The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.20

Аналіз та оцінювання впливу факторів на вимоги до системи управління оперативного угруповання військ в операціях (бойових діях): досвід російсько-української війни

Роман Войцеховський
ад'юнкт кафедри управління військами інституту
державного військового управління
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

Анотація. Досвід Збройних Сил України з 2022 року засвідчив, що саме здатність системи управління залишатися функціональною в умовах втрат, ізоляції командних пунктів, змін тактичної обстановки та перевантаження інформаційними потоками є ключовою передумовою збереження боєздатності угруповань військ. Успішні приклади децентралізації ухвалення рішень, інтеграції цифрових платформ, використання безпілотних і автономних систем, а також модульної побудови командних структур дозволяють сформулювати нові підходи до формування вимог до системи управління оперативного угруповання військ з урахуванням критерію стійкості. Отже, головною метою статті є проведення аналізу та оцінювання впливу факторів на вимоги системи управління оперативного угруповання військ в операціях (бойових діях) на основі досвіду російсько-української війни.

Основними результатами статті є те, що в ній: визначено основні зовнішні та внутрішні фактори, які впливають на вимоги до системи управління оперативного угруповання військ в операціях (бойових діях), а також проведено оцінювання їхнього впливу методом попарних порівнянь; сформовано рекомендації щодо підвищення стійкості системи управління оперативного угруповання військ; визначено основні показники вимог до живучості пунктів управління. Основними методами досліджень є: аналіз та синтез, а також експертного опитування на основі процедури попарних порівнянь для оцінювання рівня впливу факторів на стійкість системи управління оперативного угруповання військ в операціях (бойових діях). Матеріали статті можуть бути корисними військовим теоретикам та практикам, які займаються розробленням стратегій сучасного ведення війни; аналітикам у сфері безпеки та оборони, які досліджують трансформацію збройних конфліктів; дослідникам у галузі формування філософії війни, військової історії та міжнародних відносин; політикам і військовим керівникам, які формують оборонну політику та військові доктрини.

Ключові слова: автоматизація пунктів управління, бойові дії, вимоги до системи управління військами, воєнні дії, кіберзброя, живучість пунктів управління, операція оперативного угруповання військ, оперативне угруповання військ, оперативність управління, російсько-українська війна, пункти управління, система управління військами (силами), стійкість системи управління військами.

Вступ (Introduction)

Сучасні воєнні конфлікти, зокрема російсько-українська війна, що триває, продемонстрували зростання складності бойового середовища, що зумовлює принципову трансформацію вимог до системи управління оперативного угруповання військ (ОВУ).

В умовах високої динаміки бойових дій, масованого застосування високоточного озброєння, безпілотних систем, РЕБ, кібератак, засобів розвідки і впливу в усіх доменах класичні моделі централізованого управління втрачають ефективність. Це зумовлює необхідність переосмислити підходи до формування вимог до системи управління ОВУ.

Основним критерієм таких вимог стає стійкість системи управління, тобто здатність зберігати ефективність ухвалення рішень, організації командної взаємодії, обміну інформацією та контролю над підрозділами в умовах активного впливу противника та ураження критичних елементів. Фактори, що впливають на цю стійкість, можуть бути як зовнішніми (ворожі дії, електронне подавлення, фізичне ураження), так і внутрішніми (організаційна структура, цифрова зрілість, рівень автоматизації, людський фактор, резервування та адаптивність управління).

Досвід Збройних Сил України (ЗС України) з 2022 року засвідчив, що саме здатність системи управління залишатися функціональною в умовах втрат, ізоляції командних пунктів, змін тактичної обстановки та перевантаження інформаційними потоками є ключовою передумовою збереження боєздатності угруповань військ. Успішні приклади децентралізації ухвалення рішень, інтеграції цифрових платформ, використання безпілотних і автономних систем, а також модульної побудови командних структур дозволяють сформулювати нові підходи до формування вимог до системи управління ОВУ з урахуванням критерію стійкості [1]–[5].

Отже, дослідження взаємозв’язку між впливовими факторами та вимогами до системи управління ОВУ, з урахуванням досвіду сучасної війни, є надзвичайно актуальним як для теоретичного осмислення трансформацій у сфері військового управління, так і для практичного удосконалення командно-штабної діяльності, нормативного регулювання та розвитку автоматизованих систем управління в силах оборони України.

Матеріали та методи (Materials and Methods)

російсько-українська війна засвідчила зміну характеру сучасних операцій, де одним із ключових викликів стало збереження керованості військами в умовах вогневого і інформаційного впливу противника, порушення зв’язку, втрати вузлів управління, знищення командирів або зламу каналів управління. Це потребує переосмислення підходів до організації, побудови і функціонування системи управління на рівні оперативних угруповань, а також ідентифікації факторів, які впливають на її стійкість – як негативних (дестабілізуючих), так і тих, що здатні забезпечити адаптивність, живучість і безперервність управління [3–7].

Урахування бойового досвіду ЗС України, які на практиці реалізували низку інноваційних підходів до управління, децентралізації рішень, резервного зв’язку, розосередження органів управління, а також використання цифрових технологій та безпілотних систем, робить це дослідження вкрай актуальним. Його результати дозволять удосконалити теорію та практику оперативного управління, підвищити боєздатність угруповань військ та стійкість командних структур у майбутніх конфліктах. Отже, дослідження спрямоване на вирішення нагального завдання національної безпеки та оборони України, а також формування нових підходів до побудови стійких систем управління в умовах гібридної, мережецентричної та широкомасштабної війни.

Аналіз публікацій за тематикою статті показує, що сьогодні, у контексті війни нового покоління, а також мережецентричних і гібридних підходів до ведення бойових дій, проблема стійкості систем управління набуває особливої ваги. У сучасній науковій та військово-аналітичній літературі, як вітчизняній, так і закордонній, розглядаються різноманітні аспекти забезпечення цієї стійкості під впливом зовнішніх (ворожих) і внутрішніх (організаційних,

технологічних) факторів. У табл. 1 розкрито результати аналізу деяких джерел за тематикою статті.

