УДК 355.45:342.9:004.056(477) DOI 10.59226/2786-6920.2.2025.141-148

РОМАШКО ОЛЕГ МИКОЛАЙОВИЧ
старший викладач кафедри забезпечення державної безпеки,
Київський інститут Національної гвардії України
https://orcid.org/0000-0003-1601-1591

ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ВІЙСЬКОВОЇ ДІЯЛЬНОСТІ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Досліджено проблеми безпеки військової діяльності в умовах правового режиму воєнного стану. Виявлено фрагментарність правового регулювання діяльності сил оборони, а також недостатній рівень кіберзахисту критичних об'єктів. Так само потребує вдосконалення психологічна підготовка особового складу. Установлено такі виклики безпеці військової діяльності, як гібридні війни, кібератаки, інформаційно-психологічні операції.

Запропоновано напрями підвищення рівня безпеки військової діяльності, що передбачають оновлення нормативної бази, поліпшення координації, зміцнення кібероборони, модернізацію технічного оснащення, а також запровадження програм психологічної підтримки особового складу.

Ключові слова: *воєнний стан; ризики; загрози; військовослужбовці; інформаційно-психологічні операції; безпека; кібербезпека.*

Постановка проблеми. В умовах правового режиму воєнного стану питання безпеки військової діяльності набувають критичного значення, оскільки суттєво зростають ризики для особового складу, цивільного населення і стратегічних об'єктів. Аналіз чинного законодавства виявив фрагментарність нормативно-правової бази, яка регулює діяльність сил оборони і потребує вдосконалення, зокрема щодо чіткого визначення повноважень військових адміністрацій і взаємодії між військовими й цивільними інституціями [1, 2]. Недостатнім також вбачається рівень кіберзахисту критичної інфраструктури. Дослідження свідчать про зростання кількості кібератак на державний сектор та оборонні об'єкти, що створює додаткові загрози у сфері національної безпеки [3, 4]. Проблемним залишається й управління військовими ризиками: сучасні механізми прогнозування бойових дій і математичні моделі застосовуються епізодично й не інтегровані у систему прийняття рішень [5]. Не менш актуальним викликом є недостатня психологічна підготовка військовослужбовців. За даними досліджень значна частина особового складу сил безпеки й оборони зазнає стресу підвищеного рівня та психологічного виснаження, що знижує їхню стійкість і бойову ефективність [6].

Зазначені чинники зумовлюють необхідність комплексного підходу до безпеки військової діяльності, що передбачає вдосконалення правового регулювання військової діяльності, посилення кіберзахисту критичних об'єктів, розвиток системи управління ризиками й запровадження програм психологічної підготовки та реабілітації військовослужбовців. Такий підхід дасть змогу державі швидко адаптуватися до динамічного безпекового середовища, ефективно протидіяти воєнним загрозам і забезпечувати стабільність функціонування впродовж усього періоду збройного конфлікту.

Аналіз останніх досліджень і публікацій. Питання безпеки військової діяльності в умовах воєнного стану висвітлюється у працях багатьох українських науковців. Функцію забезпечення безпеки держави під час воєнного стану розглядає О. О. Глущенко, акцентуючи на ролі законодавчих механізмів та організаційних рішень [7]. Однак його праця обмежується загальним аналізом правового поля й не розкриває практичних інструментів реалізації цих механізмів у сфері військової діяльності. Організаційно-правові засади забезпечення

воєнної безпеки України аналізує Г. П. Ситник, визначає напрями вдосконалення взаємодії сил оборони [8]. Проте у дослідженні майже не розглядаються сучасні загрози інформаційно-психологічного й кібернетичного характеру, що наразі становлять ключові виклики для сектору оборони.

