

УДК УДК 343.98

DOI 10.59226/2786-6920.1.2025.143-150

КОМИССАРОВА НАТАЛЯ ОЛЕКСАНДРІВНА

*кандидат юридичних наук, доцент,
начальник кафедри державної безпеки
Київського інституту Національної гвардії України
<https://orcid.org/0000-0001-6895-6891>*

СЛИВКІН СЕРГІЙ СЕРГІЙОВИЧ

*здобувач вищої освіти
Київського інституту Національної гвардії України
<https://orcid.org/0009-0008-8865-0994>*

ЗАГРОЗИ ДЕРЖАВНІЙ БЕЗПЕЦІ ВНАСЛІДОК ДІЯЛЬНОСТІ ДИВЕРСІЙНО-РОЗВІДУВАЛЬНИХ ГРУП: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ

У статті проаналізовано загрози державній безпеці України, що постають унаслідок діяльності диверсійно-розвідувальних груп (ДРГ) в умовах сучасної гібридної війни. Розкрито основні напрями деструктивного впливу ДРГ – фізичного, інформаційного, соціального та економічного характеру. Обґрунтовано, що правова база України має значні прогалини у сфері протидії ДРГ, що знижує ефективність державного реагування на відповідні загрози. Визначено проблеми координації між Збройними Силами України, Службою безпеки України та Національною гвардією України у сфері контрдиверсійної боротьби. Запропоновано шляхи вдосконалення законодавства та організаційного забезпечення протидії ДРГ, зокрема створення єдиного міжвідомчого центру управління та прийняття спеціального нормативно-правового акту. Дослідження базується на аналізі національного контексту та міжнародного досвіду, що дає змогу сформулювати комплексний підхід до нейтралізації диверсійних загроз.

***Ключові слова:** державна безпека; диверсійно-розвідувальні групи; правове забезпечення; міжвідомча координація; гібридна війна.*

Постановка проблеми. Сучасна гібридна війна, яку веде Російська Федерація проти України, супроводжується активним використанням диверсійно-розвідувальних груп (ДРГ). Їх діяльність становить серйозну загрозу для державної безпеки, оскільки диверсанти не лише завдають фізичних втрат, а й дестабілізують внутрішню ситуацію через інформаційні атаки та психологічний тиск. З початку повномасштабного вторгнення у 2022 році Служба безпеки України (СБУ) неодноразово повідомляла про виявлення та ліквідацію ДРГ, які діяли на прифронтових територіях і навіть у тилових регіонах України [1].

Діяльність ДРГ спрямовано на підрив економіки, руйнування об'єктів критичної інфраструктури, дезорганізацію системи управління військами, проведення інформаційних операцій та створення паніки серед населення. Важливим елементом роботи ДРГ є використання інформаційного тиску та поширення фейкової інформації для підриву морального стану суспільства. Особливу небезпеку становить діяльність диверсантів у прифронтових зонах, де обмежено можливості контролю та швидкого реагування.

Незважаючи на активні заходи протидії, наявні серйозні проблеми в системі виявлення та нейтралізації ДРГ, пов'язані як із прогалинами в законодавстві,

так і з недостатньою координацією між силовими структурами. Закон України «Про боротьбу з тероризмом» не містить чіткого визначення та положень щодо протидії ДРГ, що створює правові прогалини у боротьбі з ними. Крім того, хоча Антитерористичний центр при СБУ виконує функції координації боротьби з тероризмом, відсутність конкретизації щодо ДРГ може призводити до недостатньої ефективності координації між Збройними Силами України (ЗСУ), СБУ та Національною гвардією України у випадку загрози диверсійної атаки [2].

Аналіз останніх досліджень та публікацій. Упродовж 2022–2025 років в українському та міжнародному науковому просторі значно зростає кількість досліджень, присвячених загрозам, які несуть диверсійно-розвідувальні групи (ДРГ) у контексті гібридної війни. Особливу увагу приділяють правовому регулюванню протидії ДРГ, організаційній взаємодії силових структур та досвіду іноземних держав у боротьбі з подібними формами загроз.

Зокрема, у працях М. О. Боровика, О. Г. Трембовецького та Д. Ю. Гулеватого розглядаються практичні аспекти виявлення і нейтралізації ДРГ силами Національної поліції та прикордонної служби, наголошується на необхідності чіткої координації між різними структурами [3; 4]. Аналіз операції НАТО «Resolute Support» в Афганістані демонструє, що ефективна протидія ДРГ можлива лише за умов створення об'єднаних міжвідомчих штабів із чітким розподілом обов'язків [5].