Таблиця 1. Результати аналізу досліджень та публікацій за тематикою аналізу та оцінювання впливу факторів на стійкість системи управління військами (силами) оперативного угруповання в операціях (бойових діях)

Джерело та автори	Особливості тематики	Підходи та направленість
Біліченко, С. І., Воронін, О. Г., & Кулик, В. Ю. (2021). Стійкість системи управління військами в умовах збройної боротьби. *Збірник наукових праць ЦНДІ ЗС України.*	Розглядається модель системи управління як цілісної структури із зворотним зв'язком, оцінюються фактори живучості, резервування, адаптивності.	Упровадження багаторівневої адаптації та принципів мережецентричного управління. Обґрунтовано доцільність застосування систем резервного управління. Наголос на необхідності гнучкості структури управління як відповіді на втрати командних пунктів.
Аналітичні матеріали Національного інституту стратегічних досліджень (2022–2024).	Фокус на змінах у системі управління ЗС України внаслідок широкомасштабного вторгнення рф.	Акцент на цифровій трансформації, автоматизації управління, децентралізації ухвалення рішень. Висвітлено застосування вітчизняних цифрових платформ типу "Дельта" в підвищенні оперативності реагування.
NATO STO (Science and Technology Organization) "C2 Agility in the Age of Hybrid Threats". (2020).	Аналізується концепція "agility" (гнучкість) у командно-контрольних структурах НАТО у відповідь на гібридні виклики.	Упровадження багаторівневої моделі реагування в умовах багатовекторного впливу (кібератаки, ІПСО, дезінформація). Пропонується адаптивне управління на базі мультидоменних (MDO) структур.
Command and Control in U.S. Military Operations: A Systematic Review. RAND Corporation. (2021).	Оцінювання ефективності системи С2 США у збройних конфліктах останніх років.	Підкреслено роль штучного інтелекту, автономних систем, а також важливість горизонтальної взаємодії замість вертикального управління. Розглянуто вплив ворожих електронних атак і інформаційних впливів на ухвалення рішень.
Martin van Creveld. (перевид., 2020). *Command in War.*	Класичне дослідження, переосмислене крізь призму сучасних конфліктів.	Акцент на людському чиннику в управлінні та психологічному вимірі втрати керованості. Підкреслюється, що технологічна перевага не гарантує стійкості без належної організації процесів управління.

Аналіз сучасних вітчизняних і зарубіжних публікацій демонструє, що наукове середовище дедалі більше фокусується на дослідженні динамічної стійкості систем управління в умовах складного і нестійкого бойового середовища. Українські джерела акцентують на практичному досвіді стійкості в умовах постійного впливу з боку противника, натомість західні концентруються на системній адаптації командно-контрольних структур до нових форм загроз, включаючи кібер-, РЕБ, інформаційні атаки. У російських дослідженнях наголошується на створенні технократичних, централізованих систем із високим ступенем захищеності та резервування [9–10].

У результаті аналізу літератури виявлено, що загальною тенденцією розвитку системи управління є трансформація від централізованих, вертикальних до гнучких, децентралізованих, цифрових, адаптивних, зі включенням автономних елементів, що забезпечують стійкість у реальному часі. Особливої ваги набуває здатність системи не лише зберігати функціональність під тиском, а й швидко відновлюватися після ураження [11–18]. Актуальність тематики такого дослідження беззаперечна нині, оскільки саме стійкість системи

управління (СУ) визначає ефективність військового реагування, збереження боєздатності оперативних угруповань та загальну спроможність держави до ведення війни в умовах багатофакторної загрози. російсько-українська війна продемонструвала, що боротьба за керованість – це ключовий фронт сучасного збройного протистояння.

Results (Результати)

У сучасних умовах ведення бойових дій ефективність системи управління оперативного угруповання військ визначається не лише її структурними й технічними характеристиками, а передусім її здатністю відповідати змінним і багатовекторним викликам. Формування вимог до такої системи потребує глибокого аналізу зовнішніх та внутрішніх факторів, які безпосередньо впливають на її функціонування, адаптивність і головне – стійкість.

Зовнішні фактори – це ті умови та дії, що виникають поза межами самої системи управління, але суттєво змінюють її контекст функціонування. До них належать дії противника (вогневе ураження, РЕБ, кібератаки), особливості тактичної та оперативної обстановки, характер театру воєнних дій, інтенсивність і темп операцій, рівень інформаційного протиборства. Ці фактори визначають, наскільки система управління має бути живучою, гнучкою, мобільною, прихованою та здатною до швидкого відновлення.

Внутрішні фактори стосуються організації, структури, технічного забезпечення, кадрового складу, рівня автоматизації, функціональної побудови та принципів взаємодії всередині самої системи управління. Саме внутрішні фактори формують базову спроможність системи забезпечувати ефективне планування, ухвалення рішень, доведення команд, обмін інформацією та зворотний контроль у будь-яких умовах. Недосконаліть внутрішніх механізмів або невідповідність сучасним умовам знижує загальну стійкість системи навіть за помірного зовнішнього впливу.

Беручи до уваги досвід російсько-української війни, дослідження цих двох груп факторів дозволяє цілісно визначити реальні, а не лише нормативні вимоги до системи управління ОВУ, з урахуванням характеру сучасного бою. Саме виявлення залежностей між конкретними зовнішніми загрозами й внутрішніми можливостями системи дає підґрунтя для формулювання обґрунтованих вимог, головним критерієм яких є стійкість як здатність забезпечувати безперервність управління навіть в умовах часткової деструкції.

російсько-українська війна, що триває, показує, що до основних зовнішніх факторів, які впливають на вимоги до СУ ОУВ, належать:

- масштаб і характер вогневого впливу з боку противника;
- роль і місце з’єднань (частин) в оперативній побудові військ;
- можливості високоточної зброї щодо ураження елементів СУ;
- можливості засобів радіоелектронної боротьби противника щодо придушення СУ;
- воєнно-економічні можливості країни;
- фізико-географічні та кліматичні умови.

Бойові дії в сучасних умовах характеризуються: зростаючими можливостями технічних засобів розвідки різних видів; різким підвищенням ефективності вогневих засобів ураження противника, включаючи ракетні, артилерійські системи і комплекси, безпілотні комплекси (системи), авіацію, аеромобільні підрозділи; зростанням ролі повітряних ударів і високоточної зброї противника у ході бойових дій, їх динамічністю та напруженістю.

Порівнюючи віддаленість пунктів управління (ПУ), об’єктів ОУВ від переднього краю оборони й можливості сучасних систем розвідки і засобів ураження та радіоелектронного подавлення (РЕП) [11–18], можна сказати, що ураження елементів СУ ОУВ можливе на всю глибину оперативної побудови ОУВ. При цьому особливе значення приділяється розвідувально-ударним комплексам (РУК) та іншим системам високоточної зброї як найбільш

ефективним засобам ураження; для ураження менш захищених елементів ПУ активно використовуються безпілотні комплекси середнього та дальнього радіуса дії.

