СЛУЖБА БЕЗПЕКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ТРЕНІНГОВИЙ ЦЕНТР
ОПЕРАТИВНО-БОЙОВОЇ ПІДГОТОВКИ

ОПЕРАТИВНО-БОЙОВА ДІЯЛЬНІСТЬ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В УМОВАХ ВОЄННОГО СТАНУ

Матеріали Всеукраїнської науково-практичної конференції

ВИПУСК 2

Київ
2025

УДК 351.86(06)
О-60

Рекомендовано до друку навчально-науковим тренінговим центром оперативно-бойової підготовки (протокол № 10 від 13 листопада 2025 року)

Оперативно-бойова діяльність сил сектору безпеки і оборони
О-60 в умовах воєнного стану : матеріали Всеукраїнської науково-практичної конференції (м. Київ, 30 жовт. 2025 р.). Київ : НА СБУ, 2025. Вип. 2. 257 с.

До збірника увійшли матеріали Всеукраїнської науково-практичної конференції представників сектору безпеки і оборони України, наукових та науково-педагогічних працівників, здобувачів освіти та інших зацікавлених осіб. На науковому заході розглядались такі напрямки: підготовка кадрів для потреб сил сектору безпеки і оборони в сучасних умовах; міжвідомча взаємодія у рамках реалізації заходів із забезпечення національної безпеки і оборони; безпека та захист об’єктів національної критичної інфраструктури; досвід бойового застосування сил оборони при відсічі збройної агресії рф; питання психологічного забезпечення військовослужбовців при виконанні оперативно-бойових завдань в районі проведення бойових дій; застосування стратегічних комунікацій у діяльності сил сектору безпеки і оборони (цивільно-військове співробітництво, інформаційні та психологічні операції); особливості організації спеціальної фізичної підготовки військових формувань та правоохоронних органів; застосування роботизованих систем при виконанні оперативно-бойових завдань та інші питання, пов’язані з напрямами науково-практичної конференції.

Збірник матеріалів буде корисним для здобувачів вищої освіти, аспірантів, наукових співробітників, співробітників сил безпеки і оборони України.

Автори несуть повну відповідальність за підбір, точність наведених фактів, цитат, галузевої термінології, власних імен та інших відомостей.

УДК 351.86(06)

ЗМІСТ

ВІТАЛЬНЕ СЛОВО

ВИСТУПИ УЧАСНИКІВ МІЖВІДОМЧОГО КРУГЛОГО СТОЛУ

1 ПІДГОТОВКА КАДРІВ ДЛЯ ПОТРЕБ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В СУЧАСНИХ УМОВАХ

2 МІЖВІДОМЧА ВЗАЄМОДІЯ У РАМКАХ РЕАЛІЗАЦІЇ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ

ВІТАЛЬНЕ СЛОВО

ректора Національної академії Служби безпеки України, доктора юридичних наук, професора Андрія ЧЕРНЯКА

Шановні учасники та гості конференції!

Від імені ректорату та науково-педагогічного складу Національної академії Служби безпеки України щиро вітаю Вас із проведенням Всеукраїнської науково-практичної конференції, присвяченої актуальним проблемам оперативно-бойової діяльності сил сектору безпеки і оборони в умовах воєнного стану.

Сьогодні, коли наша держава продовжує боротьбу за незалежність і територіальну цілісність, особливого значення набуває об'єднання наукового потенціалу, професійного досвіду та практичних напрацювань представників сектору безпеки й оборони. Участь у конференції дозволяє фахівцям обговорити найактуальніші виклики, визначити пріоритети розвитку системи національної безпеки та виробити практичні рекомендації для підвищення ефективності оперативно-бойової діяльності.

Попри заочний формат заходу, Ваша участь свідчить про активну позицію, готовність до співпраці й прагнення до наукового пошуку рішень, які сприятимуть зміцненню обороноздатності держави. Впевнений, що представлений досвід, інформаційно-аналітичний аналіз та результати досліджень стануть цінним внеском у спільну справу захисту України.

Бажаю учасникам конференції плідної роботи, наукового натхнення та нових здобутків на благо нашої держави.

Слава Україні!

1 ПІДГОТОВКА КАДРІВ ДЛЯ ПОТРЕБ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В СУЧАСНИХ УМОВАХ

БАБСЬКИЙ В. В.,
кандидат військових наук,
Національна академія Служби безпеки України

БАЗОВА ЗАГАЛЬНОВІЙСЬКОВА ПІДГОТОВКА. ДОСВІД І РОЗВИТОК

Кожна армія світу має власну систему тренувань, але мета у всіх однакова – зробити солдата готовим до реальних викликів сучасної війни. Військова підготовка сьогодні виходить далеко за межі маршів чи стрільб. Вона охоплює фізичну витривалість, психологічну стійкість, знання сучасної техніки й уміння діяти у складних умовах.

В умовах правового режиму воєнного стану комплектування Збройних Сил України (далі ЗС України) здійснюється з метою нарощування бойового потенціалу та створення резервів підготовленого особового складу для доукомплектування військових частин, у тому числі й покриття бойових втрат. При цьому, важливо не лише підтримувати достатній рівень укомплектованості військовослужбовцями, але і створити умови для гарантованого та якісного комплектування ЗС України професійним, підготовленим і вмотивованим персоналом, спроможним якісно виконувати завдання за призначенням [1].

Із повномасштабним вторгненням російської федерації в Україні було призупинено призов на строкову військову службу. Поповнення бойових втрат проводиться за рахунок мобілізації громадян України, які мають на теперішній час військову підготовку. Але ресурси вичерпуються і система стикнулася із необхідністю підготовки резервів, які-б мали певні навченості для виконання бойових завдань. Так в Україні виникла необхідність введення базової загальновійськової підготовки (далі – БЗВП) студентів закладів вищої освіти, яка була затверджена на державному рівні [2].