Українські дослідження у сфері національної безпеки (наприклад, на базі НІСД та ЛьвівДУВС) виявляють правовий вакуум у питанні визначення ДРГ; критикують фрагментарність нормативно-правового забезпечення. Додатково, публікації Служби безпеки України та Міністерства оборони містять офіційну статистику виявлення агентурних мереж та оперативну інформацію про активність ДРГ у прифронтових і тилових районах [6].

Дослідник Ю. Михальчишин констатує: незважаючи на зростання обізнаності про загрозу ДРГ, питання правової конкретизації та міжвідомчої взаємодії залишаються актуальними. Отже, подальше наукове осмислення цих проблем є необхідною передумовою для формування ефективної стратегії національної безпеки [7].

Завдання дослідження – оцінити стан законодавчої бази України щодо протидії ДРГ в умовах воєнного стану; визначити основні прогалини у правовому забезпеченні контрдиверсійної боротьби; проаналізувати ефективність організаційної взаємодії між силовими структурами у сфері контрдиверсійної боротьби; розробити пропозиції щодо вдосконалення

системи виявлення та нейтралізації ДРГ на рівні законодавства та міжвідомчої координації.

Мета дослідження – визначити правові та організаційні проблеми у системі протидії ДРГ та обґрунтувати шляхи їх усунення на основі міжнародного досвіду та аналізу сучасних викликів.

Виклад основного матеріалу. *Загрози державній безпеці внаслідок діяльності ДРГ.* Діяльність ДРГ становить одну з найсерйозніших загроз для державної безпеки України в умовах сучасної гібридної війни. Успішні диверсії та операції ДРГ часто мають не лише тактичні, а й стратегічні наслідки – від фізичних втрат до масштабних інформаційних та соціальних криз. Від початку повномасштабного вторгнення Росії у 2022 році було зафіксовано численні випадки проникнення та діяльності ДРГ як у прифронтових, так і в тилових районах [8].

Пряма фізична загроза від діяльності ДРГ є однією з найочевидніших. Диверсанти зазвичай працюють швидко та локально, завдаючи точкових ударів по військових об'єктах, об'єктах критичної інфраструктури та транспортних шляхах. Підриви мостів, залізничних вузлів, складів боєприпасів і логістичних центрів часто призводять до затримок у постачанні техніки та боєприпасів на передову, що суттєво впливає на бойові дії. Наприклад, підриви Каховської ГЕС у червні 2023 року спричинив масштабне затоплення та руйнування інфраструктури, що за даними СБУ, має всі ознаки диверсії.

Окрему загрозу становить діяльність ДРГ, спрямована на ліквідацію командного складу та підрозділів ППО. Успішні атаки на командні пункти та вузли зв'язку суттєво ускладнюють управління військами та координацію на полі бою. Окрім цього, диверсанти нерідко встановлюють мінні загородження та застосовують вибухові пристрої в тилових районах, що створює ризики для військових колон та цивільного транспорту [9].

Важливим інструментом діяльності ДРГ залишається інформаційна війна. Поширення фейкових новин, злом офіційних вебсайтів, створення паніки через соціальні мережі – все це використовується для підриву морального стану військових і населення. Диверсанти часто поширюють дезінформацію про нібито успіхи російських військ, втрати серед командування ЗСУ та зраду окремих підрозділів. Такі атаки спрямовано на послаблення бойового духу та створення відчуття хаосу в тилу. У 2023 році було зафіксовано серію кібератак на державні установи, у ході яких зловмисники отримали доступ до особистих даних військовослужбовців та інформації про логістику ЗСУ.

Соціальний вплив діяльності ДРГ також є вкрай небезпечним. Поширення паніки та недовіри до

влади може призводити до масових заворушень та актів громадянської непокори. Наприклад, у прифронтових районах були випадки організації масових акцій протесту, які, за даними СБУ, координувалися через агентурні мережі противника. Диверсанти активно використовують соціальні мережі для координації своїх дій та мобілізації населення до антиурядових виступів.

Діяльність ДРГ також завдає значних економічних збитків. Підриви енергетичних об'єктів та транспортної інфраструктури призводять до зупинки роботи підприємств, порушення логістичних ланцюгів та збоїв у постачанні продовольства та військової техніки. Ураження об'єктів енергетики у Харківській та Запорізькій областях спричинило тривалі перебої у постачанні електроенергії та води. Крім того, атаки на нафтобази та склади пального у Сумській та Чернігівській областях призвели до дефіциту пального у прифронтових районах, що ускладнило пересування техніки та забезпечення підрозділів на передовій.