Радіоелектронне подавлення передбачає вплив на радіоелектронні засоби системи управління військами. На сучасному етапі російсько-української війни характер цього впливу істотно посилився, оскільки суттєво зросла дальність дії засобів розвідки та ураження елементів системи управління (табл. 2).

Аналіз спроможностей провідних країн світу у сферах ведення розвідки, вогневого та радіоелектронного впливу, а також їх порівняння з наявним станом і можливостями пунктів управління ЗС України дає підстави стверджувати [1–18], що:

по-перше, досяжність засобів розвідки зазначених країн дозволяє їм здійснювати комплексну розвідку території України на глибину до 600 км;

по-друге, можливості сучасних засобів вогневого ураження забезпечують здатність завдавати ударів по пунктах управління ЗС України на всій глибині оперативної побудови угруповань військ (сил) — орієнтовно до 600 км;

по-третє, потужність та точність застосування високоточної зброї (ВТЗ) дають змогу ефективно виводити з ладу ключові елементи та компоненти пунктів управління у разі їх виявлення;

по-четверте, час реакції противника від моменту виявлення ПУ до їх вогневого ураження скоротився до 10–30 хвилин;

по-п’яте, інтеграція розвідувально-ударних контурів у провідних арміях світу забезпечує майже безперервний цикл “виявлення–рішення–ураження”, що унеможливлює тривале функціонування виявлених ПУ без ризику їх ураження;

по-шосте, засоби радіоелектронної боротьби противника здатні ефективно подавляти або дезорганізовувати роботу каналів зв’язку та автоматизованих систем управління, що суттєво знижує спроможності ПУ навіть без фізичного знищення;

по-сьоме, активне застосування безпілотних авіаційних та наземних систем у розвідувально-ударних операціях дозволяє противнику здійснювати постійний моніторинг місця розташування пунктів управління та оперативно коригувати вогонь;

по-восьме, автономні або напівавтономні дрони-камікадзе застосовуються не лише проти цілей першої лінії, а й проти командних пунктів тактичного й навіть оперативного рівнів, що вимагає нових підходів до маскування, мобільності та живучості ПУ.

Отже, у сучасних умовах немає суттєвої проблеми ураження пунктів управління та інших елементів системи управління ОУВ; основною проблемою залишається лише швидке і точне виявлення місця їх розташування. Урахування безпілотних систем як одного з ключових засобів розвідки, спостереження та ураження дає змогу об’єктивно оцінити динаміку змін у характері загроз для системи управління військами. У сучасній війні безпілотні платформи перетворюються на один із головних чинників, що визначають вимоги до побудови, мобільності, децентралізації й захищеності ПУ.

Аналіз досліджень за тематикою статті показує, що у разі застосування противником розвідувально-ударних комплексів, масованих нальотів авіації та засобів РЕП повітряного, наземного та морського базування можна очікувати, що вже в перші дні агресії може бути уражено до 30–40 % елементів СУ ОУВ і до 50 % радіоелектронних засобів ПУ подавлено перешкодами. За деякими оцінками, у разі заглушення противником понад 50–60% каналів вузла зв’язку ПУ тривалість циклу управління військами (силами) може зрости більш ніж утричі [9–18]. Стан захищеності рухомих ПУ від вогневого впливу може бути визначено імовірністю їх виживання (Рж), залежно від тривалості роботи на одному місці (рис. 1) [13].

Таблиця 2. Можливості засобів розвідки, ураження і РЕП

Найменування груп засобів	Досяжність (км)
Розвідки	
Розвідувальні групи (такт. рівень)	до 150
Розвідувальні групи (операт. рівень)	до 450
Розвідувально-ударні комплекси	до 600
Розвідувальна авіація	1000 та більше
Повітряна розвідка УКВ-діапазону	до 100
Наземна розвідка УКВ-діапазону	до 30
Наземні пости фото-, інфрачервоної та радіолокаційної розвідки	до 30
Ураження	
Диверсійно-розвідувальні групи	до 150
Диверсійно-розвідувальні групи рейнджерів	до 450
Реактивні системи залпового вогню	до 40
Польова артилерія	до 30
Розвідувально-ударні комплекси	до 500
Оперативно-тактичні ракети	до 120
Ударні безпілотні літальні апарати	до 170
Тактична авіація	300 та більше
Радіоелектронного подавлення	
УКВ-діапазону повітряні	до 150
УКВ-діапазону наземні	до 30
КВ-діапазону повітряні	до 300
КВ-діапазону наземні	до 100

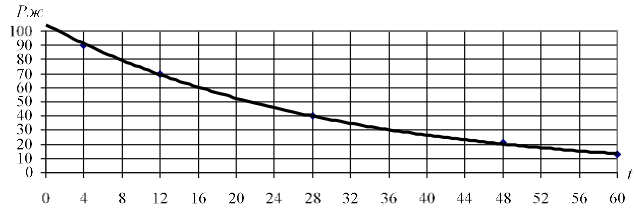


Рисунок 1. Залежність живучості рухомого ПУ від терміну його роботи на одному місці

На графіку видно, що рівень живучості рухомого ПУ, розміщеного в операційній зоні, залишається достатньо високим тільки впродовж перших 8–12 годин роботи. Крім того, можливості щодо живучості ПУ обмежені великими втратами часу на їх згортання та розгортання, необхідністю ешелонованого переміщення тощо.

Однією з вимог підвищення живучості системи ПУ ЗС України є проведення комплексу організаційних та технічних заходів, спрямованих на підвищення їхньої розвідзахищеності (маскування, створення макетів, нанесення радіо- й теплопоглинального покриття, встановлення масок із покриттями, що розсіюють радіохвилі, і тепловідбивальних екранів) (табл. 3).