Відповідно до типової програми БЗВП [3], заклади вищої освіти вже проводять заняття з теоретичної підготовки БЗВП. Під час теоретичної підготовки студенти мають засвоїти правила поводження зі зброєю та боєприпасами; порядок орієнтування на місцевості і переміщення на полі бою різними способами; порядок надання тактичної догоспітальної допомоги; порядок інженерного обладнання та маскування позицій, в тому числі з урахуванням захисту від можливого застосування противником малорозмірних БпЛА (дронів-камікадзе) та тепловізійних пристроїв тощо. Теоретичні навички мають стати основою для подальшого практичного навчання студентів.

Наступний етап підготовки – практичний, де студенти мають відпрацьовувати навички ведення вогню з індивідуальної зброї, метання ручних гранат, обладнування та маскування вогневих позицій, виконання заходів щодо захисту від малорозмірних БпЛА (дронів-камікадзе) та тепловізійних пристроїв противника, долання інженерних, мінно-вибухових загороджень, мають навчитися надавати психологічну самодопомогу, надавати першу медичну допомогу, комунікувати в колективі, виконувати бойові завдання в різних умовах обстановки, діяти у складі бойової групи та відділення, застосовувати засоби окопного РЕБ на рівні користувача, виявляти та критично сприймати дезінформацію та маніпуляцію, які здійснюються противником шляхом застосування різних каналів комунікацій. Всі ці навички мають налаштувати майбутнього захисника країни виконати поставлене бойове завдання з усім багажем знань, який він отримав під час БЗВП.

Практична підготовка – це важлива складова, якій надається велике значення. Передбачається, що вона має проходити у центрах підготовки ЗС України. Наразі ці центри готують за програмою БЗВП мобілізованих громадян України, які відразу направляються для подальшого проходження військової служби у бойові підрозділи.

У центрах підготовки має бути певна кількість інструкторів із розрахунку один інструктор на 10 студентів [2]. Зважаючи на кількість студентів, які проходять теоретичну підготовку БЗВП, виникає необхідність враховувати досвід, наприклад, Сполучених штатів Америки [4] щодо формування штатів таких центрів. Для забезпечення підготовки необхідного потенційного призовного контингенту навчальні центри армії США укомплектовані штатами, які перевищують потреби підготовки особового складу професійної армії мирного часу. Вважається, що цих додаткових «потужностей» досить для випуску першої партії в 200 тис. (громадян США) підготовлених солдатів і сержантів вже через 90–120 днів після оголошення мобілізації.

Відповідно до діючої програми БЗВП ми отримаємо фахівців, які зможуть виконувати завдання щодо оборони держави в окопах. Але на полі бою потрібні не тільки стрілки (ВОС-100), а й інші військові фахівці, наприклад, зв'язківці, сапери, артилеристи, оператори безпілотних систем, механіки-водії бронетехніки, яка, доречи, у ЗС України дуже різноманітна.

Під час проходження БЗВП мобілізованими проводиться і певна фахова підготовка. Адже програма БЗВП – це не догма. Це лише інструмент, за допомогою якого треба зробити з військовослужбовця класного «бойовика». І програма має використовуватися творчо, креативно, з урахуванням підготовки інструкторів. Тому центри мають можливість коригувати зміст програми.

Тобто інструктор, який знає, що його військовослужбовець йде після випуску, наприклад, у інженерну бригаду – зробить акцент на інженерній підготовці. Якщо військовослужбовець йде, наприклад, в

Десантно-штурмові війська, інструктор більше викладатиме тактику застосування, вогневу підготовку. Рішенням інструктора чи командира навчального центру коригується програма з урахуванням того, для кого готують цих військовослужбовців [5].

З часом, навіть дуже гарний фахівець втрачає отримані навички. Розуміючи, що навчені військовій справі студенти не підуть одразу до лав Збройних Сил, виникає необхідність передбачити заходи щодо підтримання навченості військового резерву. Тут потрібно переймати досвід країн, які вже мають таку систему. Резервісти Ізраїлю призиваються на військову службу строком на один місяць щороку [4]. Така ж система допідготовки резервів існує у Франції та Швейцарії.

Військова підготовка – це не лише вправи на полігоні. Це процес, який формує бійця як особистість. Базова загальновійськова підготовка вчить людину довіряти побратимам, не губитися у критичних ситуаціях і відповідати за свої рішення. Військовий вишкіл робить армію сильнішою, бо добре навчені солдати – це основа безпеки будь-якої держави. І цей процес має постійно удосконалюватися із врахуванням бойового досвіду.

Список використаних джерел:

1. Георгадзе О. А., Савчук Д. В. Часткова методика оцінювання укомплектованості військової частини військовослужбовцями // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України 2024. № 3(83). С. 117–121. URL: https://doi.org/10.33099/2304-2745/2024-3-83/117-121.
2. Про затвердження Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських : Постанова Кабінету Міністрів України від 21 червня 2024 р. № 734.
3. Типова програма навчальної дисципліни «Базова загальновійськова підготовка громадян України, які здобувають вищу освіту, та поліцейських» (теоретична частина). Затверджена Начальником Генерального штабу Збройних Сил України 24.02.2025 року. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/2025/02/24/typova-prohrama-navch-dystsypliny-bzvp-vo-24-02-2025.pdf.
4. Савинець О. Ю. Іноземний досвід комплектування збройних сил. Науковий вісник Ужгородського національного університету. Право. Випуск 51. Том 2. С. 34–38. URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/0fc7d39f-66eb-43ab-9d2f-d85cab089381/content.
5. «Країни-партнери “полюють” за нашою програмою БЗВП»: як адаптується система підготовки у ЗСУ. URL: https://armyinform.com.ua/ 2025/11/11/krayiny-partnery-polyuyut-za-nashoyu-programoyu-bzvp-yak-adaptuyetsya-systema-pidgotovky-u-zsu/.

