Центральний науково-дослідний інститут
Збройних Сил України
Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.02

Мультидоменна операція – сучасний погляд на адаптацію форм і способів воєнних дій до трансформації середовища викликів та загроз

Олег Семененко
доктор військових наук, професор
заступник начальника Центрального науково-дослідного інституту
Збройних Сил України з наукової роботи
ORCID: 0000-0001-6477-3414
03049, 28В Повітрофлотський проспект, Київ, Україна

Володимир Коваль
кандидат військових наук, старший науковий співробітник,
заступник начальника Генерального штабу Збройних Сил України,
ORCID:0000-0002-6209-6779
03168, 6 Повітрофлотський проспект, Київ, Україна

Водчиць Олександр Григорович
кандидат технічних наук, доцент
начальник кафедри кафедри військової підготовки
Національного авіаційного університету
Медова 1, м.Київ, Україна
ORCID:0000-0002-3294-7632

Добровольський Юзеф Броніславович
кандидат технічних наук, доцент, старший науковий співробітник
заступник начальника кафедри з навчальної роботи кафедри військової підготовки
Національного авіаційного університету
Медова 1, м.Київ, Україна
ORCID:0000-0002-1077-1402

Анотація. Актуальність статті обумовлена тим, що нині Україна стикнулася з проблемою оперативної реакції на гібридні загрози з боку росії, що охоплюють не лише військові аспекти, а й кібербезпеку, інформаційну війну, дезінформацію, невоєнні заходи та інші нетрадиційні методи ведення війни. Одним із сучасних підходів щодо адаптації форм і способів застосування сил оборони (збройних сил) України до умов розвитку кризових ситуацій воєнного характеру можна вважати перехід до планування та проведення мультидоменних операцій, тобто одночасної комбінації дій одразу у декількох просторах (доменах). Сьогодні застосування технології мультидоменних операцій вважається одним зі шляхів ефективної протидії гібридним загрозам з боку противника. Тому головною метою статті є розкриття теоретичної і практичної сутності планування та проведення мультидоменних операцій, а також особливостей їх організації та здійснення. Основними методами досліджень є методи аналізу і синтезу, дедукції та індукції. Основними результатами статті є те, що в ній визначено: ключові особливості ведення воєнних дій в

мультидоменному просторі; основні аспекти планування та проведення мультидоменних операцій; основні заходи з підготовки та реалізації мультидоменних операцій; сучасні особливості трансформації та перспективи адаптації форм і способів ведення воєнних дій Збройними Силами України у мультидоменному просторі. Матеріали статті можуть бути корисними керівникам Збройних Сил України на оперативному та стратегічному рівнях, а також науковцям і дослідникам за напрямами досліджень питань щодо застосування Збройних Сил України та забезпечення воєнної (національної) безпеки держави.

Ключові слова (Keywords): воєнні дії, домен, застосування збройних сил, збройний конфлікт, мультидоменна операція, мультидоменний простір, збройна агресія, гібридна війна, національна безпека, форми і способи ведення воєнних дій, російсько-українська війна, сили оборони держави.

“Технології – єдина зброя, яка може виграти сучасну війну” – Ерік Шмідт

Introduction (Вступ).

Аналіз досліджень і публікацій за тематикою адаптації форм і способів застосування Сил оборони (СО) України до сучасних викликів і загроз світового характеру є ключовим етапом в розробленні стратегій і тактик у сфері національної безпеки. Особливої актуальності тематика адаптації форм і способів застосування СО України до сучасних викликів та загроз набула під час активної фази російсько-української війни, що розпочалася після 24 лютого 2023 року. Збройні Сили (ЗС) й інші складові СО України були змушені шукати шляхи адаптації до нових реалій і вдосконалювати стратегії відповіді на сучасні виклики та загрози [1–11]. У цей період виникла потреба в оперативній реакції на гібридні загрози з боку росії, що охоплюють не лише військові аспекти, а й кібербезпеку, інформаційну війну, дезінформацію, невоєнні заходи та інші нетрадиційні методи ведення війни.

Результати аналізу досвіду війни, що триває в Україні та на Близькому Сході (арабо-ізраїльська війна), показують, що нині дослідження за тематикою адаптації форм і способів застосування СО до ведення сучасних війн має бути чітко сфокусовано на основних аспектах, а саме: оцінюванні ефективності застосування військ (сил) з урахуванням сучасних аспектів використання інноваційних технологій; забезпеченні кібербезпеки; вдосконаленні військової доктрини та стратегічного планування; розвитку міжнародної співпраці щодо протистояння країні-агресору для забезпечення стабільності та безпеки не лише в регіоні, а й у контексті глобального масштабу.

Сьогодні стає зрозумілим, що однією з ключових галузей досліджень є оптимізація стратегій адаптації СО до гібридних загроз, які поєднують військові, інформаційні, кібернетичні, нетрадиційні (нестандартні) та невоєнні аспекти. Важливо також вивчати можливості впровадження інновацій у військові технології й тактику ведення воєнних дій, беручи до уваги сучасні вимоги та реалії геополітичної ситуації. Подальший розвиток досліджень має на меті вдосконалення стратегій підготовки та навчання військових, а також розроблення ефективних механізмів взаємодії з іншими складовими національної безпеки та іншими країнами, союзами, блоками для забезпечення власної безпеки.

Аналіз результатів таких досліджень сприятиме оптимізації використання ресурсів та підвищенню ефективності розвитку системи оборони в умовах сучасних геостратегічних викликів.

Materials and Methods (Матеріали та методи)

Дослідження шляхів адаптації форм і способів застосування СО України до сучасного, трансформованого середовища викликів і загроз (середовища ведення воєнних дій) дозволить виявити основні закономірності та тренди подальшого розвитку оборонної сфери України, розробити стратегії адаптації та вдосконалення збройних сил до змінюваних умов обстановки, а також сприятиме підвищенню ефективності національної безпеки в умовах кризових ситуацій [1–20]. У результаті аналізу з'ясувалось, що ця тематика має велике значення для розвитку військової стратегії, тактики, організації та структури збройних сил (сил оборони), визначення національних безпекових стратегій, а також допомагає визначити ключові аспекти дослідження, а саме:

вивчення історичних прикладів та кейсів адаптації військових стратегій і тактик до кризових ситуацій. Наприклад, аналіз змін у військових стратегіях під час світових воєн, конфліктів "холодної" війни тощо;

дослідження того, як розвиток нових технологій впливає на можливості та методи застосування військової сили, що може передбачати аналіз впливу дронів, кіберзброї та інших інновацій на військову діяльність;

дослідження того, як геополітичні зміни у світі впливають на стратегію й тактику ведення воєнних дій. Адаптація може бути необхідна у зв'язку зі зміною сил і засобів противника, зон впливу та інших факторів;

аналіз впливу суспільного контексту на розвиток військових стратегій. Наприклад, як суспільство реагує на збройні конфлікти та як це впливає на ухвалення рішень військовим керівництвом;

вивчення впливу економічних обмежень на можливості адаптації збройних сил (сил оборони). Фінансові обмеження можуть позначитись на розвитку нових систем озброєння та військової техніки, а також технологій;

дослідження впливу міжнародних відносин та дипломатії на військові стратегії та можливості адаптації тощо.

Адаптація форм і способів застосування СО України до трансформованого середовища викликів і загроз потребує комплексного підходу й ретельного аналізу.

Results (Результати).

Одним із сучасних підходів до адаптації форм і способів застосування СО України до умов розвитку кризових ситуацій воєнного характеру можна вважати перехід до мультидоменних операцій (MDO), тобто одночасної комбінації дій одразу у декількох просторах (доменах). Застосування мультидоменних операцій є шляхом протидії гібридним загрозам з боку противника.

Мультидоменна операція є сучасним поглядом на трансформацію форм і способів ведення воєнних дій, орієнтованим на вирішення комплексних завдань у змінюваному геополітичному середовищі.