Важливим є й філософсько-етичний вимір. Методологічні підходи до оцінювання морально-психологічного стану військовослужбовців обґрунтовують у своїй праці В. Г. Дикун, В. М. Мороз та В. В. Стасюк [9]. Автори доводять, що психологічна стійкість і моральні орієнтири значною мірою впливають на результативність військової діяльності, однак не пропонують системних практичних механізмів підвищення цієї стійкості в умовах воєнного стану. На морально-етичних аспектах діяльності військових і цивільних осіб/структур у країнах, що зазнали агресії, зосереджуються І. Севрук та Ю. Соколовська [10]. У дослідженні акцентується на важливості гуманітарного виміру у військовій сфері, але конкретні засоби інтеграції етичних принципів у систему управління безпекою не розглядаються.

Попри наявні напрацювання, наукові дослідження переважно висвітлюють окремі складники проблеми: правові засади, організаційні механізми чи морально-психологічні аспекти. Бракує комплексного підходу, який би поєднував нормативно-правові рішення, управління ризиками, кіберзахист і психологічну підтримку військовослужбовців у єдиній системі безпеки. Саме ця прогалина зумовлює актуальність проведеного дослідження.

Мета статті – визначити шляхи підвищення рівня безпеки військової діяльності під час правового режиму воєнного стану через поєднання правових норм, етичних принципів та практичних заходів.

Виклад основного матеріалу. Для забезпечення ефективного функціонування держави та підтримання належного рівня обороноздатності в умовах воєнного стану критично важливою є безпека, яка охоплює всі сфери життєдіяльності – військову, інформаційну, економічну й гуманітарну. В умовах воєнного стану безпека передбачає реалізацію комплексних заходів, спрямованих на захист особового складу сил безпеки й оборони, цивільного населення, стратегічних об’єктів, а також державних інформаційних ресурсів. Одне з ключових завдань полягає в забезпеченні стабільного функціонування оборонного сектору і критичної інфраструктури, що дає змогу мінімізувати ризики, пов’язані з можливими диверсіями, кібератаками, руйнуванням транспортних та енергетичних комунікацій. Крім того, для підтримання громадського порядку й запобігання внутрішнім загрозам значущим елементом є створення ефективної системи координації між військовими, правоохоронними органами і цивільними установами.

Аналіз нормативно-правових актів, що визначають поняття безпеки, дає змогу стверджувати, що в умовах воєнного стану безпека військової діяльності набуває особливого значення, виходячи за межі загальноприйнятих визначень [4].

Закон України «Про національну безпеку України» визначає воєнну безпеку як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз [11]. Окрім воєнної безпеки цей Закон дає також визначення поняття державної безпеки, що охоплює значно ширший спектр заходів із захисту національних інтересів. Цей комплекс заходів спрямований на забезпечення стабільного функціонування державних інститутів, захист конституційного ладу, територіальної цілісності, прав і свобод громадян від загроз як внутрішнього, так і зовнішнього характеру. Державна безпека передбачає боротьбу з тероризмом, контррозвідувальні заходи, захист інформаційного простору, економічну безпеку та запобігання спробам дестабілізації ситуації всередині країни. У цьому контексті воєнна безпека є складовою державної безпеки, але зосереджена виключно на питаннях захисту від збройної агресії та підтримання обороноздатності країни.

Головна відмінність між цими поняттями полягає у сфері їх реалізації та характері загроз, яким вони протистоять. Якщо воєнна безпека стосується переважно збройного захисту держави від зовнішньої агресії, то державна безпека – явище більш комплексне, що охоплює також і внутрішні загрози (політична нестабільність, економічні кризи, диверсійна діяльність та інформаційні атаки). В умовах воєнного стану ці дві сфери безпеки тісно пов’язані, оскільки забезпечення стійкості державних інституцій і громадського порядку є не менш важливим, аніж безпосередній

військовий захист території. Це зумовлює потребу в узгодженні правових, організаційних і технічних заходів у межах єдиного контуру забезпечення безпеки.