Аналіз факторів впливу на живучість системи ПУ свідчить про те, що прихованість функціонування системи ПУ залежить від імовірності виявлення противником елементів ПУ і ступеня захищеності циркулюючої по каналах зв'язку інформації. Зниження прихованості функціонування ПУ в сучасних умовах пов'язане, з одного боку, з їх великим насиченням технічними засобами, розміщення і роботу яких необхідно приховати, а з іншого боку – зі зростаючими можливостями засобів розвідки ймовірного противника щодо здійснення розвідки (радіо, радіотехнічної, радіолокаційної, телевізійної, оптико-електронної, гідроакустичної тощо). Наслідками радіоелектронного впливу на лінії, вузли зв'язку ПУ є суттєве скорочення часу проходження інформації між органами управління, а також викривлення або втрата інформації. З огляду на це наразі набув розвитку такий вид інформаційних операцій, як боротьба із системами управління збройних сил. Він передбачає

фізичне знищення систем управління або комунікацій, які з'єднують ПУ з підлеглими військами (силами), з метою порушення безперервності управління.

Таблиця 3. Вимоги до живучості пунктів управління ОУВ

№ з/п	Показники живучості ПУ	Значення показників живучості ПУ за типом					
		Рухомий ПУ (блок, модуль)	Допоміжні ПУ		Повітряні ПУ		ПУ в ППД (приміщення)
			ШМ, СМ на автомоб.	КШМ, СМ на бронебаз	на літаку	на вертольоті	
1	Імовірність збереження за умов впливу уражаючих чинників звичайної зброї і ЗМУ у ході оборонних, контрнаступальних операцій, не менше ніж	0,75	0,78	0,81	0,85	0,67	0,55
2	Імовірність розкриття засобами розвідки у ході оборонних, контрнаступальних операцій, менше ніж	0,37	0,46	0,43	0,57	0,59	0,83
3	Імовірність ураження у ході оборонних, контрнаступальних операцій, не більше ніж	0,53	0,58	0,47	0,73	0,79	0,62
4	Клас захисту від уражаючих чинників від звичайної зброї і ЗМУ	IV	IV	II	–	–	IV
5	Захист від куль і осколків	–	–	+	–	–	+
6	Повітряна ударна хвиля (ПУХ): – надлишковий тиск у фронті повітряної ударної хвилі не менше, кг/см^2; – тиск проникаючої повітряної ударної хвилі у робочих відсіках не більше, кг/см^2; – час спрацювання системи захисту від ПУХ, с	 0,3 0,1 0,1	 0,3 0,1 0,1	 1 0,1 0,1	 – – –	 – – –	 0,3 0,1 0,1
7	Проникаюча радіація від вибуху нейтронного боєприпасу – кратність послаблення сумарної дози проникаючої радіації на робочих місцях бойової обслуги, одиниць, не менше ніж	2	2	4	–	–	2
8	Випромінювання радіоактивної ураженої місцевості – кратність послаблення дози гамма-випромінювання на робочих місцях, одиниць, не менше ніж	3	3	6	–	–	3
9	Світлове випромінювання ядерного вибуху: – імпульс опромінювання за захисними пристроями має бути, кал/см^2, не більше; – час спрацювання захисних пристроїв, с, не більше ніж; – час максимуму опромінення, с, не більше ніж	 4 2·10-4 0,56	 4 2·10-4 0,56	 4 2·10-4 0,2	 – – –	 – – –	 4 2·10-4 0,56
10	Електромагнітний імпульс наземного ядерного вибуху та його нормативних параметрів: – вертикальна складова напруги електричного поля, кВ·м-1, не менше ніж; – горизонтальна складова електричного поля, кВ·м-1, не менше ніж; – напруга магнітного поля, А·м-1	 40 0,5 30	 40 0,5 30	 60 2,6 270	 – – –	 – – –	 40 0,5 30
11	Отруйні речовини, бактеріальні аерозолі, радіоактивний пил – надлишковий тиск повітря в населених відсіках за номінальної продуктивності загальнообмінно-колекторних або загальнообмінних ФВУ, мм. вод. ст., не менше	25	25	50	–	–	25

Кібератаки, спрямовані проти державних та військових інформаційно-телекомунікаційних систем і мереж разом з управлінням викраденими даними роблять цей вид протиборства надзвичайно ефективним.

Для захисту від радіоелектронного впливу ПУ поряд із традиційними організаційними заходами (зміни робочих частот, каналів зв'язку та місць розгортання) необхідно

використовувати ефективні технологічні способи паролювання інформації; імітозахищені коди, що виявляють і виправляють помилки, а також протистоять нав'язуванню обманної й застарілої інформації; апаратуру підвищення імітостійкості й вірогідності інформації; апаратуру засекречування інформації гарантійної стійкості; одночасне передавання того самого повідомлення по різних каналах зв'язку або в незалежних напрямках; спеціальні заходи для нейтралізації акустичних, віброакустичних, гідроакустичних та електроакустичних каналів просочення інформації; оптико-волоконні лінії зв'язку в межах ПУ.

Природно-географічний фактор – комплекс природних умов, характерних для конкретного театру воєнних дій, країн, стратегічних та операційних напрямків, які впливають на підготовку та проведення воєнних дій. Особливістю його є незалежність впливу на СУ від діяльності та волі людини. Його елементами є: географічне положення, рельєф, гідрографія, ґрунти, рослинність, клімат тощо.

У сучасних умовах економічний фактор відіграє ключову роль у створенні обороноздатності держави. Саме він визначає відповідність економічних можливостей держави поставленим військовим цілям.

Зовнішні фактори, що впливають на СУ ОУВ, пред'являють певні вимоги до мобільності, які можна забезпечити шляхом створення рухомих ПУ на автомобільній та бронетанковій базі. Оснащеність ПУ має відповідати вимогам щодо мобільності, автономності, захищеності. Розміщуючи ПУ ОУВ, необхідно враховувати вплив розглянутих факторів.

Проаналізуємо вплив внутрішніх факторів на вимоги до системи управління оперативного угруповання військ. До основних внутрішніх факторів, які впливають на вимоги до СУ ОУВ, належать:

- склад і можливості своїх військ;
- укомплектованість і рівень підготовленості органів управління (ОУ) до виконання завдань, які покладаються на СУ;
- організація управління, форми і методи роботи ОУ;
- ступінь прихованості й маневреність ПУ;
- ступінь забезпеченості засобів зв'язку і автоматизації (ЗЗіА).

Для обґрунтування пріоритетності різних факторів, що впливають на вимоги до системи управління ОВУ, було застосовано метод аналізу ієрархій Сааті. Цей підхід дозволяє шляхом попарного порівняння кількісно оцінити відносну важливість як зовнішніх, так і внутрішніх факторів, які визначають ефективність функціонування системи управління.