Цей підхід враховує важливість інтеграції та синергії між різними сферами військової діяльності, а також інших важливих факторів. До основних аспектів цього сучасного підходу належить [8–20]:

інтегрованість доменів. MDO враховує роль суші, моря, повітря, кіберпростору та космосу як взаємозалежних складових, де дії в одному домені можуть впливати на інші, і навпаки. Інтеграція цих доменів дозволяє створювати більш ефективні та гнучкі стратегії;

використання технологій. MDO активно впроваджує передові технології, такі як штучний інтелект, кіберзахист, автономні системи та інші, для підвищення точності, ефективності та швидкості ведення операцій;

гнучкість та адаптабельність. Сучасні загрози та сценарії конфліктів можуть різко змінюватися, і MDO дає можливість більш швидко та гнучко адаптуватися до нових умов, забезпечуючи ефективну відповідь на різноманітні виклики;

синергія з іншими сферами. Поза військовою діяльністю MDO може взаємодіяти з економічними, політичними та іншими аспектами, сприяючи створенню загальної стратегії для досягнення національних та міжнародних цілей;

управління інформацією та звітність. MDO вимагає високого рівня управління інформацією для ухвалення обґрунтованих стратегічних рішень та забезпечення ефективного контролю за операціями.

Загалом, MDO є сучасним підходом до ведення війни, спрямованим на оптимізацію використання ресурсів, збільшення ефективності та зниження ризиків у високотехнологічному воєнному середовищі.

Мультидоменна операція – це військова стратегія, яка передбачає інтеграцію дій і ресурсів у різних військових та цивільних сферах (доменах) для досягнення комплексного стратегічного ефекту. Домени можуть включати сушу, море, повітря, космос, інформаційні та електромагнітні простори (рис. 1).

Основні мультидоменні простори:

суходіл (Land). Територіальні операції на земельній поверхні, у тому числі на суходолі та узбережжі;

море (Sea). Операції в морському просторі, а також на поверхні та під водою;

повітря (Air). Військові дії у повітряному просторі та в атмосфері;

космос (Space). Використання космічних ресурсів, зокрема супутників, для забезпечення комунікації, розвідки та навігації;

інформаційний (кіберпростір) (Information). Використання інформаційних технологій та мереж для здобуття, оброблення та передавання інформації.

Сучасні мультидоменні операції визначаються високим ступенем інтеграції та співпраці між збройними силами та іншими компонентами суспільства. Інформаційна влада та кіберпростір набули великого значення, адже конфлікти можуть розгортатися не тільки у фізичному, а й у віртуальному просторі.

До основних заходів з підготовки та реалізації мультидоменних операцій належать:

інтеграція та координація шляхом забезпечення ефективної взаємодії між силами та засобами у всіх доменах;

інформаційна домінанта, яка забезпечується використанням інформаційної переваги, включаючи кіберпростір, для контролю та маніпуляції;

технологічна перевага, яка забезпечується завдяки використанню передових технологій у сферах розвідки, зв’язку, автоматизації та зброї;

проведення регулярних тренувань та симуляцій для підвищення рівня підготовки та спроби різних сценаріїв;

створення гнучких командно-контрольних структур для швидкого реагування на зміни в бойовій обстановці тощо.

Мультидоменні операції стають все більш важливим аспектом стратегічного планування, оскільки сучасна військова діяльність є все більш складною та інтегрованою [6, 19]. Сучасні особливості ведення воєнних дій в мультидоменному просторі визначаються широким використанням різних технологій та стратегій, що охоплюють кілька різних доменів.

У табл. 1 наведено кілька ключових особливостей ведення воєнних дій в мультидоменному просторі з їхніми характеристиками.

Таблиця 1 – Ключові особливості ведення воєнних дій в мультидоменному просторі

№	Особливості	Характеристика	Значення для трансформації воєнних дій
1	Інтеграція та взаємодія	Забезпечення ефективної взаємодії та інтеграції різних видів сил, тобто суші, моря, повітря, космосу та інформаційного простору.	Синергія дій у всіх доменах, що дозволяє більш ефективно використовувати різноманітні військові та цивільні ресурси.
2	Цифрова війна та кіберпростір	Ведення конфліктів у кіберпросторі та використання цифрових технологій для ведення війни.	Атаки на інформаційні системи, кібершпигунство, вплив на комунікаційні мережі стають невід'ємною частиною воєнних дій.
3	Масоване використання безпілотників	Широкомасштабне використання безпілотних систем для розвідки, атак та різних завдань в усіх доменах.	Збільшення ефективності, зменшення ризиків для життя, але також виникають нові виклики, такі як небезпека від атак на дрони.
4	Гібридна війна	Використання різноманітних методів, зокрема військових, інформаційних, економічних та політичних, для досягнення стратегічних цілей.	Застосування комбінації традиційних та нетрадиційних методів для отримання переваг.
5	Гіперзвукові засоби та антизбройна протидія	Розвиток гіперзвукових засобів та систем для протидії гіперзвуковим атакам.	Збільшення швидкості та складності озброєнь, а також розвиток засобів протидії цим атакам.
6	Супутникові системи та космічні домени	Використання космічних систем для розвідки, навігації, комунікацій та ведення війни.	Забезпечення геостаціонарної переваги та реакції на виклики у сфері протидії антисупутниковим засобам.
7	Гібридне керування та штучний інтелект	Використання систем штучного інтелекту для ухвалення рішень та автоматизації бойових процесів.	Збільшення швидкості реакції та здатності до адаптації, але із супутніми проблемами у сфері етики та безпеки.

Сучасні особливості трансформації та перспективи адаптації форм і способів ведення воєнних дій ЗС України у мультидоменному просторі



ТРАНСФОРМАЦІЯ ФОРМ ВЕДЕННЯ ДІЙ В МУЛЬТИДОМЕННОМУ СЕРЕДОВИЩІ

- ✓Інтеграція технологій
- ✓Мобільність та експедиційні операції
- ✓Комплексна розвідка та спостереження
- ✓Гібридна війна на суходолі
- ✓Артилерійські та ракетні системи
- ✓Управління запасами та логістика
- ✓Гібридні загрози та протидія
- ✓Тренування та навчання

- ✓Безпілотна авіація та дрони
- ✓Гіперзвукові літальні апарати
- ✓Інтеграція та мережеві операції
- ✓Електронна війна та кіберзахист
- ✓Вертикальні злітно-посадкові засоби та вертольоти
- ✓Літальні апарати здатні до автономного польоту
- ✓Велика кількість даних та аналітика
- ✓Глобальна присутність
- ✓Розвиток гіперзвукової технології

- ✓Міжнародна безпека та захист морських шляхів
- ✓Експедиційні операції та проєкція сили
- ✓ Мультидоменна інтеграція
- ✓Антисубмаринна війна
- ✓Засоби протидії повітряним загрозам
- ✓Морська блискавична війна та гібридна війна в морі
- ✓Екологічна свідомість та інфраструктура
- ✓Глобальна присутність та здатність до доставки гуманітарної допомоги
- ✓Забезпечення повноцінної безпеки морської логістичної інфраструктури

- ✓Кіберзахист та кібербезпека
- ✓Кібервійськові операції та кібератаки
- ✓Інформаційна війна та вплив
- ✓Штучний інтелект у кіберпросторі
- ✓ Кібервійськові сили та кіберкомандування
- ✓Кіберспецоперації та кіберрозвідка
- ✓Кібергібридні загрози
- ✓Міжнародна кіберкоординація та норми

- ✓Космічна розвідка та реакція
- ✓Космічна комунікація та зв'язок
- ✓Космічна оборона та антисупутникові засоби
- ✓Космічні Збройні Сили
- ✓Співпраця в космічному просторі
- ✓Космічні міжконтинентальні засоби удару
- ✓Космічна електронна війна
- ✓Космічна екологічна свідомість

ЗДАТНІСТЬ ІНТЕГРУВАТИ СИЛИ ТА ЗАСОБИ В ЄДИНИЙ МУЛЬТИДОМЕННИЙ ПРОСТІР ІЗ ЗАСТОСУВАННЯМ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ

ВІРТУАЛЬНИЙ ПРОСТІР
- Впровадження технологій штучного інтелекту в усіх доменах.
- Впровадження хмарних мережевих технологій.

