Obrony Terytorialnej) – один з п'яти видів збройних сил Польщі, формування якого розпочалося 2015 р. Війська ТрО не належать до резерву, служба в цих військах – це вид дійсної військової служби. Штатна чисельність – 53 тис. військовослужбовців. Війська ТрО охоплюють 17 бригад територіальної оборони: по одній у кожному із 16 воєводств і дві – в Мазовецькому воєводстві[4]. Міністр оборони Польщі 18 березня 2021 р. прийняв рішення створити ще три додаткові бригади ТрО; загальна чисельність військ при цьому залишається незмінною[5].

У цьому проглядається схожість із проєктом Закону «Про основи національного спротиву», поданого Президентом України до Верховної Ради України 25 травня 2021 р. Водночас Україна не може імплементувати собі польський підхід до формування системи територіальної оборони держави з огляду на різні системи організації оборони наших держав. Польща як держава – член НАТО перебуває в загальній системі оборони НАТО, тоді як Україна повинна розраховувати на власні сили. Відповідно, завдання та структура наших систем оборони, зокрема територіальних, різняться.

Проведений аналіз створення **системи ТрО України** виявив низку її основних **проблем**:

1. Обмеженість державного бюджету щодо фінансування сектору безпеки та оборони. Ведення воєнних дій на сході держави вимагає від України зосередження значних фінансових витрат на утримання, розвиток і реформування ЗСУ.

2. В Україні значна кількість населення, особливо на південному сході, підтримує проросійський вектор розвитку держави. У процесі формування підрозділів ТрО необхідно проводити ретельний підбір особового складу, беручи до уваги партійність і політичні погляди кандидатів.

3. Наявність антиукраїнських політичних партій та рухів, які підтримують гібридну агресію Російської Федерації. Контроль над приватними проросійськими ЗМІ в Україні дає змогу РФ проводити широкомасштабні інформаційні операції, що негативно впливає на патріотизм населення та особовий склад ЗСУ.

Кількість проросійських політичних партій та рухів в Україні зростає, їхній вплив на населення поширюється, особливо в південно-східних регіонах. Такий висновок підтверджує порівняльний аналіз результатів місцевих

[3] 1 серпня 2021 р. набрав чинності Закон України № 1702-IX «Про основи національного спротиву», який вводиться в дію з 1 січня 2022 р. Документ було офіційно опубліковано в газеті «Голос України» 31 липня 2021 р. – *Ред.*

[4] Wojska Obrony Terytorialnej. – https://terytorialsi.wp.mil.pl.

[5] Serwis Rzeczypospolitej Polskiej. – https:// www.gov.pl.

Таблиця 1

Результати місцевих виборів у південних областях України у 2015 р. та 2020 р.

№ з/п	Області України	Вибори 2015 р. (Опозиційний блок), %	Вибори 2020 р. (ОПЗЖ, «Партія Шарія»), %	Зростання частки, %
1	Одеська	27,38	35,71	+8,33
2	Миколаївська	26,56	37,65	+11,09
3	Херсонська	20,31	43,74	+23,43
4	Запорізька	33,30	47,69	+14,39

виборів у 2015 р. та 2020 р. у чотирьох південних областях України[6] (*табл. 1*).

4. Запропонований проєкт Закону «Про основи національного спротиву», на наш погляд, порушує один з основних військових принципів.

Зокрема, положення, наведені у статті 1 «Визначення основних термінів», статті 7 «Керівництво національним спротивом», статті 16 «Повноваження штабів зон (районів) територіальної оборони, керівників зон (районів) територіальної оборони», надають керівникам (цивільним) обласних, місцевих, районних державних адміністрацій право управління військовими підрозділами. Такий варіант є нелогічним, ненадійним, неефективним, не відповідає положенням воєнного мистецтва та законам війни. Структура територіальної оборони, тим більше бригадного складу, повинна мати надійну, жорстку систему управління та всебічного забезпечення.

Тематика командно-штабних та оперативно-тактичних навчань угруповань військ (сил) ЗС РФ підтверджує підготовку приморської стратегічної операції. Основними цілями операції Південного військового округу можуть бути: відмежування України від акваторії Чорного моря та заволодіння приморською інфраструктурою; повне оволодіння акваторією Азовського моря; відновлення водного та енергетичного забезпечення Кримського півострова з території Херсонської області.

Як видно з висновків оцінки регіонального безпекового середовища, Росія розгорнула проти України стратегічне угруповання військ (сил) на базі Південного військового округу. Україна спроможна створити та підтримувати оборонний потенціал, здатний протистояти «гібридній» агресії РФ у південно-східному регіоні держави, сформувати і забезпечити одне стратегічне угруповання військ (сил) для відбиття вторгнення військ Південного військового округу ЗС РФ. На іншій території України доцільно організовувати систему територіальної оборони держави відповідно до характеру, методів та способів ведення воєнних і терористичних дій РФ на цій території.

Як показує історичний та світовий досвід ведення війни, територіальна оборона – одна з найскладніших складових оборони держави, що залежить від потужності воєнного потенціалу противника, базується на глибокому аналізі способів та методів ведення ним воєнних дій і потребує врахування внутрішньополітичної ситуації в державі. Основна мета територіальної оборони – посилення обороноздатності держави за рахунок ресурсів органів місцевого самоврядування та патріотично налаштованих громадян, які не підлягають мобілізації.

На наш погляд, в умовах гібридної агресії РФ **оборону України доцільно розвивати за чотирма основними напрямами:**

1) активізація заходів оборонної реформи з метою прискорення вступу до військово-політичного блоку НАТО і розгортання співробітництва з державами – членами євроатлантичного альянсу;

2) організація активної широкомасштабної протидії інформаційним та кібернетичним операціям Російської Федерації проти України;

3) створення сучасних Збройних Сил, заснованих на принципах НАТО, у складі високомобільних оперативно-тактичних об'єднань, на основі яких доцільно формувати міжвидове стратегічне угруповання військ (сил) під єдиним командуванням та управлінням, з новітньою системою всебічного забезпечення військових операцій. Стратегічне угруповання військ (сил) ЗСУ має бути спроможним успішно протистояти наступальним операціям угруповань військ (сил) Південного військового округу РФ;

4) формування сучасної системи територіальної оборони, інтегрованої в загальну систему оборони держави під керівництвом Генерального штабу ЗСУ, здатної успішно підтримувати правовий режим воєнного стану, організувати надійну охорону та оборону державної критичної інфраструктури, передусім військової, забезпечити виконання завдань дорожно-комендантської служби на всій території держави тощо.

Відповідно до статті 18 Закону України «Про оборону України» [11] «територіальна оборона України є системою загальнодержавних воєнних і спеціальних заходів, що здійснюються в особливий період». Зони відповідальності суб'єктів територіальної оборони тісно пов'язані та залежать від військово-адміністративного поділу держави.

Як зазначено в законопроєкті «Про основи національного спротиву», **основними завданнями територіальної оборони** можуть бути [7]:

1) участь у посиленні охорони та захисті державного кордону;

2) участь у захисті населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій, ліквідації наслідків ведення воєнних (бойових) дій;

3) участь у підготовці громадян України до національного спротиву;

4) участь у забезпеченні умов для безпечного функціонування органів державної влади, інших державних органів, органів місцевого самоврядування та органів військового управління;

[6] За інформацією офіційного сайту ЦВК України. – https://www.cvk.gov.ua.

5) участь в охороні та обороні важливих об'єктів і комунікацій, інших критично важливих об'єктів інфраструктури, визначених Кабінетом Міністрів України;

6) забезпечення умов для стратегічного (оперативного) розгортання військ (сил) або їх перегрупування;

7) участь у здійсненні заходів щодо тимчасової заборони або обмеження руху транспортних засобів і пішоходів поблизу та в межах зон/районів надзвичайних ситуацій та/або ведення воєнних (бойових) дій;

8) участь у забезпеченні заходів публічної безпеки і порядку в населених пунктах;

9) участь у запровадженні та здійсненні заходів правового режиму воєнного стану в разі його введення на всій території України або в окремих її місцевостях;

10) участь у боротьбі з диверсійно-розвідувальними силами, іншими збройними формуваннями агресора (противника) та не передбаченими законами України воєнізованими або збройними формуваннями;

11) участь в інформаційних заходах, спрямованих на підвищення рівня обороноздатності держави та на протидію інформаційним операціям агресора (противника).

Для виконання запропонованих завдань доцільно у складі військ ТрО мати дві складові: першу – бойовий склад; другу – систему забезпечення.

До **бойового складу військ ТрО** доцільно віднести підрозділи, призначені для боротьби з диверсійно-розвідувальними групами противника, повітряними десантами, пошуку та захоплення терористичних груп, охорони та оборони важливих об'єктів. До бойового складу доцільно залучати відомчі охоронні підрозділи.

До **системи забезпечення військ ТрО** слід віднести: авторемонтні підприємства незалежно від форм власності, дорожньо-ремонтні, мостобудівні, підрозділи ДСНС та інші структури, відповідно до їхнього призначення.

Кількість, структура та чисельність бойових підрозділів і груп забезпечення залежить від конкретних завдань ТрО та умов воєнно-політичної обстановки в зоні відповідальності територіального командування (ТрК).

Відповідно до Указу Президента України № 39/2016 від 5 лютого 2016 р. [12] «військово-адміністративний поділ території України – це розмежування території держави на військово-адміністративні зони (райони) в інтересах забезпечення оборони України. Військово-адміністративний поділ території України визначає територіальний розподіл відповідальності та повноважень органів військового управління Збройних Сил України у сфері оборони держави на суші, у повітряному та морському просторі».

Отже, військово-адміністративний поділ держави здійснюється в інтересах системи управління військами (силами) та цілковито залежить від конкретних напрямів (регіонів) загроз територіальній цілісності України, а також від методів і способів ведення воєнних дій противником.

Виходячи з воєнно-терористичних дій ЗС РФ та ФСБ, на наш погляд, найдоцільнішим може бути розподіл зон ТрО відповідно до виявлених зон реальних воєнних дій противника: перша зона – ТрК «Схід», охоплюватиме зону ведення воєнних дій з регулярними угрупованнями військ (сил) РФ; друга – ТрК «Центр», міститиме зону протидії розвідувально-терористичним діям противника; третя – ТрК «Захід», охоплюватиме зону боротьби з розвідкою та інформаційними заходами противника.

Отже, відповідно до реальної воєнно-політичної ситуації, що склалася в Україні, на наш погляд, військово-територіальний поділ держави доцільно уточнити й визначити такий **розподіл зон ТрО**:

- ТрК «Схід»: Автономна Республіка Крим, Харківська, Луганська, Донецька, Дніпропетровська, Запорізька, Херсонська, Миколаївська, Одеська області;
- ТрК «Центр»: Чернігівська, Київська (без м. Київ), Житомирська, Полтавська, Черкаська, Кіровоградська, Вінницька, Хмельницька області;
- ТрК «Захід»: Волинська, Рівненська, Тернопільська, Івано-Франківська, Чернівецька, Закарпатська, Львівська області;
- окрема зона ТрО «Київ» має охоплювати сектори, що формуються в адміністративних районах м. Києва.

Кожна зона ТрК може поділятися на сектори, що створюються в межах адміністративних районів областей.

Керівництво та управління зонами (секторами) здійснюватиметься штабами, сформованими на базі військових комісаріатів (територіальних центрів комплектування та соціальної підтримки).

Організаційно-штатна структура та кількість підрозділів ТрО залежатиме від конкретних умов:

- воєнно-політичної ситуації на території відповідальності зони (сектора);
- передбачуваних варіантів дій противника в зоні (секторі);
- наявності, кількості і стану сил безпеки та оборони (насамперед Національної Гвардії України та національної поліції) на закріпленій території відповідальності;
- кількості державних і військових об'єктів, визначених для охорони та оборони, кількості бар'єрних ділянок та їхніх характеристик тощо;
- наявності вільних мобілізаційних ресурсів, які можуть бути залучені до комплектування військ (сил) ТрО тощо.

Отже, до формування структури та складу сил ТрО не можна підходити формально-бюрократично. Роль і місце кожного ТрК, зони й сектора залежать від багатьох факторів та не можуть бути однотипними за складом та чисельністю.

Планування ТрО здійснюється Генеральним штабом ЗСУ на підставі рішення Головнокомандувача ЗСУ та затверджується Верховним Головнокомандувачем ЗСУ – Президентом України разом зі Стратегічним планом застосування ЗСУ.

ТрК підпорядковані командувачу Сухопутних військ ЗСУ, який здійснює безпосереднє командування та управління територіальною обороною. ТрК «Схід» доцільно

включити до складу Об'єднаних сил та підпорядкувати командувачу Об'єднаними силами.

Формування вихідних даних, що складають основу замислу організації ТрО, є одним з найважливіших етапів планування системи ТрО.

Військові частини ТрО не можуть бути більшими за батальйон. Для управління частинами бригадного рівня необхідно мати добре підготовлені та злагоджені штаби, надійну систему всебічного забезпечення та багато інших особливостей, порушення кожної з яких може призвести до хаосу у веденні бойових дій, дезертирства особового складу, мародерства стосовно місцевого населення тощо.

Крім того, бригади ТрО, як правило, входять до загальної системи всебічного забезпечення ЗСУ та потребують витрат на рівні бригад ЗСУ, що не виправдовує себе з погляду економії ресурсів, необхідних для забезпечення оборони держави. Разом з тим, боєздатність бригад ТрО значно поступається боєздатності військових частин ЗС РФ, якщо ми плануємо застосовувати їх для відбиття вторгнення угруповань військ (сил) РФ в Україну на інших операційних напрямах.

Один з варіантів структури ТрО показаний на *рисунку 3*. Міністерство оборони формує вихідні дані для розробки плану ТрО, а саме: перелік об'єктів критичної інфраструктури, які підлягають посиленню оборони, що затверджується КМУ; висновки з оцінки державної політики у сфері оборони, мобілізаційні спроможності держави щодо розгортання військ (сил) ТрО; перелік об'єктів ОПК для посилення їх оборони; представлення державного оборонного замовлення для затвердження КМУ, надання

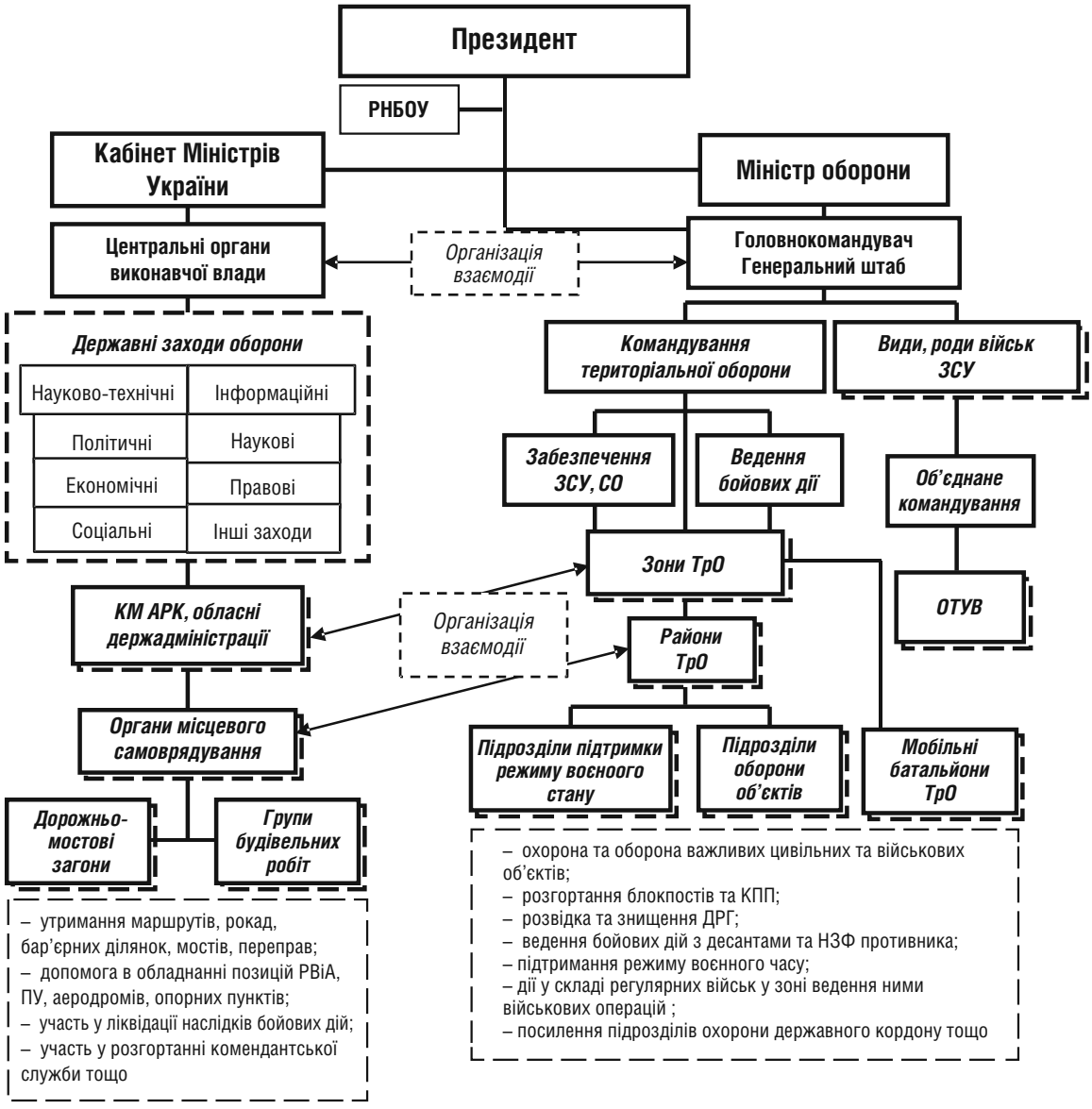


Рис. 3. Структура територіальної оборони держави (варіант)

пропозицій щодо корегування Закону України «Про бюджет України» для забезпечення оборони держави тощо.

Генеральний штаб ЗСУ збирає та аналізує інформацію, необхідну для планування, та надає пропозиції Головнокомандувачу ЗСУ для прийняття рішення на організацію ТрО. До планування ТрО залучаються командування видів ЗСУ та ТрК у частині, що їх стосується.

Планування ТрО на території ведення операції ОС здійснюється командуванням ОС як розділу єдиного Плану об'єднаної військової операції та затверджується Верховним Головнокомандувачем – Президентом України.

Командування зон та секторів здійснюють планування ТрО на закріплених територіях, узгоджуючи виділення сил і засобів для ТрО, питання матеріально-технічного забезпечення та дислокації підрозділів ТрО з органами місцевого самоврядування. Для ознайомлення з повним змістом планів ТрО допускаються особи, визначені командувачем СВ ЗСУ, а в зоні ведення військової операції – Головнокомандувачем ЗСУ.

Висновки

1. Україна спроможна створити й підтримувати оборонний потенціал, здатний протистояти «гібридній» агресії РФ у південно-східному регіоні держави, сформувати і забезпечити одне стратегічного угруповання військ (сил) для відбиття вторгнення військ Південного військового округу ЗС РФ. На іншій території України доцільно організовувати систему територіальної оборони держави відповідно до характеру, методів та способів ведення військових і терористичних дій РФ на цій території.

2. Структура й зони відповідальності системи територіальної оборони залежать від методів, способів та характеру передбачуваних варіантів воєнних дій противника і становлять основу воєнно-адміністративного поділу держави.

3. Організаційно-штатні структури територіальних командувань не можуть бути однаковими. Вони залежать від обсягу, кількості та важливості покладених на них завдань, передбачуваних бойових дій противника, наявності мобілізаційних ресурсів, кількості важливих об'єктів, призначених для оборони тощо.

4. Доцільність формування бригад ТрО є сумнівною та потребує окремих наукових досліджень та розрахунків. Якщо держава спроможна сформувати близько 24 бригад ТрО і забезпечити їх утримання, то доцільніше їх включити до складу ЗСУ й додатково розгорнути оперативно-тактичні угруповання військ (сил) ЗСУ на загрозливих операційних напрямах.

Перелік літератури

1. *Фролов В. С.* Формування перспективної моделі організації оборони України / В. С. Фролов, В. М. Семененко // Наука і оборона. – 2019. – № 3. – С. 3–9. – Режим доступу : https://doi.org/10.33099/2618-1614-2019-8-3-3-9.

2. Cybersecurity as a component of information security: A terminological aspect from the point of view of the Ukrainian information legislation [Електронний ресурс] / P. Snitsarenko, O. Zahorka, A. Pavlikovskyi, O. Oksiiuk // Problems of Infocommunications Science and Technology (PIC S&T) : 2019 IEEE International Scientific-Practical Conference Proceedings. – К. : ФОП Андреев К. В., 2019. – С. 835–838. – Режим доступу : https://doi.org/10.1109/PICST47496.2019.9061272.

3. *Илларионов А.* Вызовы информационной войны для свободного общества и возможная контрстратегия. Выступление на XIX Форуме Открытого Общества Эстонии. Таллинн, 18 сентября 2014 г. [Електронний ресурс] / А. Илларионов // Livejournal. – Режим доступу : https://aillarionov.livejournal.com/735489.html.

4. Паспорт безпеки України: підсумки та рекомендації [Електронний ресурс] / ДМГО «Центр міжнародної безпеки», Національний інститут стратегічних досліджень // Centre for International Security. – Режим доступу : https://intsecurity.org/Pasport_bezpeky_Ukrainy.pdf.

5. Український фронтир: виклики Закарпаття та Причорномор'я [Електронний ресурс] : матеріали дослідження / ДМГО «Центр міжнародної безпеки», Національний інститут стратегічних дослідження // Centre for International Security. – Режим доступу : https://intsecurity.org/UAFrontier_UA_EN.pdf.

6. Український фронтир: виклики для Таврії [Електронний ресурс] : матеріали дослідження / ДМГО «Центр міжнародної безпеки», Національний інститут стратегічних дослідження // Centre for International Security. – Режим доступу : https://intsecurity.org/ukrainian_frontier_vyklyky_dlya_tavriyi.pdf.

7. Про основи національного спротиву [Електронний ресурс] : проєкт Закону України № 5557, дата реєстрації 25.05.2021 // Верховна Рада України. Законодавство України. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72035.

8. National Security Strategy of the Republic of Poland [Електронний ресурс] : 2020 // Biuro Bezpieczeństwa Narodowego. – Режим доступу : https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.

9. Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022 [Електронний ресурс] : przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r. // Biuro Bezpieczeństwa Narodowego. – Режим доступу : https://www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf

10. Koncepcja Obronna Rzeczypospolitej Polskiej [Електронний ресурс] : Maj 2017 // Ministerstwo Obrony Narodowej. – Режим доступу : https://archiwum2019-en.mon.gov.pl/p/pliki/dokumenty/rozne/2017/07/korp_web_13_06_2017.pdf.

11. Про оборону України [Електронний ресурс] : Закон України № 1932-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1932-12.

12. Про затвердження військово-адміністративного поділу території України [Електронний ресурс] : Указ Президента України № 39/2016 від 5 лютого 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/39/2016#Text.

DOI 10.33099/2618-1614-2021-15-2-17-23
УДК 341.24

А. М. Гудзь,
старший науковий співробітник навчально-наукового центру підготовки офіцерів для багатонаціональних штабів, Національний університет оборони України імені Івана Черняховського

Силова політика Російської Федерації: стратегія й тактика реалізації

У статті розглянуті концептуальні особливості та нові тенденції силової політики Російської Федерації, стратегії й тактики їх реалізації. Установлено залежність функціонування міжнародних військово-політичних механізмів та інструментів раннього попередження від сутності військової та політичної діяльності Росії. Аргументовані рекомендації щодо необхідності вироблення превентивних заходів на ранніх стадіях зародження та розвитку міждержавних та регіональних протиріч.

Ключові слова: силова політика, міжнародний конфлікт, загрози.

Постановка проблеми. Останнім часом на міжнародній арені стрімко змінилися військово-політичні умови, які ставлять перед державами принципово нові завдання в системі міжнародних відносин та міжнародної безпеки. Якщо раніше держава мала дві чітко розмежовані функції – внутрішню та зовнішню, то сьогодні грані між ними розмиваються.

Загальна характеристика парадигми побудови державної політики будь-якої держави формується в результаті впливу багатьох об'єктивних і суб'єктивних чинників. У тісному взаємозв'язку із чинниками, пов'язаними з географічним положенням, транспортними шляхами й основними джерелами природних ресурсів силова політика Росії стала важливим інструментом впливу на національну безпеку багатьох держав, передусім України.

Дослідження трансформаційних процесів, викликаних цими чинниками, дає досить повну геополітичну картину тенденцій силової політики Російської Федерації. Загрозу становить те, що держави, які мають миролюбну політику та не проявляють ознак зовнішньої агресії, можуть стати жертвою протиріч і навіть агресії з боку іншої держави. Водночас стан міжнародної сфери може стати потужним фактором внутрішньої безпеки держави.

У статті на підставі результатів системного аналізу відкритої інформації розглядаються вірогідні сценарії силової політики Російської Федерації й тактики її реалізації на тлі регресивних процесів у європейській системі контролю над озброєннями та військовою діяльністю, а також неспроможності регіональних і глобальних безпекових організацій своєчасно впровадити нові превентивні заходи.

Практичні рекомендації можуть бути корисними при проведенні досліджень у галузі забезпечення національної безпеки України.

Мета статті – розглянути характерні особливості та нові тенденції силової політики Російської Федерації, стратегії й тактики їх реалізації; аргументувати рекомендації щодо необхідності вироблення превентивних заходів на ранніх стадіях зародження та розвитку міждержавних і регіональних протиріч.

Виклад основного матеріалу

Дослідження сучасних військово-політичних процесів, які відбуваються на міжнародній арені, дають підстави зрозуміти, що на формування зовнішньополітичної поведінки держав безпосередньо впливають перешкоди на шляху досягнення ними власних геополітичних цілей. Нині чіткішої форми набуває конфронтаційна політика досягнення цих цілей, що призводить до введення впливовими державами силових «правил гри».

Вважається, що конфронтаційні військово-політичні процеси виникають та існують із приводу суперництва між геополітичними суб'єктами за вплив на той чи інший простір. Закономірно, що реалізація силової

політики немислима без агресії та порушення інтересів інших держав і може здійснюватися за їхній рахунок. Усе це певною мірою породжує застосування крайніх (силових) форм взаємовідносин між державами з різними ступенями та інтенсивністю силового тиску.

Однак Росія намагається схилити міжнародну спільноту до думки, що процеси силового тиску не входять до стратегії її національної безпеки, в якій, зокрема, констатується: «У міжнародних відносинах не понижується роль фактору сили. Нарощування і модернізація наступальної зброї, створення і розгортання його нових видів послаблює систему глобальної безпеки, а також систему договорів та угод у галузі контролю над озброєннями»[1].

У наукових колах існує таке поняття як «конфліктна ситуація». Дослідники вважають, що вона ґрунтується на об'єктивних протиріччях інтересів у політиці низки держав та характеризується ступенем міжнародної напруженості. Конфліктна ситуація за своєю сутністю не є конфліктом, проте може слугувати передумовою міжнародного конфлікту. Іншими словами, конфліктна ситуація не породжує конфлікт прямо, а створює обставини його виникнення.

Зважаючи на те, що генерація протиріч у сучасних умовах має, на перший погляд, вигляд «броунівського руху» з постійною трансформацією їхніх форм, важко прогнозувати межу переходу до збройної фази міжнародного конфлікту.

Серед політологів та в наукових колах існує чимало визначень поняття «міжнародний конфлікт». Під час класифікації та агрегування матеріалів спостереження за певними ознаками набирають контурів елементи сукупності, які дають підстави виявити нові риси й закономірності масових явищ і процесів загалом. Таким чином, під міжнародним конфліктом можна розуміти зіткнення інтересів двох або більше сторін (держав, груп держав, народів, політичних рухів тощо), причиною якого може бути наявність (виникнення) протиріч об'єктивного чи суб'єктивного характеру.

Не зважаючи на природу виникнення протиріч та, відповідно, пов'язаних з ними проблем, загалом конфлікт завжди набирає політичної форми, оскільки протиріччя вирішуються державами з властивими особливостями їхньої внутрішньої та зовнішньої політики.

Вивчення причин конфліктів (територіальних, національних, релігійних, економічних, воєнно-стратегічних, науково-технічних) має не лише теоретичне, а й величезне практичне значення. Особливо важливим є вивчення причин та ознак зародження конфліктів на ранніх стадіях. Це пов'язано з тим, що на різних стадіях держава-опонент має застосовувати різні способи протидії.

У процесі історичного становлення конфліктологічної парадигми вивчення суспільства цікаві концепції висловлювали Т. Парсонс, К. Боулдінг, А. Рапопорт, Н. Смелзер.

Зокрема, відомий дослідник проблем миру та конфліктів А. Рапопорт класифікує конфлікти за ступенем небезпеки як «битву», «гру» та «дебати». Найнебезпечнішою він вважає «битву», оскільки в разі виникнення та розвитку її цілі не передбачені ані однією, ані другою стороною, ані міжнародним співтовариством.

У разі розгортання конфлікту у вигляді «гри» поведінка учасників має раціональний характер. На відміну від «битви», не зважаючи на прояв войовничих ознак, сторони не мають планів доводити загострення до критичного стану. Ситуація залишається контрольованою, рішення приймаються з урахуванням факторів та обставин на основі об'єктивної оцінки ситуації.

Найбільш «м'яким» є конфлікт, який розвивається як «дебати». Його ознаками є наміри учасників досягти домовленості шляхом компромісів.

Загальним для всіх наведених вище форм конфліктів є те, що впродовж їхньої активної фази змін можуть зазнати: характер зацікавленості сторін; місце конфлікту; кількість і склад учасників.

У класичному вигляді дослідники розділяють розвиток конфлікту за фазами:

- перша – загострення міждержавних відносин;
- друга – часткова реалізація системи взаємних практичних дій;
- третя – використання різноманітних засобів (не військових) для втягування в конфлікт інших держав (через двосторонні та багатосторонні договори) з метою ускладнення та загострення політичних відносин та практичних дій між учасниками;
- четверта – перехід до демонстраційного застосування сили в обмежених масштабах з метою силового тиску для досягнення своїх стратегічних цілей;
- п'ята – конфлікт із застосуванням сучасного озброєння та втягуванням у нього інших держав з метою розширення його території;
- шоста – урегулювання конфлікту та подолання його наслідків.

Останнім часом сформувалися нові ознаки виникнення та розвитку конфліктів, пов'язаних із суб'єктивними факторами, до яких можна віднести свідому цілеспрямовану зовнішню політику держав. Як свідчать недавні події в Нагірному Карабасі, Росії, Білорусі та в азійських регіонах, не варто ігнорувати такий суб'єктивний фактор, як особистісні характеристики та якості причетних до прийняття рішень державних діячів. Як результат, особистісні взаємовідносини між лідерами можуть значно вплинути на міждержавні відносини і навіть призвести до конфліктних ситуацій.

Західні дослідники вважають, що шлях до активації силової політики відкрили розбіжності поглядів держав на поняття «загрози» та спровоковані Росією регресивні процеси в європейській системі контролю над озброєннями та військовою діяльністю.

[1] Указ Президента Російської Федерації № 683 «О Стратегии национальной безопасности Российской Федерации» від 31 грудня 2015 р.

У контексті відродження ролі глобального гравця на світовій арені, Росія спрямовує свою агресивну силову політику на:

- ескалацію та підтримку в керованому стані кризи на сході України;
- нарощування власних військових можливостей;
- провокування напруженості в Арктиці, Балтиці, на Балканах, у басейнах Чорного і Середземного морів;
- підрив єдності і довіри між країнами НАТО шляхом використання їхніх соціальних і політичних сил, економічних та етнічних проблем.