ВІСЛОВУХ В. А.,
кандидат юридичних наук,
Національна академія Служби безпеки України

ОСОБЛИВОСТІ ОСВІТНЬОЇ ДІЯЛЬНОСТІ НАУКОВО-ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ ЗА ДОПОМОГОЮ АВТОМАТИЗОВАНОГО РОБОЧОГО МІСЦЯ (АРМ) В УМОВАХ ВОЄННОГО СТАНУ

Сучасні умови воєнного стану в Україні вимагають від системи вищої військової освіти високого рівня адаптивності, технологічної гнучкості та інноваційності у здійсненні освітнього процесу. Науково-педагогічні працівники вищих військових навчальних закладів (ВВНЗ) опинилися в ситуації, коли традиційні форми організації освітньої діяльності потребують трансформації відповідно до нових безпекових, організаційних та комунікаційних викликів. Одним із ефективних інструментів забезпечення безперервності освітнього процесу, підвищення його ефективності та оперативності управління навчальною інформацією виступає ***автоматизоване робоче місце (АРМ)*** науково-педагогічного працівника.

Використання АРМ сприяє оптимізації планування навчального навантаження, удосконаленню контролю знань курсантів, веденню електронної документації, підвищенню якості зворотного зв'язку між викладачем і слухачами. В умовах воєнного стану, коли частина освітнього процесу здійснюється у змішаному або дистанційному форматі, функціональні можливості АРМ набувають стратегічного значення для підтримки безперервності підготовки військових фахівців. Тож, актуальність дослідження зумовлена необхідністю комплексного аналізу особливостей освітньої діяльності науково-педагогічних працівників ВВНЗ за допомогою автоматизованих систем управління освітнім процесом в умовах воєнного стану [1, с. 107; 2, с. 21].

Автоматизоване робоче місце (АРМ) науково-педагогічного працівника є складовим елементом сучасного інформаційно-освітнього середовища вищого військового навчального закладу. Воно являє собою комплекс апаратно-програмних засобів, що забезпечують інтегровану підтримку освітньої, наукової та організаційно-методичної діяльності викладача. Основною метою створення та функціонування АРМ є підвищення ефективності управління навчальним процесом, автоматизація рутинних операцій, зменшення часу на підготовку звітної документації та забезпечення оперативного доступу до навчальної інформації.

Структура АРМ включає програмне забезпечення (системи управління навчальним контентом, текстові й табличні редактори, засоби

комунікації), бази даних освітніх матеріалів і результатів навчання, а також комунікаційні модулі для взаємодії з курсантами та адміністрацією закладу. Важливим аспектом функціонування АРМ є інтеграція з корпоративними системами управління навчальним процесом (LMS – Learning Management System) та внутрішніми обліково-аналітичними платформами (ERP – Enterprise Resource Planning), що дозволяє забезпечити єдиний інформаційний простір ВВНЗ.

Основні функції АРМ охоплюють: планування навчальних занять і навантаження, ведення електронних журналів успішності, формування звітності, облік відвідуваності, організацію електронного документообігу, а також комунікацію з курсантами через інтерактивні платформи. Таким чином, АРМ виступає інструментом цифрової трансформації освітнього процесу, який підвищує прозорість, структурованість та контрольованість усіх етапів підготовки військових фахівців [3].

Науково-педагогічні працівники є центральною ланкою у процесі впровадження та ефективного функціонування автоматизованих робочих місць у вищих військових навчальних закладах. Від рівня їхньої цифрової грамотності, педагогічної гнучкості та готовності до інновацій залежить результативність застосування інформаційних технологій у військовій освіті.

Одним із ключових аспектів є адаптація викладачів до цифрового формату роботи, що передбачає не лише оволодіння технічними навичками користування АРМ, а й перебудову педагогічних підходів відповідно до нових можливостей цифрового середовища. Підвищення рівня цифрової компетентності викладацького складу є передумовою ефективної реалізації освітніх програм у дистанційному та змішаному форматах, особливо в умовах воєнного стану.

Серед основних педагогічних переваг використання АРМ можна виокремити: індивідуалізацію навчального процесу через доступ до персоніфікованих даних курсантів; оперативний контроль знань і можливість швидкого зворотного зв’язку; аналітичне опрацювання результатів навчальної діяльності для підвищення якості підготовки. Водночас, існують і проблемні аспекти, пов’язані з експлуатацією АРМ: технічні збої, ризики кіберзагроз та витоку інформації, а також психологічна втома викладачів від постійної взаємодії з цифровими платформами.

Тому, ефективне використання автоматизованого робочого місця у ВВНЗ потребує не лише технічного удосконалення системи, але й системної роботи над розвитком цифрової культури та педагогічної адаптивності науково-педагогічних працівників, що виступають провідниками цифрових змін у сфері військової освіти [4, с. 29–30].

В умовах воєнного стану освітній процес у ВВНЗ реалізується переважно у *гібридному та дистанційному форматах*, що забезпечує безперервність навчання й гнучкість у взаємодії між усіма учасниками. Ключовим завданням стає захист інформації та кібербезпека при роботі з

АРМ, адже освітні ресурси часто містять дані обмеженого доступу. Тому важливим є використання захищених каналів зв'язку, автентифікації користувачів і резервного копіювання даних.