ФІЗИЧНИЙ ПРОСТІР
- Розвиток нових технологій кінетичного впливу на нових фізичних принципах.
- Масове впровадження роботизованих систем та засобів ситуаційної обізнаності.

КОГНІТИВНИЙ (ЛЮДСЬКИЙ) ПРОСТІР
- Розвиток технологій впливу на свідомість противника.
- Розроблення нових методів впливу на цільові аудиторії для виконання завдань за призначенням.

Рисунок 1 – Сучасні особливості трансформації та перспективи адаптації форм і способів ведення воєнних дій ЗС України у мультидоменному просторі

Представлені особливості ведення воєнних дій в мультидоменному просторі визначаються стрімким технологічним розвитком та потребою адаптації до сучасних викликів у глобальному військовому середовищі.

Основні аспекти трансформації форм та способів ведення воєнних дій наведено у табл. 2 та на рис. 1. Трансформація форм ведення воєнних дій в домені "Суходіл" містить численні аспекти, які відображають нові вимоги, технологічні та стратегічні зміни в сучасній військовій сфері.

Таблиця 2. Основні аспекти трансформації форм та способів ведення воєнних дій

№	Ключові особливості ведення воєнних дій	Характеристика	Значення для трансформації воєнних дій
		Домен "Суходіл"	
1	Інтеграція технологій	Використання сучасних технологій, таких як штучний інтелект, кіберзахист, високоточна зброя, для підвищення точності та ефективності операцій на суші.	Покращення можливостей розвідки, забезпечення точного та ефективного ведення операцій.
2	Мобільність та експедиційні операції	Розвиток та застосування мобільних військових формувань та концепцій для швидкого реагування на зміни в обстановці.	Здатність швидко пересувати сили та засоби для адаптації до нових загроз та викликів.
3	Комплексна розвідка та спостереження	Використання розвідувальних даних з різних джерел, зокрема дронів, супутникових систем, розвідувальних груп.	Забезпечення повноцінного інформаційного обліку ситуації для ефективного ухвалення рішень.
4	Гібридна війна на суходолі	Застосування різноманітних методів, зокрема інформаційних, економічних, кібер- та військових, для досягнення стратегічних цілей.	Новий рівень складності військових конфліктів, який вимагає гнучкості та адаптації.
5	Артилерійські та ракетні системи	Удосконалення та масове використання артилерійських та ракетних систем для точного ураження цілей на суходолі.	Збільшення дальності та точності ураження цілей.
6	Управління запасами та логістика	Застосування новітніх технологій для ефективного управління запасами, забезпеченням та логістикою.	Підвищення швидкості та ефективності переміщення військових формувань та матеріальних ресурсів.
7	Гібридні загрози та протидія	Заходи для захисту від гібридних загроз, таких як тероризм та гібридні атаки.	Збільшення здатності справлятися з новими формами ворожої діяльності.
8	Тренування та навчання	Застосування сучасних методів тренування та симуляцій для підготовки військових до ведення операцій на суходолі.	Забезпечення високого рівня готовності та адаптивності сил.
		Домен "Повітря"	
1	Безпілотна авіація та дрони	Широке використання безпілотних літальних апаратів (БпЛА) для розвідки, атак та логістичних завдань.	Збільшення розвідувальних можливостей, зменшення ризику для пілотів, нові виклики у сфері кіберзахисту.
2	Гіперзвукові літальні апарати	Використання та розвиток літальних апаратів, які здатні рухатися зі швидкістю, що перевищує швидкість звуку.	Збільшення швидкості та неперевершеної здатності швидко реагувати.
3	Інтеграція та мережеві операції	Взаємодія повітряних сил з іншими доменами та використання мережевих технологій для забезпечення координації та обміну інформацією.	Підвищення ефективності ведення операцій через покращену комунікацію та обмін даними.
4	Електронна війна та кіберзахист	Використання електронної війни для завдань розвідки та підтримки, а також підвищення кіберзахисту повітряних систем.	Забезпечення захисту від електронних атак та забезпечення цілісності систем.

Продовження таблиці 2. Основні аспекти трансформації форм та способів ведення воєнних дій

5	Вертикальні злітно-посадкові засоби та вертольоти	Збільшення використання вертикального зльоту та посадки (VTOL) для підвищення мобільності та ефективності ведення операцій.	Здатність діяти в умовах, де доступ до звичайних аеродромів обмежений чи неможливий.
6	Літальні апарати, здатні до автономного польоту	Розвиток літальних апаратів, здатних до автономного польоту та виконання завдань без прямого керування пілота.	Покращення ефективності та можливостей місій через автономність.
7	Велика кількість даних та аналітика	Використання великої кількості даних та аналітики для ухвалення рішень та розвідки на різних етапах завдань.	Покращення здатності до аналізу та використання розвідувальної інформації.
8	Глобальна присутність	Збільшення здатності до глобальної присутності та оперативного реагування на загрози у будь-якій точці світу.	Забезпечення швидкої реакції на ескалацію конфлікту та загрози безпеці.
9	Розвиток гіперзвукової технології	Використання гіперзвукових технологій для створення та вдосконалення засобів ведення воєнних дій у повітряному просторі.	Підвищення швидкості та ефективності ведення операцій.
Домен “Море”			
1	Міжнародна безпека та захист морських шляхів	Забезпечення безпеки морських шляхів та контроль над територіальними водами для захисту від загроз та ворожого впливу.	Збереження морської свободи та економічних інтересів.
2	Експедиційні операції та проєкція сили	Здатність до швидкого та ефективного проєктування військової сили на великі відстані для вирішення стратегічних завдань.	Гнучкість та здатність реагувати на різні загрози у різних частинах світу.
3	Мультидоменна інтеграція	Взаємодія з повітряним, сухопутним та космічним простором для синергії та забезпечення комплексного ведення операцій.	Покращення координації та ефективності між різними доменами ведення бойових дій.
4	Антисубмаринна війна	Розвиток засобів та стратегій для виявлення та протидії підводним об’єктам.	Забезпечення безпеки морського простору та уникнення підводних загроз.
5	Засоби протидії повітряним загрозам	Розвиток та застосування засобів протидії повітряним атакам для захисту кораблів та інших об’єктів.	Забезпечення безпеки від повітряних загроз та підвищення обороноздатності.
6	Морська блискавична війна та гібридна війна в морі	Використання стратегій гібридної війни у морському середовищі, зокрема асиметричних та нестандартних загроз.	Адаптація до різноманітних загроз та ведення операцій у складному середовищі.
7	Екологічна свідомість та інфраструктура	Здатність до ведення воєнних дій з урахуванням впливу на довкілля та існуючої інфраструктури.	Забезпечення сталого використання морського простору та врахування екологічних аспектів військових операцій.
8	Глобальна присутність та здатність доставляти гуманітарну допомогу	Забезпечення можливості надання гуманітарної допомоги та здатність швидко реагувати на природні катастрофи.	Використання морських сил для підтримки світових гуманітарних завдань.
9	Забезпечення повноцінної безпеки морської логістичної інфраструктури	Заходи для захисту морських баз, портів та логістичної інфраструктури від можливих загроз.	Забезпечення довгострокової операційної здатності через безпечне забезпечення та підтримку.
Домен “Кіберпростір”			
1	Кіберзахист та кібербезпека	Розвиток заходів для захисту критично важливих інфраструктур та інформаційних систем від кібератак.	Забезпечення стійкості та безпеки в інформаційному просторі.
2	Кібервійськові операції та кібератаки	Здійснення операцій у кіберпросторі з метою завдання шкоди, збирання інформації чи перешкоджання роботі супротивника.	Використання кіберзасобів як складової військового конфлікту.