Частково Російська Федерація досягла своїх цілей. Швидка мілітаризація Чорноморського регіону суттєво змінила баланс сил на її користь і загострила загрози регіональній та загальноєвропейській безпеці. Потужний арсенал російського угруповання на території Автономної Республіки Крим, у тому числі наявність носіїв ядерної зброї, сприяє:

- забезпеченню постійної присутності військово-морського флоту РФ у дальній операційній зоні (східне узбережжя Середземного моря та Сирія) під виглядом захисту російських інтересів на Близькому Сході;
- протидії планам розгортання елементів протиракетної оборони США в Румунії, відповіді на військову діяльність США/НАТО в басейні Чорного моря, тиску на Україну та Грузію в ближній операційній зоні;
- контролю над зоною підвищеної уваги (півднем України, північною та південною частинами Чорного моря, Керченською протокою, Азовським морем, Абхазьким узбережжям Грузії) [1].

Застосовуючи різні способи й методи, Росія продовжує цілеспрямовану силову політику. Згідно з Основами державної політики Російської Федерації на період до 2035 р.[2], в **Арктиці** метою Росії є отримання повного контролю над Північним морським шляхом і видобутком корисних копалин. Для цього розгортаються і відновлюються військові бази на узбережжі Північного Льодовитого океану та його островах (*рис. 1*)[3].

Ураховуючи прогнозоване зростання міжнародної економічної та військової активності та у зв'язку зі зміною клімату в регіоні, Росія створила Північне оперативно-стратегічне командування, модернізує Північний флот, формує нові підрозділи та військові частини, які готуються до дій в екстремальних умовах. Створення угруповань військ (сил) загального призначення збройних сил РФ та системи берегової охорони в Арктичній зоні має на меті забезпечення воєнної безпеки в різних військово-політичних умовах.

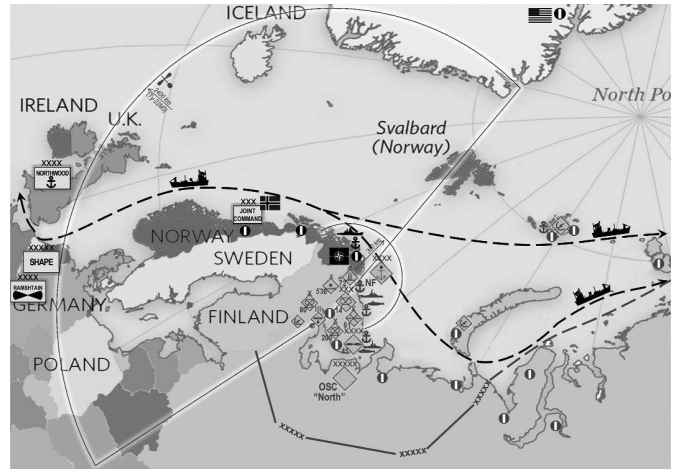


Рис. 1. Нарощування військових можливостей Росії в Арктиці

За оцінкою експертів НАТО, Альянс значно відстає від Росії у своїй здатності диктувати умови в арктичному регіоні з позиції сили.

У **Балтії** можливою метою дій Росії є створення сухопутного коридору до Калінінградської області з території Республіки Білорусь і відрізання країн Балтії від країн НАТО (*рис. 2*). Згідно зі сценаріями масштабних спільних навчань збройних сил Росії та Білорусі (типу «Запад») це завдання може бути покладене на 1-шу танкову армію Західного військового округу. Розгортання ракетних комплексів «Іскандер» у Калінінградській області, а також наявність там систем протиповітряної оборони С-400 сприятимуть створенню зони обмеженого доступу, що внеможливить швидке реагування основних сил НАТО на дії російських військ у країнах Балтії. Не виключається вірогідність розгортання на території Білорусі ракетних комплексів «Іскандер».

Рис. 2. Моделювання можливих дій Росії в Балтії

[2] Указ Президента Російської Федерації № 164 «Об основах государственной политики Российской Федерации в Арктике до 2035 года» від 5 березня 2020 р.

[3] Зазначалося автором на засіданнях Робочої групи високого рівня НАТО на рівні посадових осіб оборонних відомств, керівників верифікаційних структур та високоповажних дипломатичних представників, Брюссель, 2018 р.

Рис. 3. Формування системи присутності РФ у дальній операційній зоні

У регіоні **Середземного моря** прогнози дають підстави стверджувати, що Росія шляхом утримання військово-морських та авіаційних баз продовжить збереження своєї присутності. Окремим завданням для Росії є отримання можливості гарантованого використання Суецького каналу своїми бойовими кораблями як альтернативного маршруту виходу до Середземного моря (*рис. 3*). Про це свідчать наміри Росії щодо безпосередньої участі в модернізації та розвитку каналу, інвестування відповідних проєктів, отримання статусу їх співвласника, а також створення військово-морської бази на сході Лівії, як це вона зробила в Сирії (база ТАРТУС). Не виключається можливість розгортання там ядерного озброєння.

Водночас дії російських корабельних угруповань у Середземному морі можуть значно ускладнитись у разі блокади силами США/НАТО Босфору, Дарданелл та Гібралтарської протоки.

Передбачаючи це, Росія проводить відповідну дипломатичну роботу з турецьким керівництвом, нарощуючи співпрацю з ним у військово-економічній сфері. До поступки Туреччині можна віднести ситуацію з Нагірним Карабахом.

У **південно-західному напрямку** найамбітнішими планами Росії залишаються: окупація більшої частини території правого берега і півдня України та відрізання її від Чорного моря; створення сухопутного коридору до Криму і Придністров'я; провокування дестабілізації ситуації в Румунії та Угорщині.

Наступальні угруповання російських військ можуть бути засновані на об'єднаннях і з'єднаннях Південного, Західного і Центрального військових округів. До складу угруповання оперативно-стратегічного командування «Північ», яке може діяти на Київському та Харківському напрямках, імовірно, увійдуть 20-та загальновійськова армія та 1-ша танкова армія Західного військового округу, а також дві загальновійськові армії Центрального військового округу (*рис. 4*).

До складу угруповання оперативно-стратегічного командування «Південь» на Дніпровському та Херсонському напрямках можуть увійти об'єднання і з'єднання Південного військового округу: 8-ма та 49-та загальновійськові армії, а також 22-й армійський корпус Чорноморського флоту. Відомо, що до складу 8-ї загальновійськової армії входять 1-й і 2-й армійські корпуси (корпуси народної міліції) окупаційних військ на Донбасі.

Дії оперативних і стратегічних командувань можуть мати підтримку з боку 4-ї та 6-ї армій військово-повітряних сил і протиповітряної оборони, кораблів (катерів) Чорноморського флоту і його Каспійської флотилії, озброєних універсальними ракетними комплексами типу «Калібр». Обов'язкова складова дій Росії – блокування та повний контроль над зоною обмеженого доступу в Чорному морі та прилеглих районах його узбережжя.

Можливе також застосування ворожих угруповань з території Республіки Білорусь (з огляду на останні події).

Ураховуючи специфіку місцевості в прикордонних з Білоруссю регіонах, можна передбачити єгерські дії та застосування підрозділів повітрянодесантних військ за сприяння спільного російсько-білоруського постійно діючого оперативно-тактичного угруповання, яке налічує близько 12 тис. осіб (дві третини з них – російська складова).

На **Балканах** стратегічним союзником Росії залишається Сербія. Уповільнення її євроінтеграційних

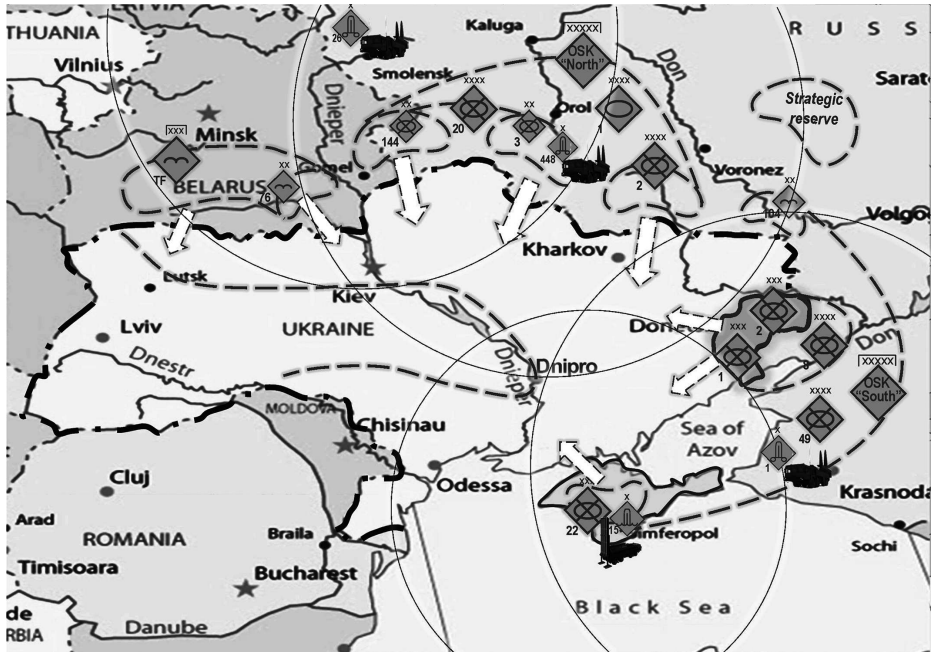


Рис. 4. Моделювання можливих дій РФ у південно-західному напрямку

процесів і блокування членства в НАТО є абсолютним пріоритетом російської політики. Поточною метою дій Росії на Балканах можна вважати провокування регіональної кризи. Одна з таких спроб – підтримка намагання Сербії досягти Адріатичного моря через Чорногорію або вихід Республіки Сербська з Боснії та Герцеговини.

Міжнародні експерти припускають, що намагання Росії поглибити конфлікт і дестабілізувати регіон триватимуть, доки діють санкції проти неї за агресію проти України. Через блокування вступу Боснії та Герцеговини до Європейського Союзу в балканській країні може знову спалахнути збройний конфлікт. За оцінкою експертів, держава Боснія та Герцеговина вже давно стала політичним полігоном для Москви і Заходу.

Теоретично можна змоделювати (*рис. 5*), що в разі успіху в діях в Україні глобальним завданням російських збройних сил може стати розгортання повномасштабного збройного конфлікту з НАТО шляхом дестабілізації ситуації в Румунії, провокування конфлікту між Румунією та Угорщиною з метою захоплення угорцями румунської ділянки території колишньої Австро-Угорщини. У такий спосіб будуть створені умови для вторгнення в Румунію російських військ з окупованих регіонів України і створення коридору до північно-східної ділянки кордону із Сербією і фактично – виходу до Адріатичного моря.

Як підтвердження намірів Росії російсько-сербське співробітництво продовжує динамічно розвиватися по всьому спектру відносин. Росія надає військову підтримку та сприяє модернізації збройних сил Сербії. Нещодавно міноборони РФ з метою підвищення бойового потенціалу поставило сербським збройним силам партію танків Т-72МС і броньованих розвідувально-дозорних машин БРДМ-2МС [2].

Загалом аналіз воєнно-стратегічної ситуації навколо України, в Північноатлантичному регіоні та на Близькому Сході може свідчити про те, що Росія ще не досягла кінцевих цілей своєї силової політики. Поки що вона не готова до відкритого масштабного протистояння зі США і НАТО.

Розтягуючи умовний фронт протистояння з Альянсом від Арктики, Скандинавії до Північної Африки, підтримуючи існуючі кризи і створюючи нові, Росія намагається створити максимально комфортні умови для переговорів із Заходом у так званому пакетному форматі, розпорошувати його зусилля і розширювати базу для можливого вигідного для Росії торгу з найважливіших для себе питань[4].

РФ, усупереч положенням Документа про глобальний обмін воєнною інформацією та Кодексу поведінки[5], вибрала тактику викривлення інформації про свою агресивну діяльність, зокрема щодо перебування військовослужбовців та озброєння поза межами національної території Росії.

Як приклад, Росія не інформує держави ОБСЄ про наявність своїх військ в окремих районах Донецької та Луганської областей України та на території Автономної

[4] Висновок автора з аналізу виступів делегацій держав – учасниць ОБСЄ на щорічних нарадах з оцінювання виконання військово-політичних зобов'язань, Відень, 2017–2019 рр.

[5] Кодекс поведінки ОБСЄ з військово-політичних аспектів безпеки є окремим документом, згідно з яким усі держави ОБСЄ щорічно офіційно надають відповіді на військово-політичний запитальник, який є невід'ємною частиною Кодексу. Інформація узагальнюється Центром запобігання конфліктів ОБСЄ.

Рис. 5. Моделювання можливих дій РФ на Балканах

Республіки Крим як таких, які перебувають поза межами Росії.

Прагнучи дистанціюватися від конфлікту й у такий спосіб зняти із себе відповідальність за те, що відбувається на Донбасі, Росія широко пропагує такі поняття, як «конфлікт в Україні», «громадянська війна», «внутрішній конфлікт», «каральна операція», «ополченці», «нацистсько-бандерівські добровольчі батальйони» тощо.

Ревізуванням офіційних звітів Спеціальної моніторингової місії ОБСЄ в Україні (СММ ОБСЄ) РФ ставить під сумнів компетентність співробітників місії. Неодноразово делегації Росії в рамках робочих органів ОБСЄ намагалися довести до держав – учасниць цієї організації, що системи «Буратіно» – це насправді муляж, який був зібраний «ополченцями» Донбасу для залякування військовослужбовців Збройних Сил України, а виявлений СММ ОБСЄ комплекс «Торн» – це помилка СММ.

Отже, серед держав ОБСЄ втрачена довіра до Російської Федерації через непередбачуваність її силової політики, яка активно використовує прогалини в чинних міжнародних документах, зокрема у Віденському документі 2011 р. про заходи зміцнення довіри та безпеки. Найбільшу стурбованість викликає те, що Росія використовує раптові (незаявлені) військові навчання та навчання нижче порогових рівнів як інструмент зовнішньої політики для демонстрації військової сили з метою значного впливу на безпеку і стабільність у регіоні ОБСЄ.

Занепокоєння держав ОБСЄ викликає також присутність значної кількості підрозділів збройних сил Росії на території Ростовської області, особливо у двадцятип'ятикілометровій зоні вздовж кордону з Україною та їх раптове нарощування під час навчань.

Аналіз подій показує, що причиною такої ситуації були: помилки міжнародних безпекових організацій через необ'єктивний її аналіз; неадекватні завдання, які випливають з даної ситуації та, як результат, розпорошення їхніх зусиль.

Неправильні оцінки намірів та дій Росії, а також занадто демократичні методи реагування на військово-політичну поведінку Кремля свідчать про недооцінку потенціалу президента Російської Федерації В. Путіна. Тому в багатьох регіонах світу виникли нові осередки напруженості, продовжує литися кров, не зникла, а навпаки, посилилася загроза глобального збройного зіткнення.

У традиційному сенсі задля забезпечення міжнародної та регіональної безпеки наголос робиться на фізичному виживанні окремих держав (особливо балканських та колишнього Радянського Союзу), на їхньому праві та можливостях функціонування в міжнародній системі керуючись власним суверенітетом. Як ми пересвідчилися на практичних діях Росії, зазначене стимулює її до порушень правил міжнародної та регіональної безпеки на користь власних інтересів.

Підсумовуючи, необхідно зауважити, що перед державами та міжнародними безпековими організаціями

постають запитання: на якій об'єктивній основі підтримуватимуться мир і безпека та ким і як вони будуть гарантовані в найближчій перспективі?

Висновки та рекомендації

Нинішню військово-політичну ситуацію навколо України, без перебільшень, можна віднести до четвертої фази розвитку конфлікту. Нині Російська Федерація застосовує доволі широкий діапазон економічних, політичних, ідеологічних, психологічних, моральних, міжнародно-правових, дипломатичних і навіть військових засобів (із застосуванням прямого збройного насилля) втягування в протиріччя інших держав у тій чи іншій формі (індивідуально, через військово-політичні союзи, двосторонні та багатосторонні договори та міжнародні організації – ОБСЄ, ООН).

За таких умов особливого значення набувають превентивні та регулятивні механізми міжнародних організацій, які можуть запобігти, нейтралізувати або «розмити» загрози повномасштабного застосування сили.

Наразі розвиток подій за нинішньої ситуації неможливо оцінити за допомогою мережевого графіку. Багатолінійна схема військово-політичних відносин Росії та Заходу не передає всієї картини розвитку подій та не дає підстави прогнозувати момент переходу від протиріч сторін до конфронтації. Тим паче, процес розвитку міжнародного конфлікту – це не простий перехід від однієї фази до іншої, а складна діалектика політичних та інших відносин сторін з питань об'єктивних і суб'єктивних протиріч, інтересів та цілей з багатовекторністю варіантів альтернативного розвитку.

Геополітичні перетворення диктують необхідність істотного інституційного зрушення в системі міжнародної безпеки. Потребує перегляду система взаємодії головних суб'єктів міжнародної політики та безпеки (ООН, НАТО, ЄС), що мають пріоритетні можливості застосовувати силу, у тому числі війська.

У зв'язку із цим потребують кардинальних змін функції міжнародних безпекових організацій з метою адекватно-превентивного реагування на нинішню військово-політичну ситуацію та недопущення її виходу на найбільш гострий політичний рівень – міжнародну політичну кризу й надалі – світову кризу, під час якої виникне пряма загроза того, що однією або декількома сторонами буде застосована військова сила. Війна – це процес, який вийшов з-під контролю. Тому необхідне впровадження нових конструктивних підходів, спрямованих на блокування механізмів ескалації конфліктних відносин.

Історія підтверджує, що надійний спосіб контролювати цей процес – застосовувати чинні механізми та інструменти контролю військової сили. Певний час європейські держави з проблемою ідентифікації ознак зародження воєнного конфлікту надійно справлялися, застосовуючи правила і процедури міжнародних договорів та угод у галузі контролю над озброєннями і військовою діяльністю.

Нині в цій галузі фактично залишилися Документ про глобальний обмін воєнною інформацією (який не передбачає процедур перевірки) та Віденський документ про заходи зміцнення довіри та безпеки 2011 року (має широкий спектр військово-політичних процедур перевірки та реагування). Зберігає свою важливість Вассенаарська домовленість про експортний контроль.

Утратили чинність або дієвість такі вкрай важливі міжнародні договори у сфері стратегічної стабільності: Договір між СРСР та США про скорочення та обмеження стратегічних наступальних озброєнь; Договір між СРСР та США про ліквідацію ракет середньої та меншої дальності.

З огляду на зростання асиметричних загроз із боку Російської Федерації підлягає ревізії безумовне виконання покладених на Збройні Сили України завдань з реалізації міжнародних зобов'язань у рамках Договору з відкритого неба та Договору про звичайні збройні сили в Європі, які «сковують» їхню діяльність. В умовах сьогодення зобов'язання за зазначеними договорами зменшують (виключають) використання військового потенціалу, ускладнюють виконання функцій Збройними Силами України та іншими причетними суб'єктами забезпечення національної безпеки (які мають «важке» озброєння) та стратегічне маскування діяльності Збройних Сил України, яка згідно із міжнародними зобов'язаннями повинна проводитися прозоро.

Ураховуючи військово-політичну ситуацію навколо України, пріоритетом держави має бути також:

- систематизація багатосторонніх та двосторонніх міжнародних зусиль з питань удосконалення міжнародних інструментів, метою яких є своєчасне виявлення та протидія новим викликам і загрозам безпеці;
- здійснення комплексного аналізу та оцінювання результативності й ефективності нормативно-правових та організаційно-функціональних засад державного управління в галузі контролю над озброєннями та військовою діяльністю;
- оптимізація функціональної вертикалі в галузі контролю над озброєннями та військовою діяльністю з метою активації незадіяних резервів ідентифікації ознак зародження воєнного конфлікту.

Перелік літератури

1. *Гудзь А. М.* Військово-політичні зобов'язання Російської Федерації в галузі контролю над озброєннями та військовою діяльністю: стан виконання [Електронний ресурс] / А. М. Гудзь, С. М. Попко // Наука і оборона. – 2020. – № 4. – С. 3–11. – Режим доступу : https://doi.org/10.33099/2618-1614-2020-13-4-3-11.

2. *Степанов А.* Минобороны РФ передало Сербии партию танков Т-72 и разведывательных машин БРДМ [Електронний ресурс] : 23.05.2021 / А. Степанов // Российская газета. – Режим доступу : https://rg.ru/2021/05/23/minoborony-rf-peredalo-serbii-partiiu-tankov-t-72-i-razvedyvatelnyh-mashin-brdm.html.

DOI 10.33099/2618-1614-2021-15-2-24-33
УДК 355.04 (477)

М. М. Лобко,
кандидат військових наук, доцент,
провідний науковий співробітник центру
воєнно-стратегічних досліджень,
Національний університет оборони України
імені Івана Черняховського, генерал-майор у відставці

Об'єднана операція як основна форма відсічі збройній агресії «гібридного» типу

У статті на основі аналізу вітчизняного законодавства, сучасних тенденцій розвитку збройної боротьби досліджуються питання об'єднаної операції як основної форми відсічі збройній агресії «гібридного» типу. Розкриваються особливості сучасних воєнних конфліктів. Проводиться короткий історичний екскурс щодо зародження та розвитку операції як форми застосування військ (сил). Розкриваються особливості та визначаються сутність і теоретичні основи об'єднаної операції. Надається визначення об'єднаних сил, що здійснюють підготовку і проведення об'єднаної операції. Автор пропонує науковцям, експертам і практикам висловити свої погляди на сутність і теоретичні основи об'єднаної операції, що розглядаються у статті.

Ключові слова: форми застосування військ (сил), військова операція, об'єднана операція, сили оборони, об'єднані сили, воєнні, невоєнні, спеціальні засоби збройної боротьби.

Постановка проблеми. На рубежі XX–XXI століть процеси розвитку і модернізації сучасного світу відбувалися під зростаючим впливом глобалізації в усіх сферах життєдіяльності людства. У результаті держави сучасного світу стають більш пов'язаними між собою та взаємозалежними. За таких умов зростає їхня вразливість від політичних, економічних, фінансових, інформаційних, кібернетичних та інших невоєнних засобів впливу.

Водночас парадоксом процесу глобалізації стало те, що він, розвиваючись чималою мірою під впливом чинників пошуку ефективніших відповідей на зростаючі глобальні виклики, сам став величезним викликом для людства. Зокрема, не вдалося впорядкувати систему міждержавних відносин, яка забезпечила б урахування більшості національних інтересів держав, насамперед економічних, фінансових, енергетичних, сировинних, трудових ресурсів тощо [1]. Це призводить до того, що й надалі триває синусоподібний розвиток людства, який породжує фінансово-економічні кризи, суперечки, конфлікти, протистояння тощо. До цього додавалися різні загальносвітові проблеми, зокрема глобальне потепління та зміна клімату, пандемії, великі природні катаклізми, подолання яких додають фінансово-економічних труднощів.

На жаль, для розв'язання суперечок у відстоюванні власних інтересів держав у різних регіонах світу нерідко застосовується воєнна сила й виникають воєнні конфлікти різної інтенсивності. Тож і на рубежі століть, як зазначено в [1, 2], воєнна сила залишається вагомим чинником політики держав у відстоюванні своїх інтересів. Слід констатувати, що під впливом процесів глобалізації змінюється світ, а отже, відбуваються зміни у змісті воєнних конфліктів. Підтвердженням цього є збройна агресія РФ проти України. Саме під час цієї збройної агресії чітко проявилися нові ознаки та зміст сучасних воєнних конфліктів.

Начальник генерального штабу збройних сил РФ генерал армії В. Герасимов у своїй доповіді так охарактеризував зміст сучасних воєнних конфліктів [3]: «Их содержание заключается в достижении политических целей с минимальным вооруженным воздействием на противника. Преимущественно за счет подрыва его военного и экономического потенциала, информационно-психологического давления, активной поддержки внутренней оппозиции, партизанских и диверсионных методов. ...Сочетание традиционных и гибридных методов уже сейчас является характерной чертой любого вооруженного конфликта. При этом если вторые могут использоваться и без открытого применения военной силы, то классические боевые действия без гибридных – уже нет».

Звідси випливає, що для нашої держави актуальною стала проблема пошуку нових ефективних форм протидії російській агресії, захисту суверенітету держави та її територіальної цілісності в межах міжнародно визнаного державного кордону України.

Аналіз останніх досліджень і публікацій. Проведений огляд публікацій із розглядуваної теми показує, що автори в основному розглядають питання операції Об'єднаних сил, яка нині проводиться на Донбасі. Утім, зазначена операція Об'єднаних сил проводиться в умовах дії Мінських домовленостей і встановлених обмежень; її проведення обмежується територіями Донецької та Луганської областей; вона не може забезпечити відсіч ймовірному повномасштабному вторгненню збройних сил РФ в Україну.

Досліджень, які стосуються об'єднаної операції як форми застосування Збройних Сил України й інших складових сил оборони для відсічі ймовірній широкомасштабній збройній агресії проти України, проводилися лише фрагментарно у світлі розгляду традиційних військових операцій та аналізу подій, що відбувалися на сході нашої країни в період з весни 2014 р. і до теперішнього часу.

Проблеми будівництва оборони держави та протидії «гібридній» збройній агресії досить ґрунтовно викладені у низці публікацій [4–8].

У [9, 10] автори розглядають проблеми оборони та її планування в умовах нового характеру воєнних конфліктів сучасності.

У [11] надається аналіз теоретичних основ сучасного російського способу ведення війни, включно з факторами, які впливають на планування і проведення операцій. Визначено основні риси поточної російської доктрини проведення операцій окремих видів і родів військ (сил) збройних сил РФ, а також її відображення на практиці.

Однак слід констатувати, що у своїх дослідженнях автори наведених та деяких інших публікацій не розглядають форми, в яких здійснюється забезпечення оборони та відсічі збройній агресії проти України.

Деякі автори розглядають форми застосування військ (сил), але в основному видів, родів Збройних Сил України [12, 13].

Варто відмітити, що питання об'єднаної операції викладені в низці керівних документів Збройних Сил України. Однак проведений аналіз показує, що положення в них надані не в повному обсязі, звужено та без урахування особливостей сучасних воєнних конфліктів і тенденцій їхнього розвитку.

Попри це, як показує проведене дослідження, об'єднана операція стає основною формою застосування сил оборони в умовах ведення воєнного конфлікту, який отримав назву «гібридного».

Тож автор вважає за необхідне викласти результати наукового дослідження об'єднаної операції як основної форми застосування сил оборони у випадку здійснення широкомасштабної збройної агресії проти України, визначити її сутність і розробити її теоретичні основи. Автор також пропонує науковцям, експертам і практикам висловити свої погляди на запропоновані визначення сутності об'єднаної операції та її теоретичні основи.

Виходячи з викладеного, **мета статті** – на основі аналізу вітчизняного законодавства, керівних документів, історичного досвіду, проведених наукових досліджень, досвіду здійснення збройної агресії РФ проти України, особливостей сучасних воєнних конфліктів, інших факторів провести дослідження об'єднаної операції як основної форми застосування військ (сил), установити її сутність і надати найважливіші положення теоретичних основ цієї операції.

Викладення основного матеріалу

Проведений аналіз показує, що сучасні воєнні конфлікти змінюють свій характер. Основним змістом воєнних конфліктів минулого була збройна боротьба, яка здійснювалась у традиційних формах: операцій, бойових дій, битв, боїв, ударів тощо [14]. Якщо в минулому одним з основних стимулюючих факторів зміни їхнього характеру слугувала поява принципово нової зброї, то на сьогодні це зумовлене насамперед стрімким розвитком технологій виробництва й особливо цифрових інформаційних (інформаційно-комунікаційних) технологій.

Розвиток цих технологій вплинув як на появу нових озброєнь, таких як високоефективні системи управління військами (силами) і зброєю, керована високоточна зброя з використанням штучного інтелекту, запровадження систем і комплексів цієї зброї в усіх сферах збройної боротьби, так і на утворення інформаційного простору в новому вимірі. Упровадження інформаційних технологій дає змогу обробляти великі масиви інформації та ухвалювати обґрунтовані рішення, впливати на психіку людей (інформаційно-психологічний вплив), на прийняття ними рішень, зміну характеру їхньої поведінки тощо. Інформаційна боротьба чинить істотний вплив на зміст збройної боротьби. Масове втілення в життя інформаційних технологій призвело до становлення й розвитку кібернетичного середовища (простору) та зростання масштабів і гостроти боротьби в ньому.

З наведеного випливає, що неодмінною складовою воєнних конфліктів стали політико-дипломатичне, економічне, інформаційне, кібернетичне протистояння, масовий вплив пропаганди на населення й військовослужбовців та інші, тобто невоєнні, засоби.

Слід підкреслити, що для воєнних конфліктів минулого також було притаманне використання невоєнних засобів боротьби. Однак через слабкість розвитку технологій того часу їхній вплив на перебіг і результати збройного протистояння був в основному допоміжним і незначним порівняно з воєнними засобами.

Необхідно додати, що воєнні дії породжують утворення значних районів (зон) руйнувань, пожеж, повеней, заражень, виведення з ладу державної та військової інфраструктури тощо. Такі наслідки воєнних дій визначають значний обсяг завдань цивільного захисту, надання гуманітарної, зокрема медичної допомоги широким верствам населення, їх евакуації з районів, де безпосередньо проводяться бойові дії. Заходи з ліквідації наслідків воєнних дій збільшують різноманітність та обсяг завдань у воєнному конфлікті з використанням невоєнних засобів.

Це вплинуло 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.

Крім згаданого, слід додати, що неодмінними атрибутами сучасних воєнних конфліктів стали такі кримінальні правопорушення, як створення й функціонування незаконних воєнізованих збройних формувань, розвідувально-підривна діяльність іноземних спеціальних служб, організована злочинність, тероризм, бандитизм, грабіжництво, насильство, мародерство, контрабанда, сепаратизм, торгівля зброєю, людьми та їхніми органами, наркоторгівля, неконтрольована міграція тощо. Існує ймовірність виникнення за певних умов конфліктів у сфері міжетнічних і міжконфесійних відносин, радикалізації та проявів екстремізму в діяльності деяких громадських об'єднань та релігійних громад, здійснення актів непокори певної частини місцевого населення, саботажу, колабораціонізму, зрадництва тощо.

Боротьба з ними ставить складні завдання перед правоохоронними органами держави та необхідність їх широкої участі у відсічі збройній агресії шляхом запровадження спеціальних засобів. Адже залучення військ (сил) до виконання таких завдань є нецільовим, розпорошенням сил і засобів та неправомірним з правового погляду.

Поєднане використання вказаних явищ і надає воєнним конфліктам так званого «гібридного» характеру, що свідчить про зміну їхнього змісту.

Саме під час здійснення збройної агресії проти нашої держави в Криму й на Донбасі РФ тією чи іншою мірою використовувала всі названі вище явища і способи впливу та боротьби, що створило значні труднощі у відсічі їй.

Водночас зазначене має негативний вплив на виконання завдань як оборони держави загалом, так і на результати відсічі збройній агресії, а в деяких випадках – аж до невиконання завдань оборони держави чи відсічі збройній агресії.

Необхідно констатувати, що основним змістом сучасних воєнних конфліктів залишається збройна боротьба. Однак невоєнні та спеціальні засоби боротьби, як показує аналіз досвіду воєнних конфліктів останніх десятиліть, мають дедалі більший вплив і навіть здатні відігравати вирішальну роль і стають основним змістом у досягненні сторонами визначеної воєнно-політичної мети збройного протистояння. Нерідко **воєнна сила** стає **фактором підтримки** (наприклад погрози чи відкритої демонстрації застосування воєнної сили) невоєнних та спеціальних засобів боротьби.