Особливе значення має налагодження *ефективної комунікації* між викладачами, курсантами та командуванням, що здійснюється через цифрові платформи. Водночас у процесі навчання необхідно враховувати психолого-педагогічні чинники, зокрема підвищене емоційне навантаження та стресові ситуації, характерні для воєнного періоду. Саме тому діяльність викладача спрямовується не лише на передачу знань, а й на підтримку морально-психологічної стійкості курсантів [2, с. 24].

Важливо зазначити, що ефективне впровадження автоматизованих робочих місць у вищих військових навчальних закладах потребує системного організаційно-методичного забезпечення, яке охоплює нормативно-правові, технічні та педагогічні аспекти. Визначальним елементом є нормативно-правова база, що включає накази Міністерства оборони України, положення про інформаційно-освітнє середовище, стандарти вищої військової освіти, а також відомчі регламенти щодо захисту інформації та використання автоматизованих систем. Ці документи встановлюють правила функціонування АРМ, порядок доступу користувачів, вимоги до технічного оснащення та безпеки даних.

Важливу роль відіграють методичні рекомендації щодо розроблення, впровадження та експлуатації АРМ у діяльності науково-педагогічних працівників. Вони мають містити інструктивно-технологічні карти користування системою, алгоритми взаємодії між підрозділами, моделі інтеграції з іншими інформаційними ресурсами та приклади кращих практик цифровізації освітнього процесу.

Не менш значущою є роль керівництва ВВНЗ у формуванні єдиного цифрового середовища. Адміністративні структури повинні забезпечувати координацію процесів автоматизації, організовувати підготовку кадрів, сприяти підвищенню цифрової компетентності викладачів, а також контролювати ефективність використання АРМ у навчальному процесі. Створення інтегрованого цифрового простору на рівні закладу освіти дозволяє підвищити якість управління освітньою діяльністю, сприяє уніфікації процесів і забезпечує інформаційну безпеку в умовах воєнного стану [5].

Слід вказати, що використання автоматизованого робочого місця науково-педагогічного працівника у вищих військових навчальних закладах довело свою ефективність як інструмент підвищення керованості, прозорості та оперативності освітнього процесу. Завдяки автоматизації планування занять, веденню електронних журналів, формуванню звітності та контролю навчальних досягнень курсантів відбувається суттєве скорочення часових витрат викладачів на рутинні операції. Це, у свою чергу, дозволяє зосередити увагу на методичній і

науковій складовій діяльності, підвищуючи якість підготовки військових фахівців.

Ефективність АРМ проявляється також у підвищенні прозорості оцінювання та покращенні зворотного зв'язку між викладачем і курсантом. Система дає змогу накопичувати й аналізувати освітні дані, що сприяє прийняттю обґрунтованих управлінських рішень на рівні кафедр та навчальних підрозділів.

Однією з ключових вимог до сучасного АРМ є наявність автономного енергозабезпечення. Для цього доцільно передбачати системи безперебійного живлення, резервні генератори, а також програмні механізми збереження даних у хмарних сховищах.

Перспективи розвитку автоматизованих систем у військовій освіті пов'язані з інтеграцією технологій штучного інтелекту, аналітичних модулів моніторингу успішності та персоналізації навчання. Використання інтелектуальних алгоритмів дає змогу прогнозувати результати навчальної діяльності, своєчасно виявляти проблемні зони та індивідуалізувати освітні траєкторії курсантів. У перспективі це сприятиме формуванню адаптивного навчального середовища, здатного швидко реагувати на зміни умов служби та потреб оборонного сектору.

Ключовим напрямом розвитку є підготовка кадрів нового типу – цифрово грамотних офіцерів-педагогів, які володіють сучасними технологіями обробки даних, аналітичного мислення та педагогічної гнучкості. Такі фахівці здатні ефективно поєднувати військову підготовку з цифровими підходами до навчання, що відповідає стратегічним завданням модернізації системи військової освіти України [3].

Отже, автоматизоване робоче місце (АРМ) науково-педагогічного працівника є важливим елементом цифрової трансформації вищої військової освіти, особливо в умовах воєнного стану. Його впровадження забезпечує підвищення ефективності управління навчальним процесом, зменшення адміністративного навантаження, удосконалення контролю знань і звітності, а також створює інтегроване інформаційне середовище для взаємодії між викладачами, курсантами та командуванням. Використання АРМ сприяє підвищенню прозорості оцінювання, оперативності прийняття управлінських рішень і безперервності освітнього процесу навіть за умов обмежених ресурсів.

Подальший розвиток системи АРМ передбачає розширення її функціональних можливостей шляхом інтеграції технологій штучного інтелекту, аналітичних інструментів моніторингу успішності та засобів персоналізації навчання. Це дозволить формувати адаптивне освітнє середовище й готувати офіцерів нового типу – цифрово компетентних, гнучких і здатних ефективно поєднувати військову та педагогічну діяльність у сучасних безпекових умовах.

Автоматизоване робоче місце науково-педагогічного працівника є необхідним елементом сучасної військової освіти, що забезпечує безперервність навчального процесу, стійкість до зовнішніх загроз,

ефективне управління освітньою діяльністю та взаємодію з курсантами у будь-яких умовах. Врахування досвіду НАТО та удосконалення енергетичної автономності АРМ є ключовими напрямами розвитку системи підготовки військових фахівців України у період воєнного стану.