Сукупність цих загроз засвідчує багатовимірний характер діяльності ДРГ. Це не лише фізична загроза для військових об'єктів та інфраструктури, а й масштабний інформаційний та психологічний тиск на суспільство. ДРГ діють на стику військової, інформаційної та економічної сфер, використовуючи слабкі місця в системі національної безпеки для завдання максимальних збитків при мінімальних ресурсах.

Відсутність єдиного центру реагування та недовілики у взаємодії між ЗСУ, СБУ та Нацгвардією часто призводять до втрати часу та неефективних дій у разі загрози диверсії. Крім того, недостатня правова регламентація діяльності ДРГ у національному законодавстві ускладнює юридичну кваліфікацію та ких дій та визначення відповідальності учасників.

Діяльність ДРГ становить системну загрозу для національної безпеки України. Вона охоплює фізичний, інформаційний, соціальний та економічний виміри, що вимагає комплексного підходу до виявлення та нейтралізації таких груп. Для цього необхідна чітка правова база, ефективна координація між силовими відомствами та сучасні технічні засоби моніторингу та реагування.

Проблеми правового забезпечення протидії ДРГ. Одна з найбільших проблем у правовому полі України полягає у відсутності чіткого визначення поняття «диверсійно-розвідувальна група». Закон України «Про боротьбу з тероризмом» (від 20.03.2003 № 638-IV) визначає терористичні акти як «загрозу або застосування насильства з політичними чи ідеологічними цілями», але діяльність ДРГ часто виходить за межі цього визначення. Диверсійно-розвідувальні

групи виконують більш комплексні завдання, поєднуючи розвідку, підривну діяльність, збір інформації про дислокацію військ і навіть інформаційні атаки. Це створює правову невизначеність, через яку дії ДРГ часто класифікуються як «державна зрада» або «незаконна збройна діяльність», що значно ускладнює юридичне переслідування диверсантів і членів їхніх агентурних мереж.

У багатьох випадках особи, затримані за участь у ДРГ, потрапляють під статті Кримінального кодексу України, які не відповідають суті їхньої діяльності. Наприклад, учасники диверсійної групи, що була виявлена у Харківській області у 2022 році, отримали звинувачення у державній зраді, хоча їх діяльність була спрямована на збір інформації для наведення артилерії та організацію диверсій на логістичних об'єктах. Відсутність окремого правового механізму для боротьби з ДРГ призводить до того, що затримані часто уникають максимальної відповідальності через прогалини у кваліфікації злочину.

Недостатня адаптація законодавства до сучасних гібридних загроз лише поглиблює цю проблему. Сучасна війна вже давно вийшла за межі класичних бойових дій – діяльність ДРГ охоплює інформаційні операції, кібератаки, створення соціальної напруги та економічного хаосу. Українське законодавство все ще базується на класичному визначенні тероризму як акту насильства. Відсутність правового інструментарію для боротьби з гібридними загрозами створює суттєві труднощі у реагуванні на такі атаки. Наприклад, Закон України «Про національну безпеку України» (від 21.06.2018 № 2469-VIII) визначає інформаційний та кіберпростір як ключові елементи національної безпеки, але не містить жодних положень щодо боротьби з агентурними мережами та інформаційними атаками, що координуються ДРГ [10; 11].

Ще однією серйозною проблемою є прогалини у визначенні повноважень силових структур під час протидії ДРГ. Закон України «Про боротьбу з тероризмом» визначає суб'єктами боротьби з тероризмом СБУ, ЗСУ, МВС, Державну прикордонну службу та Національну гвардію. Проте між цими структурами відсутній чіткий розподіл повноважень саме у сфері протидії ДРГ. Наприклад, СБУ відповідає за контррозвідку та виявлення агентурних мереж, але ліквідація диверсантів під час бойових дій залишається компетенцією ЗСУ та Національної гвардії. Це створює конфлікти в ланцюгу командування, що ускладнює прийняття оперативних рішень у кризових ситуаціях.

У 2022 році в Харківській області був зафіксований випадок виявлення ДРГ, яка займалася наведенням артилерії. Однак агентурна мережа, яка

забезпечувала диверсантів інформацією, залишилася не розкрита через відсутність координації між військовими структурами та СБУ. Це є прямим наслідком правових прогалин у регулюванні дій силових відомств у сфері боротьби з ДРГ.