Отже, в сучасних воєнних конфліктах чітко простежується використання трьох основних компонентів протиборства: **воєнних засобів** (зброї та військової техніки, що застосовуються в традиційних формах – операціях, бойових діях, битвах, боях, нанесенні ударів тощо); **невоєнних засобів** та **спеціальних засобів**.

Стає зрозумілим, що для забезпечення **досягнення визначеної мети** оборони держави, гарантованої відсічі збройній агресії необхідно, по-перше, **об'єднати завдання**, які випливають з характеру сучасних воєнних конфліктів щодо протидії цим явищам, по-друге, **поєднати зусилля** сил і засобів силових структур сектору безпеки та оборони, органів державної влади, інших державних органів у протидії згаданим вище компонентам воєнних конфліктів, по-третє, 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.

Важливо, що таке поєднання дасть змогу мобілізувати зусилля і можливості всіх складових сектору безпеки та оборони України, органів державної влади, інших державних органів, органів місцевого самоврядування, державних і місцевих ресурсів для відсічі збройній агресії.

Отже, підсумовуючи, слід зазначити, що в умовах зміни характеру сучасних воєнних конфліктів для успішного виконання завдань оборони держави та відсічі збройній агресії необхідно визначити таку **форму застосування** сил і засобів, яка б **охоплювала та об'єднувала воєнні, невоєнні і спеціальні методи, способи і засоби боротьби** та здійснювалася під **єдиним керівництвом за єдиним замислом і планом**.

Визначаючи форму застосування сил і засобів для протидії збройній агресії РФ «гібридного» типу, слід ураховувати, що Росія має значно більший економічний, воєнний, людський та інші види потенціалів порівняно з Україною. Крім того, оцінюючи можливість проведення широкомасштабної збройної агресії РФ, слід відзначити, що вона здійснюватиметься, ймовірно, за концепцією повітряно-наземної наступальної операції із задіянням усіх видів, родів військ (сил), інших військ (крім ядерних) у повітряно-космічному просторі, на суходолі та морі. Відсіч такій збройній агресії РФ за наявної переваги її потенціалів потребуватиме від України задіяння всієї державної та воєнної потуги, мобілізації та напруження всіх людських і духовних сил суспільства.

Проведений аналіз показав, що найбільш прийнятною формою комплексного застосування сил і засобів для протидії збройній агресії РФ «гібридного» типу є **«операція»**.

Важливими і найсуттєвішими ознаками, які характеризують сутність усіх операцій і відрізняють їх від інших форм застосування, є те, що вони розглядаються як **сукупність** розчленованих у просторі, але **узгоджених та взаємопов'язаних** за метою, завданнями, місцем і часом, інших **форм застосування**, таких як бойові дії, битви, бої, удари, а також маневр міжвидових та різнорідних сил і засобів, які здійснюються в рамках операції **за єдиним замислом і планом** під **єдиним керівництвом** для вирішення поставлених завдань у визначеному районі (зоні) в установлений період часу [14].

Операція як форма застосування військ (сил) у воєнному конфлікті зародилася під час російсько-японської війни 1904–1905 рр. У ній виникла вихідна форма оперативного застосування військ – армійська (корпусна)

операція, а на морі – морська битва броньованих флотів. Військові операції в основному об'єднували битви, бої, удари, що проводились арміями (армійськими корпусами) на суходолі із застосуванням, відповідно, піхоти, артилерії, кавалерії, а на морі – морські битви ескадр кораблів.

Значного розвитку операції досягли під час Першої світової війни 1914–1918 рр. У цей період зародилися й розвинулися більші за масштабом фронтові операції як початкова форма оперативно-стратегічних дій, а система операцій почала охоплювати сукупність таких операцій, кожна з яких являла собою суму операцій кількох армій, армійських (кавалерійських) корпусів, а також морської операції. При цьому головною операцією залишалась армійська операція. Поряд із цим почали зароджуватися фронтові (групи армій) операції. У цих операціях уже були задіяні нові види збройних сил та роди військ (сил) того часу, значно зросли масштаби й чисельність військ (сил) (особового складу, зброї та військової техніки).

У роки Другої світової війни 1939–1945 рр. остаточно склалася теорія і практика фронтової (групи армій) операції, яка являє собою не тільки сукупність армійських операцій, що одночасно і послідовно проводяться, а також бойові дії військово-повітряних сил, військ протиповітряної оборони, десантні та протидесантні операції. На цьому етапі з'явились окремі елементи операцій флотів, почали проводитися повітряні і протиповітряні операції в їхніх найпростіших формах (насамперед як авіаційні). У цей період виникла більша операція – групи (декількох) фронтів (груп армій) – як початкова форма стратегічних операцій, яка згодом отримала теоретичне обґрунтування. У результаті система операцій почала охоплювати сукупність операцій групи фронтів (груп армій), які проводилися на визначених стратегічних напрямах, на театрі воєнних дій або на більшій його частині, окремих операцій фронтів і флотів, а також самостійних операцій військово-повітряних сил і військ протиповітряної оборони. Операції проводились як військові, так і спільні та видів і родів військ (сил). Головною операцією стала фронтова операція (операція групи армій), теорія і практика якої отримали подальший розвиток.

Значно зросли масштаби їх проведення. Стратегічні операції об'єднувались у воєнні кампанії та проводилися за єдиним замислом і планом під єдиним керівництвом. Для їх проведення залучалися великі маси військ (сил), у тому числі коаліційні, від тисячі до кількох десятків тисяч одиниць озброєння та військової техніки, десятки мільйонів тон матеріально-технічних запасів тощо.

Розвиток операцій за різними показниками призвів до утворення в післявоєнний період системи операцій застосування військ (сил). Вона являє собою найвищу, найзагальнішу форму стратегічного та оперативного застосування військ (сил), яка склалася в державі та яка охоплює всю сукупність організованих і взаємопов'язаних між собою операцій та інших форм, спрямованих на досягнення цілей війни шляхом вирішення всього комплексу стратегічних та оперативних завдань з відповідною їх класифікацією, а також з особливими, тільки їй притаманними внутрішніми зв'язками, відношеннями та закономірностями [13].

Важливо, що в реальних умовах у кожному періоді воєнного конфлікту з усіх видів можливих операцій (бойових дій) виокремлюються й застосовуються ті, які випливають з обстановки й необхідні для виконання покладених завдань та досягнення тих чи інших цілей.

Зі здобуттям незалежності у Збройних Силах України склалася система операцій, яка охоплювала всі форми їх застосування. Основними формами застосування Збройних Сил України (військ, сил) у різні періоди їхнього розвитку були стратегічні дії, операції, бойові дії, битви, бої та удари, спеціальні, стабілізаційні дії, дії під час ведення територіальної оборони, дії миротворчих контингентів тощо.

Останнім часом до вказаних форм додались інформаційні, інформаційно-психологічні, кібернетичні операції (дії) тощо.

У сучасному розумінні 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 [14].

Операції більшого масштабу (стратегічні, оперативно-стратегічні) почали охоплювати й операції меншого масштабу (армійські, корпусні).

Це визначення операції стало класичним як таке, що розкриває сутність та охоплює всі основні показники, які характеризують зміст збройної боротьби в цій формі, та об'єднує зусилля військ (сил), задіяних у виконанні поставлених завдань і досягненні визначених цілей.

У державах – членах НАТО такі операції називають «об'єднаними». Із цим можна погодитись, адже операція об'єднує всі інші форми застосування об'єднань, з'єднань, військових частин різних видів, родів збройних сил, які виконують покладені на них завдання у взаємодії між собою задля досягнення визначеної мети цієї операції. Однією з характерних особливостей сутності таких операцій є наявність в органах військового управління держав Альянсу структурних підрозділів, які організують військово-цивільне співробітництво для співпраці із цивільними органами влади в районі проведення операції в інтересах захисту й забезпечення життєдіяльності місцевого населення і створення сприятливих умов для виконання завдань у районі операції.

Наведене трактування операції прийняте за основу і для визначення об'єднаної операції в керівних документах Збройних Сил України.

Однак об'єднана операція, визначена керівними документами Збройних Сил України, охоплює в основному воєнні засоби збройної боротьби і значною мірою не враховує зміну характеру сучасних воєнних конфліктів, їхньої «гібридності», особливостей збройної боротьби

в них, значне розширення завдань оборони держави та відсічі збройній агресії. Більше того, в зазначеній операції передбачена можливість самостійного або у взаємодії (зі Збройними Силами України) виконання завдань операції іншими складовими сил оборони. До чого це призводить ми спостерігали на певному негативному досвіді проведення антитерористичної операції на Донбасі, особливо на початковому її етапі.

Отже, спираючись на викладене, можна визначити сутність об'єднаної операції в сучасних воєнних конфліктах та з урахуванням перспектив їхнього розвитку.

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.

Складовими зазначених форм застосування військ (сил) є бої, удари, маневр з'єднань, військових частин видів і родів військ (сил) Збройних Сил України та інших військових формувань, що проводяться одночасно і послідовно за єдиним замислом і планом, під єдиним керівництвом для виконання поставлених завдань та досягнення визначеної мети.

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

Примітка. *Сутність і характеристика вказаних форм застосування загальновідомі й у подальшому не розглядатимуться.*

До **невоєнних засобів** належать 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;
- 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.

Загальна схема моделі об'єднаної операції показана на *рисунку 1*.

Рис. 1. Загальна схема моделі об'єднаної операції

Надалі дослідимо та визначимо основні положення теоретичних основ об'єднаної операції.

Мета об'єднаної операції визначається залежно від стану і перспектив розвитку воєнно-політичної та воєнно-стратегічної обстановки, визначеної воєнно-політичної та воєнно-стратегічної мети відсічі збройній агресії, складу й можливостей своїх військ (сил), характеру воєнної загрози, мети й імовірного замислу дій агресора, складу його військ (сил), їхніх можливостей, особливостей місцевості та інших факторів.

Необхідно також ураховувати, що 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.

Тому **мета об'єднаної операції** полягатиме у зриві підготовки та відбитті вогневих ударів агресора, завданні поразки його наступальним угрупованням, утриманні ключових районів території, що обороняється, шляхом проведення активних бойових дій завдати втрати угрупованням противника, що вторглися, та проведенням визначених невоєнних, спеціальних заходів, заходів спротиву створити критичні умови для його перебування на тимчасово захоплених (окупованій) території держави і припинення бойових дій.

Визначена **мета досягатиметься** проведенням усього комплексу воєнних, невоєнних і спеціальних засобів, як-от: операцій, дій, заходів, що проводитимуться одночасно і послідовно за єдиним замислом і планом під єдиним керівництвом у рамках об'єднаної операції.

Об'єднана операція зазвичай матиме такий **зміст**:

- приведення в готовність до виконання завдань за призначенням військ (сил) та їх оперативне розгортання;
- підготовку і проведення оборонних, наступальних (контрнаступальних), повітряних, морських, спеціальних, стабілізаційних, протидесантних операцій утворених угруповань військ (сил);
- бойові дії угруповань військ (сил) видів Збройних Сил України;
- битви угруповань родів військ (сил);
- бої, удари, маневр з'єднань, військових частин видів і родів військ (сил) Збройних Сил України та інших військових формувань;
- дії спеціальних військ, служб, логістики тощо;
- інформаційні, інформаційно-психологічні, кібернетичні операції (дії, заходи, акти, акції);
- гуманітарні, рятувальні (пошуково-рятувальні), евакуаційні й інші операції;
- заходи правового режиму воєнного (надзвичайного) стану;
- заходи місцевих державних адміністрацій, обласних рад оборони (в разі їх створення), органів місцевого самоврядування;
- заходи, що проводять військово-цивільні (військові) адміністрації (в разі їх створення);
- заходи єдиної державної системи цивільного захисту (надзвичайних ситуацій, евакуаційні, епідеміологічні (епізоотичні, епіфітотичні) тощо;
- спеціальні операції;
- антитерористичні операції;
- заходи й дії сил і засобів територіальної оборони;
- спеціальні, службово-бойові, оперативно-розшукові заходи й дії сил і засобів та інші форми, що використовуються правоохоронними органами.

Під час проведення об'єднаної операції у визначених зонах (районах) визначеними силами і засобами проводитимуться стратегічні дії, зокрема в інтересах цієї операції.

Доречно зауважити, що саме наведена сутність об'єднаної операції, визначений комплекс воєнних, невоєнних і спеціальних засобів та її зміст забезпечують утілення «засад всеохоплюючої оборони України» викладених у [2]. 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.

Розмах об'єднаної операції визначається метою та покладеними завданнями, показниками операцій утворених угруповань військ (сил), особливостями оперативного обладнання території, фізико-географічними умовами операційних напрямків, обстановкою, що склалася, а також характеристиками угруповань військ (сил) своїх та противника, замислом і ймовірною метою його дій та наявністю запасів матеріально-технічних засобів та інших необхідних ресурсів.

Для проведення операції визначається операційна зона, а для оперативно-тактичних (оперативних) угруповань військ (сил) – операційні райони або смуги операцій.

Проведений аналіз показує, що зародження і розвиток воєнних конфліктів відбувається за певними етапами. Отже, **об'єднана операція має готуватись і проводитися за етапами**, виходячи зі стратегічного замислу відсічі збройній агресії.

Проведене дослідження показує, що етапами об'єднаної операції доцільно встановити:

- завчасну підготовку;
- безпосередню підготовку;
- оперативне розгортання військ (сил), органів, інших сил і засобів, що беруть участь в операції, утворення угруповань військ (сил) та підготовку зони (районів) до проведення операції;
- виконання завдань та заходів операції;
- завершення операції.

Завчасна підготовка об'єднаної операції проводиться переважно в мирний час. Вона проводитиметься і в умовах, які склалися в Україні на сьогодні у зв'язку з продовженням збройної агресії РФ на Донбасі.

Завчасна підготовка операції становить комплекс взаємопов'язаних заходів, які проводяться командуванням, органами військового управління, військами (силами), іншими органами, щодо її планування, організації,

всебічного забезпечення, підготовки органів військового управління, військ (сил), інших органів та зони (району) до виконання завдань за призначенням.

На цьому етапі здійснюється оцінювання та прогнозування воєнно-політичним керівництвом держави, Міністерства оборони та керівництвом Збройних Сил України можливих варіантів розвитку воєнно-політичної, воєнно-стратегічної обстановки, встановлюються актуальні воєнні загрози та проводиться їх оцінювання. У командуванні об'єднаних сил, Об'єднаному оперативному штабі, інших органах військового управління Збройних Сил України та органах управління інших складових сил оборони під керівництвом Генерального штабу Збройних Сил України на основі оцінки і прогнозу воєнно-політичної, воєнно-стратегічної обстановки, стратегічного замислу застосування сил оборони складатимуться оперативні плани, в яких передбачатимуться різні варіанти проведення об'єднаної операції. На підставі оцінок і прогнозу за необхідності можуть прийматися (уточнюватися) довгострокові рішення на дислокацію військ (сил), визначатися ступінь їхньої вкомплектованості особовим складом, озброєнням, військовою технікою, рівень підготовки, розміри запасів матеріально-технічних засобів для підтримання готовності до оперативного реагування на випадок виникнення кризової ситуації воєнного характеру.

Безпосередня підготовка об'єднаної операції розпочинається із загостренням воєнно-політичної обстановки і з виникненням кризової ситуації воєнного характеру та отриманням оперативної директиви Президента України, Верховного Головнокомандувача Збройних Сил України (Головнокомандувача Збройних Сил України). На цьому етапі проводитиметься кризове планування, яке полягатиме в уточненні плану відсічі збройній агресії.

Зміст, терміни та обсяг завдань, заходів з безпосередньої підготовки залежатиме від ступеня загострення воєнно-політичної, воєнно-стратегічної обстановки довкола воєнного конфлікту і його ймовірного характеру. Залежно від цього безпосередня підготовка повинна вестися приховано, у стислі терміни з метою досягнення раптовості й захоплення ініціативи в підготовці. За певних умов, як свідчить досвід, підготовка операції може здійснюватися відкрито з проведенням військово-демонстративних дій.

Особливістю цього етапу має бути випереджальна активізація діяльності місцевих органів виконавчої влади, органів місцевого самоврядування, правоохоронних органів у виконанні першочергових заходів з підготовки оборони в рамках об'єднаної операції в прикордонних (з Росією) областях та областях, території яких прилягають до узбережжя морів (уточнення планів, розгортання системи управління, посилення моніторингу розвитку місцевої внутрішньої обстановки, охорони важливих об'єктів, приведення в готовність сил і засобів територіальної оборони (необхідною мірою), сил і засобів цивільного захисту, активізація інформаційної діяльності, підготовки населення до евакуації та інших важливих заходів). Проводяться заходи із забезпечення можливості безперешкодного висування і розгортання військ (сил) у визначені райони виконання завдань

Етап *оперативного розгортання військ (сил), органів, інших сил і засобів, що беруть участь в операції, утворення угруповань військ (сил) та підготовка зони (районів) до проведення операції* проводиться в послідовності, визначеній під час кризового планування відповідно до уточнених планів об'єднаної операції. Особливістю має стати випередження противника в проведенні заходів розгортання та завершення повної підготовки визначених сил і засобів до виконання поставлених завдань операції.

Виконання завдань та заходів операції відбувається згідно з визначеним замислом і розробленим планом об'єднаної операції. При цьому використовуються та задіються всі визначені форми застосування військ (сил) і визначені війська (сили), органи та їхні сили й засоби.

Залежно від масштабу, тривалості й інших показників розмаху операції виконання її оперативно-тактичних (оперативних) завдань і заходів (дій) також може проводитися за відповідними етапами.

Завершення операції відбувається після припинення воєнних дій (досягнення воюючими сторонами перемир'я). Війська (сили) займають положення, встановлене відповідними актами про припинення воєнних дій (перемир'я), і розпочинають проведення заходів з відновлення боєздатності з'єднань, військових частин, інших сил і засобів, які брали участь в операції, та проводять першочергові заходи з надання допомоги постраждалому населенню, відновленню забезпечення його життєдіяльності та діяльності місцевих органів виконавчої влади, органів місцевого самоврядування, правоохоронних органів тощо.

Для проведення відбудовних заходів у районах, де велися бойові дії, та на прилеглих до них територіях (адміністративних одиницях) утворюються військово-цивільні адміністрації з представників силових структур, місцевих органів виконавчої влади, органів місцевого самоврядування, активістів, волонтерів, на які покладаються завдання з організації проведення першочергових відновлювальних заходів. Очолюють вказані військово-цивільні адміністрації визначені посадові особи і персонал відповідного військового командування. Забезпечення виконання першочергових заходів необхідними матеріально-технічними засобами і ресурсами здійснюється Кабінетом Міністрів України, а також з використанням наявних місцевих ресурсів.

Після завершення проведення першочергових заходів та відновлення діяльності місцевих органів виконавчої влади, органів місцевого самоврядування військово-цивільні адміністрації трансформуються в цивільно-військові адміністрації з передачею відповідних владних повноважень органам державної влади та органам місцевого самоврядування. Сили й засоби об'єднаних сил надають допомогу та забезпечують військову підтримку цивільно-військовим адміністраціям і діяльності місцевих органів виконавчої влади, органів місцевого самовря-

дування з ліквідації наслідків воєнних дій та повного налагодження життєдіяльності в постраждалих районах.

Об'єднану операцію готують і проводять об'єднані сили. Для цього рішенням Президента України, Верховного Головнокомандувача Збройних Сил України (Головнокомандувача Збройних Сил України) визначається склад 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 [15].

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) формування (об'єднання) військ (сил) Збройний Сил України, інших військових формувань, органів, сил і засобів правоохоронних, розвідувальних органів зі складу сил оборони, інших органів, їхніх сил і засобів, для виконання завдань об'єднаної операції з використанням воєнних, невоєнних і спеціальних засобів.

Структурна схема об'єднаних сил показана на *рисунку 2*.

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

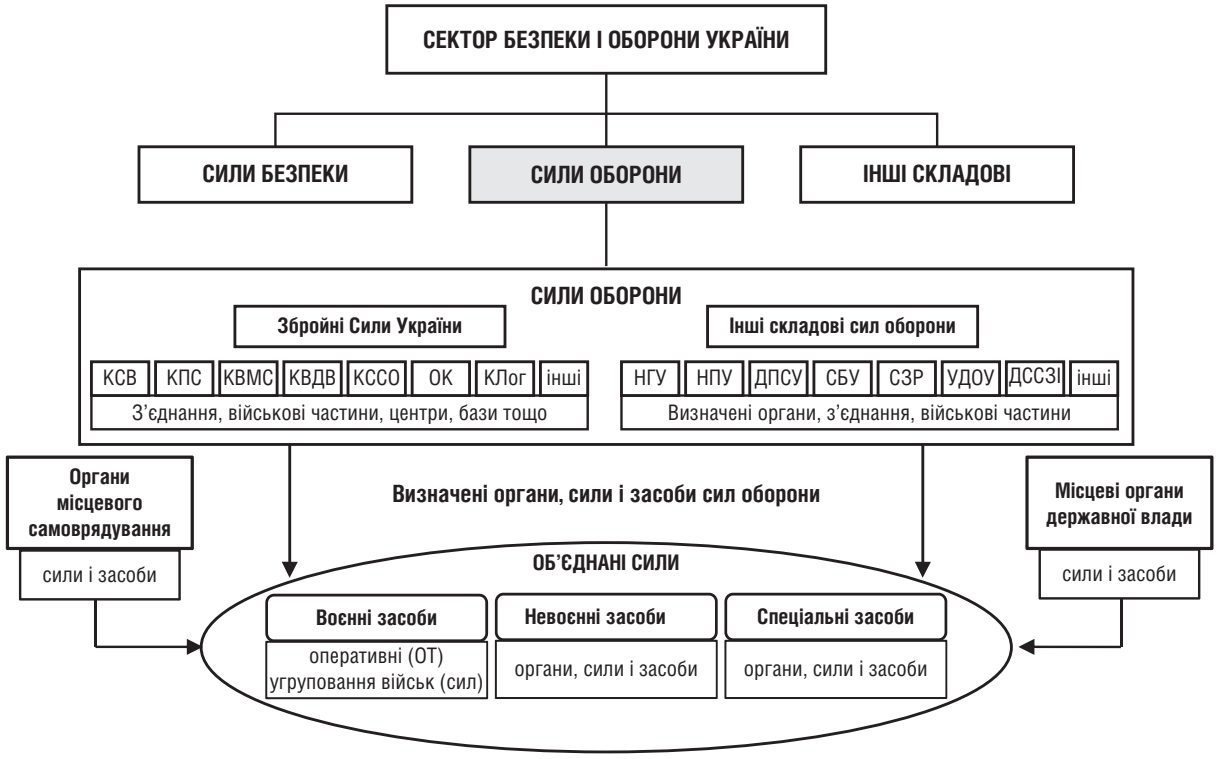


Рис. 2. Структурна схема об'єднаних сил

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 [15].

Об'єднані сили охоплюють кілька оперативно-тактичних (оперативних) угруповань військ (сил), які розгортаються на ймовірних напрямках дій угруповань противника і виконують визначені завдання в усьому діапазоні форм 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).

Таким чином, органи, підрозділи й військові частини інших складових сил оборони в рамках покладених вітчизняним законодавством завдань повинні також виконувати завдання з прикриття проміжків і флангів угруповань військ (сил), вести боротьбу з диверсійними і розвідувальними силами противника, терористичною діяльністю, повітряними десантами, здійснювати контроль за комунікаціями, які використовуються військами (силами) для маневру, підвозу й евакуації, охороняти важливі державні та військові об'єкти, забезпечувати функціонування органів місцевої влади, підтримувати правопорядок тощо, за єдиним замислом і планом операції (бойових дій) командувача об'єднаних сил і командувачів утворених оперативно-тактичних (оперативних) угруповань військ (сил).

До складу об'єднаних сил також мають входити органи, їхні сили і засоби, підпорядковані відповідним міністерствам (відомствам) та органам місцевої влади в зоні підготовки і проведення операції.

До органів (пунктів) управління об'єднаних сил мають входити представники військово-цивільних (військових) адміністрацій (у разі їх створення), представники місцевих державних адміністрацій, обласних рад оборони та органів місцевого самоврядування територій, що входять до зони об'єднаної операції. На ці органи, їхні сили й засоби мають покладатися завдання участі у виконанні завдань, що здійснюються невоєнними засобами. Це дасть можливість мобілізувати, об'єднати і підвищити дієвість заходів в інтересах усієї операції, забезпечити підтримку об'єднаних сил місцевим населенням та повною мірою задіяти місцеві ресурси тощо.

Висновки

У сучасних умовах значно змінився характер воєнних конфліктів. Для них стали властивими не лише воєнні дії, а й невоєнні, зокрема з використанням інформаційних технологій. Супутнім для воєнних конфліктів стало зростання у великих масштабах кримінальних правопорушень. Разом це надає воєнному конфлікту «гібридного» характеру й суттєво ускладнює протидію таким явищам. У зв'язку із цим поряд з воєнними засобами у збройній боротьбі дедалі більшого значення набувають невоєнні та спеціальні засоби.

Такі зміни спонукають до пошуку нових підходів щодо підготовки і здійснення оборони держави та відсічі збройній агресії.

Одним з підходів має стати розвиток нових форм застосування військ (сил). Як показало проведене дослідження, однією з форм відсічі збройній агресії 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. До його складу залучаються 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, а також місцеві державні адміністрації, органи місцевого самоврядування, інші органи та їхні сили й засоби.

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.

За такого підходу забезпечується реалізація окремих положень Стратегії воєнної безпеки України із забезпечення підготовки і ведення всеохоплюючої оборони України.

Перелік літератури

1. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» від 14 вересня 2020 р. [Електронний ресурс] : Указ Президента України № 392/2020 від 14 вересня 2020 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/392/2020#Text.

2. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» [Електронний ресурс] : Указ Президента України № 121/2021 від 25 березня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/121/2021#Text.

3. *Герасимов В.* По опыту Сирии [Електронний ресурс] / В. Герасимов // Военно-промышленный курьер. – № 9 (624). – 2016. – С. 4. – Режим доступу : https://vpk-news.ru/sites/default/files/pdf/VPK_09_624.pdf.

4. Світова гібридна війна: український фронт [Електронний ресурс] : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с. – Режим доступу : https://niss.gov.ua/publikacii/monografii/svitova-gibridna-viyna-ukrainskiy-front-monografiya.

5. *Магда Є.* Гібридна агресія Росії: уроки для Європи [Електронний ресурс] / Є. Магда. – К. : Каламар, 2017. – 268 с. – Режим доступу : https://kalamar.ua/product/gibrydna_agresia_rosii_uroki_dlia_evropi/.

6. Воєнні аспекти протидії «гібридній» агресії: досвід України [Електронний ресурс] : монографія / за заг. ред. А. М. Сиротенка. – К. : НУОУ ім. Івана Черняховського, 2020. – 176 с. – Режим доступу : https://nuou.org.ua/assets/monography/mono_gibr_viin.pdf.

7. *Илларионов А.* Вызовы информационной войны для свободного общества и возможная контрстратегия. Выступление на XIX Форуме Открытого Общества Эстонии. Таллинн, 18 сентября 2014 г. [Електронний ресурс] / А. Илларионов // Livejournal. – Режим доступу : https://aillarionov.livejournal.com/735489.html.

8. Сектор безпеки і оборони України: стратегічне керівництво та військове управління : монографія / Ф. В. Саганюк, В. С. Фролов, М. М. Лобко та ін. ; за заг. ред. І. С. Руснака. – К. : ЦЗ МО та ГШ ЗС України, 2018. – 230 с.

9. Актуальні проблеми планування оборони України: комплексний підхід [Електронний ресурс] / А. М. Сиротенко, П. В. Щипанський, А. К. Павліковський, М. М. Лобко // Наука і оборона. – 2020. – № 1. – С. 3–12. – Режим доступу : https://doi.org/10.33099/2618-1614-2020-10-1-3-12.

10. *Тимошенко Р. І.* Проблеми вдосконалення планування оборони України [Електронний ресурс] / Р. І. Тимошенко, М. М. Лобко // Наука і оборона. – 2018. – № 1. – С. 11–17. – Режим доступу : https://doi.org/10.33099/2618-1614-2018-2-1-11-17.

11. *Бєлєсков М. М.* Сучасний російський спосіб ведення війни: теоретичні основи і практичне наповнення [Електронний ресурс] : аналітична доповідь / М. М. Бєлєсков. – К. : НІСД, 2021. – 29 с. – Режим доступу : https://niss.gov.ua/sites/default/files/2021-02/analitichna-dopovid.pdf.

12. *Шамко В. Є.* Розвиток форм і способів застосування Повітряних Сил Збройних Сил України в сучасних умовах ведення збройної боротьби / В. Є. Шамко, О. М. Жарик, В. В. Коваль // Наука і техніка Повітряних Сил Збройних Сил України. – 2018. – № 2 (31). – С. 9–15.

13. Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності : зб. тез доп. наук.-практ. конф., 14–15 листоп. 2019 р. / Нац. акад. Сухопут. військ ім. Петра Сагайдачного, Наук. центр Сухопут. військ. – Львів : НАСВ, 2019. – 307 с.

14. Военный энциклопедический словарь / председ. гл. ред. комис. Н. В. Огарков ; М-во обороны СССР, Ин-т воен. истории. – М. : Воениздат, 1983. – 863 с.

15. Про національну безпеку України [Електронний ресурс] : Закон України № 2469-VIII від 21 червня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

DOI 10.33099/2618-1614-2021-15-2-34-41
УДК 355.23

В. С. Артамощенко,
кандидат військових наук, доцент, докторант Національного університету оборони України імені Івана Черняховського, полковник

Методологічний аспект формування професійної кваліфікації офіцерів сил оборони на шляху впровадження нових рівнів військової освіти

За результатами аналізу кількісних показників галузей знань, спеціальностей та спеціалізацій для підготовки військових кадрів, змісту і побудови перспективного каталогу військових посад осіб офіцерського складу, континууму професійної військової освіти та кваліфікаційних рівнів, прийнятих у збройних силах держав – членів НАТО, і на засадах класифікації рівнів мислення в когнітивній (пізнавальній) сфері за таксономією Блума обґрунтовано принцип класифікації рівнів військової освіти в Україні.

Розроблено концептуальну модель рамки кваліфікацій рівнів військової освіти на підґрунті класифікації видів економічної діяльності, класифікації професій, вимог Національній рамки кваліфікацій, перспективного змісту підготовки офіцерського складу для здобуття нових рівнів військової освіти, вимог щодо наявності відповідності спеціальності (спеціалізації) підготовки військово-обліковим спеціальностям військової посади осіб офіцерського складу. До моделі рамки кваліфікацій впроваджено кваліфікаційні рівні для оцінювання продуктивності професійної діяльності за стандартами НАТО.

Ключові слова: військова освіта, рівні військової освіти, кваліфікація.

Постановка проблеми в загальному вигляді. Стратегією воєнної безпеки України (СВБ) визначені цілі реалізації державної політики у воєнній сфері, сфері оборони і військового будівництва [1]. Наявний професійний особовий склад Збройних Сил України та інших складових сил оборони є однією з цілей СВБ. Розвиток систем військової освіти та підготовки особового складу для сил оборони, запровадження освітньо-професійних програм підготовки офіцерського, сержантського та старшинського складу з використанням досвіду бойових дій, методики підготовки, принципів і стандартів НАТО є одним із завдань СВБ.

Досвід проведення антитерористичної операції на території Донецької та Луганської областей та операції Об'єднаних сил переконливо свідчить про їхній міжвідомчий характер: у їх плануванні та реалізації беруть участь усі складові сектору безпеки та оборони. Запровадження стандартів НАТО в діяльність органів військового управління, безумовно, потребуватиме й підготовки офіцерських кадрів для всіх складових сектору безпеки та оборони.