Кінець таблиці 2. Основні аспекти трансформації форм та способів ведення воєнних дій

3	Інформаційна війна та вплив	Використання інформаційних засобів для маніпуляції громадською думкою, впливу на ухвалення рішень та формування образу ворога.	Спрямоване впливання на інформаційне поле для досягнення військових та політичних цілей.
4	Штучний інтелект у кіберпросторі	Використання штучного інтелекту для виявлення та аналізу загроз, автоматизації кіберзахисту та реалізації кібератак.	Покращення швидкості та точності реакції на кіберзагрози.
5	Кібервійськові сили та кіберкомандування	Створення та розвиток спеціалізованих військових підрозділів для ведення операцій у кіберпросторі.	Забезпечення експертної кваліфікації та здатності до ведення кібервійськових операцій.
6	Кіберспецоперації та кіберрозвідка	Застосування кіберзасобів для ведення розвідки, збирання інформації та реалізації спеціальних операцій у кіберпросторі.	Здійснення дій в кіберпросторі з метою здобуття розвідувальної інформації та забезпечення безпеки.
7	Кібергібридні загрози	Комбінація кібератак з іншими видами загроз, такими як інформаційна, гібридна війна та кібертероризм.	Ускладнення ведення війни та збільшення кількості потенційних варіантів загроз.
8	Міжнародна кіберкоординація та норми	Розвиток міжнародних стандартів, норм та договорів для регулювання кібервійськових відносин.	Забезпечення стабільності та контролю в кіберпросторі.
	Підготовка та навчання сил кібероборони	Розвиток програм підготовки та тренувань для забезпечення високої кваліфікації кіберфахівців.	Підготовка військових до ефективного функціонування у кіберпросторі та реагування на кіберзагрози.
	Домен “Космос”		
1	Космічна розвідка та реакція	Застосування супутникових систем для розвідки, навігації та забезпечення точності ведення військових операцій.	Забезпечення високої якості розвідувальної інформації та оперативної реакції на зміни в ситуації.
2	Космічна комунікація та зв’язок	Використання космічних систем для забезпечення безперервного та безпечного зв’язку між військовими частинами.	Забезпечення ефективної комунікації та координації в умовах великих відстаней.
3	Космічна оборона та антисупутникові засоби	Розвиток систем та технологій для захисту від атак на космічні активи та антисупутникових засобів.	Гарантування не перешкоджання нормальному функціонуванню космічних засобів та захист від ворожих утручань.
4	Космічні Збройні Сили	Розроблення та використання військових систем, розташованих у космічному просторі, для здійснення різноманітних завдань.	Забезпечення військової переваги та можливостей ведення операцій на різних рівнях.
5	Співпраця в космічному просторі	Розвиток міжнародної співпраці та стандартів для використання космічного простору в мирних та військових цілях.	Зменшення можливостей конфліктів у космічному просторі та спільна реалізація проєктів.
6	Космічні міжконтинентальні засоби удару	Використання космічних засобів для доставки ударів(здійснення ударів?) на великі відстані між континентами.	Здатність до стратегічного впливу та ведення глобальних операцій.
7	Космічна електронна війна	Застосування електронних впливових засобів у космічному просторі для завдань розвідки та перешкоджання супротивнику.	Забезпечення ефективності ведення електронної війни та контролю над електромагнітним простором.
8	Розвідка та навігація в космічному просторі	Використання супутникових систем для розвідки та навігації з метою підтримки операцій в інших доменах.	Забезпечення точності та надійності інформації для ведення військових операцій.
9	Космічна екологічна свідомість	Розгляд космічного простору з точки зору збереження його сталого функціонування та підтримки екологічної чистоти.	Зменшення впливу військових операцій на космічне середовище.

Розвиток нових технологій та стратегій відбувається в контексті змін у характері загроз, геополітичному середовищі та соціокультурних факторах.

Одним із ключових аспектів трансформації є застосування новітніх технологій, таких

як безпілотні системи, штучний інтелект, кіберзброя та розумні військові системи. Ці технології дозволяють збільшити точність та ефективність ведення операцій, а також зменшити ризики для військового персоналу. Стратегічні зміни полягають у переосмисленні військової доктрини та тактичних підходів до ведення сухопутних операцій. Збільшення акценту на гібридні війни, кібербезпеку, а також реагування на нові форми загроз, такі як тероризм та нестандартні бойові сценарії, стають важливими частинами стратегічного переосмислення. Зокрема, важливою стає інтеграція різноманітних видів військ та засобів ведення воєнних дій для створення більш гнучких та комплексних стратегій. Особливу увагу приділяють розвитку мобільності, комунікаційної системи та інформаційної влади для забезпечення швидкого та координованого реагування на сучасні загрози. Загалом, трансформація ведення воєнних дій на суходолі відображає необхідність впровадження інновацій та адаптації до змін, що відбуваються в сучасному військовому середовищі, для забезпечення національної безпеки та глобальної стабільності.

Трансформація ведення воєнних дій у повітряному просторі відбувається в контексті різноманітних технологічних і стратегічних змін, які визначають нові вимоги та можливості для повітряних сил. У зв'язку з виникненням передових технологій та еволюцією стратегій повітряні сили переосмислюють свою роль, переходячи від традиційних конфліктів до сучасних форм воєнних дій. Технологічні зміни передбачають розвиток нових видів літальних апаратів, використання та розвиток безпілотних (роботизованих) систем та впровадження штучного інтелекту в повітряних операціях. Ці технології сприяють підвищенню точності, маневреності та інтелектуальної здатності повітряних сил.

Стратегічні зміни відображають переосмислення завдань і функцій повітряних сил в сучасному військовому конфлікті. Збільшується акцент на інтеграцію з іншими видами військ, зокрема кібернетичними та космічними силами. Стратегії також передбачають адаптацію до гібридних загроз, таких як кібератаки та некеровані літальні апарати. Ключовими вимогами для повітряних сил стають гнучкість, мобільність та здатність адаптуватися до мінливих умов театру бойових дій. Розвиток систем комунікацій та інформаційних технологій також важливий для забезпечення ефективної координації та зв'язку під час бойових дій. Усе це свідчить про необхідність постійного інноваційного підходу та сучасного визначення ролі повітряних сил у військових стратегіях, зокрема, для забезпечення безпеки та ефективності у сучасних бойових умовах.

Трансформація форм ведення воєнних дій в домені "Море" містить низку ключових аспектів, які відображають сучасні тенденції, технологічний розвиток та стратегічні зміни в морському військовому середовищі. Трансформація ведення воєнних дій у морському просторі відбувається в умовах зміни геостратегічних умов, технологічних інновацій та потреб сучасного безпекового середовища. Одним із ключових аспектів трансформації є розвиток нових технологій у сфері морської війни. Застосування безпілотних суден, атомних та гібридних енергетичних систем, ефективних засобів розвідки та зв'язку робить можливим більш точне ведення операцій та забезпечує перевагу у морському просторі. Важливою є адаптація стратегій до зміни геостратегічних умов. Зростаюча конкуренція за ресурси, розвиток Арктики як нової арени для геостратегічних інтересів, а також вплив кліматичних змін на морські шляхи потребують нових стратегій ведення морських операцій. Умови сучасного безпекового середовища також відображають потребу у забезпеченні морської безпеки, боротьбі з транснаціональними загрозами, такими як піратство та тероризм, та здатності до ефективної взаємодії з іншими видами військ та цивільними структурами. Загалом, трансформація в морській війні визначається необхідністю адаптації до нових викликів і можливостей, що виникають у змінюваному світовому контексті, та розвитком

інноваційних стратегій і технологій для забезпечення морської безпеки й ефективного ведення операцій у цьому важливому домені.

Трансформація ведення війни в домені “Кіберпростір” відбувається у зв’язку зі стрімким розвитком технологій та змінами в характері військових загроз. Трансформація ведення воєнних дій у кіберпросторі визначається швидким технологічним розвитком та появою нових викликів у цій сфері. Здатність до адаптації та інновації стають ключовими факторами для ефективного ведення операцій у цьому просторі. У сучасному світі кіберпростір став важливим полем для ведення військових операцій, оскільки цифрові технології проникли в усі сфери життя. Розвиток штучного інтелекту, кібернетичні атаки та інші аспекти кібербезпеки створюють нові можливості для ведення війни та одночасно ставлять під загрозу національну та міжнародну безпеку. Зміни в характері загроз у кіберпросторі вимагають постійного вдосконалення стратегій та технічних рішень. Зокрема, важливою є здатність країн та військових організацій адаптувати свої підходи до нових технологій та навичок кібервійськових загроз. Інновації у сфері кібербезпеки, вивчення кіберзагроз та навчання військових осіб стають вирішальними компонентами для забезпечення успішного ведення операцій у цьому критичному просторі. З огляду на ці трансформації важливо підтримувати міжнародну співпрацю та розвивати стандарти кібербезпеки, щоб створити об’єднану оборонну лінію проти кіберзагроз та забезпечити стабільність та безпеку в цьому важливому військовому домені.