Результати попарного оцінювання подано у вигляді рейтингів, що відображають вагомість кожного фактора у відповідній групі. Рейтинги зовнішніх та внутрішніх факторів наведено у табл. 4 та на рис. 2.

Найвпливовішим зовнішнім фактором є масштаб і характер вогневого впливу, що безпосередньо впливає на необхідність підвищення живучості, мобільності та резервування СУ. Серед внутрішніх факторів домінує склад і можливості своїх військ, оскільки саме бойовий потенціал визначає обсяг, складність і швидкість управлінських рішень.

Зовнішні фактори загалом мають більший вплив (60%) на формування вимог до системи управління, особливо в умовах війни високої інтенсивності, як у випадку з російсько-українською війною.

Під час розроблення, модернізації чи трансформації системи управління ОВУ першочергову увагу слід приділяти адаптації до зовнішніх загроз, з урахуванням обмежень і потенціалу внутрішніх ресурсів.

Таблиця 4. Рейтинги зовнішніх факторів впливу на вимоги до системи управління ОВУ

Зовнішні фактори		Внутрішні фактори	
Фактор	**Рейтинг (вага)**	**Фактор**	**Рейтинг (вага)**
Масштаб і характер вогневого впливу з боку противника	**0.4481**	**Склад і можливості своїх військ**	**0.4185**
Роль і місце з'єднань (частин) в оперативній побудові військ	**0.2205**	**Укомплектованість і рівень підготовленості органів управління (ОУ)**	**0.2625**
Можливості засобів РЕБ противника щодо придушення СУ	**0.1427**	**Організація управління, форми і методи роботи ОУ**	**0.1599**
Можливості високоточної зброї щодо ураження елементів СУ	**0.0909**	**Ступінь прихованості й маневреність пунктів управління**	**0.0973**
Фізико-географічні, кліматичні умови	**0.0584**	**Ступінь забезпеченості засобами зв'язку і автоматизації**	**0.0618**
Воєнно-економічні можливості країни	**0.0394**		

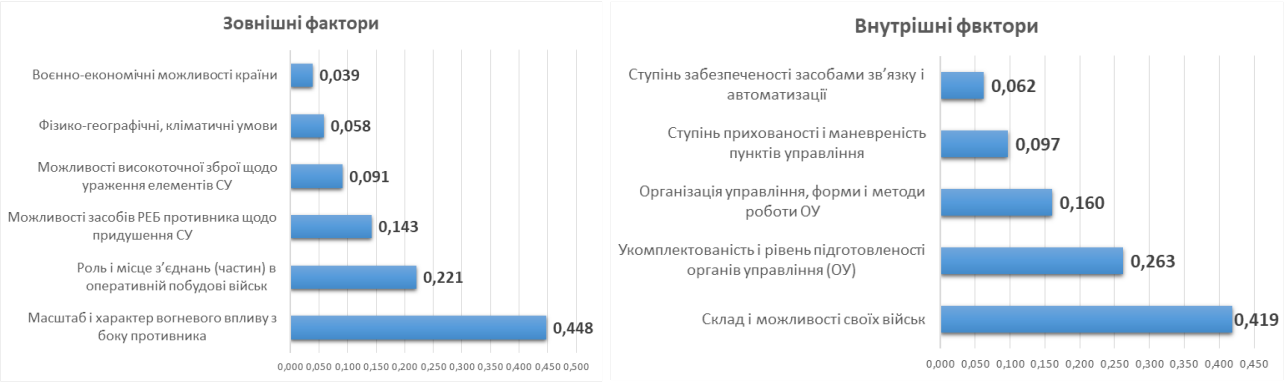


Рисунок 2. Ілюстрація результатів оцінювання зовнішніх та внутрішніх факторів, що впливають на вимоги до системи управління оперативного угруповання військ

Рекомендації (Recommendations)

Для розміщення оперативного складу та забезпечення його ефективної роботи з управління військами у ході підготовки та ведення операцій (бойових дій) створюється система ПУ, яка є сукупністю ПУ всіх ланок управління, розгорнутих за єдиним замислом, що структурно, функціонально, технічно й інформаційно взаємопов'язані між собою для забезпечення ефективної роботи постійно діючих та тимчасово створених органів управління. Кожний ПУ є сукупністю робочих місць, розташованих у захищених спорудах, будівлях або на рухомих засобах, та призначений для роботи оперативного складу ОУ. На функціонування СУ ОУВ безпосередньо впливає стан, у якому можуть знаходитися елементи СУ: ОУ, ПУ, ЗЗіА ОУВ. Вплив внутрішніх факторів призводить до змін стану елементів та СУ в цілому. При цьому під станом мають на увазі певні числові характеристики процесу їхнього функціонування в заданих умовах, такі, наприклад, як кількість працездатних або непрацездатних ПУ, можливості засобів зв'язку та автоматизації щодо вирішення покладених на них завдань (збирання, оброблення, аналізування необхідної інформації тощо в певний момент часу).

Під час планування та здійснення управління ОУ ОУВ виконують покладені на них завдання в операції ОУВ. Важливим фактором під час виконання цих завдань є рівень укомплектованості та підготовленості ОУ до виконання завдань, які покладаються на СУ ОУВ. Досягнення відповідного рівня підготовки є результатом сукупності індивідуальних

знань, умінь, навичок – з одного боку, та сукупністю навичок колективних дій – з іншого. Цю сукупність можна відобразити кількістю дій, прийомів та типових завдань у процесі підготовки. Підготовленість технічного складу ПУ необхідно враховувати шляхом оцінювання його злагодженості та натренованості у виконанні заходів розгортання та згортання елементів рухомих ПУ, зокрема робочих місць (апаратних) керівного та оперативного складу, проведення заходів маскування, інженерного обладнання районів розгортання ПУ, розгортання вузлів зв'язку та прокладання ліній зв'язку, інформаційної синхронізації баз даних для розв'язання задач на робочих місцях оперативним складом з використанням комплексів засобів автоматизації, організації захисту, охорони та оборони ПУ, створення хибних ПУ, вузлів зв'язку та імітації їхньої життєдіяльності.

Керівними документами встановлено, що орган управління вважається готовим до виконання завдань, коли він укомплектований особовим складом за посадовим призначенням не менше як на 70%. Це дає можливість встановити, що рівень укомплектованості ОВУ на початок ведення операцій (бойових дій) має бути понад 70%.