Річною національною програмою під егідою Комісії Україна – НАТО на 2021 рік визначені стратегічна мета: «професіоналізація сил оборони та створення необхідного військового резерву», та завдання: «забезпечення централізованої підготовки особового складу сил оборони оперативного рівня» (до 2025 р.) [2].

Отже, розвиток системи військової освіти як основи підготовки кадрів усіх складових сил оборони відбувається з метою досягнення нових цілей та набуття нових спроможностей за нормами, принципами і стандартами НАТО.

Міністерство оборони України має повноваження щодо формування засад військової кадрової політики у сфері оборони [3] та впроваджує проєкт розвитку системи військової освіти [4, 5], який базується на оцінюванні спільних спроможностей за складовими *DOTMLPFI* (*Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, Interoperability*) [6, 7].

Нормативною складовою спроможностей системи є законодавство (Doctrine), тобто сукупність нормативно-правових актів, що регулюють відносини між учасниками освітнього процесу [8].

У межах проєкту розвитку системи військової освіти опрацьовані зміни до законодавства, формується нова концепція військової освіти, розробляються нові стандарти, проводиться апробація нових освітніх програм підготовки, поступово змінюється система управління, вдосконалюються інфраструктура та матеріально-технічне забезпечення.

Важливим елементом перебудови структури системи є перехід до нових рівнів військової освіти: тактичного, оперативного, стратегічного [4, 9].

Військова освіта передбачає засвоєння освітньої програми з військової підготовки з метою набуття комплексу професійних компетентностей, формування та розвитку

індивідуальних здібностей особи і поглибленого оволодіння військовою спеціалізацією [8].

У свою чергу, компетентність – динамічна комбінація знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність [8].

Підтвердження необхідних компетентностей здійснюється через кваліфікацію – визнану уповноваженим суб'єктом та засвідчену відповідним документом стандартизовану сукупність здобутих особою компетентностей (результатів навчання) [8]. Отже, виникає потреба встановлення вимог до кваліфікації за рівнями військової освіти.

Питання кваліфікації регулюються законодавством [8, 10], міжнародними стандартами [11], Національним класифікатором України [12, 13], Національною рамкою кваліфікації (НРК) [14], іншими нормативно-правовими актами. Повноваження щодо реалізації державної політики у сфері кваліфікацій покладені на Національне агентство кваліфікацій [15]. Стандарти вищої освіти і професійні стандарти є підґрунтям для формування освітніх і професійних кваліфікацій та освітніх програм, в основу досягнення їхніх результатів покладено компетентнісний підхід [16].

Таким чином, перехід на нові рівні військової освіти потребує формування нових та єдиних підходів до визнання кваліфікації офіцера стратегічного, оперативного або тактичного рівнів військової освіти.

Аналіз останніх досліджень та публікацій

Питанню кваліфікації, зокрема у сфері підготовки військових кадрів, присвячено достатню кількість досліджень і публікацій в Україні та за її межами.

Так, методичні рекомендації [16] містять підходи та порядок присвоєння освітніх кваліфікацій на основі стандартів освіти і професійних кваліфікацій на основі професійних стандартів, у тому числі з використанням галузевих рамок кваліфікацій та класифікаторів професій.

Робота [17] надає методичні підходи щодо розроблення галузевих рамок кваліфікацій у Європейському просторі вищої освіти за досвідом визначення специфічних компетентностей у 13 галузях знань проєкту *TUNING*.

У науковій статті [18] розглянуто стан, проблеми і перспективи розвитку вітчизняного законодавства та нормативно-правового забезпечення процесу стандартизації військової освіти в Україні. Показано принципові шляхи вирішення питань розробки та імплементації галузевої рамки кваліфікацій у галузі знань «Воєнні науки, національна безпека, безпека державного кордону» на основі введеної в дію Національної рамки кваліфікацій. Увагу зосереджено на необхідності розвитку компетентнісного підходу однієї галузі знань.

У роботі [19] розглянуто загальні принципи та підходи до стандартизації військової освіти в Україні, що розвиваються в теоретико-методологічному дискурсі сучасної науки про освіту і потребують імплементації та широкого застосування в процесі вдосконалення системи військової освіти України. Показано зв'язок основних принципів та підходів до стандартизації вищої освіти з рамковими документами, спрямованими на розробку і закріплення спеціальностей та спеціалізацій, представлених у галузі знань «Воєнні науки, національна безпека, безпека державного кордону». Акцент зроблено на необхідності розвитку стандартизованих процедур в одній галузі знань.

У статті [20] розглянуто теоретичні аспекти побудови і формування галузевої рамки кваліфікацій у галузі знань «Воєнні науки, національна безпека, безпека державного кордону», проаналізовано й надано пропозиції щодо внесення змін до відповідної нормативно-правової бази. Тобто робота орієнтована на одну галузь знань у сфері вищої освіти.

У роботі [21] розглянуто міжнародні практики стандартизації, досвід і проблеми створення нових стандартів вищої освіти в Україні, отже, сферою дослідження є лише вища освіта.

У науковій статті [22] розкрито сутність і завдання галузевої рамки кваліфікацій у системі підготовки прикордонників країн ЄС, проаналізовано використання цього досвіду з метою його впровадження в систему професійної підготовки персоналу прикордонного відомства України. Тобто в основу покладено кваліфікацію професії.

У статті [23] розглянуто теоретичні та практичні аспекти формування галузевої рамки кваліфікацій у галузі знань «Воєнні науки, національна безпека, безпека державного кордону», проаналізовано основні аспекти побудови Європейських рамок кваліфікацій.

Національне законодавство передбачає, що військова освіта здобувається одночасно з вищою освітою або на базі вже здобутої освіти, в тому числі вищої [8]. Цей процес може відбуватися поза воєнною галуззю знань. Тоді постає низка запитань: коли здобувач освіти набуває кваліфікації офіцера тактичного рівня військової освіти; коли він набуває спеціалізації; як надавати кваліфікацію, коли вища освіта вже здобута, а потрібного рівня військової немає?

Практика діяльності на шляху стандартизації та професійної кваліфікації у сфері освіти і професійної підготовки свідчить, що саме компетентнісний підхід є основою для вимірювання якості та оцінювання результатів освіти. Так, спільна директива стратегічних командувань НАТО «Освіта і індивідуальна підготовка» (*Education and Individual Training Directive*, 075-007) [24] формулює критерії якості, розглядає освіту й індивідуальну підготовку як одне ціле для розвитку знань, умінь та навичок для подальшої професійної діяльності.

Політика професійної військової освіти США [25] надає континуум підготовки офіцера за військовими званнями, кваліфікаційними рівнями та курсами. Важливим є опис змісту підготовки офіцера на кожному рівні воєнних дій (тактичний, оперативний, стратегічний).

Отже, нерозв'язаною частиною проблеми переходу на нові рівні військової освіти є кваліфікація офіцерів складових сил оборони за рівнями військової освіти для подальшої стандартизації військових посад офіцерського складу.

Метою статті є обґрунтування принципу класифікації рівнів військової освіти та розробка концептуальної моделі рамки кваліфікацій рівнів військової освіти як складової розвитку системи військової освіти та підготовки військових кадрів для сил оборони на шляху виконання завдань оборонної реформи за нормами, принципами і стандартами НАТО.

Виклад основного матеріалу

Сьогодні підготовка кадрів в інтересах Збройних Сил України (ЗСУ) та інших складових сил оборони здійснюється в галузі знань «Воєнні науки, національна безпека, безпека державного кордону». Крім цього, підготовка кадрів для ЗСУ, Національної гвардії України (НГУ), Державної прикордонної служби України (ДПСУ), Державної спеціальної служби транспорту (ДССТ), Служби безпеки України (СБУ) здійснюється в «цивільних» галузях знань за спорідненими до військових професій спеціальностями та необхідними для професійної діяльності спеціалізаціями (*табл. 1*).

Таблиця 1

Кількісні показники цивільних галузей знань для підготовки військових кадрів

Кількість*	ЗСУ	НГУ	ДПСУ	ДССТ	СБУ
Галузі знань	20	5	8	3	5
Спеціальності	41	7	11	4	6
Спеціалізації	83	30	20	6	14

* Середні значення 2016–2021 рр. за даними Реєстру суб'єктів освітньої діяльності.

Відомо, що освітня кваліфікація за спеціальністю визначається стандартом вищої освіти, а професійна – професійними стандартами.

Професійні стандарти можуть розроблятися роботодавцями, їхніми організаціями та об'єднаннями, органами державної влади, науковими установами, галузевими радами, громадськими об'єднаннями, іншими зацікавленими суб'єктами [8, 26] з урахуванням класифікації видів економічної діяльності [12] та класифікатора професій [13]. Тобто для формування освітніх програм за цивільними спеціальностями необхідною умовою є дотримання вимог професійних стандартів.

Значна кількість військових посад офіцерського складу відповідає назвам споріднених цивільних посад (штурман, юрисконсульт, психолог, перекладач, начальник служби, науковий співробітник, лікар, викладач тощо). Для таких посад дотримання вимог професійних стандартів, які розроблятимуть цивільні робочі групи, стає обов'язковим. Водночас назви професій можуть бути розширені за потребою термінами та словами, які уточнюють місце роботи, виконувані роботи, сферу діяльності, якщо інше не передбачене в класифікаторі професій чи відповідних нормативно-правових актах [13]: військовий психолог, юрисконсульт військової частини, військовий лікар тощо.

Отже, передумовою для створення професійних стандартів військових посад офіцерського складу буде їхній перелік або каталог (*табл. 2*).

Таблиця 2

Побудова каталогу військових посад осіб офіцерського складу (*приклад*)

Військове звання	Посада	Ступінь вищої освіти	Рівень військової освіти	Рівень підготовки
Бригадний генерал	Начальник управління	Магістр	Стратегічний	L-5
	Інші…	…	…	
Полковник	Заступник начальника управління	Магістр	Стратегічний	L-4
	Командир бригади	Магістр	Оперативний	L-3
	Начальник відділу	Магістр	Оперативний	L-3
	Інші…	…	…	
Підполковник	Начальник відділення (групи)	Магістр	Оперативний	L-3
	Командир батальйону	Магістр	Оперативний	L-3
	Інші…	…	…	
Майор	Заступник командира батальйону	Бакалавр	Тактичний	L-2
	Офіцер відділення (групи)	Бакалавр	Тактичний	L-2
	Інші…	…	…	
Капітан	Командир роти	Бакалавр	Тактичний	L-1
	Інші…	…	…	
Старший лейтенант	Заступник командира роти	Бакалавр	Тактичний	L-1
	Інші…	…		
Лейтенант	Командир взводу	Бакалавр	Тактичний	L-1
	Інші…	…	…	

Каталог військових посад офіцерського складу стане основою для формування освітньої та професійної кваліфікації за рівнями військової освіти, спеціальностями (спеціалізаціями) відповідно до військових професій за військово-обліковими спеціальностями (ВОС).

Досвід практичної діяльності свідчить, що найбільшою проблемою під час формування каталогу посад є встановлення ступеня вищої освіти та рівня військової освіти.

Одним з підходів для формування вимог до встановлення рівнів військової освіти до військових посад осіб офіцерського складу є визначення рівня мислення на кожному рівні професійної діяльності.

Так, візією майбутнього офіцера армії США є офіцер – талант, спроможний досягти інтелектуальної переваги над противниками, володіючи навичками практичного та критичного мислення [27]. Ключовим компонентом континууму навчання є вироблення «розумових звичок» для поліпшення та оптимізації інтелектуальної діяльності на відповідній посаді, встановленого рівня (військового звання) в потрібний час [28]. Такий підхід дає змогу структурувати військову освіту і підготовку офіцерів за рівнем мислення в майбутній професійній діяльності за посадою.

Найпоширенішою класифікацією рівнів мислення є так звана таксономія Блума, розроблена та опублікована 1956 р. американським педагогом-дослідником Бенджаміном Блумом [29]. Так, у когнітивній (пізнавальній) сфері сформульовані шість послідовних рівнів складності: знання (*knowledge*), розуміння (*comprehension*), застосування (application), аналіз (*analysis*), синтез (*synthesis*), оцінювання (*evaluation*).

Отже, рівні мислення, за таксономією Блума, є основним принципом для розрізнення та класифікації рівнів військової освіти (*рис. 1*).

У практичній діяльності офіцер відповідно до посади, яку обіймає, опікується питаннями тактики (бою, бойових дій), оперативного мистецтва (підготовки й ведення операцій) або стратегії (стратегічних дій, стратегії розвитку, стратегічного планування тощо). Отже, набуття різних за рівнем складності компетентностей відбувається поступово в міру просування кар'єрою. Неможливо навчити лейтенанта одразу планувати стратегічні дії, він повинен пройти всі рівні. Поступово набуті компетентності та здобутий офіцером досвід за попереднім рівнем надає йому можливість опанувати подальший.

Таким чином, складність (рівні) мислення є визначальною у формуванні інтегральних (ключових) освітніх та професійних компетентностей посад офіцерського складу, які будуть ознакою їхньої кваліфікації за рівнями військової освіти. Такий підхід не виключає набуття вищих рівнів мислення під час формування інших компетентностей.

Наступним етапом упровадження нових рівнів військової освіти є їхня кваліфікація. У сфері вищої освіти регулятором щодо розроблення, ідентифікації, співвіднесення, визнання, планування та розвитку кваліфікацій є Національна рамка кваліфікацій [8].

Водночас військова освіта здобувається не лише зі здобуттям вищої освіти, а й на базі вже здобутої вищої, у сфері формальної або неформальної освіти [8]. Найбільше це характерно для військових професій, де вища освіта здобута в цивільних галузях знань, про що йшлося вище. Крім цього, оперативна або стратегічна освіта здобуватиметься на базі вищої освіти, і якщо здобувач має ступінь «бакалавр», у тому числі й у цивільній галузі знань, він може здобути ступінь «магістра» в галузі знань «Воєнні науки, національна безпека, безпека державного кордону» одночасно зі здобуттям оперативної чи стратегічної військової освіти.

Однак здобувач військової освіти може вже мати ступінь магістра (доктора філософії, доктора наук), тобто він набув необхідних освітніх компетентностей, і здобуття військової освіти буде пов'язане з набуттям лише професійних компетентностей у сфері неформальної освіти.

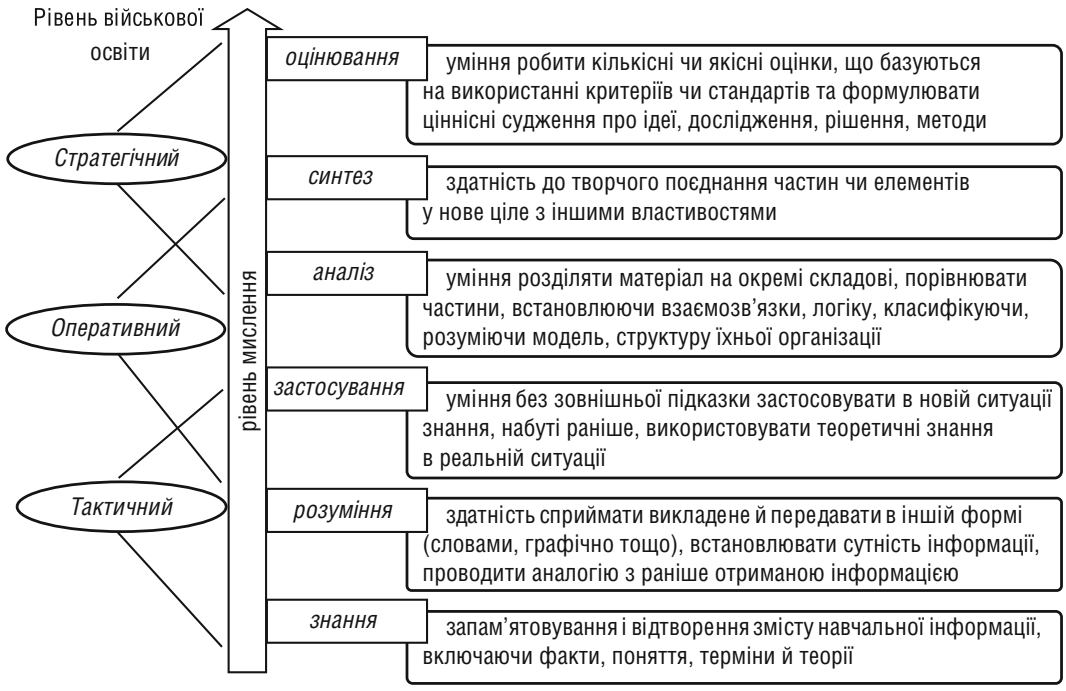


Рис. 1. Класифікація рівнів військової освіти за таксономією Блума

За вказаних умов необхідним регулятором здобуття професійних компетентностей за рівнями військової освіти стає «рамка кваліфікацій рівнів військової освіти», яка, на відміну від поглядів попередніх наукових досліджень [18–23], не обмежуватиметься лише однією галуззю знань «Воєнні науки, національна безпека, безпека державного кордону» у сфері вищої освіти. Такий документ дасть можливість кваліфікувати рівні військової освіти для всіх складових сектору безпеки та оборони.

Кваліфікація професій в одній сфері діяльності розглядається в низці досліджень [21, 22, 30, 31], при цьому ключовими у формуванні кваліфікації є посада (професія) та основний зміст діяльності за цією посадою.

Отже, посада (професія) є визначальним чинником у формуванні переліку компетентностей для подальшої кваліфікації за рівнями військової освіти, а ключовим у формування професійних компетентностей є перелік службових (посадових) обов'язків військової посади чи групи таких посад.

З огляду на те, що каталог посад групує посади за військовим званням, ступенями вищої освіти та рівнями військової освіти, достатньо буде описати дескриптори формування інтегральних компетентностей для кожного рівня військової освіти, загальну та спеціальну кваліфікацію.

Звернімося до підходу, який діє у збройних силах держав – членів НАТО.

Спільна директива стратегічних командувань НАТО «Освіта і індивідуальна підготовка» (*BI-Strategic Command Directive* 075-007) передбачає, що кваліфікаційні рівні об'єднані у шкалу, яка дає змогу визначати ступінь професійної компетентності (експертизи), необхідний для виконання основних обов'язків та завдань за посадами у структурі НАТО [24].

Обов'язки та завдання визначаються за шкалою кваліфікаційних рівнів продуктивності, визначають глибину знань та вмінь, на досягнення яких спрямоване здобуття певного рівня освіти й індивідуальної підготовки. Для опису здобутих компетентностей використовуються ключові слова-позначення. Кваліфікаційні рівні базуються на модифікованій версії загальних описів професійних навичок, які використовуються для деталізації «Кодів спеціальностей та видів професійної діяльності НАТО» (*NATO Occupation Codes*) [24]. Коди НАТО, кваліфікаційні рівні та стислі описи компетентностей, які їм відповідають, наведені в *таблиці 3*.

Отже, рамка кваліфікацій рівнів військової освіти має містити код професії НАТО (NATO Occupation Code).

Розгляньмо шляхи здобуття рівнів військової освіти у сфері неформальної освіти.

Так, у вищих військових навчальних закладах Збройних Сил України з 2018 р. проводиться апробація нової системи курсів підготовки офіцерського складу на відповідних рівнях військової освіти [4, 32].

На тактичному рівні військової освіти:

Таблиця 3

Коди та кваліфікаційні рівні для оцінювання продуктивності професійної діяльності

Код	Рівень	Ключові слова	Опис компетентності
100	Базовий (Basic Level)	Слідує	Компетенції, необхідні для успішного виконання завдання чи кількох елементів такого завдання в структурованому середовищі під контролем. Несподівана ситуація потребує рекомендацій щодо подальших дій
200	Середній (Intermediate Level)	Допомагає	Компетенції, необхідні для успішного виконання комплексу завдань самостійно під мінімальним контролем
300	Просунутий (Advance Level)	Застосовує	Компетенції, необхідні для тлумачення вказівок і настанов та успішного планування, самостійного виконання завдань, а також готовності контролювати інших
400	Експертний (Expert Level)	Уможливлює/ радить	Компетенції, необхідні для виконання широкого спектра складних професійних та/або технічних робіт, спираючись на попередню освіту, навчання та практичний досвід, здатність до розв'язання незвичних і нечітко визначених проблем
500	Рівень майстра (Master Level)	Ініціює/ формує/ впливає	Компетенції, необхідні для виконання дуже складної професійної діяльності, що охоплює аспекти технічних питань, фінансів та якості в даній функціональній сфері. Здатність надавати консультативну допомогу підлеглим структурам, визначати ймовірність та оцінювати ризики, розуміти наслідки нових рішень, технологій і тенденцій

а) для призначення на первинні військові посади осіб офіцерського складу:

- базовий курс L-1A (для набуття загальнопрофесійних компетентностей);
- фаховий курс L-1B (для набуття фахових компетентностей за спеціальністю та спеціалізацією);

б) для просування по службі на посади у військовому званні не нижче «капітан» – командний курс L-1C;

в) для просування по службі на посади у військовому званні не нижче «майор» – командно-штабний курс (L-2).

Курси передбачають вивчення процедур прийняття військових рішень за стандартами НАТО – TLP (*Troop Leading Process*) та MDMP (*Military Decision Making Process*).

На оперативному рівні військової освіти проходить апробацію «курс офіцерів об'єднаних штабів» (L-3), який

передбачає вивчення процесів планування операцій угруповань військ (сил) в об'єднаних штабах за стандартами НАТО – JOPP (*Joint Operation Planning Process*).

На стратегічному рівні військової освіти апробується «курс керівного складу стратегічного рівня» (L-4) для підготовки осіб офіцерського складу стратегічного рівня військової освіти у військовому званні не нижче «полковник». Також заплановане впровадження «курсу стратегічного управління вищого рівня та державної політики» (L-5) для підготовки керівників структурних підрозділів апарату Міністерства оборони України, Генерального штабу Збройних Сил України, державних органів сектору безпеки та оборони, центральних органів виконавчої влади, до сфери відповідальності яких належать питання оборони держави.

Нова система курсів підготовки також має знайти відображення в рамці кваліфікацій рівнів військової освіти.

Таким чином, складовими рамки кваліфікацій рівнів військової освіти є класифікація виду економічної діяльності, класифікація професії, відповідність Національній рамці кваліфікацій, код професії за стандартом НАТО, рівень військової освіти, курс (рівень) підготовки для її здобуття, спеціальність (спеціалізація) відповідно до ВОС посади.

Концептуальна модель рамки кваліфікацій рівнів військової освіти наведена в *таблиці 4*.

Отже, прикладами кваліфікації рівнів військової освіти можуть бути:

- фахівець у сфері оборони, офіцер тактичного рівня L-1 (код НАТО – 200), механізованих військ Сухопутних військ Збройних Сил України;
- професіонал у сфері оборони, офіцер оперативного рівня L-3 (код НАТО – 400), Державної прикордонної служби України;
- менеджер у сфері оборони, офіцер стратегічного рівня L-5 (код НАТО – 500), стратегічне керівництво в секторі безпеки та оборони.

Рамка кваліфікацій рівнів військової освіти має стати складовою нової Концепції розвитку системи військової освіти, яка затверджуватиметься Кабінетом Міністрів України та складе підґрунтя для розроблення професійних стандартів військових посад офіцерського складу і професійної кваліфікації офіцерського складу для всіх складових сектору безпеки та оборони.

Висновки

Таким чином, на шляху впровадження нових рівнів військової освіти в підготовці офіцерських кадрів для Збройних Сил України та інших складових сектору безпеки та оборони обґрунтовано принцип класифікації рівнів військової освіти, сформульовано методологічний підхід та розроблено концептуальну модель рамки кваліфікацій рівнів військової освіти, яка надалі стає підґрунтям для формування професійних стандартів та освітніх програм підготовки офіцерського складу на тактичному, оперативному і стратегічному рівнях військової освіти, стандартизації військової освіти України в НАТО. Це дасть змогу в подальшому здійснювати роздільну підготовку кадрів сектору безпеки та оборони на тактичному рівні і спільну підготовку військових кадрів для органів військового управління оперативного і стратегічного рівнів поєднанням формальної та неформальної освіти.

Перспективи подальших досліджень. Напрямом подальших досліджень є розроблення концепції розвитку системи військової освіти на шляху досягнення операційної сумісності Збройних Сил України та збройних сил держав – членів НАТО, у тому числі з питань підготовки військових кадрів.

Перелік літератури

1. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 р. «Про Стратегію воєнної безпеки України» [Електронний ресурс] : Указ Президента України № 121/2021 від 25 березня 2021 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/121/2021#n2.

Таблиця 4

Концептуальна модель рамки кваліфікацій рівнів військової освіти

Розділи, складові	**Класифікатор видів економічної діяльності**					
	Розділ	84	Державне управління та оборона			
	Код		84.22	Діяльність у сфері оборони		
Розділи класифікації професій	4.3. Фахівці			4.2. Професіонали	4.1. Вищі керівники, менеджери	
Рівень НРК	6			7, 8, 9		
Код професії (*NATO Occupation Code*)	100	200	300	400		500
Рівень військової освіти офіцера	Тактичний			Оперативний	Стратегічний	
Рівень підготовки	L-1		L-2	L-3	L-4	L-5
Спеціалізація відповідно до ВОС	Род військ (сил, виду забезпечення) виду ЗСУ (іншої складової сил оборони)			Виду ЗСУ (НГУ, ДПСУ, ДССТ, СБУ)	Стратегічне керівництво в секторі безпеки та оборони	

2. Про Річну національну програму під егідою Комісії Україна – НАТО на 2021 рік [Електронний ресурс] : Указ Президента України № 189/2021 від 11 травня 2021 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/189/2021#Text.

3. Про національну безпеку України [Електронний ресурс] : Закон України № 2469-VIII від 21 червня 2018 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19.

4. *Артамощенко В. С.* Управління змінами щодо розвитку системи військової освіти на засадах програмно-проектного менеджменту [Електронний ресурс] / В. С. Артамощенко, О. Ю. Фаворська // Наука і оборона. – 2019. – № 3. – С. 40–44. – Режим доступу : https://doi.org/10.33099/2618-1614-2019-8-3-40-44.

5. Про організацію виконання окремих заходів оборонної реформи на середньострокову перспективу [Електронний ресурс] : наказ Міністерства оборони України № 283 від 14 серпня 2020 р.. – Режим доступу : https://www.mil.gov.ua/content/mou_orders/mou_2020/nm_283.pdf.

6. NATO Glossary of Abbreviations used in NATO Documents and Publications [Електронний ресурс] : AAP-15(2020) // NATO Standardization Office. – Режим доступу : https://nso.nato.int/nso/zPublic/ap/PROM/AAP-15%20(2020)%20EF.pdf.

7. NATO Glossary of Terms and Definitions (English and French) [Електронний ресурс] : AAP-06. Edition 2020 // NATO Standardization Office. – Режим доступу : https://nso.nato.int/nso/zPublic/ap/PROM/AAP-06%202020%20EF.pdf.

8. Про освіту : Закон України № 2145-VIII від 5 вересня 2017 року [Електронний ресурс] : / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2145-19#Text.

9. *Полторак С. Т.* Трансформація системи військової освіти України на шляху до досягнення стандартів НАТО [Електронний ресурс] / С. Т. Полторак // Наука і оборона. – 2018. – № 2. – С. 3–10. – Режим доступу : https://doi.org/10.33099/2618-1614-2018-3-2-3-10.

10. Про вищу освіту [Електронний ресурс] : Закон України № 1556-VII від 1 липня 2014 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1556-18.

11. International Standard Classification of Education [Електронний ресурс] : ISCED-2011 // The UNESCO Institute for Statistics. – Режим доступу : http://uis.unesco.org/sites/default/files/documents/isced-2011-en.pdf.

12. Класифікація видів економічної діяльності ДК 009:2010: Національний класифікатор України: наказ Держспоживстандарту України від 11 жовтня [Електронний ресурс] / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/rada/show/vb457609-10#Text.

13. Класифікатор професій ДК 003:2010: Національний класифікатор України : наказ Держспоживстандарту України № 327 від 28 липня 2010 р. [Електронний ресурс] / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/rada/show/va327609-10#n4.

14. Про затвердження Національної рамки кваліфікацій [Електронний ресурс] : постанова Кабінету Міністрів України № 1341 від 23 листопада 2011 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.

15. Статут Національного агентства кваліфікацій [Електронний ресурс] : затверджений постановою Кабінету Міністрів України № 1029 від 5 грудня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1029-2018-%D0%BF#n14.

16. Розроблення освітніх програм [Електронний ресурс] : методичні рекомендації / В. М. Захарченко, В. І. Луговий, Ю. М. Рашкевич, Ж. В. Таланова ; за ред. В. Г. Кременя. – К. : Пріоритети, 2014. – 120 с. – Режим доступу : https://lib.iitta.gov.ua/9356/1/Rozroblennya_osv_program_20_04.pdf.

17. *Таланова Ж. В.* Підходи до розроблення галузевих рамок кваліфікацій в Європейському просторі вищої освіти [Електронний ресурс] / Ж. В. Таланова // Центр дистанційного навчання НАДУ. – Режим доступу : http://212.111.196.8:8081/dlc/24_25102013/talanova.pdf.

18. *Вавілова Н.* Законодавство та нормативно-правова база щодо формування галузевої рамки кваліфікацій у галузі знань «Воєнні науки, національна безпека, безпека державного кордону»: стан, проблеми, перспективи [Електронний ресурс] / Н. Вавілова // Збірник наукових праць «Військова освіта» Національного університету оборони України імені Івана Черняховського. – 2020. – № 2 (42). – С. 18–26. – Режим доступу : https://doi.org/10.33099/2617-1783/2020-2/18-26.

19. *Вітер Д.* Принципи та підходи до стандартизації військової освіти в Україні [Електронний ресурс] / Д. Вітер // Збірник наукових праць «Військова освіта» Національного університету оборони України імені Івана Черняховського. – 2020. – № 2 (42). – С. 89–99. – Режим доступу : https://doi.org/10.33099/2617-1783/2020-2/89-99.

20. *Мітягін О.* Формування галузевої рамки кваліфікацій у галузі знань «Воєнні науки, національна безпека, безпека державного кордону» [Електронний ресурс] / О. Мітягін // Збірник наукових праць «Військова освіта» Національного університету оборони України імені Івана Черняховського. – 2020. – № 2 (42). – С. 186–195. – Режим доступу : https://doi.org/10.33099/2617-1783/2020-2/186-195.

21. *Бахрушин В. Є.* Стандартизація вимог до вищої освіти, як інструмент забезпечення якості вищої освіти: рівні вищої освіти та предметні області [Електронний ресурс] / В. Є. Бахрушин // Освітня аналітика України. – 2020. – № 2 (9). – С. 50–66. – Режим доступу : https://doi.org/10.32987/2617-8532-2020-2-50-66.

22. *Балендр А.* Галузева рамка кваліфікацій у системі підготовки прикордонників країн Європейського Союзу: сутність і завдання / А. Балендр // Збірник наукових праць НАДПСУ. – (Педагогічні науки). – 2017. – № 1 (8). – С. 30–41.

23. *Цевельов О.* Стандартизація військової освіти: підходи та принципи [Електронний ресурс] / О. Цевельов // Збірник наукових праць «Військова освіта» Національного університету оборони України імені Івана Черняховського. – 2020. – № 2 (42). – С. 316–324. – Режим доступу : https://doi.org/10.33099/2617-1783/2020-2/316-324.

24. Education and Individual Training Directive [Електронний ресурс] : Bi-Strategic Command Directive 075-007 : 10 September 2015 // Allied Command Transformation. – Режим доступу : https://www.act.nato.int/images/stories/structure/jft/ptecs/etd-075-007.pdf.

25. Officer Professional Military Education Policy [Електронний ресурс] : CJCSI 1800.01F : 15 May 2020 // Joint Chiefs of Staff. – Режим доступу : https://www.jcs.mil/Portals/36/Documents/Doctrine/education/cjcsi_1800_01f.pdf?ver=2020-05-15-102430-580.