У контексті військових операцій безпека являє собою складне явище, що передбачає мінімізацію неприпустимого ризику, пов'язаного з можливістю завдання шкоди життю та здоров'ю військовослужбовців, цивільного населення, а також пошкодження військової техніки та інфраструктури. Йдеться не лише про фізичний захист особового складу й техніки, але й про кібербезпеку, інформаційну безпеку та психологічну стійкість. В умовах воєнного стану нормативно-правові акти встановлюють чіткі процедури і протоколи для мінімізації ризиків та запобігання втратам, а також розширюють поняття безпеки, зокрема як захист від нетрадиційних форм агресії. Отже, потрібен комплексний підхід і постійне вдосконалювання стратегій безпеки з огляду на мінливість військової обстановки та появу нових загроз [12].

Зовнішніми загрозами є агресивні дії противника, спрямовані на порушення територіальної цілісності й суверенітету держави [6]. До таких належать: прямі військові вторгнення, артилерійські, ракетні та дронові удари, диверсійні акти й кібератаки, спрямовані на підрив обороноздатності країни.

Внутрішні загрози становлять серйозний виклик для національної безпеки, оскільки можуть дестабілізувати не лише військову сферу, а й суспільство загалом. Диверсійні й терористичні акти спрямовані на підрив оборонного потенціалу держави, створення хаосу та паніки серед населення, що ускладнює координацію дій військових і правоохоронних органів.

Інформаційні атаки, зокрема поширення дезінформації та кібератаки, здатні підірвати довіру до державних інституцій і деморалізувати як військових, так і цивільне населення. У таких умовах підтримання боєздатності військових підрозділів потребує не тільки фізичної і технічної готовності, а й інформаційної стійкості, психологічної підготовки та ефективної системи управління.

Особлива увага приділяється мінімізації шкоди для цивільного населення і навколишнього середовища. Під час військових операцій має враховуватися необхідність захисту цивільного населення від негативних наслідків бойових дій і запобігання екологічним катастрофам. В умовах воєнного стану пріоритетними завданнями є забезпечення безпеки критичної інфраструктури, захист інформаційного простору, а також запобігання виникненню надзвичайних ситуацій техногенного і природного характеру [3, 13].

Важливий аспект становить інформаційна безпека, яка передбачає протидію ворожій пропаганді, кібератакам і психологічним операціям, спрямованим на деморалізацію військових і суспільства. Особливу роль також відіграє технічна модернізація, зокрема оснащення військових підрозділів сучасним озброєнням, засобами зв'язку й розвідки, що підвищує їхню ефективність у бойових умовах.

Психологічна підготовка військовослужбовців та підтримання їхнього морального духу є не менш важливими, адже стресостійкість і мотивація особового складу безпосередньо впливають на здатність виконувати бойові завдання. Безпека військової діяльності у воєнний час – не лише питання захисту території, а й комплексна система заходів, яка потребує гнучкості, адаптивності й постійного вдосконалювання у відповідь на нові виклики й загрози [12].

Правове регулювання військової діяльності є основою забезпечення безпеки в умовах воєнного стану. На необхідності адаптувати законодавство до сучасних викликів через інтеграцію міжнародних стандартів і розроблення спеціалізованих нормативно-правових актів наголошують Ю. О. Загуменна та В. В. Сокуренко [1].

Важливим аспектом вбачається впровадження ефективних правових інструментів для врегулювання відносин між військовими і державними інституціями, аби запобігати правовим колізіям і зловживанням. Особливої уваги потребує розроблення нормативно-правових актів, що регламентують діяльність резервістів і добровольчих формувань, оскільки їхня участь у військових операціях має бути чітко визначеною. Тож комплексний підхід до правового регулювання військової діяльності є запорукою ефективного функціонування оборонного сектору в умовах сучасних загроз.

Правове регулювання військової діяльності має враховувати не лише загальні принципи національної безпеки, а й специфічні виклики, що виникають під час воєнного стану. Одним із ключових напрямів удосконалення є розроблення законодавчих ініціатив,

спрямованих на підвищення оперативності прийняття рішень у військовій сфері. Для забезпечення ефективності військового управління необхідно запроваджувати гнучкі правові механізми, які уможливлюють швидке реагування на зміну бойової обстановки. Крім того, особливу роль відіграє посилення правового контролю за діяльністю військових адміністрацій, що забезпечує належний рівень підзвітності та відповідальності за прийняті рішення. Важливим є завдання створення дієвих процедур для регулювання взаємодії між військовими структурами і цивільними органами влади, зокрема щодо використання матеріальних і залучення людських ресурсів для оборонних потреб.