Злагодженість функціонування, єдність форм і методів роботи структурних підрозділів та посадових осіб ОВУ залежать від рівня їхньої особистої професійної підготовки, раціонального розподілу завдань та оперативного складу між центрами (групами) ПУ, відпрацьованості типових (формалізованих) алгоритмів їхнього функціонування за шатними ситуаціями, інструкцій з організації роботи центрів (груп) ПУ, технологічної можливості сумісної роботи технічних засобів зв'язку та інформаційно-аналітичного забезпечення роботи ОВУ.

Форма роботи ОВУ – обраний порядок взаємовідносин, інформаційного забезпечення ОВУ та їхніх структурних підрозділів, розподілу робіт між виконавцями. Залежно від рівня підготовки ОВУ, умов обстановки, отриманих завдань, їхнього обсягу, послідовності та часу виконання формами роботи ОВУ можуть бути: індивідуальна; у складі функціональних груп; дистанційна (у тому числі у формі відеоконференцій); комбінована (змішана).

Метод роботи ОВУ є сукупністю правил, прийомів та способів виконання поставлених завдань під час підготовки і в процесі ведення операцій (бойових дій). Залежно від рівня підготовки ОВУ, умов обстановки, отриманих завдань, їхнього обсягу, послідовності та часу виконання методами роботи ОВУ можуть бути: послідовний, паралельний, комбінований.

Відповідно до вимог щодо забезпечення ергономічних умов [17] для роботи посадових осіб ОВУ, як показує досвід ведення бойових дій, а також результати досліджень на заходах оперативної підготовки, оперативна місткість основного командного пункту (ОКП) має забезпечувати розміщення близько 220 осіб основного та постійного оперативного складу. Оперативна місткість стаціонарних ПУ визначається насамперед можливостями споруд, що мають спеціальний фортифікаційний захист для забезпечення необхідного рівня живучості.

Для своєчасного та якісного виконання завдань управління робота оперативного складу на ПУ організовується зазвичай у три зміни – основна зміна, зміна підсилення та зміна, яка відпочиває (кожна по 30%). З урахуванням цього, оперативна місткість ОКП має передбачати необхідну кількість автоматизованих робочих місць (АРМ) для основної чергової зміни, яка працює разом з командувачем, місць у складі структурних підрозділів ОКП для зміни підсилення, яка надає їй практичну допомогу в оперативній роботі, та місць для відпочинку третьої зміни. При цьому необхідно дотримуватися ергономічних вимог, що регламентують організацію робочих місць, взаємне розташування засобів відображення інформації, органів управління і засобів зв'язку в межах робочого місця.

Приміщення ОКП, де розгортаються автоматичні робочі місця (АРМ) та місця відпочинку, мають бути обладнані системами електроживлення, вентиляції та опалення для підтримання необхідного температурного режиму й відносної вологості повітря. Крім того, на ОКП слід передбачити місця для розміщення засобів індивідуальної спеціальної обробки, засобів пожежогасіння, засобів надання першої медичної допомоги, індивідуального дозиметричного контролю випромінювання.

Якщо не врахувати вплив фактора ергономічних умов на ПУ, це може призвести до неможливості забезпечення ефективного функціонування системи ОВУ.

На діяльність ОВУ має суттєвий вплив фактор готовності (повнота відпрацювання) документів щодо управління військами. Зазначені документи можуть мати текстову або графічну форму. Нині форми директивних документів (наказів, розпоряджень) недостатньо формалізовані та часто дублюються за змістом. Це призводить до зниження якості та оперативності виконання завдань управління військами (силами). У зв'язку із цим, обґрунтований перелік документів та їхня форма для організації спільної роботи різних суб'єктів сектору безпеки і оборони України набувають особливого значення.

Важливе значення має оснащеність ПУ сучасними системами зв'язку, автоматизації, у тому числі інформаційно-аналітичним забезпеченням.

Засоби зв'язку та автоматизації мають забезпечувати оперативному складу ПУ умови для своєчасного збирання й аналізування інформації для ухвалення відповідних рішень, доведення їх до виконавців і отримання результатів. Водночас, досвід [4], [8] свідчить про таке:

– у системі зв'язку здебільшого використовується застаріла аналогова елементна база, несумісна з телекомунікаційними мережами України та сучасними засобами автоматизації управління (75% засобів зв'язку ІВФ переведені на цифрову елементну базу). Якість зв'язку (особливо в польових мережах), пропускна здатність каналів, захищеність ліній та їхня стійкість щодо впливу засобів радіоелектронної боротьби є недостатніми;

– сертифікованих засобів захисту інформації, у тому числі й криптографічних, немає;

– терміни готовності частин, у яких знаходиться польова (рухома) база ПУ оперативних командувань, не забезпечують в особливий період ефективне функціонування системи управління;

– в ОВУ немає дієвих важелів впливу на підготовку засобів зв'язку, автоматизації управління та обслуги вузла зв'язку ТПУ;

– технічні засоби засекреченого зв'язку ЗС України несумісні з аналогічними технічними засобами ІВФ.

На цей час, за результатами аналізу досвіду розвитку систем управління військами (силами) провідних країн світу, основні тенденції в цій галузі спрямовуються на автоматизацію діяльності посадових осіб ОВУ – як ключовий напрям підвищення оперативності та обґрунтованості ухвалення рішення командувачем щодо обстановки, що склалася.

Серед основних факторів впливу на автоматизацію діяльності посадових осіб ОВУ та процеси управління військами (силами) доцільно визначити три:

– рівень технічного забезпечення посадових осіб ОВУ;

– рівень інформаційного забезпечення посадових осіб ОВУ;

– рівень аналітичного (спеціального математичного та програмного) забезпечення посадових осіб ОВУ.

Водночас, необхідно зазначити, що другий та третій фактор впливу безпосередньо взаємопов'язані та окремо не можуть використовуватися, однак з метою більшої деталізації аналізу розглянемо їх окремо.

Зокрема, під технічним забезпеченням посадових осіб ОВУ мають на увазі сукупність технічних засобів (комплексів засобів), які функціонально призначені для забезпечення збирання, оброблення, зберігання, відображення, обміну інформацією між посадовими особами ОВУ.

Оснащення ними робочих місць посадових осіб безпосередньо впливає на оперативність управління військами (силами) за рахунок скорочення часу виконання управлінських завдань.