26. Про затвердження Порядку розроблення та затвердження професійних стандартів [Електронний ресурс] :

постанова Кабінету Міністрів України № 373 від 31 травня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/373-2017-%D0%BF#Text.

27. Developing Today's Joint Officers for Tomorrow's Ways of War [Електронний ресурс] : The Joint Chiefs of Staff Vision and Guidance for Professional Military Education & Talent Management : 01 May 2020 // Joint Chiefs of Staff. – Режим доступу : https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817.

28. *Kem J. D.* The Right Education and Training at the Right Time: Deciding What to Teach and Ensuring It Happens [Електронний ресурс] / J. D. Kem, W. E. Bassett // Journal of Military Learning. – April 2018. – P. 3–16. – Режим доступу : https://www.armyupress.army.mil/Portals/7/journal-of-military-learning/Archives/KEM-Right-education-a.pdf.

29. *Bloom B. S.* Taxonomy of educational objectives: The classification of educational goals : Hand book I: Cognitive Domain / B. S. Bloom. – New York : Longman, 1994. – 99 p.

30. *Дутчак М.* Актуальність та передумови розроблення галузевої рамки кваліфікацій у системі спорту в Україні [Електронний ресурс] / М. Дутчак // Вісник Прикарпатського університету. – (Фізична культура). – 2020. – № 35. – С. 24–31. – Режим доступу : https://doi.org/10.15330/fcult.35.24-31.

31. *Мельник С. В.* Розроблення макету проектів Галузевої рамки кваліфікацій та Галузевої тарифної сітки з оплати праці педагогічних та науково-педагогічних працівників [Електронний ресурс] / С. В. Мельник // Державна наукова установа «Інститут освітньої аналітики». – Режим доступу : https://iea.gov.ua/wp-content/uploads/2020/06/AZ_Melnik_2018_ Rozroblennya-maketu-proektiv-Galuzevoyi-ramki-kvalifikatsij-ta-.pdf.

32. *Сиротенко А. М.* Набуття сумісності військової освіти і підготовки кадрів сил оборони на засадах якості. Національні вимоги і стандарти НАТО [Електронний ресурс] / А. М. Сиротенко, В. С. Артамощенко // Наука і оборона. – 2021. – № 1. – С. 48–53. – Режим доступу : https://doi.org/10.33099/2618-1614-2021-14-1-48-53.

DOI 10.33099/2618-1614-2021-15-2-42-49
УДК: 004.056

А. Д. Білюга,
ад'юнкт кафедри історії війн і воєнного мистецтва, Національний університет оборони України імені Івана Черняховського, підполковник

Кіберзброя: сучасні загрози національній безпеці та шляхи протидії

Функціонування сучасного суспільства визначається низкою факторів, які, зокрема, пов'язані з розвитком комп'ютерних технологій. З поглибленням комп'ютеризації суспільства з'явилась якісно нова сфера обміну інформацією – кіберпростір. Світовий досвід показує, що захист кіберпростору (кібербезпека), поряд із боротьбою з таким негативним феноменом, як тероризм, став чи не найголовнішою проблемою людства.

Потужним засобом проведення незаконних дій та боротьби в кіберпросторі стала кіберзброя. Провідні країни світу розглядають кіберзброю як фактор, потенційно здатний впливати на перебіг воєнних дій і завдавати збитки економіці, порушувати управлінські функції конкретних держав тощо. Ураховуючи різноманітність дефініцій кіберзброї, автором запропоноване власне визначення цього виду зброї, проведений історіографічний опис кіберзброї, розглянутий досвід застосування кіберзброї в різних сферах людської діяльності. Надані пропозиції щодо подальшого поглиблення відносин України з НАТО в боротьбі з кіберзброєю.

Ключові слова: кіберзброя, кіберпростір, комп'ютерні системи, кібератаки, національна безпека, кібербезпека, НАТО.

Постановка проблеми в загальному вигляді. Протягом останніх 5 тис. років від становлення перших держав і до сьогодення неодмінним супутником цивілізації є війни та збройні конфлікти. У них застосовувалися найрізноманітніші види зброї – від мечів і списів до сучасного озброєння та військової техніки. Починаючи з 80-х рр. XX ст. зброя фізичного впливу поступово трансформувалась у кіберзброю, розпочався перехід від кінетичного ураження до інформаційного. Руйнівні наслідки від застосування кіберзброї почали зростати в геометричній прогресії. Наприклад, у журналі *Cybercrime Magazine* зазначено, що кіберзлочинність у світі зростатиме на 15% щороку і до 2025 р. збитки становитимуть 10,5 трлн дол. США порівняно з 3 трлн дол. США у 2015 р. [1]. Тобто за наявності могутнього військового потенціалу кіберзброя поступово набуває більш руйнівного та критично небезпечного характеру, аніж класичні види озброєння та військової техніки.

Аналіз останніх досліджень і публікацій. З розвитком інформаційних технологій міждержавне протиборство набуває нових форм, пов'язаних з боротьбою в кіберпросторі, що в перспективі може трансформуватись у кібервійну. Різні аспекти зазначеної тематики у своїх наукових працях розкривали П. Біленчук, М. Гуцалюк, Ю. Даник, Д. Дубов, М. Козир, В. Костенко, О. Кравчук, П. МакБарні (P. McBurney), С. Меле (S. Mele), Т. Рід (T. Rid.), Т. Ткачук та ін. Зокрема, в монографії Д. Дубова зазначено, що у 2010 р. США вже були готові завдати воєнного удару у відповідь на кібератаки на американські комп'ютерні системи [2, с. 51]. Однак, попри значну кількість наукових праць, присвячених кіберзброї, її визначенню та застосуванню, це питання залишається недостатньо розкритим і потребує подальших наукових досліджень.

Метою статті є аналіз визначень поняття «кіберзброї», визначення потенційних напрямів протидії цьому різновиду зброї та авторські пропозиції щодо вжиття відповідних заходів у сфері забезпечення кібернетичної безпеки України.

Виклад основного матеріалу

Із середини XX ст. за швидких темпів розвитку інформаційно-технічних систем мали місце злочини, пов'язані з незаконним отриманням інформації, порушенням роботи комп'ютерів тощо. Загалом статистику комп'ютерних злочинів вели від 1958 р., злочинами вважали випадки псування і розкрадання комп'ютерного устаткування; крадіжку інформації; шахрайство чи крадіжку грошей, вчинені із застосуванням комп'ютерів, або крадіжку машинного часу. Комп'ютер уперше був використаний як інструмент для пограбування банку в 1966 р. у Міннесоті. У 1968 р. у США було зафіксовано 13 подібних злочинів; у 1975 р. – 85 [3, с. 5–6].

У 1980-х роках з розвитком мережі Інтернет інтерес людства до цифрового (віртуального) простору

кардинально зріс. Це спонукало до створення інститутів, шкіл, курсів і навчальних програм, метою яких було всебічне опанування комп'ютерних систем та Інтернету. Удосконалення інформаційних технологій створило умови для ефективного розвитку суспільства: комунікаційні засоби стали невід'ємною складовою діяльності людей у всіх сферах, комп'ютери розширили комунікаційні, просторові та часові межі. Водночас мережа Інтернет стала засобом отримання величезних прибутків, зокрема й нелегальних. Цей процес стимулював дії шахраїв-хакерів, які активізували злочинну діяльність із використанням комп'ютерів у мережі Інтернет. Так, у 1981 р. у мас-медіа з'явилась інформація про появу комп'ютерного вірусу та його вплив на комп'ютерні системи [4, с. 92], у 1985 р. за допомогою комп'ютерного вірусу було виведено з ладу систему голосування Конгресу США [5, с. 11]; 2000 р. – вірус Jer розмістили на одному із сайтів, що поклало початок новій технології поширення вірусів у мережі Інтернет і мало «епідемічний» характер [6, с. 21]. Починаючи від 1970-х рр. і до початку XXI ст. кіберзброю визначали як комп'ютерні віруси, метою яких було викликати несправність у певній операційній системі чи окремій сервісній програмі (*табл. 1–2*) [7, с. 7–15].

З розвитком Інтернету речей (англ. Internet of Things, IoT – система речей, що під'єднані до мережі Інтернет), зокрема промислового Інтернету (англ. Industrial Internet of Things, IioT – система об'єднаних комп'ютерних мереж) спостерігається тенденція зростання впливу комп'ютерних вірусів не лише на окремі комп'ютери, а й на комп'ютерні системи загалом, що інколи набувало руйнівного характеру державних масштабів (*табл. 2*).

Однією з характерних особливостей кінця XX ст. стало підвищення функціонування обчислювальної техніки та інформаційно-комунікаційних систем на якісно новий рівень. Прогрес таких технологій спонукав військово-політичне керівництво провідних країн світу зосередити увагу на забезпеченні безпеки кібернетичного середовища від впливу кіберзброї. Так, у США протягом 1994 р. було зафіксовано більш ніж 300 тис. випадків несанкціонованого втручання злочинців у федеральні комп'ютерні мережі; приблизно 30 країн, зокрема Іран, активно вели розробки технологій, цільовим призначенням яких було ведення інформаційної війни, яка могла би стати для США «кібернетичним Чорнобилем» [8, с. 696]. Такі дії злочинних структур і радикально налаштованих країн стали «сигналом» для провідних країн до забезпечення належного рівня національної безпеки.

Сучасний цифровий простір і швидкий розвиток інформаційних технологій створили новітнє середовище обміну інформацією та застосування кіберзброї, який прийнято називати кіберпростір. В українському законодавстві «кіберпростір» визначається як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [9].

Інший підхід до кіберпростору пропонують у Північноатлантичному альянсі. У Доктрині ведення операцій у кіберпросторі зазначено, що кіберпростір – це глобальний домен з'єднаних між собою комунікаційних, інформаційних та інших електронних систем, мереж та їхніх даних, у яких обробляється, зберігається та передається інформація [10]. Фахівці НАТО наголошують на тому, що кіберпростір є ширшим, ніж Інтернет. Засоби, досяжні

Таблиця 1

Вплив вірусів на комп'ютери

	Назва комп'ютерного вірусу						
	Creeper	Rabbit	Elk Cloner	Brain	Virus Hoax	One Half	I Love You
Рік	поч. 1970-х	1974	1981	1986	1988	1994	2000
Цільове призначення	Збій системи	Зниження продуктивності системи	Перевертання зображення, повідомлення з погрозами	Виведення з ладу дискет	Зміна конфігурації портів і напряму обертання дисководів	Повна втрата даних на дисках	Увімкнення за замовчуванням обробника скриптів і приховування розширень приєднаних файлів

Таблиця 2

Вплив вірусів на працездатність комп'ютерних систем

	Назва комп'ютерного вірусу			
	Backdoor	Slammer	P2P ботмережі	Троянські програми
Рік	Початок 2000-х	2003	2007	2008 – теперішній час
Цільове призначення	Самостійне під'єднання зловмисників до комп'ютерів та їх зараження	Сповільнення швидкості мережі Інтернет, знищення мережі Інтернет у країні	Незаконне проникнення через мережу Інтернет, WAP/GPS та шахрайське заволодіння інформацією	Ураження комп'ютерних систем державного масштабу, отримання інформації про користувачів, отримання доступу до мобільних телефонів, смартфонів тощо

через кіберпростір, можуть бути об'єктами застосування кіберзброї, зокрема технічні прилади, що не під'єднанні до мережі Інтернет.

У США кіберпростір не пов'язують виключно з комунікаційними, інформаційними та іншими електронними системами, зокрема у Стратегії національної кібербезпеки США кіберпростір згадується як компонент фінансового, соціального, державного та політичного життя Америки [11, с. 1].

Виходячи із цього, можемо дійти висновку, що кіберпростір перетворився не лише на окрему, поряд із традиційними – «земля», «море», «повітря» та «космос» – сферу збройної боротьби, а й став невід'ємною частиною повсякденної людської діяльності.

Разом з тим, опанування кіберпростору кіберзлочинцями призвело до масштабніших проявів застосування вірусних програм, унаслідок чого на урядових порталах мали місце «викрадення» чи пошкодження службової інформації, світові економічні компанії та об'єкти атомної енергетики зазнавали величезних збитків. Наприклад, у червні 2017 р. кібератака на Україну за допомогою вірусу Petya завдала значних збитків державному сектору і бізнесу, заморозивши бізнес-процеси в країні на кілька днів. Серед постраждалих державних інституцій – Кабінет Міністрів України, КП «Київський метрополітен», Національний поштовий оператор «Укрпошта», Міжнародний аеропорт «Бориспіль» тощо.

Фактично кіберзброя стала зброєю першого удару, метою якої є системні порушення управління та функціонування держави противника; як цілі для ураження чи взяття під контроль почали розглядатися не лише збройні сили, їхні системи управління, інфраструктура та комунікації, а й об'єкти економіки, населення та керівництво держави [12, с. 14]. Отже, розвиток ІТ-технологій, активне використання мережі Інтернет і незаконні дії кіберзлочинців призвели до появи абсолютно нового виду зброї, який отримав назву «кіберзброя».

Світова практика свідчить, що не існує єдиного визначення «кіберзброї», оскільки вона постійно функціонально модифікується та вдосконалюється. Проте деякі національні та міжнародні документи дають зрозуміти сутність цього явища. Міжнародною групою вчених у Керівництві із застосування норм міжнародного права в кібервійнах зазначено, що кіберзброя є засобом ведення кібервійни, що має наступальний характер. За своїм задумом та призначенням вона здатна пошкоджувати, знищувати, спричиняти тяжкі наслідки в процесі застосування. До кіберзасобів можна віднести будь-який пристрій, прилад чи механізм, обладнання чи програмне забезпечення, що використовується для ведення кібератак [13, с. 141–142]. Результатом впливу на інформаційні системи можуть стати людські жертви, вплив на інфраструктуру, «параліч» певної сфери економіки, банківської системи чи дезорганізація системи управління під час ведення воєнних дій.

У статті «Кіберзброя» (Cyber-Weapons) американські вчені Т. Рід та П. МакБарні розглядають кіберзброю як один з видів зброї: комп'ютерний код, який використовується з метою погрози чи заподіяння фізичної, функціональної та психологічної шкоди структурам, системам чи фізичним особам [14].

Італійський спеціаліст із кібербезпеки Стефано Мелє пропонує визначення кіберзброї в міжнародно-правовій площині. На думку автора, кіберзброєю може бути пристрій чи будь-який набір інструкцій для комп'ютера, що використовується в конфліктах між державними та недержавними суб'єктами з метою заподіяння (прямо чи опосередковано) фізичних збитків людям чи предметам, а також пошкодження та/або виведення з ладу інформаційних систем [15, с. 7].

Фахівці з питань боротьби в кіберпросторі А. Медін та С. Марінін стверджують, що кіберзброя – це спецзасоби, які мають руйнівний вплив на комп'ютерні системи та мережі противника. Нею може бути будь-який інструмент нанесення збитків противнику, що володіє стандартизованим спеціальним програмним забезпеченням [16, с. 3].

Загальновідомим прикладом застосування кіберзброї стало використання комп'ютерного вірусу «Stuxnet». Вірус набув поширення у 2010 р. як перша програма, що була скерована проти енергосистем Ірану [17]. Метою вірусу стали комп'ютерні системи, які контролювали атомні електростанції. Фактично Stuxnet вважається різновидом кіберзброї, створеним за підтримки певної держави (держав). Створення комп'ютерного вірусу «Stuxnet» стало можливим завдяки масштабній розвідувальній операції на об'єкті критичної інфраструктури, де були порушені основні принципи побудови системи безпеки комп'ютерних систем.

Вважаємо, що термін «кіберзброя» (англ. cyber-weapons) слід розуміти як поєднання двох понять, де «кібер» (англ. cyber) характеризує процес, що відбувається в інформаційних мережах зв'язку, переважно в Інтернеті; «зброя» (англ. weapon) – засіб для нападу на когось (щось) [18].

У Законі України «Про основні засади забезпечення кібербезпеки України» зазначено, що кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти

кіберзахисту [9]. Тобто у вузькому розумінні кібератака – це замах на комп'ютерну безпеку інформаційної системи, а в широкому вона розглядається як пошук рішень, методів, кінцевою метою яких є отримання контролю над віддаленою системою для дестабілізації її працездатності. Таким чином, кібератаки проводяться із застосуванням кіберзброї (інформаційно-комунікаційних технологій, програмного забезпечення, комп'ютерного технічного обладнання тощо), яка застосовується переважно спеціально підготовленими особами в галузі кібернетики та інформаційних технологій.

У процесі дослідження розвитку кіберзброї автором виявлені деякі суперечності, наявні в чинних документах США. Наприклад, у Стратегії національної кібербезпеки США (2018) зазначено, що противники (Росія, Китай, Іран та Північна Корея) безперервно виготовляють нову та ефективну кіберзброю [11, с. 2–3]. Водночас у Словнику військових та суміжних термінів Міністерства оборони США (зі змінами від січня 2021 р.), який є основним документом у військовій термінології збройних сил США, термін «кіберзброя» (cyber-weapon) не згадується; запропоновані лише визначення «кіберпростір» (cyberspace), «кібератака» (cyberspace attack), «можливості кіберпростору» (cyberspace capability), «кібероборона» (cyberspace defense), «використання кіберпростору» (cyberspace exploitation), «операції в кіберпросторі» (cyberspace operations), «кібербезпека» (cybersecurity) та «перевага в кіберпросторі» (cyberspace superiority) [19, с. 55–56].

У Національній стратегії з кібербезпеки Великої Британії на 2016–2021 рр. відсутнє формулювання визначення «кіберзброї», проте зазначені дефініції «кіберзалежних злочинів» (cyber-dependent crimes) та «кіберзлочинів із застосуванням кіберпростору» (cyber-enabled crimes). Далі пояснюється, що «кіберзалежні злочини» – це злочини, які можуть бути вчинені тільки використовуючи інформаційно-комунікаційні пристрої, котрі можуть виступати як інструментом злочину, так і його ціллю (наприклад розробка та поширення шкідливих програм з метою фінансового збагачення, злом з метою викрадення, пошкодження, викривлення або знищення даних та/або мережі чи діяльності); «злочини із застосуванням кіберпростору» – «традиційні» злочини (наприклад шахрайство чи викрадення даних), масштаб яких можна збільшити за рахунок комп'ютерів, комп'ютерних мереж та інших інформаційно-комунікаційних технологій [20, с. 17]. Аналіз дефініцій «кіберзалежні злочини» та «злочини із застосуванням кіберпростору» в кримінально-правовій площині дає підстави стверджувати, що будь-які злочинні дії в кіберпросторі відбуваються безпосередньо із застосуванням кіберзброї. У свою чергу, такі дії є проявом суспільно-небезпечного явища, яке прийнято називати «кібертероризмом».

Для уточнення сутності поняття «кіберзброї» пропонується порівняльна таблиця (*табл. 3*).

Отже, виходячи з наведеного вище, автор пропонує таке визначення:

Кіберзброя – технічно-технологічний комплекс, що складається зі спеціального комп'ютерного обладнання, технологій та програм, призначених для цілеспрямованого порушення роботи інформаційно-технічних систем, викривлення, пошкодження, заволодіння або знищення критично важливої інформації, що може призвести до катастрофічних наслідків техногенного характеру.

Кіберзброя є важливим, ефективним і відносно економним компонентом проведення нелегальних операцій у кіберпросторі, що породжує такий негативний феномен, як кіберзлочинність. Кіберзлочини як складова організованої злочинності мають тенденцію до зростання і набули транснаціонального характеру.

Протидія незаконній діяльності у кіберпросторі стала нагальною проблемою для суспільства та потребує рішучих заходів. Проведений аналіз наступальної дії кіберзброї надає можливість сформулювати підходи до розв'язання цієї проблеми. Міжнародний досвід протидії кіберзброї має відносно давню історію. У 1947 р. США, Канада, Велика Британія, Австралія та Нова Зеландія як члени Англосаксонського клубу створили секретну систему «ECHELON» – першу систему, яка на початковій стадії свого функціонування забезпечувала уряди зазначених країн розвідувальною інформацією, переважно військового характеру, про країни Варшавського договору. На той час не існувало комп'ютерних систем та Інтернету, але керівництво країн об'єктивно оцінювало реальні та потенційні загрози й урахувало існуючий науково-технічний прогрес [21]. На цей час система «ECHELON» трансформована в інші структури, але продовжує виконувати безперервний моніторинг операцій, які ведуться в комп'ютерних системах: банківські перекази, перехоплення інформації кримінального характеру, прослуховування та перехоплення телефонних розмов, відстежування локації кіберзброї, запобігання кібертероризму тощо. Отже, *ця система виконує функції кіберрозвідки та є надзвичайно важливим механізмом протидії кіберзброї в усьому світі.*

Науковці факультету комп'ютерних наук Університету Бундесвера (ФРН) Р. Кох та М. Голлінг досліджували вплив кіберзброї на складні системи зброї [22]. У результаті досліджень вони встановили, що її функціональність базується передусім на аналізі та ідентифікації кібератак, установленні джерел кіберзброї та її знешкодження (*рис. 1*):

- планування на випадок надзвичайної ситуації (*Emergency Planning*) – передбачає наявність плану дій у таких випадках;
- управління ризиками (*Risk Management*) – необхідність створення єдиної системи управління ризиками, пов'язаними із застосуванням кіберзброї;
- система постачання (*Supply Chain*) – особлива увага зосереджена на виробленні єдиних вимог щодо закупівлі «надійних» комплектуючих частин та програмного забезпечення;

Таблиця 3

Порівняльна таблиця кіберзброї та її впливу

№ з/п	Автор/джерело	Складові кіберзброї, її призначення та вплив		
		Компоненти/суб'єкти застосування	Призначення	Об'єкт впливу
1.	Керівництво із застосування норм міжнародного права в кібервійнах	Пристрій, прилад, механізм, обладнання, програмне забезпечення	Пошкодження, знищення, тяжкі наслідки	Системи зброї, системи управління, цивільні та військові особи тощо
2.	Т. Рід та П. МакБарні	Комп'ютерний код	Погроза, заподіяння шкоди	Структури, системи, фізичні особи
3.	С. Меле	Пристрій чи будь-який набір інструкцій для комп'ютера	Заподіяння фізичних збитків; пошкодження та/або виведення з ладу	Люди, предмети, інформаційні системи
4.	А. Медін, С. Марінін	Спецзасоби	Руйнівний вплив, нанесення збитків	Комп'ютерні мережі, стандартизоване спеціальне програмне забезпечення
5.	Закон України «Про основні засади забезпечення кібербезпеки України» (визначення «кібератака»)	Засоби електронних комунікацій (включно з інформаційно-комунікаційними технологіями, програмними, програмно-апаратними засобами, іншими технічними й технологічними засобами та обладнанням)	Порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту	Безпека інформаційної системи
6.	Національна стратегія з кібербезпеки Великої Британії (визначення «кіберзалежні злочини»)	Пристрої на основі інформаційно-комунікаційних технологій	Розробка та поширення шкідливих програм, злом з метою викрадення, пошкодження, викривлення чи знищення даних та/або мережі або діяльності	Інформаційно-комунікаційні пристрої
7.	Національна стратегія з кібербезпеки Великої Британії (визначення «злочини із застосуванням кіберпростору»)	Пристрої на основі інформаційно-комунікаційних технологій	Шахрайство чи викрадення даних	Фізичні особи, комерційні компанії, організації

• *Hardware Regeneration by Design* – забезпечення стабільної роботи основної системи зброї (з довгим життєвим циклом) при заміні комерційних електронних комплектуючих (з коротким життєвим циклом), тому пропонується під час замовлення нових систем зброї визначати вимоги до таких замін ще на стадії проєктування зазначених систем;

• виробничі потужності (*Production Capabilities*) – розвиток оборонної технологічної та промислової бази ЄС, зокрема виробництво власних електронних компонентів для найважливіших систем зброї;

• аналіз загроз (*Threat Analysis*), на підставі якого визначаються заходи за всіма визначеними компонентами протидії.

Ураховуючи досвід провідних країн та міжнародних організацій щодо протидії кіберзброї, нам необхідно критично оцінювати боротьбу в кіберпросторі, вирішувати питання протидії кіберзброї, тобто переходити до активних принципів оборони. У цьому контексті необхідно підкреслити важливість функціонування Національного координаційного центру кібербезпеки, який є робочим органом Ради національної безпеки і оборони України

Рис. 1. Методи запобігання та захисту від кіберзброї [22]

[23]. Діяльність цього органу базується на забезпеченні координації діяльності суб'єктів національної безпеки та оборони України під час реалізації Стратегії кібербезпеки України, підвищенні ефективності системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки.

Поряд із цим, в Україні ефективно діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA (*Computer Emergency Response Team of Ukraine*), яка функціонує в рамках Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України [24]. Основною метою діяльності CERT-UA є системний захист діяльності державних інститутів та громадян України від незаконного доступу в кіберпростір нашої держави, протидія кіберзброї тощо. *Проте цей орган не має повноважень слідчого органу і не може здійснювати слідчі дії та притягати до відповідальності кіберзлочинців*.

На виконання спільних Директив Міністерства оборони України та Генерального штабу Збройних Сил України завершився черговий етап реформування Збройних Сил України, в результаті якого в загальнодержавній системі боротьби з кіберзброєю в лютому 2020 р. створено новий орган військового управління – Командування Військ зв'язку та кібернетичної безпеки Збройних Сил України [25]. Проте, на нашу думку, термін «кібернетична безпека» не повною мірою відповідає чинному законодавству. Відповідно до змін, внесених у Закон України «Про оборону», зазначено, що «Підготовка держави до оборони в мирний час включає... здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії...» [26]. Отже, *доцільним було би визначення «Командування Військ зв'язку та кібернетичної оборони Збройних Сил України»*.

Значним кроком у забезпеченні кібербезпеки України стало ухвалення Радою національної безпеки і оборони України Стратегії кібербезпеки України на 2021–2025 роки [27]. Важливим стратегічним завданням зазначеного документа є створення у складі Збройних Сил України окремого роду військ – сил кібероборони, забезпечивши його належними фінансовими, кадровими і технічними ресурсами для стримування збройної агресії в кіберпросторі та відсічі агресору.

З 2014 р. Російська Федерація веде гібридну війну проти України, проте масштаби цієї війни поширюються не лише на політичну, економічну, військову та інформаційну сфери, а й на війну в кіберпросторі, що супроводжується регулярними кібератаками. У зв'язку із цим в Україні вже створена система протидії кіберзброї та боротьби з нею. Водночас вважаємо, що ця система має певні вразливості:

- недостатньо розвинені виробничі потужності, що забезпечують розроблення та виготовлення електронно-обчислювальних машин, переважно комплектуючі частини та програмне забезпечення забезпечуються іноземними постачальниками;
- закупівля імпортного програмного забезпечення створює ризики щодо наявності шпигунських складових, які можуть дестабілізувати роботу комп'ютерної мережі та бути об'єктом кібератак;
- державні органи та суб'єкти забезпечення кібербезпеки не спроможні повністю контролювати процеси, які відбуваються в мережі Інтернет, адже вузли управління цією «павутиною» розташовані, як правило, поза межами України;
- рівень фінансування кібернетичної галузі не дає змоги надійно забезпечувати захист від кіберзброї, що значно підвищує ризики кібератак.

Розв'язання зазначених проблем є вкрай важливою складовою забезпечення національної безпеки України та потребує підтримки, насамперед з боку НАТО, де питанням боротьби в кіберпросторі приділяється велика увага.

У Північноатлантичному альянсі значна увага приділяється питанню захисту мереж зв'язку та інформаційних систем, а також надається сприяння союзникам щодо підвищення кіберзахисту на національному рівні [28, с. 19]. Створено групу кіберзахисту швидкого реагування, щорічно проводяться навчання «Кіберлокація» з метою вироблення інноваційних рішень у сфері кіберзахисту.

Пріоритетними цілями партнерства України з НАТО у військовій сфері, зокрема у сфері кіберзахисту, є розвиток спроможностей органів державної влади та військового управління. Виконавши всі військово-політичні процедури, у червні 2020 р. Україна отримала статус партнера НАТО з розширеними можливостями [29], що надало можливість Україні долучитися до спільних програм, зокрема в боротьбі з кібертероризмом. На цей час триває переговорний процес щодо участі України в аналітичному процесі (NATO reflection process) для формування Стратегічної концепції НАТО-2030 [30]. У результаті подальшої співпраці Україна матиме можливість отримати досвід боротьби країн – членів НАТО в протидії кіберзброї та брати безпосередню участь у міжнародних заходах у сфері кібербезпеки.

Висновки

Ураховуючи поточну ситуацію в Україні у сфері запобігання впливу кіберзброї, на нашу думку, було б доцільно:

- підвищити рівень кіберзахисту об'єктів критичної інфраструктури держави та приватного сектору, насамперед тих, які розташовані в районі проведення операції Об'єднаних сил і належать до юрисдикції Міністерства оборони України та Збройних Сил України;
- ужити заходів для вдосконалення комплексної системи кібербезпеки, яка виконувала би функції на випередження кібератак, ідентифікації джерел кіберзброї та її фінансування;

• провести критичний аналіз кадрового забезпечення підрозділів кібербезпеки, їхньої вкомплектованості, перспектив проходження військової служби майбутніх офіцерів за спеціальністю «Кібербезпека»;

• внести пропозиції щодо створення міжнародних підрозділів з кібербезпеки, що значно підвищить ефективність їхньої діяльності в боротьбі з кіберзброєю;

• удосконалити нормативно-правове забезпечення у сфері кібербезпеки з урахуванням сучасних загроз національній безпеці України.

Таким чином, забезпечення кібербезпеки, запобігання кібератакам та знищення кіберзброї противника повинні бути пріоритетом для України. Навіть попри позитивні зміни в питаннях забезпечення кібербезпеки ця система потребує подальшого вдосконалення. Держава повинна володіти необхідними інструментами та можливостями з нейтралізації реальних і потенційних загроз національній безпеці України. Вважаємо, що найефективніший спосіб протидії кіберзброї – це збільшення інвестування в кібербезпеку, координація дій складових сектору безпеки та оборони у сфері кібербезпки та їх інтеграція в єдину структуру, подібну до кібервійськ країн – членів НАТО.

Перелік літератури

1. *Morgan S.* 2021 Report: Cyberwarfare in the C-Suite [Електронний ресурс] : Cybercrime facts and statistics : Jan 21, 2021 / S. Morgan ; Cybersecurity Ventures // Cybercrime Magazine. – Режим доступу : https://cybersecurity ventures.com/wp-content/uploads/2021/01/ Cyberwarfare-2021-Report.pdf.

2. *Дубов Д. В.* Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

3. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти / П. Д. Біленчук, М. В. Гуцалюк, О. В. Кравчук, М. В. Козир ; за заг. ред. П. Д. Біленчука. – К. : Наука і життя, 2008. – 291 с.

4. *Расторгуев С. П.* Инфицирование как способ защиты жизни. Вирусы: биологические, социальные, психические, компьютерные / С. П. Расторгуев. – М. : Яхтсмен, 1996. – 332 с.

5. *Безруков Н. Н.* Компьютерные вирусы / Н. Н. Безруков. – М. : Наука, 1991. – 160 с.

6. *Цветков В. Я.* Технологии и системы информационной безопасности : аналитический обзор / В. Я. Цветков. – М. : ВНТИЦ, 2001. – 89 с.

7. Комп'ютерна вірусологія : навч. посібник / за заг. ред. Б. В. Наркіна. – К., 2012. – 309 с.

8. *Антипенко В. Ф.* Борьба с современным терроризмом: международно-правовые подходы / В. Ф. Антипенко. – К. : ЮНОНА-М, 2002. – 723 с.

9. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 5 жовтня 2017 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

10. Allied Joint Doctrine for Cyberspace Operations [Електронний ресурс] : NATO Standard AJP-3.20 : Edition A Version 1 : January 2020 // NATO Standardization Office. – Режим доступу : https://nso.nato.int/nso/zPublic/ap/PROM/AJP-3.20%20EDA%20V1%20E.pdf.

11. National Cyber Strategy of the United States of America [Електронний ресурс] : September 2018 // The White House. – Режим доступу : https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

12. *Даник Ю. Г.* Кібербезпека до кібероборони / Ю. Г. Даник, С. І. Вдовенко // Оборонний вісник. – 2020. – № 10. – С. 10–15.

13. Tallinn Manual on the International Law Applicable to Cyber Warfare [Електронний ресурс] // Cambridge University Press. – Режим доступу : https://doi.org/10.1017/CBO9781139169288.

14. *Rid T.* Cyber-Weapons [Електронний ресурс] / T. Rid, P. McBurney // The RUSI Journal. – 2012. – Volume 157, Issue 1. – P. 6–13. – Режим доступу : https://doi.org/10.1080/03071847.2012.664354.

15. *Mele S.* Legal Considerations on Cyber-Weapons and Their Definitions [Електронний ресурс] / S. Mele // Journal of Law & Cyber Warfare. – 2014. – Vol. 3, № 1. – P. 52–69. – Режим доступу : https://www.jstor.org/stable/26432559.

16. *Мелин А. В.* Использование киберпространства террористическими и экстремистскими организациями / А. В. Мелин, С. О. Маринин // Зарубежное военное обозрение. – 2012. – № 10 (787). – С. 3–8.

17. Stuxnet – перша цифрова зброя-вірус? [Електронний ресурс] // BBC News Україна. – Режим доступу : https://www.bbc.com/ukrainian/news/2011/02/110215_stuxnet_virus_oh.

18. Definition of weapon noun from the Oxford Advanced Learner's Dictionary [Електронний ресурс] // Oxford Learner's dictionaries – Режим доступу : https://www.oxfordlearnersdictionaries.com/definition/english/weapon?q=weapon.

19. DOD Dictionary of Military and Associated Terms [Електронний ресурс] : as of January 2021 // Joint Chiefs of Staff. – Режим доступу : https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

20. National Cyber Security Strategy 2016–2021 [Електронний ресурс] // UK Government. – Режим доступу : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

21. *Perrone J.* The Echelon spy network [Електронний ресурс] / J. Perrone // The Guardian. – Режим доступу : https://www.theguardian.com/world/2001/may/29/qanda.janeperrone.

22. *Koch R.* Weapons systems and cyber security – a challenging union / R. Koch, M. Golling // Proceedings of 2016 8th International Conference on Cyber Conflict: Cyber Power, 31 May – 03 June 2016, Tallinn, Estonia / NATO CCD COE Publications. – Tallinn, 2016. – P. 191–203.

23. Про Національний координаційний центр кібербезпеки [Електронний ресурс] : Указ Президента України № 242/2016 від 07 червня 2016 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/242/2016#Text.

24. Computer Emergency Response Team of Ukraine. – Режим доступу: https://cert.gov.ua/about-us.

25. Перший етап реформування Збройних Сил суттєво наблизив їх до набуття взаємосумісності з НАТО, – Андрій Таран. – Режим доступу: https://www.kmu.gov.ua/news/pershij-etap-reformuvannya-zbrojnih-sil-suttyevo-nabliziv-yih-do-nabuttya-vzayemosumisnosti-z-nato-andrij-taran.

26. Про оборону України [Електронний ресурс] : Закон України № 1932-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1932-12#Text.

27. Глава держави провів засідання РНБО, на якому застосовано санкції до злодіїв у законі та доручено провести аудит державних земель у Конча-Заспі та Пущі-Водиці [Електронний ресурс] // Офіційне інтернет-представництво Президента України. – Режим доступу : https://www.president.gov.ua/news/glava-derzhavi-proviv-zasidannya-rnbo-na-yakomu-zastosovano-68465.

28. *Голопатюк Л.* Адаптація до загроз / Л. Голопатюк, І. Пилипчук // Україна до НАТО. – 2019. – № 1 (1). – С. 16–19.

29. Програма розширених можливостей НАТО для України: у Міноборони назвали всі переваги (УНН) [Електронний ресурс] // Офіційний вебсайт Міністерства оборони України. – Режим доступу : https://www.mil.gov.ua/ministry/zmi-pro-nas/2020/07/24/programa-rozshirenih-mozhlivostej-nato-dlya-ukraini-u-minoboroni-nazvali-vsi-perevagi-(unn).

30. Ольга Стефанішина: Україна прагне долучитися до аналітичного процесу NATO reflection process для формування Стратегічної концепції НАТО-2030 [Електронний ресурс] // Урядовий портал. – Режим доступу : https://www.kmu.gov.ua/news/olga-stefanishina-ukrayina-pragne-doluchitisya-do-analitichnogo-procesu-nato-reflection-process-dlya-formuvannya-strategichnoyi-koncepciyi-nato-2030.

DOI 10.33099/2618-1614-2021-15-2-50-60
УДК 308:355.02(477)«2005/2021»

І. С. Печенюк,
кандидат історичних наук, старший науковий співробітник, доцент кафедри історії війн і воєнного мистецтва, Національний університет оборони України імені Івана Черняховського,

С. І. Печенюк,
кандидат історичних наук, провідний науковий співробітник науково-дослідного відділу прикладних соціологічних досліджень, Науково-дослідний центр гуманітарних проблем Збройних Сил України

Динаміка зміни рейтингів державних інститутів сектору безпеки та оборони України (2005–2021)

У статті проаналізовано й узагальнено результати досліджень громадської думки, що проводилися в нашій країні впродовж 2005–2021 рр., у частині підтримки діяльності та довіри суспільства до основних державних інститутів сектору безпеки та оборони України та визначено значущість кожного з них. З'ясовано причини та висвітлено динаміку зміни рейтингів Збройних Сил України, Служби безпеки України, міліції та Національної поліції України й інших інститутів сектору безпеки та оборони в досліджуваний період. Виявлено взаємозв'язки та взаємозалежність у діяльності цих інститутів. Установлено, що з початком збройної агресії Російської Федерації проти нашої країни довіра українського суспільства до інститутів, відповідальних за національну безпеку держави, суттєво зросла. З-поміж них упродовж останніх п'ятнадцяти років найбільш авторитетним інститутом були та залишаються Збройні Сили України. Автори висловили припущення, що в умовах збройного конфлікту та інформаційної війни інститути сектору безпеки та оборони матимуть високий рівень суспільної довіри.

Ключові слова: державні інститути, рівень суспільної довіри, громадська думка, національна безпека, сектор безпеки та оборони.

Актуальність обраної теми зумовлена тим, що наприкінці XX – на початку XXI ст. Україна зазнала радикальних реформ у всіх сферах суспільного життя. Зазначені перетворення відбуваються вже майже три десятиліття і виявилися складними та болісними для українського суспільства. Усе це породжує певний інтерес до новітньої історії нашої держави. З одного боку, в минулому можемо віднайти причини сьогоднішніх проблем, а з другого – аналізуючи історичний досвід, можемо надати відповіді на запитання щодо раціональних шляхів їх подальшого розвитку.

У межах такого аналізу найбільш прискіпливо розглядаються політичні, економічні, соціальні та культурні аспекти вітчизняної історії. Проте значно менше уваги приділяється історії розбудови системи забезпечення національної безпеки України. Варто зазначити, що в сучасному світі в контексті воєнної безпеки будь-якої держави вирішуються практично всі питання міжнародних відносин, економічних та інших стосунків між державами [1, с. 5–6]. Тому вивчення й узагальнення досвіду розбудови сектору безпеки та оборони України, ставлення (рівень довіри) громадськості до його державних інститутів є одним з основних показників їхньої ефективної діяльності. Водночас такий спосіб зворотної комунікації вказує на наявні проблеми, що потребують пошуку шляхів подальшого вдосконалення роботи органів державної влади та військового управління.

Відповідно до Закону України № 2469-VIII «Про національну безпеку України» від 21 червня 2018 р. (зі змінами) *сектор безпеки і оборони* – це система органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України (далі – державних інститутів), діяльність яких перебуває під демократичним цивільним контролем і відповідно до Конституції та законів України за функціональним призначенням спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об'єднання, які добровільно беруть участь у забезпечення національної безпеки України. При цьому на сили безпеки покладено *функції із забезпечення національної безпеки*, а на сили оборони – *функції із забезпечення оборони держави* (захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних і потенційних загроз) [2].

Ураховуючи особливості діяльності інститутів сектору безпеки та оборони України, дослідження громадської думки щодо їхнього функціонування, аналіз зовнішніх і внутрішніх чинників, що впливають на ставлення громадян до них, є важливим елементом забезпечення національної безпеки держави. Особливої актуальності

такі дослідження набувають в умовах загострення інформаційного протиборства.

Аналіз попередніх досліджень і публікацій. Проблема довіри до державних інститутів була й залишається в центрі уваги українських і зарубіжних дослідників, які представляють різні галузі науки, зокрема філософію, соціологію, психологію, економіку, державне управління тощо. Одним з відомих сучасних американських філософів, який досліджує довіру, є Ф. Фукуяма [3]. Саме довіру він визначає як ключову характеристику розвиненого суспільства, тому в основу поділу суспільств за рівнем розвитку Ф. Фукуяма поклав поширеність у них довіри, що проявляється як на індивідуальному рівні, так і на рівні соціальному (довіра до соціальних інститутів і держави загалом). На його думку, чим поширенішою є довіра, тим розвиненішим є суспільство.

Відомий сучасний польський соціолог П. Штомпка [4] розглядає довіру як фундаментальний аспект суспільного життя, особливо повсякденного. Розглядаючи феномен довіри в суспільстві, дослідник аналізує основні категорії цієї теорії в культурологічній соціології постмодерну, включно із сутністю ідеї довіри, її різновидами, функціями, та шукає джерела недовіри в соціальному плані й відновлення довіри на всіх рівнях суспільства. Особливе місце автор відводить застосуванню теорії довіри для аналізу та регулювання суспільних відносин у таких ключових сферах, як політичний устрій держави, розвиток науки, процес глобалізації.

В Україні особливості феномену довіри в соціогуманітарному дискурсі сучасної держави досліджувала В. Нападиста [5]; аспекти довіри до соціально-політичних інститутів та органів публічної влади та їх репутації вивчали О. Волянська [6; 7], Г. Зеленко [8], М. Іжа, Т. Пахомова, О. Князєва [9], Т. Федорів [10], М. Чабанна [11]; суспільну підтримку влади та довіру до її органів у системі державного управління досліджували А. Кохан [12], В. Токарева і Ю. Носачова [13], О. Кучабський і С. Погорєлий [14]; дослідженням зв'язків між соціально-економічними показниками та індексами міжособистісної та інституційної довіри займалися Т. Меркулова і Г. Богданова [15] та ін.

Дослідники Л. Амджадін та О. Гончарук у своїй праці [16] простежили динаміку феномену довіри населення до армії та загалом до інститутів сектору безпеки та оборони України в 1994–2013 рр. і спробували з'ясувати причини таких змін. Окремо варто звернути увагу на результати національного дослідження, проведеного протягом листопада-грудня 2018 р. колективом Харківського інституту соціальних досліджень [17] щодо оцінки суспільством діяльності поліції, яким є рівень довіри до неї після проведеної реформи. Водночас у звіті наведені основні показники діяльності поліції в країні та регіонах.

Мета і завдання дослідження. Мета нашої статті полягає в тому, щоб на основі збору, аналізу та узагальнення результатів досліджень громадської думки в Україні впродовж 2005–2021 рр. через зміни рівня підтримки діяльності й довіри суспільства до основних державних інститутів сектору безпеки та оборони України, *з'ясувати* причини зміни їхніх рейтингів, *визначити* значущість кожного з них і *виявити* взаємозв'язки та взаємозалежність між ними.

Методи дослідження

Методичною основою дослідження стали загальнонаукові принципи об'єктивності, науковості й системності, які реалізувалися шляхом застосування низки методів, зокрема аналізу, синтезу, узагальнення, візуального аналізу даних, аналізу рядів динаміки та методу індексів. *Загальнонаукові методи* (аналіз, синтез, узагальнення) дали змогу здійснити теоретичне осмислення підходів до довіри як соціального явища й теоретично опрацювати емпіричні дані (результати опитувань громадської думки). *Порівняльний соціологічний аналіз* застосовувався для зіставлення та порівняння динамічних рядів даних, що відображають рівень довіри (підтримку діяльності) українського суспільства до деяких державних інститутів, для оцінки варіативності в часі (динаміки) індексів довіри (підтримки діяльності). *Візуалізація даних* за допомогою електронних таблиць Microsoft Office Excel у формі графіків і діаграм допомогла посилити сприйняття статистичної інформації та виявити взаємозв'язки, взаємозалежності та кореляції між окремими аспектами досліджуваного явища. Сутність *методу індексів* полягала у зведенні результатів відповідей на кожне запитання до одного показника, що, у свою чергу, дало в подальшому змогу їх порівняти та знайти відмінності. У дослідженні використовувалися два індекси – індекс довіри до державного інституту та індекс підтримки діяльності державного інституту, що зумовлено різною постановкою запитань: в одному випадку об'єктом дослідження була підтримка діяльності державного інституту, а в другому – довіра до нього.

Індекс довіри до державного інституту розраховується як різниця між кількістю тих, хто довіряє (повністю і частково) та кількістю тих, хто не довіряє (повністю і частково) відповідному інституту. *Індекс підтримки діяльності державного інституту* розраховується як «повністю підтримую» + половина «підтримую окремі заходи» – «не підтримую». Значення індексів можуть коливатися від –100 до +100 балів, де –100 вказує на повну відсутність довіри (підтримки діяльності), а +100 – на повну довіру (підтримку діяльності).

Характеристика емпіричної бази. В основу аналізу цієї розвідки покладено результати опитувань громадської думки, які проводилися провідними українськими аналітичними та соціологічними компаніями/установами. Основний масив даних представлений результатами опитувань, проведених Українським центром економічних та політичних досліджень ім. О. Разумкова (Центр Разумкова) [18–35], рідше такі опитування проводили Фонд «Демократичні ініціативи» імені Ілька Кучеріва [36–38], Київський міжнародний інститут соціології

[39; 40], Центр «Соціальний Моніторинг» [41; 42] та ін. [43–47]. Під час більшості опитувань у середньому було охоплено близько 2000 респондентів у всіх регіонах України (після квітня 2014 р. – крім тимчасово окупованих територій АР Крим, м. Севастополь та окремих районів Донецької та Луганської областей України, далі – ОРДЛО), які репрезентують доросле населення країни за основними соціально-демографічними показниками. Теоретична похибка вибірок не перевищує 2,3% з імовірністю 0,95. Водночас маємо певний нюанс, що з 2014 р. із досліджуваної сукупності випала частина критично налаштованого населення – мешканці Криму та ОРДЛО, що не могло не вплинути на результати опитувань.

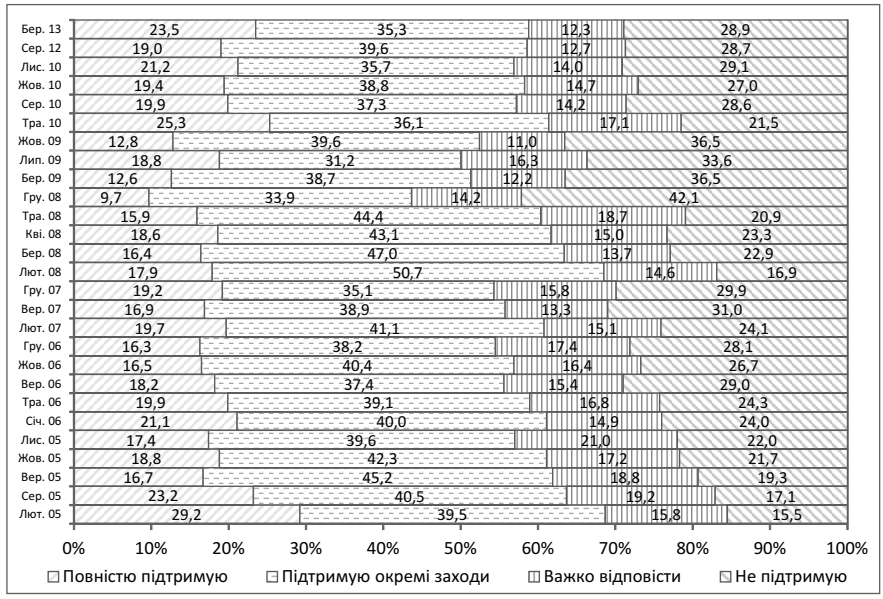
В опитуваннях соціологічної служби Центру Разумкова у 2005–2013 рр. запитання формулювалося так: *«Чи підтримуєте ви діяльність Збройних Сил України?»* (аналогічно для Служби безпеки України, органів внутрішніх справ, міліції) з варіантами відповіді «повністю підтримую», «підтримую окремі заходи», «не підтримую» та «важко відповісти». Пізніше в опитуванні соціологічної служби Центру Разумкова довіру до соціальних інститутів визначали через запитання *«Якою мірою Ви довіряєте таким соціальним інституціям?»*. Респонденту на вибір пропонувалися варіанти відповіді: «зовсім не довіряю», «скоріше не довіряю», «скоріше довіряю», «повністю довіряю», «важко відповісти». Подібним чином формулювали запитання та варіанти відповіді до них і інші соціологічні установи. Так, наприклад, Соціологічна група «Рейтинг» ставила запитання *«Наскільки Ви довіряєте таким інституціям?»* із варіантами відповіді «цілком довіряю», «швидше довіряю», «важко відповісти», «швидше не довіряю», «зовсім не довіряю». У дослідженні Програми USAID «Нове правосуддя» запитання звучало так: *«Наскільки Ви довіряєте?»* і запропонували перелік організацій. Далі респондент обирав з варіантів відповіді «повністю довіряю», «скоріше довіряю», «скоріше не довіряю», «зовсім не довіряю», «і довіряю, і не довіряю одночасно», «важко сказати» або міг відмовитися відповідати.

Традиційно соціологічні установи разом з іншими соціальними інститутами держави (Церквою, Президентом України, Верховною Радою України, Кабінетом Міністрів України, засобами масової інформації (ЗМІ) тощо) найчастіше вивчали ставлення українців до Збройних Сил України (ЗСУ), Служби безпеки України (СБУ) та органів внутрішніх справ, міліції (Національної поліції України (НПУ)). Згодом (з початком збройної агресії Російської Федерації (РФ)) Центр Разумкова став включати до анкет і опитувальників інші інститути сектору безпеки та оборони – Національну гвардію України (НГУ), Державну прикордонну службу України (ДПСУ) та Державну службу України з надзвичайних ситуацій (ДСНС).

Авторами зібрано, проаналізовано й узагальнено наявні у вільному доступі результати досліджень громадської думки зазначених вище організацій у частині, що стосувалася рейтингів інститутів сектору безпеки та оборони України в період з 2005 р. до початку 2021 р., і на їхній основі досліджено зміни у сприйнятті громадськістю результатів діяльності цих інститутів.

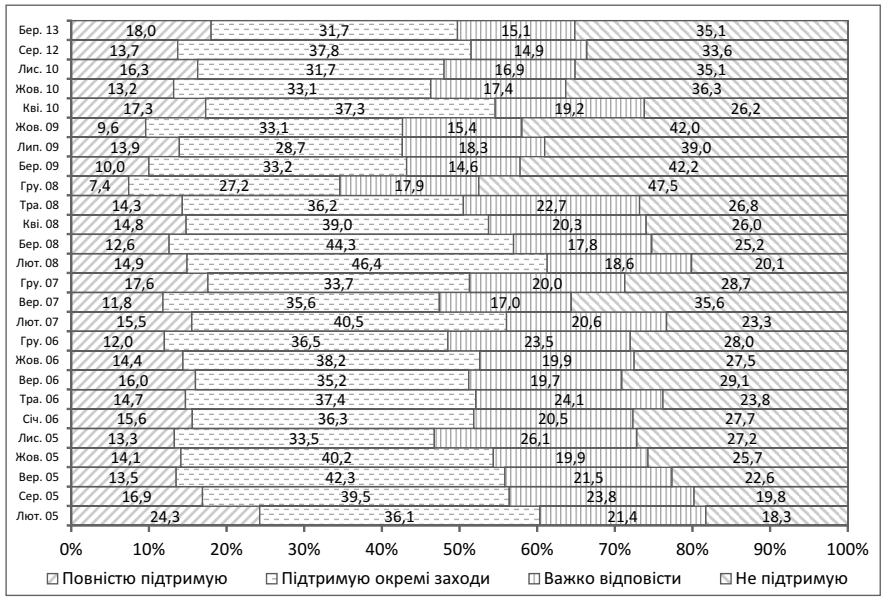
Результати

На *рисунках 1, 2* і *3* наведена *структура підтримки діяльності* окремих інститутів сектору безпеки та оборони України в період 2005–2013 рр. Як видно на *рисунках 1* і *2*, серед українців переважає частка тих, хто



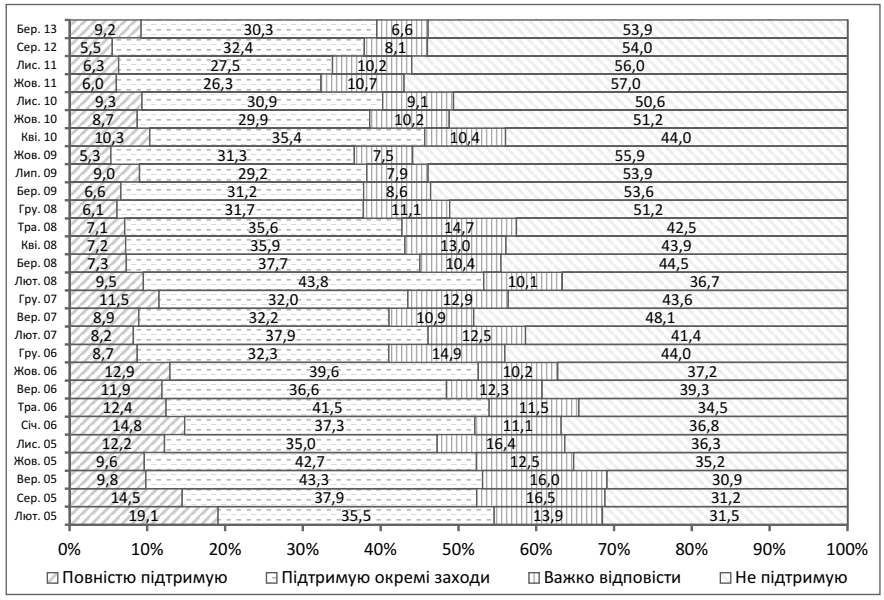
[Складено авторами згідно з 18]

Рис. 1. Структура підтримки українцями діяльності ЗСУ впродовж 2005–2013 рр. (за даними соціологічної служби Центру Разумкова), %



[Складено авторами згідно з 19]

Рис. 2. Структура підтримки українцями діяльності СБУ впродовж 2005–2013 рр. (за даними соціологічної служби Центру Разумкова), %

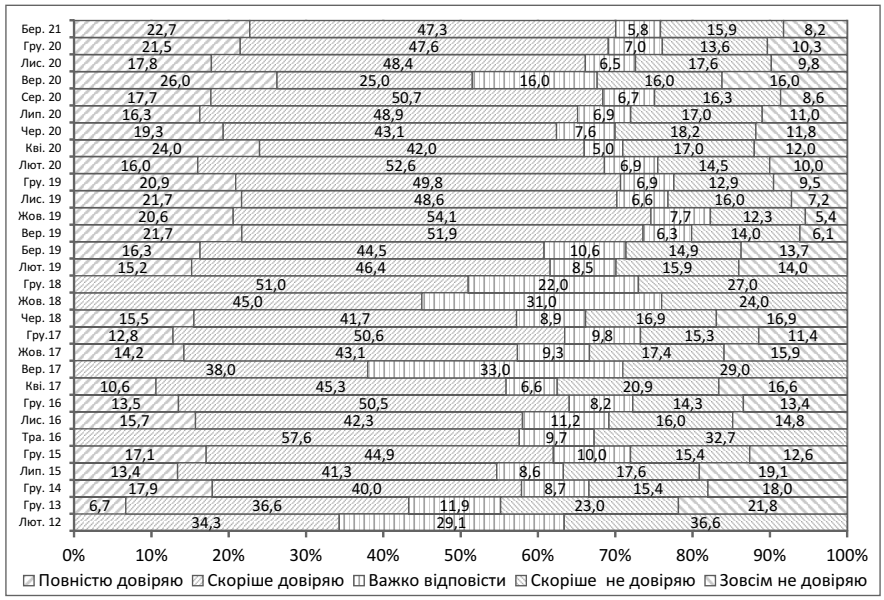


[Складено авторами згідно з 20]

Рис. 3. Структура підтримки українцями діяльності органів внутрішніх справ і міліції впродовж 2005–2013 рр. (за даними соціологічної служби Центру Разумкова), %

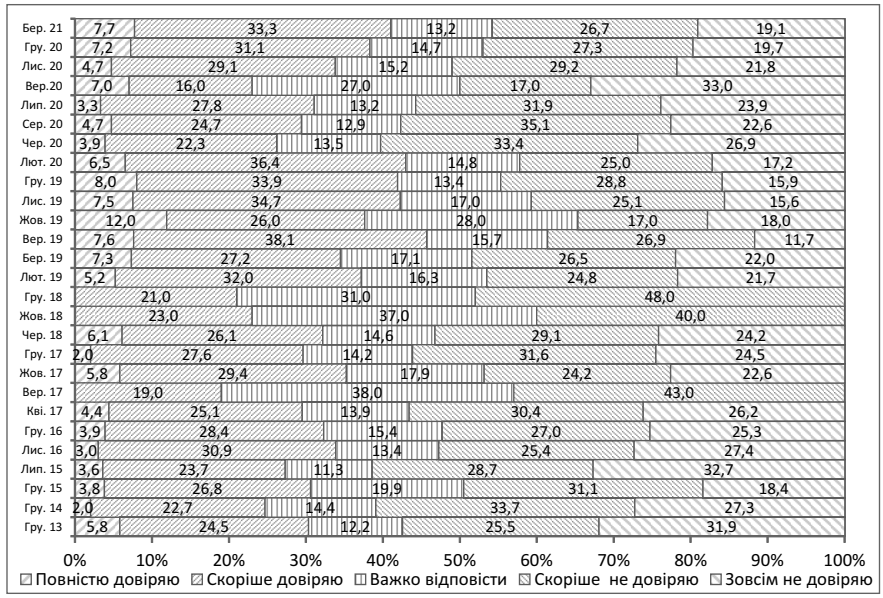
підтримував діяльність ЗСУ та СБУ (сумарно «повністю підтримую» та «підтримую окремі заходи»), ніж однозначно не підтримував. Водночас діяльність органів внутрішніх справ та міліції до 2008 р. (*рис. 3*) населення України частіше підтримувало, ніж не підтримувало, а починаючи з 2008 р. діяльність цих інститутів українці переважно не підтримували.

Структура довіри до інститутів сектору безпеки та оборони України представлена на *рисунках 4–9*. Так, на *рисунку 4* відображено, що з 2012 р. і донині частка тих, хто *довіряє* ЗСУ, **суттєво** переважає над тими, хто не довіряє. Крім того, частка тих, хто не має чіткої думки щодо свого ставлення до цього соціального інституту, переважно



[Складено авторами згідно з 21–47]

Рис. 4. Структура довіри українців до ЗСУ впродовж 2012–2021 рр. (за даними українських соціологічних компаній), %



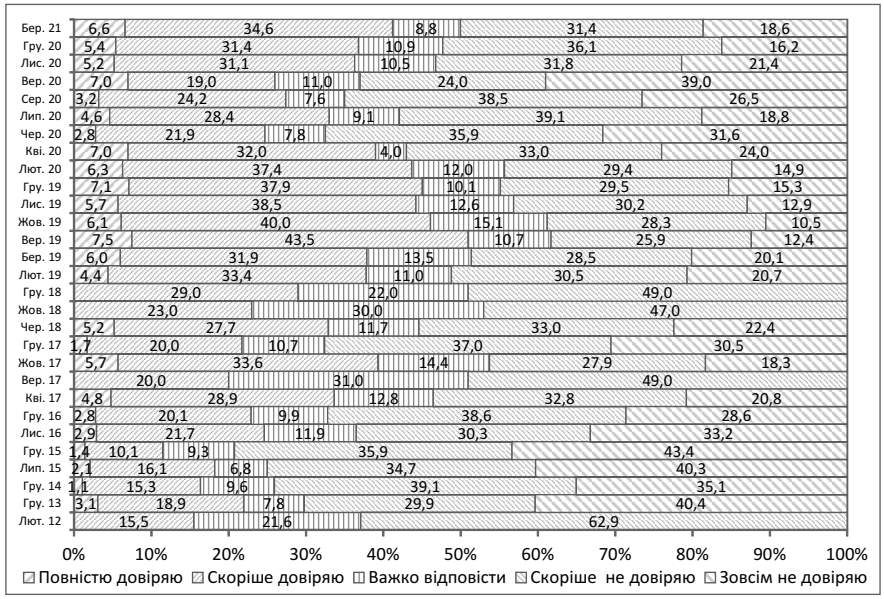
[Складено авторами згідно з 21–38; 40–43; 45; 46]

Рис. 5. Структура довіри українців до СБУ впродовж 2013–2021 рр. (за даними українських соціологічних компаній), %

перебуває в межах 7–11% (окрім декількох випадків, коли це значення досягало 29–33%) (у середньому 11%).

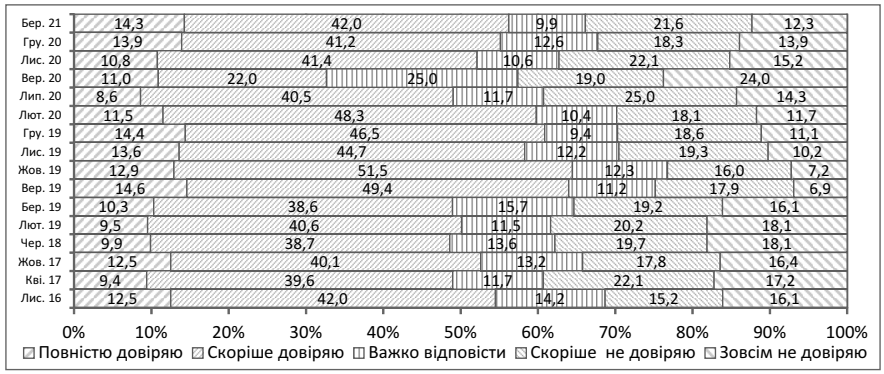
Упродовж аналогічного періоду (*рис. 5*) щодо довіри до НПУ (до листопада 2015 р. – міліції) спостерігалася протилежна ситуація – частка тих, хто цьому інституту не довіряє, *суттєво переважала* над тими, хто довіряє. Ситуація дещо вирівнялася (кількість тих, хто довіряє НПУ, була майже такою, як і тих, хто не довіряє) на рубежі 2019 і 2020 рр. Водночас частка тих, хто не визначився зі своєю думкою, в середньому була на рівні 14%.