Значущий аспект правового регулювання військової діяльності – гармонізація національного законодавства з міжнародними стандартами безпеки й гуманітарного права. Дотримання положень Женевських конвенцій та інших міжнародних угод дає змогу не лише забезпечити правомірність дій військових формувань, але і зміцнити міжнародну підтримку та співпрацю у сфері безпеки. Зокрема, адаптація українського законодавства до стандартів НАТО та Європейського Союзу сприятиме поліпшенню взаємодії з міжнародними партнерами, підвищенню ефективності оборонного планування та розвитку оборонно-промислового комплексу.

Окремої уваги потребує питання правового забезпечення кібербезпеки у військовій сфері. Сучасні конфлікти характеризуються активним застосуванням інформаційних технологій для ведення бойових дій, що створює нові виклики для правового регулювання. Немає чітких правових норм щодо відповідальності за кіберзлочини, так само, як і механізмів їх запобігання. Це може спричинити значні загрози для національної безпеки. Тому необхідно вдосконалювати законодавство в частині захисту критичної інформаційної інфраструктури, розробити норми, що визначають відповідальність за кібератаки на військові об’єкти, а також забезпечити ефективні механізми співпраці між державними органами і міжнародними партнерами у сфері кібероборони. Комплексний підхід до правового регулювання кіберзахисту дасть змогу не лише мінімізувати ризики атак, але й зміцнити інформаційну стійкість держави в умовах воєнного стану.

У період дії режиму воєнного стану держава постає перед значними загрозами інформаційного характеру, зокрема поширенням дезінформації, кібератаками та втручанням у функціонування інформаційних систем оборонного сектору [3]. Зазначені загрози спрямовано на дестабілізацію суспільства, підрив довіри до державних інституцій та порушення функціонування критичної інфраструктури. Особливу небезпеку становить використання соціальних мереж і месенджерів для миттєвого поширення дезінформації та маніпуляцій.

У сучасних конфліктах кібербезпека набуває особливого значення. На необхідності створення ефективних механізмів захисту критичної інформаційної інфраструктури, розроблення нормативних актів для регулювання відповідальності за кіберзлочини та протидію інформаційно-психологічним операціям противника наголошує Т. Ковальова [2]. Крім того, важливим аспектом є формування національної стратегії кібербезпеки, яка б охоплювала і військовий, і цивільний сектори, забезпечуючи комплексний підхід до захисту державних інформаційних ресурсів. Потребує розширення співпраця з міжнародними партнерами, зокрема в межах кіберполітики ЄС і НАТО, для обміну досвідом і розроблення спільних стандартів безпеки. Актуалізується так само й питання підготовки кваліфікованих фахівців у сфері кібероборони, оскільки стрімкий розвиток технологій вимагає постійного вдосконалювання навичок фахівців у сфері інформаційної безпеки. Упровадження сучасних систем штучного інтелекту для аналізу кібератак та оперативного реагування на них може значно підвищити рівень кіберзахисту держави.

Психологічна підготовка військовослужбовців є важливим чинником успішного виконання бойових завдань. Увагу на необхідності розроблення програм психологічної підтримки та реабілітації для зниження рівня стресу й підвищення морального духу особового складу акцентують В. І. Федорчук-Мороз і Л. Ф. Бондарчук [6]. Ефективними методами психологічної підготовки вбачається моделювання бойових ситуацій, проведення психологічних тренінгів та використання методів когнітивно-поведінкової терапії. Важливо забезпечити доступ до кваліфікованої психологічної допомоги як у зоні бойових дій, так і після повернення військовослужбовців до мирного життя, що сприятиме їхній соціальній адаптації.