Трансформація форм ведення військових дій в домені “Космос” відбувається у контексті швидкого розвитку космічних технологій та стратегічних змін у геостратегічному середовищі. Цей процес передбачає не лише технічні аспекти, а й формування нових стратегій і тактик, спрямованих на забезпечення національної безпеки в космічному просторі. З появою нових технологій, таких як супутники, космічна зброя та системи космічної розвідки, роль космосу у військовій сфері стала надзвичайно важливою. Країни активно працюють над розробленням та вдосконаленням засобів космічного ведення бойових дій, щоб забезпечити стратегічну перевагу та контроль у космічному просторі. Водночас, зміни у геостратегічному середовищі вимагають адаптації стратегій ведення війни в космічному просторі. Зростаюча конкуренція між країнами за ресурсами та впливом у космосі робить актуальним розроблення і реалізацію ефективних стратегій, спрямованих на збереження національної безпеки у цьому новому військовому домені. У цьому контексті виникає потреба в міжнародному співробітництві та розробленні міжнародних стандартів регулювання космічної війни з метою запобігання конфліктам та забезпечення стабільності в космосі. Заходи національної та міжнародної політики слід спрямовувати на створення збалансованих та стійких стратегій ведення війни в космічному просторі для збереження миру та стабільності на планетарному рівні. Трансформація ведення військових дій у космічному просторі визначається боротьбою за контроль та використання ресурсів цього домену, а також вирішенням питань міжнародної кооперації та екологічної стійкості.

Російсько-українська війна показала, що нині активно відбувається трансформація сучасних форм і способів ведення воєнних дій у результаті впливу як фактора гібридизації, так і фактора технологічності військового протистояння. До основних видів операцій, які характеризують ведення воєнних дій в російсько-українській війні, належать точкові та масовані дронові удари, масовані та комбіновані безпілотні операції, а також, з метою протистояння дронам – антидронові операції тощо.

Точкові та масовані дронові удари стали важливою складовою стратегій сучасної війни.

Точкові дронові удари – удари, спрямовані на конкретні об’єкти чи цілі на обмеженій площі. Точкові удари намагаються мінімізувати колатеральні збитки та спрямовуються на

визначені, часто стратегічно важливі, об’єкти. Точкові дронові удари потребують точного визначення цілей, великої точності ударів, здатності штучного інтелекту розпізнавати та обирати цілі, а також координації з іншими системами.

Масовані дронові удари – удари, коли багато дронів виконують синхронізовані атаки на великі території чи групи цілей. Метою таких ударів є максимізація впливу і покриття площі території. Масовані дронові удари потребують великої кількості дронів, синхронізації атак, ефективної комунікації та управління групою дронів. Використовують алгоритми розподілу цілей для оптимального покриття території.

До основних заходів з підготовки та здійснення дронових ударів належать:

розвідка та розпізнавання. Необхідно мати надійну розвідку для точного визначення цілей;

технічна підготовка. Забезпечити дрони високою точністю, високою швидкістю та можливістю ухилення від протиповітряних засобів;

комунікація та керування. Забезпечити надійну систему керування та комунікації між дронами та операторами;

захист від засобів протидії. Здійснювати заходи з протидії (антивіруси, системи захисту від електромагнітних засобів тощо).

Важливо відзначити, що використовувати дрони у військових діях слід згідно з міжнародними нормами та правилами, і у зв’язку із цим можуть виникати етичні та гуманітарні питання.

Масована безпілотна операція – координована діяльність великої кількості безпілотних апаратів (дронів) з метою впливу на визначену область чи об’єкти, часто з використанням значної кількості дронів для одночасної атаки чи виконання різних завдань.

Масовані безпілотні операції є сучасним підходом до ведення операцій, який може забезпечити велику гнучкість та ефективність в різних ситуаціях. Урахування етичних, правових та безпекових питань є важливим аспектом під час розроблення та реалізації таких операцій.

Комбінована безпілотна операція – вид військової стратегії, що використовує комбінацію різних типів безпілотних апаратів та їхню взаємодію для досягнення комплексних стратегічних цілей. Ця стратегія передбачає застосування різноманітних дронів з різними функціями та можливостями в єдиній, координованій операції. Комбіновані безпілотні операції використовують різні типи дронів для максимізації ефективності та широкого спектра можливостей у різних сценаріях. Ефективне планування, інтеграція технологій та забезпечення безпеки є ключовими компонентами успішної реалізації таких операцій.

Антидронова операція – військова чи цивільна діяльність, спрямована на виявлення, ідентифікацію, взаємодію або нейтралізацію безпілотних апаратів (дронів), які можуть становити загрозу для безпеки, конфіденційності( ) або порушувати закони і правила. Антидронова операція вимагає комплексного підходу, щоб виявляти та нейтралізувати можливі загрози, які можуть виникнути в результаті використання дронів.

Основні характеристики та заходи з проведення наведених вище видів сучасних операцій у різних доменах представлено у табл. 3.

У сучасному бойовому середовищі ведення війни стає все більш залежним від використання безпілотної авіації, зокрема точкових та масованих дронових ударів, масованих та комбінованих безпілотних операцій і заходів для протистояння дронам (антидронових операцій).

Мультидоменні операції передбачають взаємодію та координацію між різними доменами або сферами діяльності, такими як інформаційна безпека, мережеві комунікації,

оброблення даних, хмарні обчислення та інші. Ось деякі з основних сучасних технологій, що використовуються в системі мультидоменних операцій:

штучний інтелект (AI): AI використовується для автоматизації процесів ухвалення рішень, аналізу великих обсягів даних, прогнозування тощо. У мультидоменних операціях AI може бути застосовано для автоматизації реакції на загрози, виявлення аномалій та покращення загальної ефективності операцій;

Таблиця 3. Основні характеристики та заходи з проведення масованих та комбінованих безпілотних операцій та антидронових операцій

Характеристика	Зміст основних заходів
Масована безпілотна операція	
Масованість	Кількість дронів: масовані безпілотні операції передбачають значну кількість дронів, які можуть бути використані для широкого спектра завдань.
Різноманітні функції	Атаки: відповідно до потреб оператора дрони можуть виконувати атаки з повітря або на землі. Розвідка та розвідувальні завдання: дрони можуть використовуватися для збирання розвідувальної інформації та передавання даних.
Координація і комунікація	Системи керування: є необхідність надійних та забезпечених систем керування для ефективної координації дій великої кількості дронів. Комунікаційні мережі: створення надійних комунікаційних мереж для передавання команд та отримання інформації в режимі реального часу.
Автоматизація і штучний інтелект	Автономія: деякі масовані операції можуть передбачати автономні дрони, які самостійно виконують завдання на основі програмування та аналізу навколишньої обстановки. Штучний інтелект: використання алгоритмів штучного інтелекту для виявлення та аналізу цілей, а також для оптимізації рішень у реальному часі.
Безпека та виклики	Захист від перешкод: розроблення засобів захисту від електромагнітних перешкод та інших загроз для безпілотних систем. Інформаційна безпека: захист від хакерських атак та забезпечення конфіденційності та цілісності даних.
Застосування в різних сферах	Військове використання: масовані безпілотні операції широко застосовуються військовими для здійснення атак, розвідки та інших завдань. Цивільне використання: застосування у цивільних сферах, таких як розвідка природних катастроф, аграрний сектор тощо.
Комбінована безпілотна операція	
Різноманітні дрони	Тактичні апарати: дрони, спроєктовані для атак та розвідки на близьких відстанях. Стратегічні дрони: дрони, здатні діяти на великій відстані та виконувати завдання великого масштабу. Розвідувальні дрони: призначені для збирання інформації та розвідки без втручання в бойовий простір.
Інтеграція та координація	Спільні комунікації: забезпечення ефективного обміну інформацією між різними видами дронів та командними центрами. Системи керування: розроблення єдиної системи керування для координації всієї мережі безпілотних апаратів.
Автоматизація та штучний інтелект	Системи автономії: використання технологій автономії для здійснення незалежних рішень дронами в реальному часі. Штучний інтелект: упровадження алгоритмів штучного інтелекту для аналізу та інтерпретації отриманих даних та автоматизації процесів ухвалення рішень.
Розподіл завдань	Спеціалізація дронів: використання дронів з різними спеціалізованими можливостями для ефективного виконання конкретних завдань. Взаємодія між класами: забезпечення взаємодії та синхронізації роботи різних класів дронів.
Адаптивність та гнучкість	Реагування на зміни: здатність мережі дронів адаптуватися до змін у бойовій обстановці та переключати фокус на найбільш важливі завдання. Резервні механізми: упровадження заходів безпеки та запасних механізмів для уникнення втрат у разі втрати окремих дронів.