Список використаних джерел:

1. Павлиш Т., Басараб В., Терещенко О., Рогів М. Цифровізація освітнього процесу в закладах вищої освіти в умовах воєнного стану. Освітні обрії. 2023. Т. 56 (1). С. 106–109. DOI: https: // doi.org / 10.15330 / obrii. 56.1.106–109.
2. Stanishovskyi A. The use of interactive methods in the training of tactical officers in military educational institutions. *Economics and Education*. 2022. № 7 (2). С. 20–25. DOI: https: // doi.org / 10.30525 / 2500–946X / 2022–2-3.
3. Ding L. – J., Li J. – M., Hui B. – H. Will Teacher-AI Collaboration Enhance Teaching Engagement? *Behavioral Sciences*. 2025. № 15 (7). DOI: https: // doi.org / 10.3390 / bs15070866.
4. Бобро Н. Цифровізація освіти в контексті формування університету нового покоління. *Український Педагогічний журнал*. 2025. № 2. С. 27–34. DOI: https: // doi.org / 10.32405 / 2411–1317–2025–2-27–34.
5. Messenger S., Trout J. The carlisle experience for distance learners: a powerful alternative: веб-сайт. URL: https: // warroom. armywarcollege. edu / articles / cedl/ (дата звернення: 27.10.2025).

ДЕМЧЕНКО О. М.,
Національна академія Служби безпеки України

АНАЛІЗ ПРОЦЕСУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ З ВИКОРИСТАННЯМ ОСВІТНІХ ТЕХНОЛОГІЙ

Abstract

The professional training of security sector specialists is a key factor in ensuring national security in Ukraine. This thesis analyzes the process of professional preparation at the National Academy of the Security Service of Ukraine, emphasizing the use of modern educational technologies such as digital platforms, blended learning, and simulation environments.

The study examines both theoretical and practical components of training, highlighting interactive and practical approaches, including case studies, operational simulations, and stress-resilient training scenarios. Integration of educational technologies enhances the development of critical thinking, analytical skills, and practical competencies necessary for effective performance in modern security contexts. The results demonstrate that implementing these methods improves training efficiency, strengthens readiness to respond to emerging threats, and contributes to the overall resilience of the national security system.

У сучасних умовах посилення загроз національній безпеці України, зростання ролі інформаційно-кібернетичного виміру безпеки та необхідності швидкого реагування на гібридні виклики, професійна підготовка фахівців сектору безпеки набуває стратегічного значення. Вищий навчальний заклад *контррозвідувального* спрямування – Національна академія Служби безпеки України (далі – НА СБУ) – виступає ключовим осередком формування кадрового резерву, який повинен бути готовим до виконання завдань оперативної, контррозвідувальної, інформаційної та кібербезпеки.

Професійна підготовка передбачає не лише оволодіння теоретичними знаннями, але й розвиток практичних навичок, критичного мислення, аналітичних здібностей та морально-психологічної стійкості. У цьому контексті використання сучасних освітніх технологій є необхідною умовою підвищення ефективності освітнього процесу та підготовки фахівців, здатних швидко і адекватно реагувати на загрози різного рівня. Застосування сучасних освітніх технологій в освітньому процесі фахівців сектору безпеки включає використання цифрових платформ, систем управління навчанням (*Learning management system – LMS*), змішаного навчання (*blended learning*), дистанційних курсів та симуляційних середовищ. Ці системи дозволяють викладачам створювати інтерактивні курси, контролювати засвоєння матеріалу, проводити онлайн-тестування та надавати зворотний зв’язок. Крім того, застосування LMS сприяє формуванню електронного освітнього середовища, у якому відбувається постійна взаємодія між викладачем і здобувачем освіти.

Одним із важливих аспектів є використання інтерактивних симуляційних платформ, де здобувачі вищої освіти можуть відпрацьовувати алгоритми реагування на кризові та оперативні ситуації у безпечному середовищі. Такі методи дозволяють формувати критичне мислення та навички прийняття рішень під тиском часу, що є критично важливим для фахівців безпекового сектору.

Процес професійної підготовки включає кілька ключових компонентів:

1. Структура освітньої підготовки – включає теоретичні курси з національної безпеки, міжнародного права, кібербезпеки та спеціальних дисциплін НА СБУ.
2. Методи навчання – лекції, семінари, кейс-стаді, практичні заняття на полігонах та лабораторні роботи з цифровими симуляторами.
3. Практична спрямованість – відпрацювання оперативних дій у моделях реальних ситуацій, участь у оперативно-тактичних навчаннях з оперативними підрозділами СБУ та силових структур.
4. Система оцінювання – комбіноване оцінювання знань та практичних навичок через тестування, симуляції та аналіз кейсів.

Використання технологій змішаного навчання дозволяє оптимізувати час на підготовку, поєднуючи дистанційні лекції та практичні

заняття. Особлива увага приділяється розвитку аналітичних здібностей та комунікаційних навичок. Наприклад, цифрові симулятори можуть відтворювати ситуації кібератак, в яких здобувачі вищої освіти аналізують загрози, приймають рішення та оцінюють наслідки своїх дій.

Практична спрямованість підготовки передбачає:

– відпрацювання навичок на спеціалізованих полігонах;

– участь у кризових навчаннях з реальними сценаріями;

– застосування кейс-методу для аналізу реальних ситуацій, що відбувалися в Україні та світі.

Інноваційні методи оцінювання включають моделювання оперативних подій, роботу з віртуальними середовищами, командні завдання та презентації рішень. Це дозволяє оцінювати не лише знання, а й здатність приймати оперативні рішення в умовах обмеженого часу та інформації.

Значну увагу приділено психологічній підготовці фахівців. Стресостійкість, здатність працювати в умовах високої напруженості та ефективна комунікація є невід'ємними складовими професійної компетентності. Використання освітніх технологій у цьому випадку включає симуляції конфліктних ситуацій та ігрові методики для розвитку емоційного інтелекту.

Подальший розвиток освітніх технологій у підготовці фахівців сектору безпеки передбачає інтеграцію штучного інтелекту для персоналізації освітнього процесу, застосування віртуальної та доповненої реальності для відпрацювання кризових сценаріїв, а також розвиток платформ для міжвузівської та міжнародної співпраці. Такі інновації дозволяють підвищити якість підготовки, скоротити час на оволодіння ключовими компетенціями та забезпечити високу адаптивність фахівців до умов сучасних загроз.