Системний підхід до психологічної підготовки дає змогу підвищити рівень згуртованості військових підрозділів і створює умови для ефективного виконання бойових завдань у складних умовах. Слід зауважити, що необхідно також інтегрувати етичні принципи, зокрема дотримання норм міжнародного гуманітарного права та захист прав військовослужбовців і членів їхніх сімей [12].

Ефективне управління військовими ризиками передбачає ідентифікацію загроз, їх оцінювання та розроблення стратегій мінімізації. Використання математичних моделей, зокрема диференціальних рівнянь Ланчестера, уможливлює прогнозування розвитку бойових дій і прийняття обґрунтованих рішень щодо розподілу сил і засобів [5]. З історичних джерел відомо, що у 1916 р., під час Першої світової війни, британський інженер Ф. В. Ланчестер розробив систему диференціальних рівнянь для моделювання взаємодії ворогуючих сил. Ці рівняння описують динаміку чисельності військ двох протиборчих сторін у процесі бою, враховуючи інтенсивність ураження противника та власні втрати. Основними є лінійний закон Ланчестера, що застосовується для аналізу стародавніх війн, і квадратичний закон Ланчестера, який моделює сучасні конфлікти з використанням далекобійної зброї.

Застосування зазначених моделей дає змогу не лише прогнозувати результати прямих бойових зіткнень, але й оцінювати ефективність таких стратегічних рішень, як розподіл ресурсів, планування операцій та вибір оптимальних тактик. У сучасному воєнному контексті, де гібридні війни й кіберзагрози стають дедалі поширенішими, аналіз ризиків має враховувати не лише фізичні, а й інформаційні аспекти. Це потребує інтеграції математичних моделей з аналізом даних про кібербезпеку та інформаційні операції, що уможливить прогнозування й запобігання потенційним загрозам в інформаційному просторі.

Захист критичної інфраструктури та інформаційного простору – невід'ємна складова безпеки військової діяльності. Дослідники наголошують на необхідності розроблення національної стратегії кібербезпеки, яка б ураховувала специфіку воєнного стану й передбачала заходи протидії дезінформації та пропаганді [13].

Проаналізувавши наявну інформацію, можемо сформувати такі шляхи підвищення рівня безпеки військової діяльності.

1. Розроблення спеціалізованих навчальних програм, які мають містити правові аспекти, кібербезпеку та психологічну підготовку. Для ефективного реагування на сучасні виклики необхідно створювати комплексні навчальні курси для військовослужбовців, які б охоплювали правові аспекти ведення бойових дій, захист інформаційного простору та протидію кіберзагрозам. Окрему увагу потрібно приділити психологічній підготовці, оскільки стресостійкість військовослужбовців безпосередньо впливає на їхню боєздатність.

2. Модернізація технічного оснащення підрозділів сил безпеки і оборони задля мінімізації ризиків. Запровадження таких сучасних технологій, як автоматизовані системи управління військами, розвідувальні безпілотні літальні апарати та засоби електронної боротьби, уможливить підвищення ефективності військових операцій. Крім того, необхідно вдосконалювати систему індивідуального захисту військовослужбовців, зокрема бронежилети, каски та засоби тактичної комунікації.

3. Створення ефективної системи обміну інформацією між підрозділами. В умовах воєнного стану швидкість і точність передачі інформації відіграють критичну роль у прийнятті оперативних рішень. Для цього потрібно розвивати безпечні канали зв'язку, що унеможливлюють перехоплення даних противником. Поліпшення координації дій також потребує впровадження єдиних стандартів взаємодії між різними силовими структурами.

4. Постійний моніторинг та аналіз ризиків для виявлення загроз і розроблення стратегій протидії. Військові аналітичні центри повинні регулярно оцінювати поточні й потенційні загрози, використовуючи сучасні методи аналізу даних і прогнозування. Це дасть змогу своєчасно виявляти небезпеки, адаптувати військові стратегії та розробляти нові тактичні рішення, спрямовані на нейтралізацію ризиків.