Діяльність ДРГ частково врегульована через існуючі антитерористичні заходи, але вона не підпадає під окреме правове регулювання. У 2022 році РНБО ініціювала розроблення Закону «Про протидію диверсійно-розвідувальним групам», однак станом на 2025 рік цей законопроект так і не був ухвалений. Відсутність цього закону створює правовий вакуум, через який силові структури часто діють на основі внутрішніх наказів і тимчасових директив, що обмежує ефективність та швидкість реагування на загрози ДРГ.

Окремої уваги потребує проблема координації між силовими відомствами під час протидії ДРГ. На практиці Антитерористичний центр при СБУ виконує функцію координації між відомствами, але через відсутність чітких процедур обміну інформацією та єдиної системи реагування між військовими структурами та СБУ часто виникають затримки у прийнятті рішень. У випадку проникнення ДРГ у прифронтові райони оперативна інформація від військової розвідки може невчасно передаватися до СБУ, що знижує ефективність боротьби з диверсантами.

Вирішення цієї проблеми потребує створення єдиного міжвідомчого штабу під безпосереднім керівництвом РНБО, який забезпечить координацію між ЗСУ, СБУ, Національною гвардією та прикордонниками у сфері протидії ДРГ. Такий штаб має отримати повноваження щодо прийняття оперативних рішень у режимі реального часу та забезпечити прямий зв'язок між підрозділами на рівні командування.

Отже, для ефективної протидії ДРГ необхідно внести зміни до законодавства, розробити окремий нормативний акт щодо протидії ДРГ, чітко визначити повноваження силових структур та створити єдину систему координації на рівні РНБО. Без системних змін у правовій та організаційній площині протидія ДРГ залишатиметься фрагментарною та недостатньо ефективною.

Організаційні проблеми у протидії ДРГ. Протидія ДРГ вимагає високого рівня координації та оперативності від силових структур. Однак на практиці наявні організаційні проблеми, які суттєво знижують ефективність реагування на загрози ДРГ. Насамперед це стосується відсутності єдиного центру управління, слабкої взаємодії між різними структурами та недостатньої готовності до дій у критичних ситуаціях.

Одна з головних проблем полягає у відсутності централізованого управління операціями з протидії ДРГ. Закон України «Про боротьбу з тероризмом» покладає основну відповідальність за координацію антитерористичних заходів на СБУ через Антитерористичний центр. Однак на практиці СБУ виконує переважно функції контррозвідки та виявлення агентурних мереж, тоді як фізична ліквідація ДРГ та проведення зачисток залишається у компетенції Збройних сил України та Національної гвардії України.

Через таке розмежування повноважень під час реальних бойових дій виникають конфлікти інтересів та дублювання завдань. Наприклад, у 2022 році в Харківській області виявлена ДРГ, яка займалася наведенням артилерії на позиції ЗСУ, була ліквідована силами Нацгвардії. Однак СБУ не змогла оперативного отримати доступ до захопленої техніки та засобів зв'язку, оскільки юридично операція вважалася військовою, а не контррозвідувальною. Це засвідчує відсутність механізму спільного управління операціями між різними силовими відомствами [12].

Ще однією проблемою є обмежений рівень обміну інформацією між СБУ, ЗСУ та НГУ. Оперативні дані про пересування диверсантів, плани ворожих груп та агентурні мережі часто залишаються у відомчому обігу і не передаються в режимі реального часу між структурами. У 2023 році в Донецькій області українські військові перехопили групу диверсантів, які планували здійснити підриг мосту через Сіверський Донець. Військові отримали інформацію про підготовку до теракту від місцевих мешканців, однак через відсутність оперативного каналу зв'язку із СБУ ця інформація не була вчасно передана до Антитерористичного центру. Це призвело до затримки у прийнятті рішення та створило ризик зриву операції.

Недостатня координація виявляється і в процесі оперативного реагування на загрози у прифронтових зонах. Сили спеціального призначення (СБУ, ЗСУ, НГУ) часто працюють окремо, без чіткого обміну інформацією та узгоджених дій. У прифронтових районах, особливо у міських умовах, це може призводити до «дружнього вогню», коли підрозділи різних відомств не мають чіткої взаємодії та не володіють оперативною обстановкою на полі бою. Відомий випадок у Маріуполі на початку 2022 року став яскравим прикладом такої неузгодженості. Під час зачистки міста група бійців НГУ вступила у бій із підрозділом СБУ, оскільки обидва підрозділи діяли за різними планами операції, не маючи єдиного каналу координації.