Впровадження освітніх технологій у професійну підготовку фахівців сектору безпеки є стратегічно важливим. Воно підвищує ефективність навчання, формує практичні навички, критичне мислення та готовність до дій у сучасних безпекових умовах.

Системний підхід до поєднання теоретичної та практичної підготовки дозволяє формувати висококваліфікованих фахівців, здатних ефективно реагувати на загрози національній безпеці та забезпечувати стабільність і обороноздатність держави.

Список використаних джерел:

1. Сліпенюк В. В., Клименко А. С. Удосконалення кадрового забезпечення СБУ в контексті реалізації політики національної безпеки України. Ефективність державного управління, 2023.
2. Як Національна академія СБУ навчає Сили оборони перемагати ворога. АрміяInform, 07 травня 2023.
3. Академія служби безпеки України Національна. Енциклопедія Сучасної України.
4. NATO Defence College. Education and Training for Security Sector Professionals: Best Practices. Rome: NDC, 2021.

5. European Commission. Digital Education Action Plan 2021–2027. Brussels: EC, 2021.
6. Богуш В. М., Бровко В. Д., Мамченко С. М. Підготовка фахівців з кібербезпеки у межах спеціальності 256 «Національна безпека». Київ : НА СБУ, 2021.

ДЯЧЕНКО А. А.,
Національна академія Служби безпеки України

ВИКОРИСТАННЯ ПРОГРАМНОГО ПРОДУКТУ MICROSOFT POWERPOINT ПІД ЧАС ПРОВЕДЕННЯ ЗАНЯТЬ З ВІЙСЬКОВОЇ ТОПОГРАФІЇ

Microsoft PowerPoint – це програма, що може містити текстові матеріали, фотографії, малюнки, слайд-шоу, звукове оформлення й дикторський супровід, відеофрагменти й анімацію, тривимірну графіку. Основною відмінністю презентацій від інших способів подання інформації є їхня особлива насиченість змістом й інтерактивність, тобто здатність певним чином змінюватися й реагувати на дії користувача.

При вивченні тем у військовій топографії (за виключенням практичних, польових занять) важко досягти реалістичності теоретичного матеріалу. Цього можна досягти за допомогою мультимедійної презентації.

Переваги програмного продукту Microsoft PowerPoint для військової топографії:

дозволяє демонструвати відзнятий раніше матеріал і дії курсантів;

дозволяє демонструвати відеосюжети;

вона дозволяє зменшити непродуктивні витрати живої праці викладача на пояснення того, що може бути зображено 1–2 слайдами;

дає здобувачам вищої освіти широкі можливості вільного вибору власного темпу і послідовності навчання при використанні презентацій у години самостійної підготовки;

припускає диференційований підхід до курсантів (слухачів);

підвищує оперативність й об’єктивність контролю й оцінки результатів навчання;

гарантує безперервний зв’язок у відносинах «викладач – здобувач вищої освіти»;

підвищує мотивацію навчання;

сприяє розвитку продуктивних, творчих функцій мислення, росту інтелектуальних здатностей, формуванню операційного стилю мислення. Презентація дозволяє підвищити успішність занять із використанням демонстраційних засобів і підвищити ймовірність переконання аудиторії на 43 %.

Для викладача:

зображення з екрана дозволяє дати візуальний ряд і не губити часу, відволікаючись на розбірливе написання тексту на дошці;

з появою нових матеріалів корегувати не весь курс, а конкретні слайди по певних темах;

для створення відеоматеріалів за допомогою Microsoft PowerPoint не обов'язково бути художником, шаблони дизайну забезпечують високу якість результату, а використання всіх можливостей Microsoft PowerPoint дозволяє створювати ефектні проекти.

Найбільш ефективною є інтерактивна мультимедійна презентація. У таких презентаціях реалізована можливість вибирати, як спосіб вивчення навчального матеріалу, так і ступінь подробиць викладення матеріалу, вони дозволяють адаптувати інформацію й забезпечити індивідуальний підхід до кожного здобувача вищої освіти. Презентації з переходами між різними слайдами дозволяють створити різні сценарії проведення заняття.

Вказівки по створенню ефективної презентації.

Перш ніж приступитися до роботи над презентацією, варто домогтися повного розуміння того, про що ви збираєтеся розповідати. У презентації не повинно бути нічого зайвого. Кожен слайд повинен являти собою необхідну ланку й працювати на загальну ідею презентації.

Користуйтеся готовими шаблонами при виборі стилю символів і кольорів. Не бійтеся творчого підходу. Експериментуйте при розміщенні графіки й створенні спецефектів.

Не перевантажуйте слайди зайвими деталями. Іноді краще замість одного складного слайда представити більше простіших. Не слід намагатися «заштовхати» в один слайд занадто багато інформації.

Додаткові ефекти не повинні перетворюватися в самоціль. Їх варто звести до мінімуму й використати тільки з метою привернути увагу глядача до ключових моментів демонстрації.

Звукові й візуальні ефекти в жодному разі не повинні виступати на передній план і затуляти корисну інформацію.

Мультимедійна презентація повинна мати наступні ознаки:

зручну систему навігації, що дозволяє легко переміщатися по презентації;

використання мультимедійних можливостей сучасних комп'ютерів й Інтернет (графічних вставок, анімації, звуку якщо необхідно й ін.);

розбивку заняття на невеликі логічно замкнуті блоки (слайди). Кожен слайд презентації повинен мати заголовок;

посилання на літературні джерела, електронні бібліотеки й на джерела інформації в мережі Інтернет;

доступність – швидке завантаження, без ускладнення ефектами.