Під інформаційним забезпеченням посадових осіб ОВУ мають на увазі наявність необхідного систематизованого, класифікованого, кодифікованого достовірного та повного інформаційного ресурсу, з яким працюють посадові особи ОВУ і на підставі якого оперативно

обґрунтовується рішення командувача. Важливу роль в процесі обміну інформаційним ресурсом та його актуалізації відіграє досконала система уніфікованих документів, яка безпосередньо впливає на оперативність відпрацювання документів з планування операцій (бойових дій).

У зазначеному контексті варто відзначити, що повноцінне інформаційне забезпечення ОВУ можна вважати створеним лише після систематизації інформаційних ресурсів ЗС України та держави, їхньої класифікації, кодування, створення відповідних баз (банків) даних для їх зберігання, чого наразі немає.

Під аналітичним (спеціальним математичним та програмним) забезпеченням посадових осіб ОВУ мають на увазі сукупність інформаційних, інформаційно-розрахункових задач, їхніх комплексів та моделей операцій (бойових дій). За своїм функціональним призначенням аналітичне забезпечення безпосередньо впливає як на оперативність планування операцій (бойових дій), так і на ступінь обґрунтованості рішення командувачем за обстановкою, що склалася.

Перелік інформаційних, інформаційно-розрахункових задач, їхніх комплексів та моделей операцій (бойових дій) для всіх ОВУ не може бути сталим. Він має містити певну сукупність задач та моделей, які притаманні будь-якому ОВУ, а решта – має відповідати його конкретному функціональному призначенню. Крім того, оснащеність ОВУ сучасними системами автоматизації, в тому числі інформаційно-аналітичним забезпеченням, впливає на чисельність його структурних підрозділів.

Висновок (Conclusion)

Сучасна війна, зокрема російсько-українська, підтвердила принципову зміну характеру загроз для системи управління військами: вона дедалі більше стає об’єктом високоточного, багатоаспектного і багатоджерельного впливу – від кінетичних засобів ураження до радіоелектронних і кіберзасобів. Найбільш критичним зовнішнім фактором є масштаб і характер вогневого впливу противника, який безпосередньо визначає потребу у високій мобільності, маневреності та захищеності пунктів управління. Це саме стосується і впровадження нових принципів просторової організації командних структур. Зростання досяжності засобів розвідки, розширення можливостей високоточної зброї та скорочення циклу “виявлення–ураження” призвели до фактичного зникнення “глибини безпеки” навіть для командних пунктів оперативного рівня.

Активне застосування безпілотних систем як для виявлення, так і для ураження ПУ робить традиційні підходи до побудови системи управління застарілими. Це вимагає впровадження децентралізованих, мережецентричних, багаторівневих рішень із резервуванням управління.

Проблема ураження пунктів управління сьогодні не технічна, а розвідувальна: у разі виявлення об’єкта — його знищення є майже гарантованим. Тому вимоги до системи управління мають ґрунтуватися на принципах скритності, постійної зміни місцеположення, швидкого згортання / розгортання та використання цифрових автономних засобів.

Провідні країни світу вже реалізують інтеграцію розвідувально-ударних контурів, у тому числі з використанням БпЛА, що дозволяє їм вести безперервне полювання на командні центри супротивника. Україні необхідно враховувати цей досвід для випереджального розвитку власних систем СУ.

Результати попарного оцінювання методом Сааті засвідчили перевагу зовнішніх факторів у формуванні вимог до СУ ОУВ, при цьому внутрішні фактори також залишаються критично важливими для реалізації необхідних змін.

Отже, стійкість системи управління ОУВ у сучасній війні має розглядатися як головна вимога до її побудови, і саме від здатності до адаптації, самовідновлення, децентралізації та цифрової трансформації залежатиме боєздатність угруповань ЗС України в умовах високотехнологічного протистояння.

Подяки (Acknowledgments)
Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

Використані джерела

1. Біліченко, С. І., Воронін, О. Г., & Кулик, В. Ю. (2021). Стійкість системи управління військами в умовах збройної боротьби. *Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України*, *3* (84), 34–42.
2. *Трансформація системи управління Збройними Силами України в умовах повномасштабної війни: аналітична записка*. (2023). Національний інститут стратегічних досліджень. https://niss.gov.ua
3. Застосування цифрових рішень у системі управління силами оборони: виклики війни та перспективи розвитку. Інститут проблем національної безпеки. (2023). *Науковий вісник ІПНБ*, *2*, 45–53.
4. Пархоменко, М. С., & Чорний, П. П. (2023). Удосконалення структури управління угрупованнями військ в умовах інтенсивного вогневого впливу противника. *Воєнна думка*, *7*, 22–30.
5. Кузьменко, С. М. (2023). Децентралізація управління як фактор підвищення стійкості системи управління військами в умовах гібридної війни. *Збірник наукових праць Харківського національного університету Повітряних Сил*, *4* (74), 85–92.
6. NATO Science and Technology Organization. (2020). *Command and control agility in the age of hybrid threats* (STO-TR-HFM-260). NATO.
7. Peltz, J. L., Paul, L., & Johnson, B. (Ред.). (2021). *Command and control in U.S. military operations: A systematic review*. RAND Corporation. https://doi.org/10.7249/RRA394-1
8. Van Creveld, M. (2020). *Command in war*. Harvard University Press.
9. Управление войсками в условиях современных операций: от автоматизации до цифрового суверенитета. (2022). *Военная мысль*, *9*, 11–18.
10. Уроки Сирії та України: трансформація систем управління військами. (2023). Центр воєнно-стратегічних досліджень ГШ ЗС РФ. *Вестник Академии военных наук*, *1* (74), 26–35.
11. *Платформа “Дельта” як інструмент ситуативної обізнаності* [Презентаційні матеріали]. (2023). ГУР МО України. https://gur.gov.ua
12. Олійник, А. О., & Козаченко, О. М. (2023). Особливості забезпечення стійкості системи управління військами в умовах повномасштабної війни. *Сучасні інформаційні технології у сфері безпеки та оборони*, *2* (45), 17–26. https://doi.org/10.33099/2618-1614/2023-45-2-17–26.
13. Якименко, О. О. (2023). Фактори впливу на систему управління в умовах інформаційного та кібервпливу противника: український досвід. *Воєнна безпека і стратегія*, *1*, 41–48.
14. *Уроки російсько-української війни: як зберігати керованість військами в умовах сучасного бою: аналітичний звіт.* (2023). Центр оборонних стратегій. https://defence.org.ua
15. Sabbagh, D. (2023, 10 вер.). How Ukraine’s battlefield coordination is reshaping modern command and control. *The Guardian*. https://www.theguardian.com/world/2023/sep/10/ukraine-command-and-control
16. Ігнатов, С. В., & Остапчук, В. М. (2023). Інноваційні підходи до побудови стійкої системи управління в умовах війни нового типу. *Схід*, *4* (184), 55–62. https://doi.org/10.21847/1728-9343.2023.4(184).285534
17. *Defence Command Paper Refresh 2023: Mobilising for Secure Britain* (розділ про C2 resilience). (2023). UK Ministry of Defence. https://www.gov.uk/government/publications/defence-command-paper-2023

18. Коваль, О. В., & Дубовик, М. М. (2023). Удосконалення системи оперативного управління в Збройних Силах України з урахуванням досвіду війни 2022–2023 років. *Збірник наукових праць НАОУ*, *2* (79), 73–80.