Подібна ситуація і з довірою до СБУ (*рис. 6*): з кінця 2013 р. серед респондентів більше тих, хто інституту не довіряє, ніж тих, хто довіряє (крім проміжку часу на рубежі 2019–2020 рр., коли баланс довіри був близьким



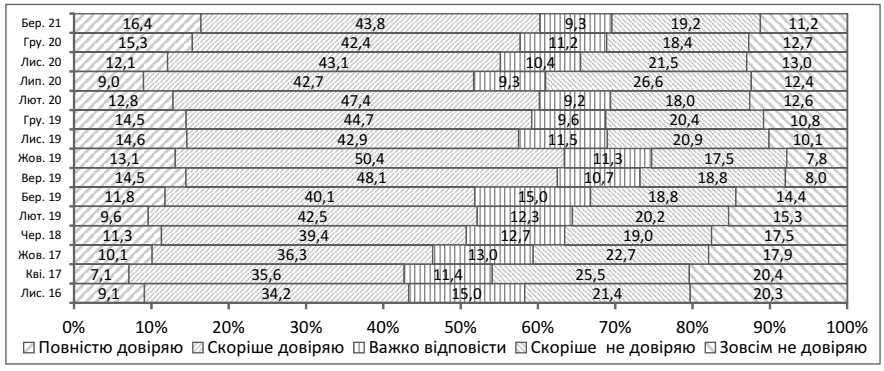
[Складено авторами згідно з 21–43; 45–47]

Рис. 6. Структура довіри українців до НПУ впродовж 2012–2021 рр.
(за даними українських соціологічних компаній), %



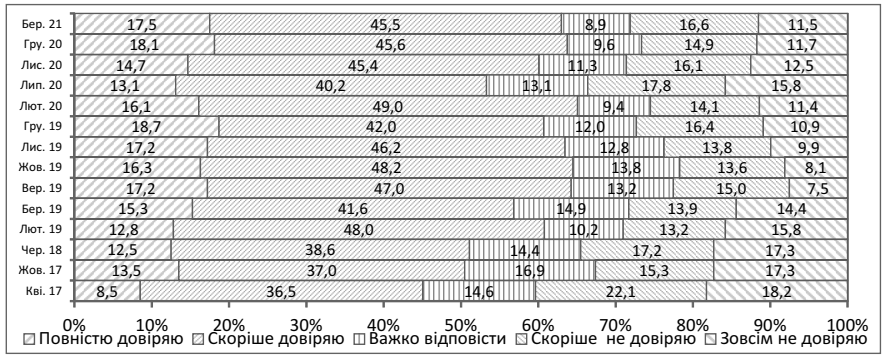
[Складено авторами згідно з 21–35; 43]

Рис. 7. Структура довіри українців до НГУ впродовж 2016–2021 рр.
(за даними українських соціологічних компаній), %



[Складено авторами згідно з 21–35]

Рис. 8. Структура довіри українців до ДПСУ впродовж 2016–2021 рр.
(за даними українських соціологічних компаній), %



[Складено авторами згідно з 22–35]

Рис. 9. Структура довіри українців до ДСНС України впродовж 2017–2021 рр. (за даними українських соціологічних компаній), %

до нуля). Варто зазначити, що частка тих, хто не має чіткої думки щодо довіри до СБУ, дещо вища, якщо порівняти таку із ЗСУ та НПУ, і становить у середньому 19% (у деяких випадках цей показник досягав 40%).

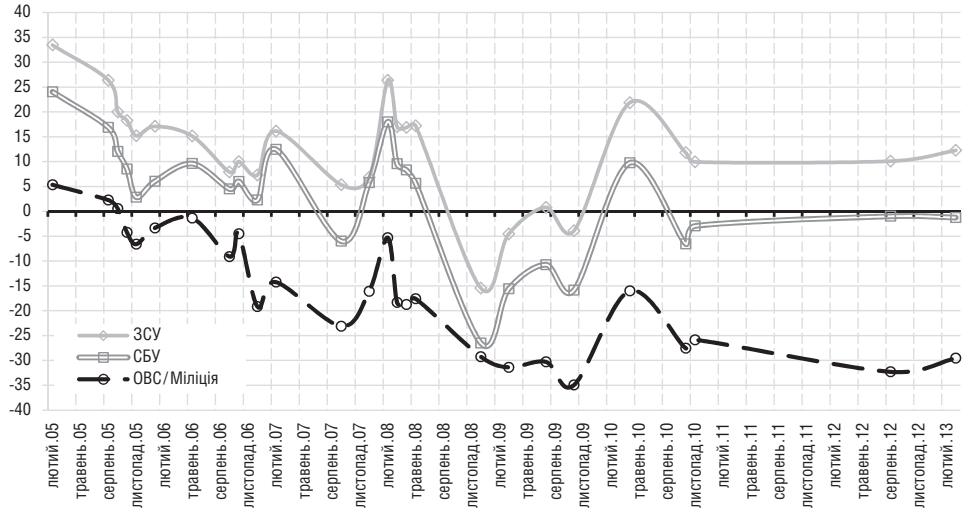
Що стосується структури довіри до НГУ, ДПСУ та ДСНС, то українці в досліджуваний період (з 2016 р.) їм більше довіряли, ніж не довіряли (*рис. 7–9*). Частка тих, хто не мав чіткої позиції, була незначна і становила в середньому 12%.

Пояснення результатів

Динаміку зміни рейтингів (у нашому випадку – рівня підтримки діяльності або рівня довіри) державних інститутів зручно аналізувати візуально, тобто шляхом відображення на графіках індексів підтримки діяльності (*рис. 10*) та індексів довіри (*рис. 11*). Це зумовлено різною постановкою запитань – в одному випадку об'єктом дослідження була підтримка діяльності державного інституту, а в іншому – довіра до нього. В основу першого графіка (*рис. 10*) покладено виключно результати опитувань соціологічної служби Центру Разумкова за 2005–2013 рр., а іншого графіка (*рис. 11*) – тільки результати опитувань соціологічної служби Центру Разумкова та Фонду «Демократичні ініціативи» імені Ілька Кучеріва за 2013–2021 рр., які працювали за єдиним методологічним підходом, що дає змогу простежити динаміку зміни індексів довіри.

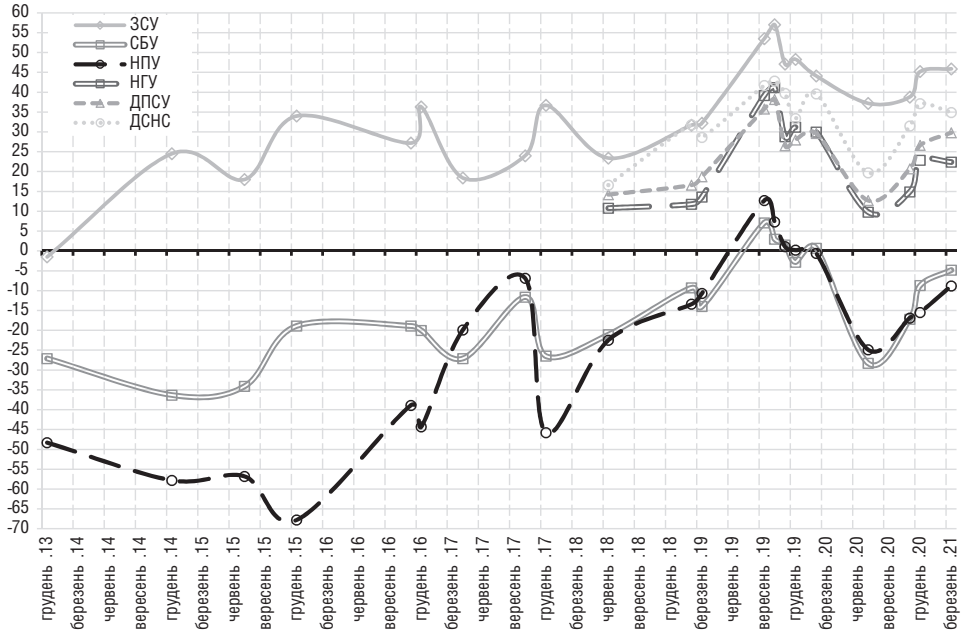
Розгляньмо динаміку зміни індексів підтримки діяльності державних інститутів сектору безпеки та оборони України у 2005–2013 рр. (*рис. 10*).

Як видно з *рисунка 10*, індекс підтримки діяльності органів внутрішніх справ, міліції був переважно від'ємним (після вересня 2005 р.). Підтримка діяльності СБУ до середини 2008 р. була переважно позитивною,



[Складено авторами згідно з 18–20]

Рис. 10. Динаміка підтримки українцями діяльності інститутів сектору безпеки та оборони України впродовж 2005–2013 рр. (за даними соціологічної служби Центру Разумкова), %



[Складено авторами згідно з 21–38]

Рис. 11. Динаміка довіри українців до інститутів сектору безпеки та оборони України впродовж 2013–2021 рр. (за даними українських соціологічних компаній), %

а станом на початок 2010 р. – негативною, після короткого сплеску підтримки (середина 2010 р.) кількість тих, хто підтримує, і тих, хто не підтримує, майже вирівнялася. Підтримка діяльності ЗСУ була переважно позитивною (крім проміжку у 2008–2009 рр., коли переважали критичні оцінки). Крім того, візуальний аналіз кривих графіків указує на наявність зв'язку між індексами підтримки діяльності ЗСУ, СБУ та міліції. Це підтверджується високими значеннями коефіцієнтів лінійної кореляції – для пари ЗСУ – СБУ він становить 0,938; для СБУ – міліції – 0,819; ЗСУ – міліції – 0,725. Примітно, що в цей період респонденти не особливо відрізняли ці інститути – поведінка графіків схожа, різний лише рівень підтримки їхньої діяльності. Проте на початку наступного періоду (*рис. 11*) крива графіка ЗСУ поводиться діаметрально протилежно до СБУ та НПУ.

Отже, спробуємо прокоментувати динаміку зміни рейтингів, відображених на *рисунку 10*. Напряму стверджувати про причини підтримки чи не підтримки діяльності державних інститутів сектору безпеки та оборони українцями не можемо, проте певні коливання, на нашу думку, можуть бути пов'язані з вагомими подіями державного та міжнародного рівня, що відбулися напередодні проведення опитувань. Так, на проміжку з вересня 2007 р. до лютого 2008 р. відбулося зростання рівня їхньої підтримки, що можемо пояснити очікуванням населенням після виборів до Верховної Ради України. Проте вже з квітня до грудня 2008 р. відбувається спад рівня підтримки, зумовлений російсько-грузинським збройним конфліктом улітку 2008 р. та низкою важливих внутрішньодержавних подій, пов'язаних з парламентською кризою в Україні восени 2008 р.

Чергове зростання рівня підтримки державних інститутів сектору безпеки та оборони відбувається на проміжку з грудня 2008 р. до квітня 2010 р., з невеликим його зниженням у жовтні 2009 р. Це можемо пояснити очікуваннями з боку населенням після виборів узимку та навесні 2010 р. стосовно Президента та народних депутатів України, а також відставкою уряду, очолюваного Ю. Тимошенко. Проте вже з квітня до листопада 2010 р. відбувся спад рівня підтримки, зумовлений низкою внутрішньодержавних подій, пов'язаних насамперед з підписанням 21 квітня в Харкові на рівні перших осіб держав угоди про базування Чорноморського флоту Росії в Севастополі (до 2042 р.) та скасування Конституційним Судом України (1 жовтня) політреформи 2004 р. і переходом України від парламентсько-президентської до президентсько-парламентської форми правління.

Розгляньмо динаміку зміни індексів довіри до інститутів сектору безпеки та оборони України у 2013–2021 рр. (*рис. 11*).

На *рисунку 11* графічно відображені індекси довіри до зазначених інститутів. Візуально за рівнем довіри їх умовно можна звести у дві групи – перша група («оборонна») охоплює ЗСУ, ДСНС, ДПСУ та НГУ, а друга група («правоохоронна») – СБУ та НПУ. Різниця в рівні довіри між максимальними значеннями для другої групи та мінімальними для першої групи в один і той самий час

становить близько 20–30% пунктів. Причина такого розподілу, на нашу думку, полягає в тому, що зазначені структури в межах своїх повноважень і компетенції відповідають за різні напрями роботи. Важливість цих напрямів (або ефективність роботи самих інститутів) населення оцінює по-різному, тому й самі інститути мають різний рівень довіри (рейтинг).

Станом на грудень 2013 р. (*рис. 11*) індекси довіри до ЗСУ, СБУ та міліції мали від'ємні значення (тобто частка тих, хто цим інститутам не довіряє, переважала над тими, хто довіряє). Для ЗСУ ситуація почала змінюватись у 2014 р. – з початком збройної агресії РФ проти України. Станом на грудень 2014 р. суттєво зросла довіра до ЗСУ (з –1,5% до 24,5%), а довіра до НПУ (з –48,3% до –57,8%) і СБУ (з –27,1% до –36,3%) продовжувала зменшуватися.

Заміри липня 2015 р. і листопада 2016 р. свідчать, що довіра до НПУ та СБУ стала зростати (від –56,8% до –38,9% та –34,1% до –18,9% відповідно). Якщо в цей півторарічний часовий проміжок міліція пережила реформу і ребрендинг у НПУ, то із СБУ суттєвих змін не відбулося.

Чергове зростання рівня довіри до ЗСУ відбулось у грудні 2017 р., коли пройшов обмін полоненими, а суттєве падіння рівня довіри до СБУ і НПУ, на нашу думку, спричинене серією вибухів та обстрілів (замах на народного депутата І. Мосійчука, вбивство громадської активістки А. Окуєвої) восени 2017 р.

Довіра до всіх інститутів, що розглядаються, за даними опитування жовтня 2019 р. також зросла. Це, на нашу думку, може бути пов'язане зі зміною влади – виборами Президента України (березень-квітень 2019 р.) та виборами до Верховної Ради (липень 2019 р.).

Проте починаючи з лютого 2020 р. простежується спад рівня довіри до всіх без винятку інститутів сектору безпеки та оборони. На це, на нашу думку, вплинула низка внутрішньодержавних подій, насамперед пов'язаних з епідемічною ситуацією та запровадженням в Україні карантину, а згодом і введенням надзвичайної ситуації через пандемію Covid-19; а на й так низький рівень довіри до СБУ та НПУ суттєво вплинули події, пов'язані із захопленням заручників у центрі Луцька та «ліквідацією терориста» на Мосту метро в Києві влітку 2020 р.

Отже, з урахуванням інформаційного протиборства в публічному просторі різні інститути сектору безпеки та оборони по-різному представлені у ЗМІ – «на слуху» зазвичай ЗСУ (в контексті подій антитерористичної операції та операції Об'єднаних сил (з 30 квітня 2018 р.) на території Луганської та Донецької областей), СБУ та НПУ часто опинялися в центрі резонансних політичних скандалів, тоді як НГУ, ДПСУ і ДСНС менше представлені у ЗМІ. Щодо частоти отримання даних, то у 2005–2010 рр. здійснювалося по три-п'ять опитувань щомісячно, у 2011 р. – жодного і далі намітилася тенденція до збільшення частоти опитувань принаймні для ЗСУ – по одному-два опитування у 2012–2015 рр., тричотири – у 2016–2018 рр., шість опитувань – у 2019 р., вісім – у 2020 р. Це ускладнює аналіз отриманих даних, адже через нерегулярність опитувань інтервали між точковими оцінками мають різі розміри.

Висновок

Проаналізувавши результати досліджень громадської думки в Україні упродовж 2005–2021 рр. щодо рівня підтримки діяльності та довіри суспільства до державних інститутів сектору безпеки та оборони з'ясовано основні причини зміни їхніх рейтингів. До цих причин належать вагомі чи резонансні внутрішньополітичні (очікування громадськістю позитивних змін від парламентських і президентських виборів, розчарування як реакція на низку політичних криз, замахи на життя та вбивство відомих осіб тощо) та зовнішньополітичні (російсько-грузинський збройний конфлікт, анексія Криму, збройна агресія РФ проти нашої держави та ін.) події, що передували проведенню опитувань.

Рівень довіри (як і підтримки діяльності) до інститутів сектору безпеки та оборони доволі різний, що зумовлюється різними функціями, завданнями та напрямами їхньої діяльності у сфері національної безпеки держави. Тому рівень довіри до кожного окремо взятого інституту формується під дією комплексу чинників і відображає ставлення суспільства до нього. Упродовж останніх п'ятнадцяти років найавторитетнішим інститутом сектору безпеки та оборони були ЗСУ – впродовж 2005–2013 рр. рівень підтримки (сумарно повної та часткової) їхньої діяльності становив у середньому 58,3% і досягав максимум 68,7%, а у 2013–2021 рр. рівень довіри до них складав у середньому 59,9% і досягав максимум 74,7%. Інші державні інститути мають дещо нижчі показники.

Установлено, що між інститутами зберігаються тісні взаємозв'язки, певний паритет і ієрархія відносно один до одного та встановлено пряму залежність рівня підтримки/довіри (рейтингу) суспільства до їхньої діяльності. Як виняток, за весь досліджуваний період було лише декілька випадків, коли кардинально відбулося порушення співвідношення паритету довіри до них (довіра до ЗСУ зростала, а до інших інститутів – різко знижувалася).

З викладеного можемо зробити припущення, що допоки триватиме збройна агресія РФ проти України довіра до інститутів сектору безпеки та оборони (за умови їх ефективної діяльності та відсутності прогресу на дипломатичному рівні) залишатиметься на відносно високому рівні. Найімовірніше збережеться й розподіл інститутів на дві групи – умовно «оборонну» (перша група) та умовно «правоохоронну» (друга група). При цьому через зовнішню загрозу довіра до першої групи буде вищою, ніж до другої. Це насамперед може бути пов'язане з тим, що явна зовнішня військова загроза сприймається суспільством більш чітко, ніж внутрішні загрози (які,

до того ж, часто пов'язані з політичною боротьбою окремих партій і політиків).

На нашу думку, зростанню (підтриманню на високому рівні) довіри до інститутів сектору безпеки та оборони з боку суспільства сприятиме їх мінімальне залучення (недопущення залучення) у процеси внутрішньополітичної боротьби, покращення взаємодії між окремими інститутами сектору безпеки та оборони, чітке розмежування на законодавчому рівні повноважень і відповідальності конкретних структур, що працюють у суміжних сферах, об'єктивне висвітлення у ЗМІ їхньої діяльності тощо.

Потребує подальшого вивчення вплив різних чинників (внутрішньо- та зовнішньополітичних тощо) на формування довіри українців до інститутів сектору безпеки та оборони України, виявлення механізмів ефективної комунікації цих інститутів із суспільством тощо.

Перелік літератури

1. *Кузьмук О. І.* Формування та еволюція Воєнної організації (сектору безпеки і оборони) України (1991–2012) : монографія / О. І. Кузьмук. – К. : НУОУ ім. Івана Черняховського, 2013. – 436 с.

2. Про національну безпеку України [Електронний ресурс] : Закон України № 2469-VIII від 21 червня 2018 р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

3. *Фукуяма Ф.* Доверие: социальные добродетели и путь к процветанию / Ф. Фукуяма ; [пер. с англ. Д. Павловой, В. Кирющенко, М. Колопотина]. – М. : АСТ, 2008. – 730 с.

4. *Штомпка П.* Доверие – основа общества / П. Штомпка ; [пер. с пол. Н. В. Морозовой]. – М. : Логос, 2012. – 440 с.

5. *Нападиста В.* Феномен довіри у соціогуманітарному дискурсі сучасної України [Електронний ресурс] / В. Нападиста // Наукові записки Інституту політичних та етнонаціональних досліджень ім. І. Ф. Кураса НАН України. – 2016. – № 1 (81). – С. 207–222. – Режим доступу : https://ipiend.gov.ua/wp-content/uploads/2018/07/napadysta_fenomen.pdf.

6. *Волянська О. В.* Тенденції трансформації довіри до соціальних інститутів [Електронний ресурс] / О. В. Волянська // Вісник Національної юридичної академії України імені Ярослава Мудрого. – (Філософія, філософія права, політологія, соціологія). – 2012. – № 2 (12). – С. 322–328. – Режим доступу : https://dspace.nlu.edu.ua/handle/123456789/1928.

7. *Волянська О. В.* Довіра до публічної влади та чинники, що її зумовлюють у надзвичайних ситуаціях [Електронний ресурс] / О. В. Волянська // Вісник Національного юридичного університету імені Ярослава Мудрого. – (Філософія, філософія права, політологія, соціологія). – 2020. – № 2 (45). – С. 167–180. – Режим доступу : https://doi.org/10.21564/2075-7190.45.200938.

8. *Зеленко Г.* Довіра до суспільно-політичних інститутів в Україні і наслідки її дефіциту для країни [Електронний ресурс] / Г. Зеленко // Studia Politologica Ucraino-Polona. – 2018. – Вип. 8. – С. 108–118. – Режим доступу : http://journals.uran.ua/spup/article/view/164041.

9. *Іжа М.* Довіра до органів публічної влади в контексті досягнення цілей сталого розвитку [Електронний ресурс] / М. Іжа, Т. Пахомова, О. Князєва // Збірник наукових праць НАДУ. – 2020. – Спецвипуск. – С. 97–101. – Режим доступу : https://doi.org/10.36030/2664-3618-2020-si-97-101.

10. *Федорів Т. В.* Довіра як методологічна основа формування репутації органів державної влади [Електронний ресурс] / Т. В. Федорів // Економіка та держава. – 2013. – № 2. – С. 127–130. – Режим доступу : http://www.economy.in.ua/pdf/2_2013/35.pdf.

11. *Чабанна М. В.* Довіра до політичних інститутів: передумови та наслідки для демократії [Електронний ресурс] / М. В. Чабанна // Магістеріум. Політичні студії. – 2014. – Вип. 58. – С. 8–14. – Режим доступу : http://ekmair.ukma.edu.ua/handle/123456789/3287.

12. *Кохан А. І.* Суспільна підтримка влади – основа нової управлінської філософії [Електронний ресурс] / А. І. Кохан // Інвестиції: практика та досвід. – 2013. – № 11. – С. 126–129. – Режим доступу : http://www.investplan.com.ua/pdf/11_2013/33.pdf.

13. *Токарева В. І.* Громадська підтримка як чинник результативності реформ в Україні [Електронний ресурс] / В. І. Токарева, Ю. В. Носачова // Сучасні суспільні проблеми у вимірі соціології управління : матеріали XIII Всеукраїнської науково-практичної конференції, м. Маріуполь, 3 березня 2017 р. – Маріуполь : ДонДУУ, 2017. – С. 143–146. – Режим доступу : http://rp.dsum.edu.ua/handle/123456789/2365.

14. *Кучабський О. Г.* Довіра до органів публічної влади як ключовий фактор ефективності системи державного управління [Електронний ресурс] / О. Г. Кучабський, С. С. Погорєлий // Публічне управління: теорія та практика. – 2013. – Вип. 1. – С. 103–108. – Режим доступу : http://nbuv.gov.ua/UJRN/Pubupr_2013_1_19.

15. *Меркулова Т. В.* Довіра і соціально-економічний розвиток: кластерний аналіз зв'язку показників [Електронний ресурс] / Т. В. Меркулова, Г. С. Богданова // Вісник Харківського національного університету імені В. Н. Каразіна. – (Серія «Економічна»). – 2016. – Вип. 91. – С. 74–79. – Режим доступу : https://periodicals.karazin.ua/economy/article/view/8654.

16. *Амджадін Л.* Довіра до армії та інших силових структур в Україні / Л. Амджадін, О. Гончарук // Українське суспільство 1992–2013. Стан та динаміка змін. Соціологічний моніторинг / за ред. В. Ворони, М. Шульги. – К. : ІС НАНУ, 2013. – С. 341–352.

17. Оцінка діяльності Національної поліції України за допомогою опитування громадської думки (національний звіт, 2018 рік) [Електронний ресурс] / Д. Кобзін, С. Щербань, К. Коренева, А. Черноусов. – Харків : ХІСД, 2019. – 52 с. – Режим доступу : https://t1p.de/yz51.

18. Чи підтримуєте ви діяльність Збройних сил України (динаміка, 2005–2013) [Електронний ресурс] : 01.06.2014 // Internet Archive. – Режим доступу : https://t1p.de/1ze3.

19. Чи підтримуєте ви діяльність Служби безпеки України (динаміка, 2005–2013) [Електронний ресурс] : 31.05.2014 // Internet Archive. – Режим доступу : https://t1p.de/2lay.

20. Чи підтримуєте ви діяльність органів внутрішніх справ, міліції? (динаміка, 2005–2013) [Електронний ресурс] : 31.05.2014 // Internet Archive. – Режим доступу : https://t1p.de/zcvc.

21. Оцінка громадянами ситуації в країні, ставлення до суспільних інститутів, електоральні орієнтації [Електронний ресурс] : 22.11.2016 // Разумков Центр. – Режим доступу : https://is.gd/bLHUT1.

22. Ставлення громадян України до суспільних інститутів, електоральні орієнтації [Електронний ресурс] : 18.05.2017 // Разумков Центр. – Режим доступу : https://is.gd/pWcpdG.

23. Ставлення громадян України до суспільних інститутів, електоральні орієнтації [Електронний ресурс] : 23.10.2017 // Разумков Центр. – Режим доступу : https://is.gd/42a2sM.

24. Довіра громадян України до суспільних інститутів [Електронний ресурс] : 06.07.2018 // Разумков Центр. – Режим доступу : https://is.gd/ZTUU0Z.

25. Рівень довіри до суспільних інститутів та електоральні орієнтації громадян України [Електронний ресурс] : 20.02.2019 // Разумков Центр. – Режим доступу : https://is.gd/5o1Nhz.

26. Рівень довіри до суспільних інститутів та електоральні орієнтації громадян України [Електронний ресурс] : 27.03.2019 // Разумков Центр. – Режим доступу : https://is.gd/E3REdd.

27. Оцінка громадянами ситуації в країні та діяльності влади [Електронний ресурс] : 17.09.2019 // Разумков Центр. – Режим доступу : https://is.gd/mLaJOM.

28. Оцінка громадянами ситуації в країні та діяльності влади, рівень довіри до соціальних інститутів та політиків (соціологія) [Електронний ресурс] : 11.10.2019 // Разумков Центр. – Режим доступу : https://is.gd/c0FF7N.

29. Оцінка громадянами ситуації в країні та діяльності влади, рівень довіри до соціальних інститутів та політиків (соціологія) [Електронний ресурс] : 11.11.2019 // Разумков Центр. – Режим доступу : https://is.gd/UKdF2V.

30. Підсумки-2019: громадська думка (соціологія) [Електронний ресурс] : 10.01.2020 // Разумков Центр. – Режим доступу : https://is.gd/7QBczC.

31. Оцінка громадянами ситуації в країні, рівень довіри до виконавчих та правоохоронних органів влади, оцінка діяльності Уряду (лютий 2020 р., соціологія) [Електронний ресурс] : 21.02.2020 // Разумков Центр. – Режим доступу : https://is.gd/YKOQIf.

32. Початок нового політичного року: довіра до соціальних інститутів (липень 2020 р.) [Електронний ресурс] : 04.09.2020 // Разумков Центр. – Режим доступу : https://is.gd/pvCjWl.

33. Оцінка громадянами ситуації в країні, рівень довіри до соціальних інститутів та політиків, електоральні орієнтації громадян (жовтень–листопад 2020 р.) [Електронний ресурс] : 10.11.2020 // Разумков Центр. – Режим доступу : https://is.gd/9EbeUs.

34. Україна-2020: невиправдані очікування, неочікувані виклики. Підсумки року у дзеркалі громадської думки (грудень 2020 р.) [Електронний ресурс] : 16.12.2020 // Разумков Центр. – Режим доступу : https://is.gd/Vgq8jp.

35. Оцінка ситуації в країні, довіра до інститутів суспільства та політиків, електоральні орієнтації громадян (березень 2021р.) [Електронний ресурс] : 16.03.2021 // Разумков Центр. – Режим доступу : https://is.gd/uIYrYr.

36. Громадська думка: підсумки 2013 року [Електронний ресурс] : 27.12.2013 // Фонд «Демократичні ініціативи» ім. Ілька Кучеріва. – Режим доступу : https://is.gd/EiMIFl.

37. Кому більше довіряють українці: владі, громадськості, ЗМІ?.. [Електронний ресурс] : 03.08.2015 // Фонд «Демократичні ініціативи» ім. Ілька Кучеріва. – Режим доступу : https://is.gd/RTFy6e.

38. Громадська думка, грудень-2017: виборчі рейтинги і рейтинги довіри [Електронний ресурс] : 23.01.2018 // Фонд «Демократичні ініціативи» ім. Ілька Кучеріва. – Режим доступу : https://is.gd/GQnM8z.

39. Довіра українців до соціальних інституцій [Електронний ресурс] : 18.04.2012 // КМІС. – Режим доступу : https://t1p.de/wlo8.

40. Довіра соціальним інститутам, грудень 2018 р. [Електронний ресурс] : 29.01.2019 // КМІС. – Режим доступу : https://t1p.de/q6e7.

41. Моніторинг громадської думки населення України: Червень 2020 [Електронний ресурс] : 23.06.2020 // Центр «Соціальний Моніторинг». – Режим доступу : https://is.gd/0DV7Qh.

42. Думки та погляди населення України: Серпень 2020 [Електронний ресурс] : 21.08.2020 // Центр «Соціальний Моніторинг». – Режим доступу : https://is.gd/MQoE13.

43. Суспільно-політичні настрої населення (3–6 вересня) [Електронний ресурс] : 16.09.2020 // Соціологічна група «Рейтинг». – Режим доступу : https://is.gd/OtPakH.

44. Структури МВС мають позитивний баланс довіри населення – результати дослідження (ІНФОГРАФІКА) [Електронний ресурс] : 05.10.2016 // Internet Archive. – Режим доступу : https://t1p.de/cu6p.

45. Перше коло всеукраїнських опитувань громадян, суддів та правників щодо судової реформи та сприйняття корупції [Електронний ресурс] : 2017 // Програма USAID «Нове правосуддя». – Режим доступу : https://is.gd/G0O9Xb.

46. Результати другого всеукраїнського опитування населення України щодо довіри до судової влади, судової реформи та сприйняття корупції [Електронний ресурс] : жовтень 2018 // Програма USAID «Нове правосуддя». – Режим доступу : https://is.gd/fOmOrR.

47. Українці найбільше довіряють ЗСУ та лікарям – опитування [Електронний ресурс] : 24.04.2020 // Дзеркало тижня. Україна. – Режим доступу : https://t1p.de/wmt8.

DOI 10.33099/2618-1614-2021-15-2-61-65
УДК 355.4

О. М. Загорка,
доктор військових наук, професор, головний науковий співробітник центру воєнно-стратегічних досліджень, Національний університет оборони України імені Івана Черняховського,

С. В. Поліщук,
кандидат військових наук, доцент кафедри радіотехнічних та спеціальних військ, Національний університет оборони України імені Івана Черняховського, полковник,

В. В. Коваль,
кандидат військових наук, старший науковий співробітник, начальник Воєнно-наукового управління, Генеральний штаб Збройних Сил України, полковник,

І. О. Загорка,
старший науковий співробітник центру воєнно-стратегічних досліджень, Національний університету оборони України імені Івана Черняховського

Оцінка впливу загострення воєнно-політичної обстановки на виникнення кризової ситуації: методичний аспект

Для забезпечення воєнної безпеки держави передусім необхідно здійснювати прогнозування розвитку воєнно-політичної обстановки задля своєчасного вжиття заходів з метою запобігання переростанню її в кризову ситуацію. У статті запропоновано методику оцінювання впливу загострення воєнно-політичної обстановки на виникнення кризової ситуації на підставі експертного прогнозування змінювання показників, що характеризують розвиток воєнно-політичної обстановки, за часом.
Порядок застосування методики показаний на прикладі оцінювання впливу загострення воєнно-політичної обстановки на виникнення кризової ситуації з використанням методу таксономії.

Ключові слова: безпека держави, воєнно-політична обстановка, кризова ситуація, метод таксономії, експертне оцінювання.