Загалом у військовій топографії якісна мультимедійна презентація дозволяє інтенсифікувати навчальний процес і скоротити час для засвоєння матеріалу.

Список використаних джерел:

1. Intel®Навчання для майбутнього. Київ : Видавнича група BHV, 2024. 416 с.
2. Microsoft Power Point 2022. Крок за кроком : практ. посіб. / Пер. с англ. 416 с.
3. Хайбрейкен Дж. Вивчи PowerPoint за 10 хв.: Пер. с англ. Москва : Вид. дім «Вільямс», 2021. 192 с.
4. Ненси Дюартэ. Slide:ology. Мистецтво створення видатних презентацій. Київ : Манн Фербер, 2020. 288 с.

ПАНЧИШИН А. Б.,
викладач кафедри,
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

ПСИХОЛОГІЧНА ПІДГОТОВКА ВІЙСЬКОВОСЛУЖБОВЦІВ, ЯК ФАКТОР ПІДВИЩЕННЯ БОЄГОТОВНОСТІ ВІЙСЬК

Психологічна підготовка військовослужбовців є складовою військової підготовки та одним із основних її елементів, одним із базових елементів боєготовності підрозділів. В умовах триваючої з 2014 року гібридної російсько-української війни та, особливо, з початком в 2022 році повномасштабної збройної агресії росії, психологічна підготовка військовослужбовців займає ще більш важливе значення. Викликано в першу чергу це тим, що на даний момент Сили Оборони України на 80–90 % складаються не з професійних кадрових військових, а з осіб, які є добровольцями або мобілізованими у зв'язку із оголошенням воєнного стану. За таких умов удосконалення порядку проведення психологічної підготовки з врахуванням реалій сьогодення та передового досвіду армій країн світу на цьому напрямку набуло першочергової актуальності.

Відомо, що військова служба пов'язана з дією широкого спектру екстремальних чинників, що висуває підвищені вимоги до їх психологічних якостей. Кратно їх вплив посилюється в умовах війни та безпосередньої участі військовослужбовців у бойових діях та виконанні бойових завдань в умовах небезпеки для життя і безпосереднього зіткнення з противником. Сучасним бойовим діям притаманні граничний динамізм та небезпека бойових ситуацій, бойові дії часто доводиться вести проти переважаючих сил противника, в умовах реальної загрози одночасного використання противником різних видів озброєнь, за нестачі інформації про противника, в умовах відсутності звичайного чергування сну та відпочинку. Небезпека, перевантаження, перевищення межі людських можливостей, активність і вогонь противника, складність розв'язуваних завдань та необхідність граничної напруги всіх сил знижують бойову ефективність особового складу, провокуючи розвиток у військовослужбовців негативних психічних станів, проявами яких можуть бути невпевненість, пригніченість, апатія, розпач, приреченість,

занепокоєння, тривога та страх. Участь у бойових діях ставить до людини вимоги, що суперечать її інстинкту самозбереження, спонукає вчиняти дії всупереч природним потребам.

Окрім цього, військова служба характеризується існуванням та домінуванням формальних відносин над неформальними, жорсткою структурою на умовах субординації та специфіки цілей і завдань. Керівництво в армії засноване на принципах єдиноначальності, жорсткої військової дисципліни і субординації, військовій організації притаманні високий ступінь змін *(постійна кадрова плинність у підрозділах в результаті реорганізації, поповнення, бойових втрат, тощо*) і майже постійний високий рівень залучення до виконання завдань. Водночас вона також характеризується високою динамікою, невизначеністю та новизною ситуацій, суперечливістю або частковою відсутністю інформації, дефіцитом часу, тривогою та напруженістю, загрозою здоров'ю та життю, тобто чинниками, що є джерелами значного психічного навантаження та психічної напруги, вимагаючи від індивідуума досить високого рівня розвитку психологічної готовності та стресостійкості. Сучасні умови ведення бойових дій вимагають суттєвого перегляду системи психологічної підготовки військовослужбовців, де особливої важливості набуває питання формування психологічної готовності осіб, які обмежений проміжок часу проходять військову підготовку, до безпомилкового виконання бойових завдань, що будуть пов'язані з ризиком для життя. Розроблення сучасної моделі структури психологічної готовності до військової діяльності сприятиме належній підготовці особи до виконання обов'язків військової служби в умовах воєнного стану, сприятиме підвищенню боєготовності та мінімізації бойових втрат.

Відомо, що більшості мобілізованих військовослужбовців, які в цивільному житті не мали дотичності до військової служби, на першому етапі важко прийняти ряд аксіомних понять та принципів військової служби, зокрема таких як військова дисципліна, збільшені фізичні та психічні навантаження, втрата традиційної емоційної підтримки, публічність та зміна якості життя. В сучасних умовах до згаданих також додається вагомий стресовий чинник постійного перебування вказаної категорії осіб в умовах очікування подальшої участі в бойових діях, що досить часто формується на ґрунті короткотермінового терміну військової підготовки, недостатніх військових знать та навиків.