Отже, належний рівень безпеки військової діяльності потребує системного підходу, який би поєднував правові, організаційні й технологічні заходи. Інтеграція сучасних рішень у військове управління, розвиток інформаційного захисту, удосконалювання технічного оснащення та підтримання морально-психологічного стану

особового складу є ключовими чинниками ефективності оборонних стратегій. Особлива увага має приділятися взаємодії військових структур із державними інституціями і міжнародними партнерами, що сприятиме зміцненню обороноздатності та національної безпеки України.

Висновки й перспективи подальших досліджень. Здійснено комплексний аналіз безпеки військової діяльності в умовах воєнного стану. Досліджено нормативно-правові акти, встановлено основні зовнішні і внутрішні загрози. Проаналізовано стан кіберзахисту і психологічної підготовки військовослужбовців, а також розглянуто практику управління ризиками з використанням сучасних підходів.

Результати дослідження ключовими визначають такі проблеми: фрагментарність правового регулювання; недостатня захищеність критичної інформаційної інфраструктури; обмеженість механізмів управління військовими ризиками; низький рівень системної психологічної підтримки особового складу. На основі цього сформовано шляхи підвищення рівня безпеки військової діяльності, які передбачають удосконалення законодавчої бази, поліпшення міжвідомчої координації, зміцнення кібероборони, модернізацію технічного оснащення, а також запровадження програм психологічної підтримки.

Подальші дослідження доцільно зосередити на розробленні спеціалізованих механізмів правового регулювання діяльності військових адміністрацій, створенні нових стратегій кіберзахисту та протидії інформаційній агресії, а також адаптації методів управління військами до умов гібридної війни. Перспективним напрямом є інтеграція технологій штучного інтелекту у сферу військового управління та розвиток інноваційних підходів до підготовки військовослужбовців, що дасть змогу підвищити їхню стійкість і готовність до динамічних умов сучасних конфліктів.

Перелік джерел посилання

1. Глущенко О. Функція забезпечення безпеки держави в умовах воєнного стану. *Часопис Київського університету права*. 2023. № 1. С 53–56. DOI: https://doi.org/10.36695/2219-5521.1.2023.10.

2. Дикун В., Мороз В., Стасюк В. Методологія дослідження морально-психологічного стану особового складу військ (сил) : навч. посіб. Київ : 7БЦ, 2023. 383 с. URL: https://surl.lt/pypwdf (дата звернення: 25.08.2025).

3. Загуменна Ю., Сокуренко В. Національна безпека України в умовах воєнного стану: теоретико-правовий аналіз. *Вісник Національної академії правових наук України*. 2024. Т. 31. № 2. С. 114–138. DOI: https://doi.org/10.31359/1993-0909-2024-31-2-114.

4. Про Національну гвардію України : Закон України від 13.03.2014 р. № 876-VII. URL: https://surl.li/shrmjm (дата звернення: 25.08.2025).

5. Ковальова Т. Нормативно-правове забезпечення антикорупційного законодавства під час дії воєнного стану в секторі безпеки та оборони. *Науковий вісник КІ НГУ*. 2024. № 2. С. 103–107. DOI: https://doi.org/10.59226/2786-6920.2.2023. 103-107.

6. Корнієнко Д., Толстоносов Д. Удосконалення організаційно-правових засад діяльності Національної гвардії України по забезпеченню громадської безпеки. *Право і суспільство*. 2020. Т. 1. № 6-2. С. 208–213. DOI: https://doi.org/10.32842/2078-3736/2020.6.2.1.31.

7. Медвідь Л. П., Симчукевич Ю. В. Правові аспекти застосування сил оборони під час воєнного стану. *Науковий вісник Ужгородського національного університету. Право*. 2024. Т. 2. № 82. С. 216–221. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.34.

8. Про забезпечення надійності й безпечної експлуатації будівель, споруд та інженерних мереж : Постанова Кабінету Міністрів України від 05.05.1997 р. № 409. URL: https://surl.li/qnrhhc (дата звернення: 25.08.2025).

9. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://surl.li/kkzrje (дата звернення: 25.08.2025).

10. Севрук І., Соколовська Ю. Морально-етичні аспекти діяльності цивільних та військових на території країни, що зазнала військової агресії: український досвід. *Вісник Львівського університету. Філософсько-політологічні студії*. 2022. № 41. С. 78–87. DOI: https://doi.org/10.30970/PPS.2022.41.11.

11. Ситник Г. Організаційно-правові засади забезпечення воєнної безпеки України : курс лекцій. Київ : САК Лтд, 2023. 112 с. URL: https://surl.li/vgxzxo (дата звернення: 25.08.2025).

12. Федорчук-Мороз В., Бондарчук Л. Безпека праці в контексті впливу окремих чинників психічного здоров'я працівників в умовах воєнного стану. *Науковий вісник ДонНТУ*.

2023. № 2 (11). С. 161–169. DOI https://doi.org/10.31474/2415-7902-2023-2-11-161-169.

13. Фівкін П. Теоретико-прикладні проблеми діяльності військових адміністрацій в Україні. *Юридичний науковий електронний журнал*. 2024. № 5. С. 355–360. DOI: https://doi.org/10.32782/2524-0374/2024-5/88.

References

1. Hlushchenko O. (2023). *Funktsiia zabezpechennia bezpeky derzhavy v umovakh voiennoho stanu* [The function of ensuring the security of the state in conditions of martial law]. *Chasopys Kyivskoho universytetu prava*, no. 1, pp. 53–56. DOI: https://doi.org/10.36695/2219-5521.1.2023.10 [in Ukrainian].

2. Dykun V., Moroz V., Stasiuk V. (2023). *Metodolohiia doslidzhennia moralno-psykholohichnoho stanu osobovoho skladu viisk (syl)* [Methodology for researching the moral and psychological state of military personnel (forces)]. Kyiv : 7BTs. Retrieved from: https://surl.lt/pypwdf (accessed 25 August 2025) [in Ukrainian].

3. Zahumenna Yu., Sokurenko V. (2024). *Natsionalna bezpeka Ukrainy v umovakh voiennoho stanu: teoretyko-pravovyi analiz* [National security of ukraine under martial law: theoretical and legal analysis]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*, no. 31 (2), pp. 114–138. DOI: https://doi.org/10.31359/1993-0909-2024-31-2-114 [in Ukrainian].

4. *Zakon Ukrainy "Pro Natsionalnu hvardiiu Ukrainy" № 876-VII* [Law of Ukraine about the National Guard of Ukraine activity no. 876-VII]. (2014, March 13). Retrieved from: https://zakon.rada.gov.ua/laws/show/876-18#Text (accessed 25 August 2025) [in Ukrainian].

5. Kovalova T. (2024). *Normatyvno-pravove zabezpechennia antykoruptsiinoho zakonodavstva pid chas dii voiennoho stanu v sektori bezpeky ta oborony* [Current issues of regulatory and legal security of anti-corruption legislation during the effect of martial status in the sector of security and defense]. *Naukovyi visnyk KI NHU*, no. 2, pp. 103–107. DOI: https://doi.org/10.59226/2786-6920.2.2023.103-107 [in Ukrainian].

6. Korniienko D., Tolstonosov D. (2020). *Udoskonalennia orhanizatsiino-pravovykh zasad diialnosti Natsionalnoi hvardii Ukrainy po zabezpechenniu hromadskoi bezpeky* [Improvement of the organizational and legal framework of the National Guard's of Ukraine activities to ensure public security]. *Pravo i suspilstvo*, no. 6, pp. 208–213. DOI: https://doi.org/10.32842/2078-3736/2020.6.2.1.31 [in Ukrainian].

7. Medvid L. P., Symchukevych Yu. V. (2024). *Pravovi aspekty zastosuvannia syl oborony pid chas voiennoho stanu* [Legal aspects of the application of the defense forces during the state of martial]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: pravo*, vol. 2 (82), pp. 216–221. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.34 [in Ukrainian].