Відсутність єдиного центру управління операціями також впливає на логістичне забезпечення

та технічну підтримку силових структур. У випадках тривалих операцій із виявлення та нейтралізації ДРГ підрозділи ЗСУ та НГУ часто стикаються з нестачею засобів зв'язку, боєприпасів та бронетехніки через відсутність єдиного каналу постачання. Логістичні підрозділи ЗСУ забезпечуються за однією системою, а підрозділи НГУ та СБУ – за іншими, що ускладнює координацію постачання та оперативне перекидання техніки у зони бойових дій.

Окремою проблемою є відсутність єдиної бази даних щодо діяльності ДРГ та агентурних мереж. СБУ та ЗСУ володіють окремими базами оперативних даних, які не інтегровані в єдину інформаційну мережу. Це ускладнює ідентифікацію диверсантів, що діють під прикриттям цивільного населення. У 2023 році було зафіксовано випадок, коли група ДРГ діяла у Харківській області протягом двох місяців, використовуючи фальшиві документи. Військова розвідка передавала інформацію до ЗСУ, але через відсутність оперативного зв'язку із СБУ група продовжувала діяти, поки її випадково не виявили під час перевірки на блокпості.

Також суттєвою проблемою залишається відсутність єдиної системи обліку та координації агентурної роботи у тилових районах. ДРГ часто отримують підтримку від місцевої агентури, яка забезпечує прихисток, інформацію про маршрути пересування та допомогу у логістиці. На практиці СБУ та військова розвідка діють окремо в цій сфері, що призводить до дублювання зусиль та втрати цілісної картини операційної обстановки.

Отже, ключовими організаційними проблемами у протидії ДРГ залишаються відсутність єдиного центру управління, слабка координація між структурами, відсутність оперативного каналу зв'язку та логістичного забезпечення. Для вирішення цих проблем необхідно створити єдиний міжвідомчий центр під керівництвом РНБО, який забезпечить постійний обмін інформацією, оперативне планування та координацію дій силових відомств у режимі реального часу. Інтеграція баз даних між СБУ, ЗСУ та НГУ, створення єдиного каналу комунікації та централізоване логістичне забезпечення дозволить значно підвищити ефективність протидії ДРГ і забезпечити швидке реагування на загрози у прифронтових зонах.

Вдосконалення правової та організаційної бази протидії ДРГ. Ефективна протидія ДРГ потребує не лише вдосконалення оперативно-тактичної підготовки силових структур, а й створення надійної правової та організаційної основи. Сьогодні правове регулювання протидії ДРГ залишається фрагментарним та недостатньо адаптованим до реалій сучасної гібридної війни. Відсутність чіткого

визначення ДРГ, правових норм щодо застосування сили, а також слабка координація між відомствами суттєво ускладнюють боротьбу з диверсантами на оперативному рівні.

Передусім необхідно внести зміни до чинного законодавства, щоб діяльність ДРГ отримала чітку правову кваліфікацію. У Законі України «Про боротьбу з тероризмом» варто закріпити визначення ДРГ як організованої групи, що діє за вказівкою іноземних держав або недержавних утворень з метою збору інформації, проведення диверсій та дестабілізації внутрішньої ситуації в країні. Така класифікація дозволить чітко визначити механізми реагування та порядок застосування сили під час виявлення ДРГ.

Окрім цього, доцільно прийняти окремий закон «Про протидію диверсійно-розвідувальним групам», у якому необхідно закріпити порядок виявлення, нейтралізації та кримінальної відповідальності учасників ДРГ. У законі варто передбачити чітку процедуру взаємодії між Збройними силами України (ЗСУ), Службою безпеки України (СБУ) та Національною гвардією України (НГУ) під час проведення контрдиверсійних операцій. Важливо встановити правовий механізм для застосування сили проти ДРГ без ризику перевищення повноважень або правової відповідальності військовослужбовців.

Крім законодавчих змін, необхідно створити єдиний центр управління операціями з протидії ДРГ. Антитерористичний центр при СБУ на сьогодні виконує переважно координаційну функцію, але не володіє прямими оперативними повноваженнями щодо реагування на загрози в прифронтових зонах. Для забезпечення оперативного реагування на диверсійні загрози варто створити Об'єднаний центр контрдиверсійної боротьби (ОЦКБ) під безпосереднім керівництвом Ради національної безпеки і оборони України (РНБО). ОЦКБ повинен мати пряме повноваження на координацію операцій між ЗСУ, СБУ, НГУ та іншими силовими структурами, у тому числі підрозділами територіальної оборони та прикордонної служби.