Продовження таблиці 3. Основні характеристики та заходи з проведення масованих та комбінованих безпілотних операцій та антидронових операцій

Безпека та етика	Захист від кіберзагроз: забезпечення безпеки мережі та захист від кібератак. Етичні аспекти: урахування етичних принципів у використанні безпілотних систем у військових операціях.
Антидронова операція	
Виявлення та розпізнавання	Використання радарів, сенсорів теплового зображення, оптичних камер і систем виявлення для розпізнавання дронів у повітрі. Урахування різних характеристик дронів, зокрема розміру, швидкості, форми та інших параметрів.
Ідентифікація та класифікація	Використання систем ідентифікації, які можуть визначати тип та модель дронів. Застосування баз даних для класифікації дронів та розпізнавання їхніх виробників.
Взаємодія та перехоплення	Використання сигналів збою для перешкоджання роботі дронів та втраті контролю над ними. Застосування систем перехоплення, таких як радіочастотні або інші методи блокування сигналу дрона.
Фізичне втручання	Використання засобів фізичного втручання для знищення або роботи дронів, наприклад, використання лазерів чи інших енергетичних систем.
Захист від кіберзагроз	Запобігання можливості хакерського втручання та взяття під контроль дронів. Захист від атак на інфраструктуру та системи управління.
Розвідка та контррозвідка	Здійснення постійного моніторингу повітряного простору для виявлення потенційних загроз. Застосування дронів або інших засобів для виявлення та розпізнавання дронів.
Використання технічних засобів	Встановлення антидронових систем, таких як радари, сигнальні блокатори та перехоплювачі. Застосування технічних засобів для виявлення та блокування безпілотних апаратів.
Тренування та навчання персоналу	Підготовка персоналу для ефективної взаємодії та реагування на різні сценарії антидронових операцій. Використання симуляторів та тренувальних майданчиків для навчання.
Легіслятивні заходи	Встановлення правил та обмежень щодо використання дронів у певних зонах або на певній відстані від об’єктів, що потребують захисту.
Координація з аеропортами та повітряним контролем	Співпраця з аеропортами та повітряними службами контролю за безпілотними апаратами для виявлення та усунення можливих загроз.
Забезпечення безпеки	Встановлення систем захисту від кібератак та забезпечення відповідних заходів безпеки для антидронових систем.

блокчейн: блокчейн-технологія забезпечує децентралізовану та надійну систему збереження даних, яка може бути корисною для забезпечення безпеки даних та перевірки ідентичності в мультидоменних операціях;

кібербезпека: технології кібербезпеки, такі як мережеві фаєрволи, системи виявлення втручань (IDS), системи управління доступом (IAM), шифрування даних та багато інших, використовуються для захисту мультидоменних операцій від кібератак;

хмарні обчислення: хмарні сервіси надають можливість зберігати та обробляти дані в різних доменах через віртуальні обчислювальні ресурси, що дозволяє полегшити обмін даними та спільну роботу між різними доменами;

інтернет речей (IoT): IoT пристрої забезпечують збирання та обмін даними між різними об’єктами та системами. У мультидоменних операціях їх можуть використовувати для збирання даних з різних доменів та забезпечення їхнього аналізу та управління;

автоматизація процесів: використання різних інструментів автоматизації, таких як роботи зі штучним інтелектом (Robotic Process Automation, RPA) або автоматизовані системи

управління, дає можливість оптимізувати процеси в мультидоменних операціях та знижувати рівень помилок;

аналітика даних: технології аналізу даних, такі як машинне навчання, обробка природної мови (NLP) та інші, допомагають витягати цінні інсайти з великих обсягів даних, що збираються з різних доменів для підтримки ухвалення рішень в мультидоменних операціях.

Ці технології може бути використано окремо або в поєднанні для створення інтегрованих систем управління та оптимізації мультидоменних операцій.

Дослідження сучасних технологій у системі мультидоменних операцій має велике значення під час конфлікту, такого як російсько-українська війна, з кількох причин:

забезпечення безпеки та обороноздатності: завдяки використанню передових технологій у системі мультидоменних операцій країни мають можливість забезпечити більш ефективний контроль над своїми територіальними інтересами та зменшити ризики військових загроз;

кібербезпека та інформаційна війна: у сучасних конфліктах велику увагу приділяють кібербезпеці та інформаційній війні. Завдяки дослідженню новітніх технологій країни захищають свої інформаційні ресурси та інфраструктуру від кібератак, а також здійснюють власні операції у цій сфері;

ефективне використання ресурсів: завдяки розробленню та впровадженню сучасних технологій управління є можливість оптимізувати використання ресурсів, які можуть бути обмеженими під час конфлікту;

міжнародна співпраця: дослідження сучасних технологій у системі мультидоменних операцій може сприяти співпраці між країнами, які спільно працюють над вирішенням сучасних безпекових викликів;

моральний та етичний аспект: використання передових технологій також потребує обговорення моральних та етичних питань, що можуть виникати в результаті їх впровадження, зокрема, у сфері автоматизації та роботизації військових операцій.

Отже, дослідження сучасних технологій в системі мультидоменних операцій під час російсько-української війни, що триває, є критично важливим для забезпечення національної безпеки, ефективного використання ресурсів та успішного ведення військових операцій.

Discussions (Обговорення).

До основних перспектив трансформації форм та способів ведення воєнних дій у сучасному бойовому середовищі належать:

глибокий, динамічний розвиток технологій: перспективи передбачають постійний розвиток технологій у галузі безпілотної авіації, удосконалення систем штучного інтелекту та збільшення автономії дронів;

інтеграція з іншими технологіями: взаємодія безпілотних систем з кібернетичними та іншими сучасними технологіями для створення високоефективних та складних військових стратегій;

етичні та правові аспекти: виробництво та використання дронів потребує уваги до етичних та правових питань, зокрема тих, що стосуються конфіденційності, безпеки та відповідальності.

Загалом, упровадження безпілотних технологій відкриває нові можливості для ведення військових дій, забезпечуючи більш ефективну та безпечну стратегію порівняно з традиційними методами. Водночас виникають нові виклики, пов’язані із захистом від антидронових загроз, регулюванням використання та розвитком етичних стандартів у військовій сфері.

Conclusion (Висновок).

У контексті російсько-української війни, що триває, дослідження та впровадження сучасних технологій в системі мультидоменних операцій мають велике стратегічне значення. Зважаючи на сучасні виклики у сфері безпеки, зокрема кіберзагрози, гібридні атаки та інформаційну війну, ефективне використання передових технологій стає ключовим аспектом для забезпечення національної безпеки та обороноздатності.

Дослідження у цій сфері допомагають країнам зміцнювати свої оборонні потенціали, покращувати захист важливої інфраструктури, ефективно реагувати на загрози та забезпечувати безпеку своїм громадянам. Крім того, це сприяє міжнародній співпраці та обміну досвідом між країнами у боротьбі з сучасними безпековими викликами.