8. *Postanova Kabinetu Ministriv Ukrainy "Pro zabezpechennia nadiinosti y bezpechnoi ekspluatatsii budivel, sporud ta inzhenernykh merezh" № 409* [Resolution of the Cabinet of Ministers of Ukraine "On ensuring the reliability and safe operation of buildings, structures and engineering networks" activity no. 409]. (1997, May 5). Retrieved from: https://surl.li/qnrhhc (accessed 25 August 2025) [in Ukrainian].

9. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 2469-VIII* [Law of Ukraine about the National Security of Ukraine activity no. 2469-VIII]. (2018, June 21). Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 25 August 2025) [in Ukrainian].

10. Sevruk I., Sokolovska Yu. (2022). *Moralno-etychni aspekty diialnosti tsyvilnykh ta viiskovykh na terytorii krainy, shcho zaznala viiskovoi ahresii: ukrainskyi dosvid* [Moral and ethical aspects of civil and military activities on the territory of a country subjected to military aggression: Ukrainian experience]. *Visnyk Lvivskoho universytetu. Seriia: filosofsko-politolohichni studii*, vol. 41, pp. 78–87. DOI: https://doi.org/10.30970/PPS.2022.41.11 [in Ukrainian].

11. Sytnyk H. (2023). *Orhanizatsiino-pravovi zasady zabezpechennia voiennoi bezpeky Ukrainy* [Organizational and legal principles of ensuring military security of Ukraine]. Kyiv : SAK Ltd. Retrieved from: https://surl.li/abzlmw (accessed 25 August 2025) [in Ukrainian].

12. Fedorchuk-Moroz V., Bondarchuk L. (2023). *Bezpeka pratsi v konteksti vplyvu okremykh chynnykiv psykhichnoho zdorovia pratsivnykiv v umovakh voiennoho stanu* [Occupational safety in the context of the impact of individual factors on mental health of workers in times of war]. *Naukovyi visnyk DonNTU*, vol. 2 (11), pp. 161–169. DOI:

https://doi.org/10.31474/2415-7902-2023-2-11-161-169 [in Ukrainian].

13. Fivkin P. (2024). *Teoretyko-prykladni problemy diialnosti viiskovykh administratsii v Ukraini* [Theoretical and applied problems of the military administration in Ukraine]. *Yurydychnyi naukovyi elektronnyi zhurnal,* no. 5, pp. 355–360. DOI: https://doi.org/10.32782/2524-0374/2024-5/88 [in Ukrainian].

Стаття надійшла до редакції / Received: 10.09.2025
Прорецензовано / Revised: 23.09.2025
Схвалено до друку / Accepted: 30.09.2025

ROMASHKO Oleh
Senior Lecturer, Department of State Security,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-1601-1591

WAYS TO ENHANCE THE SECURITY OF MILITARY ACTIVITIES UNDER THE LEGAL REGIME OF MARTIAL LAW

The article examines the key problems of ensuring the security of military activities under the legal regime of martial law. Based on the analysis of current regulatory acts and scientific publications, it is established that legislative regulation remains fragmented, the level of cybersecurity of critical infrastructure is insufficient, risk management lacks a comprehensive approach, and the psychological training of military personnel requires systematic improvement. External and internal threats are identified, including hybrid forms of warfare, information and psychological operations, and cyberattacks that significantly affect the state's defense capability. As a result of the study, the following ways to enhance the security of military activities have been identified: improvement of the regulatory framework in line with international standards, development of interagency coordination, strengthening of cyber defense, modernization of technical equipment, and expansion of psychological support programs for personnel. The obtained results are important for strengthening Ukraine's defense capacity, ensuring the resilience of critical infrastructure, and reducing risks in the modern context of hybrid warfare. Prospects for further research are related to the development of models for assessing military risks and the integration of artificial intelligence technologies into the field of security.

Keywords: *martial law; military activity; risks; threats; military personnel; regulatory acts; information and psychological operations; security; cybersecurity.*