Центр має працювати в режимі реального часу, забезпечуючи безперебійний обмін інформацією між відомствами. Для цього необхідно створити єдину електронну базу даних щодо діяльності ДРГ, агентурних мереж та відомостей про ворожі операції. Інтеграція даних військової розвідки, контррозвідки та оперативних служб дозволить виявляти зв'язки між агентурними мережами, відстежувати маршрути пересування диверсантів та запобігати майбутнім атакам на критичну інфраструктуру.

Особливої уваги потребує вдосконалення системи оперативного реагування на загрози ДРГ у

прифронтових зонах. Сьогодні ЗСУ та НГУ діють у зоні бойових дій на основі власних оперативних директив, що часто призводить до неузгодженості дій. Створення єдиного оперативного штабу при ОЦКБ дозволить проводити комплексні операції із залученням сил спеціального призначення, безпілотних літальних апаратів (БПЛА) та засобів радіоелектронної боротьби (РЕБ).

Окремої уваги потребує правове регулювання застосування сили під час контрдиверсійних операцій у мирний час. Сьогодні застосування зброї проти ДРГ регулюється загальними нормами про правомірне використання сили, що створює правову невизначеність. Для усунення цієї проблеми необхідно прийняти нормативний акт, що визначатиме порядок використання зброї та засобів РЕБ у випадку виявлення ДРГ. Це дозволить військовослужбовцям діяти в межах закону без ризику переслідування за перевищення повноважень.

Крім правових змін, необхідно посилити кадрове забезпечення та матеріально-технічну базу підрозділів, що залучаються до боротьби з ДРГ. Особливо це стосується підрозділів спеціального призначення (СБУ, ЗСУ, НГУ), які виконують ключову роль у виявленні та нейтралізації ДРГ. Підвищення рівня підготовки, постачання сучасних засобів зв'язку, приладів нічного бачення та ударних БПЛА дозволить значно підвищити ефективність бойових операцій проти ДРГ.

Інформаційна складова також потребує вдосконалення. ДРГ часто використовують соціальні мережі та месенджери для координації своїх дій і вербування агентів серед місцевого населення. Для боротьби з цими загрозами варто створити інформаційний підрозділ при ОЦКБ, який відповідатиме за виявлення та блокування інформаційних каналів, пов'язаних із діяльністю ДРГ. Окрім цього, необхідно запровадити моніторинг підозрілих фінансових операцій та активності в інтернеті підозрюваних осіб.

Отже, вдосконалення правової та організаційної бази протидії ДРГ має передбачати прийняття окремого закону про ДРГ, створення єдиного центру управління операціями при РНБО, вдосконалення нормативної бази щодо застосування сили та посилення матеріально-технічного забезпечення силових структур. Комплексний підхід, що поєднує правові, організаційні та технічні заходи, дозволить створити ефективну систему контрдиверсійної боротьби та захистити державну безпеку України від загроз ДРГ.

Висновки та перспективи подальших досліджень. Аналіз сучасних викликів у сфері державної безпеки України засвідчує, що діяльність ДРГ

є однією з найбільших загроз у контексті гібридної війни. Виявлені проблеми у правовому та організаційному забезпеченні боротьби з ДРГ вимагають системного підходу до їх вирішення на рівні законодавства, координації між відомствами та технічного оснащення силових структур.

Серед ключових проблем можна виділити правову невизначеність щодо діяльності ДРГ, відсутність єдиної системи координації між ЗСУ, СБУ та Національною гвардією, а також слабку інтеграцію інформаційних баз даних і каналів зв'язку. Відсутність чіткого правового механізму для застосування сили проти ДРГ у мирний час також ускладнює реагування на загрози у прифронтових зонах.

Для вдосконалення правової бази необхідно внести зміни до Закону України «Про боротьбу з тероризмом», закріпивши чітке визначення ДРГ та механізми притягнення до відповідальності за участь у їх діяльності. Прийняття окремого Закону «Про протидію диверсійно-розвідувальним групам» дозволить врегулювати порядок застосування сили та координацію між відомствами під час контрдиверсійних операцій.

У сфері організації контрдиверсійної боротьби необхідно створити Об'єднаний центр контрдиверсійної боротьби (ОЦКБ) під керівництвом Ради національної безпеки і оборони України (РНБО). Центр повинен забезпечувати оперативний обмін інформацією між відомствами, інтеграцію баз даних та централізоване управління операціями з виявлення і нейтралізації ДРГ у прифронтових зонах.