References

1. Bilichenko, S. I., Voronin, O. H., & Kulyk, V. Yu. (2021). Resilience of the military command system under armed conflict conditions. *Scientific Journal of the Central Research Institute of the Armed Forces of Ukraine*, *3* (84), 34–42.
2. *Transformation of the Command System of the Armed Forces of Ukraine during the Full-Scale War: Analytical Note*. (2023). National Institute for Strategic Studies. https://niss.gov.ua.
3. Application of digital solutions in the defense command system: wartime challenges and development prospects. (2023). Institute for National Security Issues. *Scientific Bulletin of the INSI*, *2*, 45–53.
4. Parkhomenko, M. S., & Chornyi, P. P. (2023). Improving the command structure of military groups under intensive enemy fire. *Military Thought*, *7*, 22–30.
5. Kuzmenko, S. M. (2023). Decentralization of command as a factor for increasing resilience of the military command system under hybrid war conditions. *Scientific Journal of the Kharkiv National Air Force University*, *4* (74), 85–92.
6. NATO Science and Technology Organization. (2020). *Command and Control Agility in the Age of Hybrid Threats* (STO-TR-HFM-260). NATO.
7. Peltz, J. L., Paul, L., & Johnson, B. (Eds.). (2021). *Command and Control in U.S. Military Operations: A Systematic Review*. RAND Corporation. https://doi.org/10.7249/RRA394-1
8. Van Creveld, M. (2020). *Command in War*. Harvard University Press.
9. Commanding troops in modern operations: From automation to digital sovereignty. (2022). *Military Thought (Russian Journal)*, *9*, 11–18.
10. Lessons from Syria and Ukraine: Transformation of troop command systems. (2023). Center for Military-Strategic Research of the General Staff of the RF Armed Forces. *Bulletin of the Academy of Military Sciences*, *1* (74), 26–35.
11. *Delta Platform as a Tool for Situational Awareness* [Presentation materials]. (2023). Defence Intelligence of Ukraine. https://gur.gov.ua
12. Oliinyk, A. O., & Kozachenko, O. M. (2023). Features of ensuring resilience of the military command system under full-scale war conditions. *Modern Information Technologies in the Security and Defense Sector*, *2* (45), 17–26. https://doi.org/10.33099/2618-1614/2023-45-2-17-26.
13. Yakymenko, O. O. (2023). Factors influencing the command system under enemy informational and cyber attacks: Ukrainian experience. *Military Security and Strategy*, *1*, 41–48.
14. *Lessons from the Russo-Ukrainian War: How to Maintain Command and Control in Modern Combat: Analytical Report*. (2023). Center for Defense Strategies. https://defence.org.ua
15. Sabbagh, D. (2023, Sept. 10). How Ukraine's battlefield coordination is reshaping modern command and control. *The Guardian*. https://www.theguardian.com/world/2023/sep/10/ukraine-command-and-control
16. Ihnatov, S. V., & Ostapchuk, V. M. (2023). Innovative approaches to building a resilient command system under new types of warfare. *Skhid*, *4* (184), 55–62. https://doi.org/10.21847/1728-9343.2023.4(184).285534
17. *Defence Command Paper Refresh 2023: Mobilising for Secure Britain* (Section on C2 Resilience). (2023). UK Ministry of Defence. https://www.gov.uk/government/publications/defence-command-paper-2023
18. Koval, O. V., & Dubovyk, M. M. (2023). Improving the operational command system of the Armed Forces of Ukraine based on the experience of the 2022–2023 war. *Scientific Journal of the National Defence University of Ukraine*, *2* (79), 73–80.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

Analysis and Assessment of the Influence of Factors on the Requirements for the Command and Control System of an Operational Military Grouping in Operations (Combat Actions): The Experience of the Russo-Ukrainian War

Roman Voitsechovskyi
Adjunct Lecturer at the Department of Troop Command and Control,
Institute of State Military Management
National Defence University of Ukraine
03049, Povitrianykh Syl Avenue, 28, Kyiv, Ukraine
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

Abstract. The experience of the Armed Forces of Ukraine since 2022 has demonstrated that the ability of the command and control system to remain functional under conditions of losses, isolation of command posts, changes in the tactical situation, and information overload is a key prerequisite for maintaining the combat effectiveness of military groupings. Successful examples of decentralised decision-making, integration of digital platforms, use of unmanned and autonomous systems, and modular command structures allow for the development of new approaches to formulating requirements for the command and control system of operational military groupings based on the criterion of resilience.

The main purpose of this article is to analyse and assess the influence of various factors on the requirements for the command and control system of operational military groupings in operations (combat actions), drawing on the experience of the Russo-Ukrainian war.

This article identifies the main external and internal factors influencing the requirements for the command and control system and evaluates their impact using the method of pairwise comparisons. It offers recommendations for enhancing the resilience of the command and control system and defines key indicators for the survivability of command posts. The research methodology combines analysis and synthesis with expert surveys, utilising the pairwise comparison procedure to assess the level of influence of each factor on the system's resilience in operational contexts.

The findings of this article may be of use to military theorists and practitioners developing modern warfare strategies; security and defence analysts studying the transformation of armed conflicts; researchers in the philosophy of war, military history, and international relations; as well as policymakers and military leaders shaping defence policies and doctrines.

Keywords: automation of command posts, combat actions, requirements for command and control systems, military operations, cyber weapons, survivability of command posts, operational military grouping operations, operational military grouping, command responsiveness, Russo-Ukrainian war, command posts, command and control systems, resilience of command and control systems