Загалом, інвестування у дослідження сучасних технологій в системі мультидоменних операцій є критично важливим елементом стратегії забезпечення національної безпеки та успішного ведення військових операцій в умовах сучасного геополітичного середовища.

Recommendations (Рекомендації).

Мультидоменні операції, які охоплюють різні види бойових дій і використовують різноманітні військові та невійськові засоби, стають важливою частиною стратегічного планування в сучасному бойовому середовищі.

Пропонуємо основні рекомендації щодо формування перспектив розвитку таких операцій, враховуючи досвід російсько-української війни та війни Ізраїлю проти Хамасу у 2023 році.

1) Інтеграція різних видів військ. Розвиток та удосконалення систем комунікації та зв’язку між складовими збройних сил, включаючи сухопутну, повітряну, морську та космічну компоненту, що сприятиме більш ефективній координації та спільній роботі між різними галузями військової діяльності.

2) Інформаційна війна та кібернетичні аспекти. Зростаюча роль кібернетичних операцій та інформаційної війни в мультидоменних конфліктах. Налагодження кіберзаходів для впливу на ворожі системи зв’язку, електронні системи та інфраструктуру.

3) Використання безпілотних технологій. Інтенсивний розвиток та застосування безпілотних апаратів у всіх сферах військової діяльності, зокрема розвідці, атаках, транспортуванні та медичній допомозі. Ефективне використання дронів може забезпечити перевагу в бойових діях.

4) Синергія із силами спеціального призначення. Важливість сил спеціального призначення, які можуть виконувати різноманітні завдання в різних областях бойової зони. Оперативна мобільність та гнучкість таких сил роблять їх ключовим компонентом мультидоменних операцій.

5) Застосування технологій гібридної війни та досвід сучасних конфліктів. Урахування гібридних загроз, до яких належать не тільки військові, а й політичні, економічні та інші аспекти. Адаптація стратегій до особливостей гібридної війни та використання досвіду конфліктів для побудови більш комплексних стратегій.

6) Розвиток інновацій в технологіях та зброї. Застосування передових технологій, таких як штучний інтелект, розпізнавання образів та кіберфізичні системи. Удосконалення зброї та екіпірування для забезпечення точності, маневреності та надійності в умовах мультидоменного конфлікту.

7) Урахування геополітичного аспекту і міжнаціональної співпраці. Розвиток стратегій, що враховують геополітичні реалії та можливість міжнаціональної співпраці в мультидоменних операціях. Об’єднання зусиль різних країн може стати ключовим елементом для забезпечення стабільності та протидії загрозам.

8) Розвиток гуманітарних аспектів. Урахування гуманітарних аспектів у плануванні та проведенні операцій. Збалансовані стратегії, які враховують потреби місцевого населення, можуть сприяти збереженню життів та відновленню стабільності після завершення конфлікту.

9) Застосування невійськових методів протистояння. Розвиток та впровадження невійськових методів протистояння, таких як дипломатія, економічний тиск та інші неагресивні стратегії для досягнення мети без ескалації конфлікту.

10) Активне застосування технологій ведення асиметричних війн. Урахування можливостей асиметричних загроз і технік ведення війни. Оптимізація стратегій для ведення боротьби з малочисельними, але технологічно розвиненими противниками.

11) Забезпечення кібербезпеки. Зростаюча увага до кібербезпеки у мультидоменних операціях, враховуючи можливість кібератак на важливі військові та цивільні інфраструктури.

12) Наголос на навчання та підготовку. Розвиток програм навчання та підготовки для військових та цивільних кадрів, спрямованих на розуміння та ефективне використання різноманітних засобів і методів у мультидоменних операціях.

З огляду на зазначені аспекти, мультидоменні операції стають необхідними для ефективного ведення війни в сучасному світі, особливо під час конфліктів, де використовуються різноманітні технології та визначені гнучкі та адаптивні стратегії. Наведені основні аспекти мультидоменних операцій враховують динаміку сучасного бойового середовища та розвиваються відповідно до сучасних викликів і тенденцій у військовій сфері. Мультидоменні операції потребують інтеграції різноманітних засобів та стратегій для досягнення комплексної та ефективної реакції на сучасні загрози.

Acknowledgments (Подяки).

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

Список використаних джерел

1. Donald M. Snider, & Lewis Sorley (2016). *Understanding War: An Annotated Bibliography*. Washington, DC. Strategic Studies Institute, U.S. Army War College. P. 157.
2. Matthew Kroenig (2018). *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters*. Oxford. Oxford University Press. P. 312.
3. Пилипенко, О., & Базар, О. (2015). *Військове мистецтво України: історія та сучасність*. Київ. Критика. С. 256.
4. Sun Tzu. *The Art of War.* (приблизно V століття до н.е). Античний Китай.
5. Carl von Clausewitz. (1832). *On War.* Berlin. Dümmlers.
6. Шуст, В., & Павелко, А. (2018). *Військова стратегія: теорія та практика.* Київ. НУОУ. С. 320.
7. lection Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DMZJ893.
8. Election Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DGP72MH.
9. Menacing Malware Shows the Dangers of Industrial System Sabotage.
10. Горбулін, В. (2017, 3 листопада). Який Фенікс народиться зі згарища світової гібридної війни? *Дзеркало тижня*.
11. Daniel T. Lasica. (2009). *Strategic Implications of Hybrid War: A Theory of Victory.* School of Advanced Military Studies.
12. John, R., & Davis, Jr. Defeating Future Hybrid Threats. *Military Review*, September-

October 267, 2013. 7. *Armed Forces Journal*: *Hybrid vs. compound war (eng.)* (1.10.2009). http://armedforcesjournal.com/hybrid-vscompound-war/
13. Горбач, В. (2017). *Військова стратегія України.* Київ. НУОУ. С. 256.
14. Семененко, О., Водчиць, О., Толок, П., Митченко, С., Гетьман, А., & Тарасов, О. (2023). Основні теоретичні та практичні аспекти ведення проксі-війн та гібридних війн у сучасному глобальному геополітичному та безпековому середовищі: історія, теорія, практика, форми та методи, досвід для України. *Соціальний розвиток і безпека*, *№ 13 (3),* С.1–23. https://doi.org/10.33445/sds.2023.13.3.1
15. Портнов, А. (2017). *Українські війни: від розпаду Радянського Союзу до сучасних конфліктів.* Київ. КМ-Букс. С. 312.
16. Аброськін, І. (2022). *Гібридна війна: загрози та відповіді.* Київ. Якабу Паблішинг. 305 с.
17. Нові технології: зміна характеру нерегулярної війни. *Modern Diplomacy*. https://moderndiplomacy.eu/2020/05/11/emerging-technologies-changing-nature-of-irregular-warfare.
18. Сунгуровський, М., & Гаврилюк, О. (2019). *Військова реформа в Україні: стратегічні виклики та шляхи вирішення*. Київ. Інститут проблем національної безпеки ім. І. Яворницького. С. 160.
19. Семененко, О., Коверга, В., Остапенко, О., Кравченко, Ю., Митченко, С., & Тарасов, О. (2022). Аналіз військових витрат Росії та їх структури в період 2010-2022 рр. (деякі аспекти впливу та наслідків російсько-української війни для України). *Соціальний розвиток і безпека, № 12 (5),* С. 116–129. https://doi.org/10.33445/sds.2022.12.5.11.
20. Семененко, О., Воронченко, І., Москаленко, І., Абрамова, М., & Харитонов, К. (2021). Методологічний підхід до оцінки здатності національної економіки забезпечити достатній рівень обороноздатності. *Соціальний розвиток і безпека, 11(5),* 133–145. https://doi.org/10.33445/sds.2021.11.5.13
21. Соломицький, А., Семененко, О., Онофрійчук, П., Слюсаренко, М., Баранов, С., & Мітченко, С. (2022). Прогнозування ризику збройного конфлікту на основі аналізу військових витрат. *Соціальний розвиток і безпека, 12 (1),* 164–174. https://doi.org/10.33445/sds.2022.12.1.15
22. Семененко, О., Дейнега, О., Воронченко, І., Борисюк, С., Митченко, С., & Таран О. (2021). До питання про трансформацію форм і методів воєнних дій в умовах гібридних війн. *Соціальний розвиток і безпека, 11 (2),* 256–271. https://doi.org/10.33445/sds.2021.11.2.22
23. Wojtowicz, T., & Król, D. (2019). Багатодоменна битва. *Нова доктрина збройних сил США.* Zeszyty naukowe akademii sztuki wojennej. Т. 112, № 3. С. 64–78.
24. Семененко, О., Таран, О., Митченко, С., & Бутенко, Р. (2022). Рекомендації щодо адаптування форм і способів застосування сил оборони України до умов ведення воєнних дій з урахуванням впливу фактору гібридизації. *Збірник наук. пр. ЦНДІ ЗС України*, *2 (101),* 16–31.