Окрему увагу варто приділити технічному забезпеченню підрозділів спеціального призначення, включаючи засоби радіоелектронної боротьби, безпілотні літальні апарати (БПЛА) та сучасні системи зв'язку. Посилення агентурної роботи та вдосконалення методів інформаційної протидії дозволить ефективніше виявляти агентурні мережі противника та блокувати діяльність ДРГ ще на етапі підготовки диверсій.

Отже, ефективна протидія ДРГ вимагає комплексного підходу, що поєднує правове регулювання, організаційну координацію та технологічне оснащення силових структур. Реалізація цих заходів дозволить підвищити рівень національної безпеки України та забезпечити оперативне реагування на загрози ДРГ у зоні бойових дій та в тилових регіонах.

Список використаних джерел

1. УКРІНФОРМ. Василь Малюк: СБУ викрила 11 агентурних мереж з початку 2024 року. URL: <https://surl.lu/ksuhob> (дата звернення: 05.01.2025).
2. Про боротьбу з тероризмом: Закон України від 20 березня 2003 № 638-IV. URL: <https://surl.li/wblayc> (дата звернення 05.01.2025).

3. Боровик М. О. Протидія диверсійно-розвідувальним групам противника підрозділами Національної поліції України в умовах воєнного стану. *Науковий вісник Львівського державного університету внутрішніх справ*. 2024. № 2. С. 45–58.

4. Трємбовецький О. Г., Гулеватий Д. Ю. Методика роботи штабу прикордонного загону щодо пошуку і ліквідації диверсійно-розвідувальних груп противника. *Наука і техніка Повітряних Сил Збройних Сил України*. 2018. № 4. С. 119–127.

5. Операція «Resolute Support» в Афганістані: досвід боротьби з диверсійно-розвідувальними групами. URL: nato.int. (дата звернення: 05.01.2025).

6. Суходоля О. М., Бобро Д. Г., Іванюта С. П., Кондратов С. І. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. Київ : НІСД, 2019. 224 с.

7. Михальчишин Ю. Контррозвідка в Україні від УНР до сьогодні. Львів: СПОЛОМ, 2021. 79 с.

8. ТСН. Діяльність розвідників-диверсантів бойовиків посилилася одразу на кількох напрямках. URL: <https://surl.lu/veulwz> (дата звернення 05.01.2025).

9. МВС. Гвардійці покращували навички протидії диверсійно-розвідувальним групам. URL: <https://surl.li/arvjys> (дата звернення 05.01.2025).

10. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://surl.li/cwtmxx>. (дата звернення: 05.01.2025).

11. Чайка Є. С. Нормативно-правове регулювання контррозвідувального забезпечення в Україні. *Академічні візії*. № 29(2024). DOI: <https://doi.org/10.5281/zenodo.10874942>.

12. Вітер Д., Цевельов О., Безбах В. Робота штабу органу охорони кордону під час організації протидії диверсійно-розвідувальним групам. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України* № 3(73) 2021. С. 53–59.

References

1. UKRINFORM. Vasył Maliuk: SBU vykryla 11 ahenturnykh merezh z pochatku 2024 roku [The Security Service of Ukraine uncovered 11 agent networks since the beginning of 2024]. Retrieved from: <https://surl.lu/ksuhob> (accessed 03 January 2024) [in Ukrainian].

2. Zakon Ukrainy: «Pro borotbu z teroryzmoz» No 638-IV vid 20 March 2003 [Law of Ukraine «On Combating Terrorism» activity 2003, March 20 No. 638-IV]. Retrieved from: <https://surl.li/wblayc> (accessed 5 January 2025) [in Ukrainian].

3. Borovyk, M. O. (2024). *Protydiia dyversiino-rozviduvalnym hrupam protyvnyka pidrozdilamy*

Natsionalnoi politsii Ukrainy v umovakh voiennoho stanu [Countering enemy sabotage and reconnaissance groups by units of the National Police of Ukraine under martial law]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav*. No 2. pp. 45–58 [in Ukrainian].

4. Trembovetskyi, O. H., Hulevatyi, D. Yu. (2018). *Metodyka roboty shtabu prykordonnoho zahonu shchodo poshuku i likvidatsii dyversiino-rozviduvalnykh hrup protyvnyka* [Methodology of border guard headquarters operations for detecting and eliminating enemy sabotage and reconnaissance groups]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrain*. No 4. pp. 119–127 [in Ukrainian].

5. *Operatsiia «Resolute Support» v Afhanistani: dosvid borotby z dyversiino-rozviduvalnymy hrupamy* [Operation «Resolute Support» in Afghanistan: Experience in countering sabotage and reconnaissance groups]. Retrieved from: nato.int. (accessed 03 January 2025) [in Ukrainian].