Постановка проблеми. Воєнна безпека держави забезпечується насамперед об'єктивним оцінюванням воєнно-політичної обстановки (ВПО), яка складається навколо країни, і своєчасним ужиттям заходів з недопущення переходу загострення ВПО в кризову ситуацію та виникнення воєнного конфлікту. Для своєчасного прийняття рішень щодо протидії наростаючій загрозі у воєнній сфері необхідно мати відповідні методичні положення щодо оцінювання впливу загострення ВПО на виникнення кризової ситуації. В умовах ВПО, що склалася навколо України, розробка таких методичних положень є важливим та актуальним науковим і практичним завданням.

Питанням аналізу ВПО, зокрема кризових ситуацій, та оцінювання рівня воєнної небезпеки присвячено чимало праць.

Воєнно-політичний аспект виникнення кризової ситуації розглянутий у праці [1]. При визначенні кризової ситуації здійснюється аналіз загроз, які зумовлюють її виникнення. Однак підходи до оцінювання впливу загроз на виникнення кризової ситуації не розглядаються.

У монографії [2] наведено методику визначення поточного рівня воєнної небезпеки для держави з використанням методу аналізу ієрархій [3]. Для оцінювання рівня воєнної небезпеки запропоновано базову множину показників у політичній, воєнній та інших сферах взаємовідносин між державами, які характеризують ВПО. Наведені показники доцільно врахувати під час визначення кризової ситуації.

Особливості загострення ВПО в умовах гібридної війни розглянуті в монографії [4], що також доцільно врахувати в процесі визначення кризової ситуації.

У праці [5] у загальному вигляді наведено умовну векторну модель ВПО. Зазначено, що головним узагальненим показником ВПО є її напруженість. Запропонована шкала вимірювання дій (намірів) воєнно-політичних сил, яка містить так звані класи ВПО: спокійна, загострена, кризова. Кризовому класу ВПО відповідає рівень напруженості 0,75 і більше. Однак у праці недостатньо повно визначені ознаки (показники) дій (намірів) воєнно-політичних сил, які відповідають класам ВПО.

Методика визначення показника ступеня загострення обстановки в прикордонній сфері з використанням методу таксономії наведена в монографії [6]. Відповідно до призначення методика не пристосована для оцінювання впливу загострення ВПО на виникнення кризової ситуації. Однак її основні положення доцільно використати під час розв'язання цієї задачі.

Таким чином, у розглянутих публікаціях питання впливу ВПО на кризові ситуації досліджувалися недостатньо повно. Тому **метою** статті є розроблення методики оцінювання впливу загострення ВПО на виникнення кризової ситуації.

Виклад основного матеріалу. Під кризовою ситуацією розуміється загрозливий стан розвитку ВПО (переломний момент у розвитку ВПО), який характеризується

Таблиця 1

Показники для оцінювання впливу загострення ВПО на виникнення кризової ситуації (варіант)

№ з/п	Назва показників	Коефіцієнти важливості показників	Прогнозовані значення показників за часовими етапами					Опорні значення показників
			Δt_1	Δt_2	Δt_3	Δt_4	Δt_5	
1	Рівень дипломатичних відносин між державами	0,07	0,90	0,75	0,45	0,30	0,10	0,20
2	Ступінь здійснення політичного тиску на державу	0,04	0,15	0,25	0,40	0,50	0,80	0,85
3	Ступінь втручання у внутрішні справи держави	0,03	0,05	0,15	0,25	0,40	0,60	0,60
4	Рівень підтримки сепаратистських та опозиційних сил	0,05	0,30	0,40	0,55	0,75	0,90	0,90
5	Ступінь дискредитації внутрішньої та зовнішньої політики держави	0,03	0,10	0,30	0,50	0,80	0,90	0,90
6	Ступінь висування територіальних претензій	0,05	0,30	0,40	0,70	0,85	0,90	1,00
7	Ступінь активізації підтримки окремих етнічних груп	0,04	0,10	0,30	0,50	0,70	0,80	0,80
8	Рівень економічних відносин між державами	0,04	0,80	0,70	0,50	0,20	0,10	0
9	Ступінь застосування заходів щодо дестабілізації внутрішньої обстановки	0,03	0,30	0,40	0,50	0,70	0,90	1,00
10	Ступінь виконання міжнародних договорів у сфері безпеки	0,03	0,60	0,45	0,30	0,20	0.10	0
11	Кількість проведених військових навчань поблизу кордону держави	0,07	1	0	1	0	2	2
12	Кількість військових баз, що розгорнуті поблизу кордону держави	0,08	0	1	1	2	3	3
13	Кількість військ, що дислокуються поблизу кордону держави	0,10	40000	50000	60000	80000	90000	90000
14	Рівень оснащення військ наступальною зброєю	0,08	0,30	0,40	0,50	0,65	0,75	0,75
15	Ступінь активізації авіаційної розвідки об'єктів і військ	0,09	0,40	0,50	0,75	0,85	0,90	0,90
16	Ступінь активізації провокацій на кордоні держави	0,05	0,20	0,30	0,60	0,80	0,90	0,95
17	Ступінь активізації шпигунства і проведення диверсій	0,04	0,30	0,35	0,45	0,60	0,80	0,80
18	Рівень підготовки військових аеродромів і військово-морських баз для розв'язання воєнного конфлікту	0,08	0,50	0,60	0,70	0,80	0,90	1,0

таким загостренням відносин між державами, що може призвести до розв'язання воєнного конфлікту.

Воєнно-політична обстановка характеризується множиною показників. Тому задача оцінювання впливу загострення ВПО на виникнення кризової ситуації стає багатокритеріальною. Для її розв'язання необхідно насамперед визначити показники в політичній і воєнній сфері, які характеризують стан відносин між державами, та їх змінювання за часом. Сукупність показників для оцінювання впливу загострення ВПО на виникнення кризової ситуації (варіант) визначена з урахуванням праць [2, 4–6] і наведена в *таблиці 1*.

Прогнозовані значення показників визначаються експертами за етапами (періодами) розвитку ВПО Δt_i ($i = \overline{1,m}$), де m – кількість етапів (періодів). Тривалість етапів

$$\Delta t_i = t_i - t_{i-1} \qquad (1)$$

де t_i, t_{i-1} – час закінчення і початок етапу відповідно.

Опорні значення показників, які відповідають виникненню кризової ситуації, також визначаються експертами.

Для прогнозування ступеня загострення ВПО з урахуванням можливості виникнення кризової ситуації необхідний інтегральний показник, який має враховувати не лише опорні значення часткових показників (*табл. 1*), а також їхню важливість. Сукупність значень показників за етапами розвитку ВПО створюють багатовимірні об'єкти, що дає підстави для оцінювання інтегрального показника застосувати відомий таксономічний метод [7], допрацьований у праці [6]. При використанні методу таксономії порівняння багатовимірних об'єктів звичайно здійснюється з еталонним об'єктом, якому відповідають максимальні значення показників – стимуляторів і мінімальні значення показників – дестимуляторів. У нашому випадку з використанням допрацьованого методу таксономії порівняння здійснюється з об'єктом, якому відповідають опорні значення показників. Для порівняння об'єктів (альтернатив) також використовується так звана таксономічна відстань, яка визначається між точками – показниками в багатомірному просторі за правилами аналітичної геометрії.

Структурна схема методики оцінювання впливу загострення ВПО на виникнення кризової ситуації наведена на *рисунку 1*.

Коефіцієнти важливості (значущості) показників, наведені в *таблиці 1*, визначаються експертами з використанням методу ранжирування [8, 9].

Експерти розташовують показники в порядку їхньої значущості щодо загострення ВПО і приписують кожному показнику числа натурального ряду, які відповідають їхнім рангам.

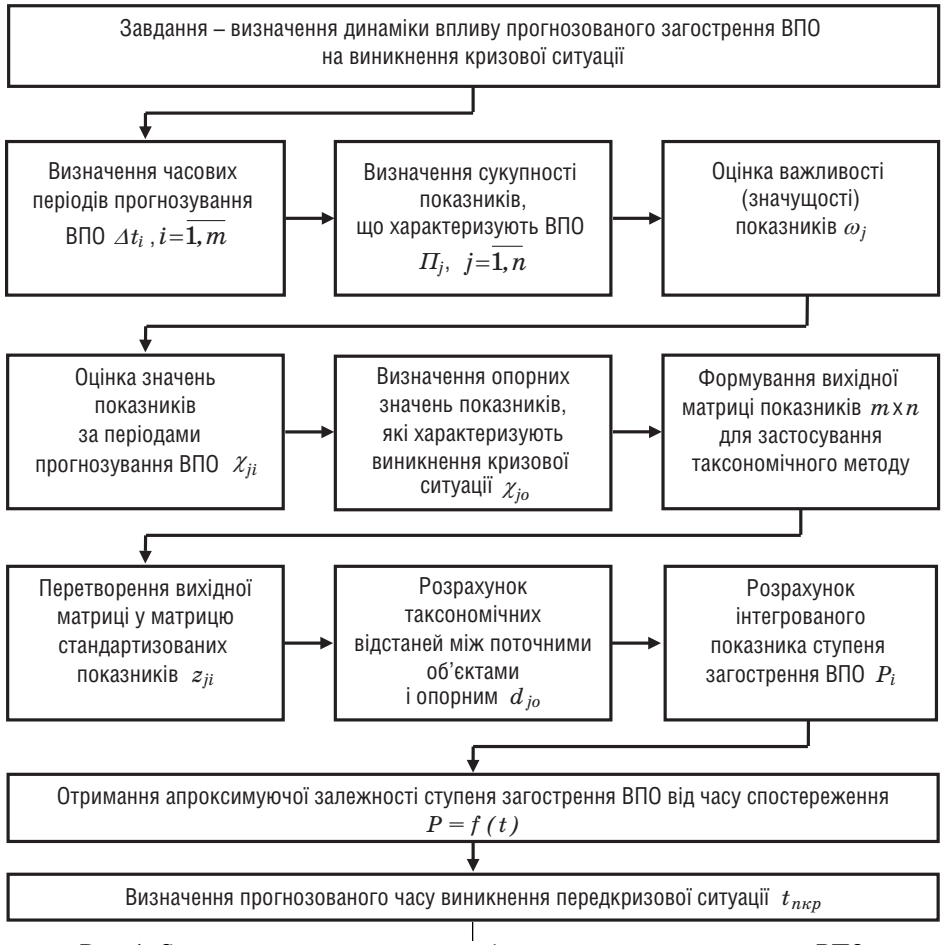


Рис. 1. Структурна схема методики оцінювання впливу загострення ВПО на виникнення кризової ситуації

Коефіцієнти, які характеризують вплив показників на загострення ВПО, визначаються за формулою [8]

$$s_{jk}=1-\frac{r_{jk}-1}{n};\ j=\overline{1,n};\ k=\overline{1,K}, \qquad (2)$$

де n – кількість показників;

K – кількість експертів;

r_{jk} – ранг, що наданий j-му показнику k-м експертом.

Потім коефіцієнти S_{jk} нормуються

$$в_{jk}=\frac{S_{jk}}{\sum\limits_j S_{jk}};\ \sum_j в_{jk}=1. \qquad (3)$$

Якщо компетентність експертів однакова, коефіцієнт важливості j-го показника визначається за формулою

$$\omega_j=\frac{1}{K}\sum_K в_{jk},\ k=\overline{1,K}. \qquad (4)$$

Якщо компетентність k-го експерта оцінюється коефіцієнтом ξ_k, $\sum\limits_k \xi_k = 1$, то

$$\omega_j=\sum_k \xi_k в_{jk}. \qquad (5)$$

Вірогідність експертного оцінювання важливості показників перевіряється з використанням коефіцієнта конкордації [8].

Сукупність значень опорних показників також відповідає багатовимірному об'єкту. Тому вихідна матриця показників для використання методу таксономії формується відповідно до *таблиці 1*, в останньому рядку якої наводяться значення опорних показників.

Під час перетворення вихідної матриці у стандартизовану значення показників розраховуються за формулою

$$z_{ji}=\frac{\chi_{ji}-m_j}{\sigma_j};\ j=\overline{1,n};\ i=\overline{1,m}, \qquad (6)$$

де χ_{ji} – значення j-го показника для i-го періоду (етапу) розвитку ВПО;

$$m_j=\frac{1}{m}\sum_i \chi_{ji};\ \sigma_j=\sqrt{\frac{1}{m}\sum_i\left(\chi_{ji}-m_j\right)^2}. \qquad (7)$$

Таксономічна відстань d_{io} від кожного i-го об'єкта до опорного визначається за формулою [7]

$$d_{io}=\left(\sum_j \omega_j^2\left(Z_{ji}-Z_{jo}\right)^2\right)^{1/2};\ j=\overline{1,n}, \qquad (8)$$

Таблиця 2

Матриця стандартизованих показників

Часові періоди розвитку ВПО, *i*	Показники, *j*																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1,56	–1,31	–1,38	–1,42	–1,57	–1,51	–1,65	1,38	–1,30	1,60	0	–1,51	–1,45	–1,50	–1,61	–1,47	–1,25	–1,46
2	1,04	–0,93	–0,91	–1,00	–0,92	–1,13	–0,89	1,05	–0,91	0,86	–1,22	–0,60	–0,94	–0,92	–1,10	–1,13	–1,00	–0,88
3	0	–0,35	–0,43	–0,36	–0,27	0,03	–0,13	0,39	–0,52	0,12	0	–0,60	–0,43	–0,34	0,17	–0,09	–0,50	–0,29
4	–0,52	0,03	0,28	0,50	0,70	0,61	0,64	–0,61	0,26	–0,37	–1,22	0,30	0,60	0,53	0,68	0,61	0,25	0,29
5	–1,21	1,18	1,22	1,14	1,03	0,80	1,02	–0,94	1,04	–0,86	1,22	1,21	1,11	1,12	0,93	0,95	1,25	0,88
6	–0,87	1,38	1,22	1,14	1,03	1,19	1,02	–1,27	1,43	–1,35	1,22	1,21	1,11	1,12	0,93	1,13	1,25	1,46

де Z_{jo} – стандартизоване значення j-го показника для опорного об'єкта.

Розрахунок ступеня загострення ВПО (таксономічного показника) Pi здійснюється за формулами

$$\begin{aligned} \overline{d_o} &= \frac{1}{m}\sum_i d_{io};\ i=\overline{1,m};\\ \sigma_o &= \left(\frac{1}{m}\sum_i \left(d_{io}-\overline{d_o}\right)^2\right)^{1/2};\\ d_o &= \overline{d_o}+3\sigma_o;\\ P_i &= 1-\frac{d_{io}}{d_o}. \end{aligned} \qquad (9)$$

Для отримання залежності ступеня загострення ВПО від часу $P = f(t)$ доцільно використати відомий метод найменших квадратів. Це дає можливість визначати ступінь загострення ВПО в будь-який час спостереження.

Залежність $P = f(t)$ найбільш просто знаходиться у вигляді багаточлена

$$P = a + вt + ct^2 + dt^3 + \ldots \qquad (10)$$

Визначення коефіцієнтів a, $в$, c, d . . . здійснюється шляхом розв'язання системи алгебраїчних рівнянь:

$$\begin{aligned} &a+в\sum_i t_i + C\sum_i t_i^2 + \ldots = \sum_i P_i;\\ &a\sum_i t_i + в\sum_i t_i^2 + C\sum_i t_i^3 + \ldots = \sum_i t_i P_i;\\ &a\sum_i t_i^2 + в\sum_i t_i^3 + C\sum_i t_i^4 + \ldots = \sum_i t_i^2 P_i;\ i=\overline{1,m};\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \qquad (11)$$

У *таблиці 1*, як приклад, наведені опорні та прогнозовані значення показників розвитку ВПО, отримані експертами. Результати визначення експертами коефіцієнтів важливості показників з використанням методу ранжирування також наведені в *таблиці 1*.

Вихідна матриця показників за періодами (етапами) розвитку ВПО для застосування методу таксономії відповідає *таблиці 1*. Матриця стандартизованих показників наведена в *таблиці 2*.

Таксономічні відстані і ступені загострення ВПО за періодами спостереження, розраховані за формулами (8, 9), наведені в *таблиці 3*.

Таблиця 3

Таксономічні відстані і ступені загострення ВПО

Показники	Часові періоди спостереження за розвитком ВПО, *i*				
	1	2	3	4	5
Таксономічні відстані, d_{io}	0,6499	0,5390	0,3630	0,2455	0,0618
Ступені загострення ВПО, P_i	0,3484	0,4596	0,6360	0,7538	0,9380

У нашому випадку кількість періодів спостереження за розвитком ВПО $m = 5$. Можна прийняти, що тривалість часу періоду спостереження $\Delta t_i = 2$ місяці.

Для знаходження прямолінійної залежності $P = a + вt$ система рівнянь відповідно (11) має вигляд:

$$\begin{aligned} 50a + 30b &= 3{,}14;\\ 30a + 220b &= 21{,}76. \end{aligned} \qquad (12)$$

Після розв'язання системи рівнянь маємо залежність $P = 0{,}19 + 0{,}073t$.

Для знаходження квадратичної залежності $P = a + вt + Ct^2$ складена система рівнянь:

$$\begin{aligned} 50a + 30b + 220C &= 3{,}14;\\ 30a + 220b + 1800C &= 21{,}76;\\ 220a + 1800b + 15664C &= 173{,}69. \end{aligned} \qquad (13)$$

Для розв'язання системи рівнянь використаний метод Гауса та отримана залежність

$$P = 0{,}251 + 0{,}0468t + 0{,}00219t^2. \qquad (14)$$

Отримані залежності ступеня загострення ВПО від часу спостереження наведені на *рисунку 2*.

Апроксимуюча залежність $P = f(t)$ дає можливість визначити прогнозований час виникнення передкризової ситуації $t_{пкр}$, що викликає необхідність своєчасного прийняття рішучих дій з метою стабілізації ВПО. Якщо прийняти, що зона передкризової ситуації починається при ступені загострення ВПО $P = P_{пкр}$, то формули для визначення прогнозованого часу $t_{пкр}$ мають вигляд:

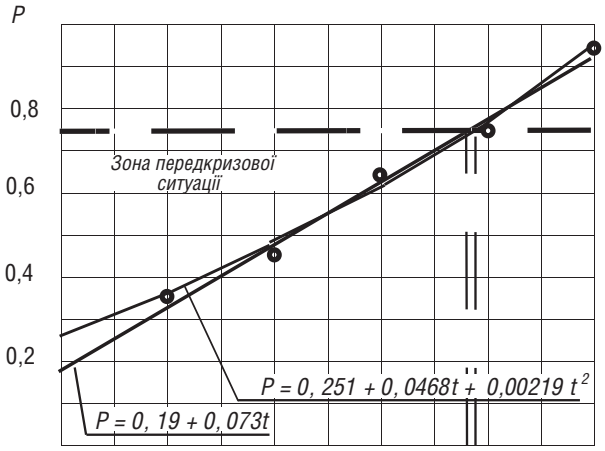


Рис. 2. Залежності ступеня загострення ВПО від часу спостереження

$$t_{ПКР}=\frac{P_{ПКР}-a}{в}\,(лінійна\ залежність);\qquad (15)$$

$$t_{ПКР}=\frac{-в+\sqrt{в^2-4C\,(a-P_{ПКР})}}{2C}\,(квадратична\ залежність).$$

Для прикладу, що розглядається, при $P_{ПКР} = 0{,}75$ (*рис. 2*) $t_{ПКР}$ перебуває в діапазоні 7,67–7,82 місяці.

У *таблиці 4* наведені суми квадратів різниць (Δ) між значеннями ступеней загострення ВПО.

З аналізу *таблиці 4* випливає, що застосування прямолінійної та квадратичної функції для отримання залежності $P = f(t)$ при вихідних даних, що розглядаються, практично рівнозначне. Однак у разі застосування прямолінійної функції зменшується обсяг обчислень.

Таблиця 4

Суми квадратів різниць між значеннями ступенів загострення ВПО

Номер періоду спостереження за розвитком ВПО, *i*	Поточний час спостереження *t*, міс.	Ступінь загострення ВПО, P_i	Прямолінійна залежність		Квадратична залежність	
			P	2	P	2
1	2	0,35	0,336	0,0002	0,35336	0
2	4	0,46	0,482	0,0004	0,47324	0,0002
3	6	0,64	0,628	0,0001	0,61064	0,0008
4	8	0,75	0,774	0,0006	0,76556	0,0002
5	10	0,94	0,92	0,0004	0,938	0
	–	–	–	0,0017	–	0,0012

Запропонована методика, структурна схема якої наведена на *рисунку 1*, дає змогу оцінювати змінювання ступеня загострення ВПО за часом спостереження, визначати прогнозований час переходу загострення ВПО в зону передкризової ситуації.

Методика ґрунтується на прогнозуванні експертами змінювання за часом (періодами) спостереження показників, які характеризують розвиток ВПО, та експертному оцінюванні їхньої важливості. Під час прогнозування експерти повинні враховувати змінювання показників у попередніх періодах розвитку ВПО, тобто до початку прогнозування. Достовірність результатів, а саме визначення змінювання ступеня загострення ВПО, яке отримується з використанням наведеної методики, в основному залежить від достовірності експертних оцінок. Тому важливим є застосування для прогнозування змінювання показників, що характеризують ВПО, ефективних (надійних) експертних методів і залучення для прогнозування підготовлених фахівців. Однак проблема вибору (обґрунтування) методу прогнозування змінювання показників за часом, які характеризують ВПО, потребує проведення окремого дослідження.

Висновки. Запропоновано методику оцінювання впливу загострення ВПО на виникнення кризової ситуації. У методиці за інтегральний показник прийнятий ступінь загострення ВПО, який визначається з використанням методу таксономії. Інтегральний показник розраховується за даними експертного оцінювання прогнозованих значень чинників, які характеризують ВПО у періодах прогнозування. Для визначення ступеня загострення ВПО в будь-який час прогнозування здійснюється його апроксимація багаточленами з використанням методу найменших квадратів.

Порядок застосування методики показаний на прикладі.

Перелік літератури

1. *Омельченко Ю. И.* Методологический аспект оценки кризисных ситуаций / Ю. И. Омельченко, В. А. Милешкевич // Военная мысль. – 1998. – № 3. – С. 56–60.

2. *Богданович В. Ю.* Воєнна безпека України: методологія дослідження та шляхи забезпечення / В. Ю. Богданович. – К. : Дельта, 2002. – 322 с.

3. *Саати Т.* Аналитическое планирование: организация систем / Т. Саати, К. Кернс ; пер. с англ. Р. Г. Вачнадзе. – М. : Радио и связь, 1991. – 224 с.

4. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – Харків : Фоліо, 2017. – 496 с.

5. *Бочарніков В. П.* Системні воєнно-політичні риси сучасного конфлікту на території України : монографія / В. П. Бочарніков, С. В. Свєшніков, Р. І. Тимошенко. – Харків : ХНУПС, 2019. – 206 с.

6. Теоретичні основи інформаційно-аналітичного забезпечення процесів охорони державного кордону (у контексті завдань національної безпеки України в прикордонній сфері) : монографія / В. П. Городнов, М. М. Литвин, Д. В. Іщенко, В. А. Кириленко. – Хмельницький : вид-во НА ДПС України, 2009. – 473 с.

7. *Плюта В.* Сравнительный многомерный анализ в экономическом моделировании / В. Плюта ; пер. с польск. В. В. Иванова. – М. : Финансы и статистика, 1989. – 176 с.

8. *Денисов А. А.* Теория больших систем управления : учебн. пособие для студентов вузов / А. А. Денисов, Д. Н. Колесников. – Л. : Энергоиздат, 1982. – 288 с.

9. *Бешелев С. Д.* Экспертные оценки / С. Д. Бешелев, Ф. Г. Гурвич. – М. : Наука, 1973. – 160 с.

V. M. Telelym, *Doctor of Military Sciences, Professor, Professor at the National Security and Defence Strategy Department, the National Defence University of Ukraine named after Ivan Cherniakhovskyi,*
V. I. Yefimenko, *Senior Lecturer at the National Security and Defence Strategy Department, the National Defence University of Ukraine named after Ivan Cherniakhovskyi,*
P. A. Minieiev, *Leading Researcher at the National Security and Defence Strategy Department, the National Defence University of Ukraine named after Ivan Cherniakhovskyi*

On the development and implementation of the Defence Plan of Ukraine

The article considers some historical aspects of ensuring systemic nature for planning in the field of defence. The problems of defence planning in Ukraine are analysed, in particular, the lack of legal framework for government regulation of strategic planning at both legislative and executive levels, the absence of some important definitions in legislative documents and the presence of incorrect (erroneous) provisions. Ways to improve the system of national strategic planning are proposed. The article also contains suggestions concerning the alignment of planning timeframes with the presidential term of the President of Ukraine, extension of the authority of the Ministry of Defence of Ukraine, and the procedure for approving the documents of the Defence Plan of Ukraine.

Key words: defence planning, defence plan of Ukraine, system of government strategic planning

V. S. Frolov, *Candidate of Military Sciences, Senior Researcher, Leading Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine named after Ivan Cherniakhovskyi,*
V. M. Semenenko, *Candidate of Technical Sciences, Senior Researcher, Deputy Head of the Centre for Military and Strategic Studies, the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Colonel*

Organization of territorial defence of Ukraine under the hybrid war with Russia

Taking into account a possible large-scale invasion of the armed forces of the Russian Federation in Ukraine, the issue of the organization of territorial defence under the hybrid threats is acute. The real essence of the current aggressive policy of Russia is reflected by the four main directions of threats to the national interests of Ukraine as well as the sequence of the main actions of the Russian Federation against Ukraine during the hybrid aggression that described in the article. The organization of the territorial defence system, as a component of the defence system of Ukraine, is an insufficiently studied element of the organization of the defence of Ukraine. The article considers the main problems of the organization of the territorial defence system in Ukraine, foreign experience, possible tasks and a feasible structure of the territorial defence of Ukraine. The relevance of this article is confirmed by the draft Law «On the Fundamentals of National Resistance» submitted by the President of Ukraine to the Verkhovna Rada of Ukraine on May 25, 2021.

Key words: territorial defence, hybrid war, organization of defence of Ukraine, aggression of the Russian Federation.

A. M. Hudz, *Senior Researcher at the Multinational Staff Officers Training and Research Centre, the National Defence University of Ukraine named after Ivan Cherniakhovskyi*

Power politics of the Russian Federation: strategy and tactics of implementation

The article examines the conceptual characteristics and new trends in the power politics of the Russian Federation, strategies and tactics of their implementation. It specifies the dependence of the functioning of international military-political mechanisms and early warning tools on the essence of Russia's military and political activity as well as proposes recommendations concerning the need to develop preventive measures at early stages of the emergence and development of interstate and regional conflicts.

Key words: power politics, international conflict, threats.

M. M. Lobko, *Candidate of Military Sciences, Associate Professor, Leading Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Major General (ret.)*

The joint operation as the main form of repelling armed aggression of the «hybrid» type

The article, based on the analysis of domestic legislation and current trends in the development of ways of armed struggle, examines the issues of the joint operation as the main form of repelling armed aggression of the «hybrid» type. Features of modern military conflicts are revealed. The author presents a brief historical digression on the origin and development of the operation as a form of employment of forces. Features and theoretical foundations of the joint operation are revealed and defined together with the description of Joint Forces that prepare and conduct a joint operation. The author invites researchers, experts and practitioners to express their views on the essence and theoretical foundations of the joint operation, which are discussed in the article.

Key words: forms of employment of forces; military operation; joint operation; defence forces; joint forces; military, non-military, special means of armed struggle.

V. S. Artamoshchenko, *Candidate of Military Sciences, Associate Professor, Doctoral Student at the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Colonel*

A methodological aspect of formation of professional qualification of officers of defence forces on the way of introduction of new levels of military education

In the article, based on the analysis of quantitative indicators of areas of knowledge, specialties and specializations for military training, the content and structure of a prospective catalogue of military officer positions, continuum of professional military education and qualification levels adopted in the armed forces of NATO member states and on the basis of classification of cognitive thinking according to Bloom's taxonomy, a principle of classification of levels of military education in Ukraine is sub-

stantiated. A conceptual model of the framework of qualifications of military education levels is developed. The model is based on the classification of economic activities, classification of professions, requirements of the National Qualifications Framework, prospective content of officer training for new levels of military education, requirements for compliance of military training specialties (specializations) with military ocupations. Qualifications levels have been introduced into the qualifications framework model to assess the performance of professional activities according to NATO standards.

Key words: military education, levels of military education, qualification.

A. D. Biliuha, *PhD Student at the History of War and Military Art Department, the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Lieutenant Colonel*

Cyberweapons: current threats to national security and ways of counteraction

The functioning of modern society is determined by a number of factors, which, in particular, are related to the development of computer technology. With the deepening computerization of society, a qualitatively new field of information exchange has appeared – cyberspace. World experience shows that the protection of cyberspace (cybersecurity) along with the fight against such a negative phenomenon as terrorism has become perhaps the most important problem of mankind.

Cyberweapons have become a powerful tool for conducting illegal actions and fighting in cyberspace. The world's leading countries view cyberweapons as a factor that can potentially influence the course of warfare and cause damage to the economy, disrupt the administrative functions of states, and so on. Given the variety of definitions of cyberweapons, the author proposes his own definition of this type of weapon, presents a historiographical description of cyberweapons, considers the experience of employment of cyberweapons in various fields of human activity. The author provides suggestions for further deepening Ukraine's relations with NATO in the fight against cyberweapons.

Key words: cyberweapons, cyberspace, computer systems, cyber-attacks, national security, cybersecurity, NATO.

I. S. Pecheniuk, *Candidate of Historical Sciences, Senior Researcher, Associate Professor at the History of War and Military Art Department, the National Defence University of Ukraine named after Ivan Cherniakhovskyi,*
S. I. Pecheniuk, *Candidate of Historical Sciences, Leading Researcher at the Applied Sociological Research Department, the Research Centre for Humanitarian Problems of the Armed Forces of Ukraine*

Trends in the ratings of state institutions of the security and defence sector of Ukraine (2005–2021)

The article deals with the analysis and summarized results of public opinion polls conducted in Ukraine during 2005–2021 concerning support and public confidence with regard to the main state institutions of the security and defence sector of Ukraine. The significance of each of them is determined. The reasons and trends in the ratings of the Armed Forces of Ukraine, the Security Service of Ukraine, the militsiya and the National Police of Ukraine and other institutions in the period under study are clarified. The interrelations and interdependence of activities of these institutions are revealed. It is found out the significant increasing of confidence of the Ukrainian society in the institutions responsible for the national security of the state after beginning of the armed aggression of the Russian Federation against Ukraine. Among them, the Armed Forces of Ukraine have been and remain the most authoritative institution for the last fifteen years. The authors conclude that under the conditions of armed conflict and information war the state institutions of the security and defence sector would have a high level of public confidence.

Key words: state institutions, level of public confidence, public opinion, national security, security and defence sector.

O. M. Zahorka, *Doctor of Military Sciences, Professor, Chief Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine named after Ivan Cherniakhovskyi,*
S. V. Polishchuk, *Candidate of Military Sciences, Associate Professor at the Radio Engineering and Special Troops Department, the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Colonel,*
V. V. Koval, *Candidate of Military Sciences, Senior Researcher, Head of the Military Science Directorate, the General Staff of the Armed Forces of Ukraine, Colonel,*
I. O. Zahorka, *Senior Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine named after Ivan Cherniakhovskyi*

Assessment of the impact of the aggravation of the military-political situation on the emergence of a crisis situation: a methodical aspect

To ensure the military security of the state, first of all, it is necessary to forecast the evolution of the military-political situation in order to take timely measures to prevent it from escalating into a crisis situation. The article proposes a technique for assessing the impact of the aggravation of the military-political situation on the emergence of a crisis situation on the basis of expert forecasting of variation of indicators characterizing the evolution of the military-political situation over time.

The procedure for applying the technique is shown on the example of assessing the impact of the aggravation of the military-political situation on the emergence of a crisis situation using the method of taxonomy.

Key words: state security, military-political situation, crisis situation, taxonomy method, expert assessment.