References

1. Donald M. Snider, & Lewis Sorley (2016). *Understanding War: An Annotated*

Bibliography. Washington, DC. Strategic Studies Institute, US Army War College. P. 157.

2. Matthew Kroenig (2018). *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters*. Oxford. Oxford University Press. P. 312.
3. Pylypenko, O., & Bazar, O. (2015). *Military art of Ukraine: history and modernity*. Kyiv. Criticism. C. 256.
4. Sun Tzu. *The Art of War*. (approximately V century BC). Ancient China.
5. Carl von Clausewitz. (1832). *On War*. Berlin. Dümmlers.
6. Shust, V., & Pavelko, A. (2018). *Military strategy: theory and practice*. Kyiv. NUOU. P. 320.
7. lesson Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DMZJ893.
8. Election Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DGP72MH.
9. Menacing Malware Shows the Dangers of Industrial System Sabotage.
10. Gorbulin, V. (2017). What kind of Phoenix will be born from the ashes of the global hybrid war? 3d of November. *Mirror of the week*.
11. Daniel T. Lasica. (2009). Strategic Implications of Hybrid War: A Theory of Victory. *School of Advanced Military Studies*.
12. John, R., & Davis, Jr. Defeating Future Hybrid Threats. (2013). *Military Review*, September-October 267. 7. Armed Forces Journal: Hybrid vs. compound war (eng.) (1.10.2009). http://armedforcesjournal.com/hybrid-vscompound-war/
13. Horbach, V. (2017). *Military strategy of Ukraine*. Kyiv. NUDU. P. 256.
14. Semenenko, O., Vodchyts, O., Tolok, P., Mytchenko, S., Hetman, A., & Tarasov, O. (2023). The main theoretical and practical aspects of conducting proxy wars and hybrid wars in the modern global geopolitical and security environment: history, theory, practice, forms and methods, experience for Ukraine. *Social development and security*, No. 13 (3), pp. 1–23. https://doi.org/10.33445/sds.2023.13.3.1
15. Portnov, A. (2017). *Ukrainian wars: from the collapse of the Soviet Union to modern conflicts*. Kyiv. KM-Buks. P. 312.
16. Abroskin, I. (2022). *Hybrid warfare: threats and responses*. Kyiv. Yakabu Publishing. 305 p.
17. New technologies: changing the nature of irregular warfare. (2020). Modern Diplomacy. https://moderndiplomacy.eu/2020/05/11/emerging-technologies-changing-nature-of- irregular-warfare.
18. Sungurovskyi, M., & Gavrilyuk, O. (2019). *Military reform in Ukraine: strategic challenges and solutions*. Kyiv. Institute of National Security Problems named after I. Yavornytskyi. P. 160.
19. Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O. (2022). Russia's military expenditures analysis and their structure in the period 2010-2022 (some aspects of the influence and consequences of the russian-Ukrainian war for Ukraine). *Social development and security*, No. 12 (5), pp. 116–129. https://doi.org/10.33445/sds.2022.12.5.11.
20. Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharitonov, K. (2021). A methodological approach to assessing the ability of the national economy to ensure a sufficient level of defense capability. *Social Development and Security*, 11(5), 133–145. https://doi.org/10.33445/sds.2021.11.5.13
21. Solomytskyi, A., Semenenko, O., Onofriychuk, P., Slyusarenko, M., Baranov, S., &

Mitchenko, S. (2022). Forecasting the risk of armed conflict based on the analysis of military costs. *Social Development and Security*, 12 (1), 164–174.https://doi.org/10.33445/sds.2022.12.1.15

22. Semenenko, O., Deinega, O., Voronchenko, I., Borysyuk, S., Mytchenko, S., & Taran, O. (2021). To the question of the transformation of the forms and methods of military operations in the conditions of hybrid wars. *Social Development and Security*, 11 (2), 256–271.https://doi.org/10.33445/sds.2021.11.2.22
23. Wojtowicz, T., & Król, D. (2019). Multi-domain battle. The new doctrine of the Armed Forces of the United States. *Zeszyty naukove akademii sztuki wojennej*. Vol. 112, No. 3.
P. 64–78.
24. Semenenko, O., Taran, O., Mytchenko, S., & Butenko, R. (2022). Recommendations on the forms and methods of use of the Defense Forces of Ukraine adapting to the conditions of conducting military operations, taking into account the influence of the hybridization factor.

Центральний науково-дослідний інститут
Збройних Сил України
Military Science. Vol. 2 No. 1 (2024)

A multi-domain operation – a modern view at the forms and methods of military operations adapting to the environment of challenges and threats transformation

Oleh Semenenko
doctor of military sciences, professor
Deputy Head of the Central Research Institute

of the Armed Forces of Ukraine for scientific
work 03049, 28B Povitroflotskyi prospect, Kyiv,
Ukraine ORCID: 0000-0001-6477-3414

Volodymyr Koval
candidate of military sciences, senior researcher,

Deputy Chief of the General Staff of the Armed Forces of Ukraine,
03168, 6 Povitroflotskyi Prospect, Kyiv, Ukraine

ORCID: 0000-0002-6209-6779

Oleksandr Vodchyts
candidate of technical sciences,
docent Head of the department

Department of military training National Aviation
University Kyiv, Ukraine

ORCID: 0000-0002-3294-7632

Yuzef Dobrovolskyi
candidate of technical sciences, associate professor, senior
researcher Deputy Head of the Department of Academic Affairs

Department of military training National Aviation
University Kyiv, Ukraine

ORCID: 0000-0002-1077-1402

Abstract. Relevance of the article is due to the fact that Ukraine is currently faced with an operational response to hybrid threats from russia problem of, that include not only military aspects, but cyber security, information warfare, disinformation, non-military measures and other non-traditional methods of warfare also. One of the modern approaches to adopt the forms and methods of Defense Forces (Armed Forces) of Ukraine application of the to the conditions of the development of crisis situations of a military nature the transition to planning and conducting multi-domain operations, i.e. the simultaneous combination of actions in several spaces (domains) at once may be considered. The use of multi-domain operations technology is considered one of the ways to counter the enemy's hybrid threats effectively today. Therefore, the main goal of the article is to reveal the

theoretical and practical essence of planning and conducting multi-domain operations, as well as the peculiarities of their organization and implementation. The main methods of research are methods of analysis and synthesis, deduction and induction. The main results of the article are what is defined in it: key features of a multi-domain space military operations conducting; basic aspects of planning and carrying out multi-domain operations; main measures for the preparation and implementation of multi-domain operations; modern features of the transformation and prospects for adapting the forms and methods of military operations conducting by the Armed Forces of Ukraine in the multi-domain space. The materials of the article can be useful to the leaders of the Armed Forces of Ukraine at the operational and strategic levels, as well as to scientists and researchers in the barnches of research on issues related to the Armed Forces of Ukraine use and ensuring the military (national) security of the State.

Keywords: military operations, domain, use of armed forces, armed conflict, multi-domain operation, multi-domain space, armed aggression, hybrid war, national security, forms and methods of conducting military operations, russian-Ukrainian war, State Defense Forces.