6. Sukhodolia, O. M., Bobro, D. H., Ivaniuta, S. P., Kondratov, S. I. (2019). *Orhanizatsiini ta pravovi aspekty zabezpechennia bezpeky i stiikosti krytychnoi infrastruktury Ukrainy* [Organizational and legal aspects of ensuring the security and resilience of Ukraine's critical infrastructure] analit. dop. Kyiv : NISD 224 p. [in Ukrainian].

7. Mykhalchysyn, Yu. (2021). *Kontrrozvidka v Ukraini vid UNR do sohodennia* [Counterintelligence in Ukraine from the UNR to the present day]. Lviv : SPOLOM. 79 p. [in Ukrainian].

8. TSN. *Diiialnist rozvidnykiv-dyversantiv boiovykiv posylylasia odrazu na kilkikh napriamkakh* [The activities of the militants' reconnaissance and sabotage units have intensified in several areas at once]. Retrieved from: <https://surl.lu/veulwz> (accessed 03 January 2025) [in Ukrainian].

9. MVS. *Hvardiitsi pokrashchuvaly navychky protydii dyversiino-rozviduvalnym hrupam* [Guardsmen improved their skills in countering sabotage and reconnaissance groups]. Retrieved from: <https://surl.li/arvjys> (accessed 03 January 2025) [in Ukrainian].

10. Zakon Ukrainy: «Pro natsionalnu bezpeku Ukrainy» No 2469-VIII vid 21.06.2018 [Law of Ukraine «On the National Security of Ukraine» activity 2018, June 21 No 2469-VIII]. Retrieved from: <https://surl.li/cwtmxx> (accessed 5 January 2025) [in Ukrainian].

11. Chaika, Ye. S. (2024). *Normatyvno-pravove rehuliuвання kontrrozviduvalnoho zabezpechennia v Ukraini* [Regulatory and legal regulation of counterintelligence support in Ukraine]. *Akademichni vizii*. No 29. DOI: <https://doi.org/10.5281/zenodo.10874942>.

12. Viter, D., Tsevelov O., Bezbach, V. (2021). *Robota shtabu orhanu okhorony kordonu pid chas*

orhanizatsii protydivnykh dyversiiino-rozviduvalnym hrupam [The work of the border guard headquarters during the organization of counteraction to sabotage and reconnaissance groups]. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy. No 3(73), pp. 53–59.

Стаття надійшла до редакції / Received: 08.04.2025

Процеженовано / Revised: 16.04.2025

Схвалено до друку / Accepted: 26.04.2025

Komissarova Natalia

Candidate of Legal Sciences, Associate Professor,
Head of the Department of State Security
of the Kyiv Institute of the National Guard of Ukraine

Slyvkin Serhii

higher education student of the Kyiv Institute
of the National Guard of Ukraine

**THREATS TO STATE SECURITY RESULTING
FROM THE ACTIVITIES OF SUBVERSION
AND INTELLIGENCE GROUPS:
LEGAL AND ORGANIZATIONAL ASPECTS**

This publication analyzes the threats to Ukraine's national security posed by the activities of sabotage and reconnaissance groups (SRGs) in the context of modern hybrid warfare. It highlights the main areas of destructive impact caused by SRGs – physical, informational, social, and economic. The study substantiates that the current Ukrainian legal framework contains significant gaps in countering SRGs, which undermines the state's

capacity for timely and effective response. Key issues in the coordination between the Armed Forces of Ukraine, the Security Service of Ukraine, and the National Guard of Ukraine in counter-sabotage operations are identified. The article proposes ways to improve legislation and organizational mechanisms, including the establishment of a unified interagency command center and the adoption of a specialized regulatory act. The analysis combines national insights and international experience to form a comprehensive approach to neutralizing sabotage threats.

Special attention should be paid to the technical support of special forces units, including electronic warfare equipment, unmanned aerial vehicles (UAVs) and modern communication systems. Strengthening intelligence work and improving information countermeasure methods will allow for more effective detection of enemy intelligence networks and blocking the activities of DRGs at the stage of preparing sabotage.

Therefore, effective countermeasures against DRGs require a comprehensive approach that combines legal regulation, organizational coordination and technological equipment of law enforcement agencies. The implementation of these measures will allow for an increase in the level of national security of Ukraine and ensure a prompt response to DRG threats in the combat zone and in the rear regions.

Keywords: national security; sabotage and reconnaissance groups; legal framework; interagency coordination; hybrid warfare.