Зазначені чинники адаптації можуть досить сильно впливати на стан боєготовності як самого військовослужбовця, так і підрозділу загалом. За таких умов першочерговою в таких випадках є роль командира підрозділу, на якого покладається фактично основна функція первинної адаптації новобранця до умов військового життя. Командир підрозділу повинен володіти достеменною інформацією про морально-психологічний стан кожного підпорядкованого йому військовослужбовця. Безпосередній командир в першу чергу повинен проводити

індивідуальні бесіди з тими військовослужбовцями, які демонструють різні ознаки неадаптованої поведінки (страх, порушенні дисципліни, ухилення від виконання завдань, конфлікти з іншими, алкоголізм, симуляція, тощо) для з'ясування причин такої поведінки, після чого надавати допомогу такій особі, як порадою, так і психологічною допомогою. Якщо ж подібна поведінка притаманна більшій частині особового складу підрозділу, необхідно переглянути функціонування військової системи, частіше її командної структури. Варто зазначити, що найбільш критичний період адаптації мобілізованої особи – це перші декілька тижнів в армії, причому важливим є недопущення прояву неприйнятних форм поведінки загалом, а від командирів очікується високий ступінь розуміння чутливості новобранців до всього нового.

З огляду на такі специфічні ознаки військової служби та військової організації загалом, необхідно зокрема передбачити певний час для адаптації та подальшої психологічної підготовки мобілізованих, які зазвичай не мають навиків військової служби та розуміння сутності механізму функціонування військової організації загалом. При цьому слід також врахувати, що на даний час мобілізованими є як правило не дуже молоді особи (в середньому 40–55 і більше років), яким в силу віку важче адаптуватися до змін.

Загальна підготовка військових до бойових дій, поряд із забезпечення належної фізичної форми, технічною та тактичною підготовкою, в обов'язковому порядку повинна передбачати повноцінну загальну психологічну підготовку військовослужбовця. Основа належної підготовки – це навчання та тренування для здобуття практичних навиків, при цьому потрібно пам'ятати, що така підготовка має суттєве значення для психологічної готовності військовослужбовця і підвищення рівня стресостійкості, відчуття безпеки та впевненості військово-службовця у значній мірі залежить саме від якості такої підготовки. Водночас, загальна передбойова психологічна підготовка військових повинна охоплювати навчання та тренування з військової психології (подолання тривоги, страху, паніки під час бойових дій, іншим сталим стресовим воєнним факторам, їх запобіганню та подоланню).

Важливим фактором психологічної підготовки військових є їх детальне та належне (з урахуванням режиму секретності) інформування про план, основні цілі та заходи військової операції. Поінформованість військових про події, територію, просторово-часові орієнтири, сили супротивника, локації санітарних частин, бойову та логістичну підтримку, систему зв'язку, шляхи можливих напрямів відступу впливає на їх відчуття безпеки та готовність до боротьби. Для військових надзвичайно важлива вся доступна інформація про супротивника, оскільки таким чином зменшується страх невідомості, тому не існує виправдань для того, щоб цю інформаційну потребу вчасно не задовольнити. Чим більше деталей щодо території противника, його воєнної сили, звичок, слабкостей та переваг, чим конкретніші факти про

стан справ на території, де буде проходити військова операція, тим більше це сприятиме впевненості військових, що відповідає народній мудрості: «не такий страшний ворог, як його малюють».

Важливо також зазначити, що повинні бути різні підходи до проведення психологічних тренувань командира та рядового військовослужбовця, оскільки в першому випадку таке тренування (підготовка) повинно бути більш глибшим, з приділенням більшої уваги психології командування, лідерства, способам прийняття рішень, психології навчання мотивації, методам спостереження за психологічною бойовою готовністю бійця та підрозділу загалом, комунікації, моделям психологічної профілактики і допомоги рядовим під час психологічної кризи, основам ПСИОП, ПТСР, тощо.

Страх та бойовий стрес логічні та очікувані на полі бою, однак через їхній можливий потенційно руйнівний ефект їм необхідно присвятити окрему увагу в рамках загальної психологічної підготовки до бойових дій. Недостатня тренованість та підготовка військових, відсутність військового чи бойового досвіду, невпевнений непрофесійний командир, слабкі емоційні зв'язки та недостатність довіри між військовими загалом можуть провокувати появу страху на полі бою. Страх – це емоційна реакція на небезпеку, невідомість або загрозу, природний механізм, який може сприяти виживанню, оскільки допомагає уникнути небезпеки або ризику, це психологічний термін, який відображає емоційну реакцію, що виникає перед сприйняттям реальної або уявної небезпеки, це вроджений інстинкт, який допомагає людині виживати і підготовляє організм до можливих загроз. Страх активує нервову систему і наводить нас в стан тривоги, фізіологічні відповіді на страх включають підвищене серцебиття, прискорене дихання, підвищену пітливість, збудження м'язів та інші фізичні прояви, що підсилює нашу готовність до реагування на небезпеку.

Однак страх має і свої негативні наслідки, зокрема, хронічний стрес, спричинений тривожністю і постійним напруженням, може негативно впливати на фізичне і психічне здоров'я людини. Тому важливо розуміти страх і навчитися ефективно його керувати. Інтенсивне (довготривале) відчуття страху та неможливість його подолання – це серйозний стресогенний чинник, який призводить до відчуття загального виснаження, т.зв. «бойової втоми», відчуття безвольності, апатії, звуження сприйняття, зниження когнітивних функцій та інших симптомів бойового стресу та бойової ефективності загалом. Слід також пам'ятати, що бойові стресові реакції, окрім страху, можуть бути також викликані іншими чинниками: фізичними (втратою сну, дегідратацією, поганим харчуванням, тощо) або психосоціальними стресорами (сімейними, емоційними проблемами, нестачею відчуття єдності у підрозділі, недовірою до командира, соратників, тощо).

Заходи запобігання страху та бойового стресу є складовою частиною психологічної підготовки військовослужбовців до бойових дій.

Здатність контролювати страх та зменшення негативних наслідків стресу можна і потрібно тренувати. З досвідом контроль над страхом стає дедалі ефективнішим, але процес пристосування до умов бойового стресу слід починати набагато раніше від самих бойових дій і такий зокрема має передбачати:

• навчання, тобто вивчення природи, причин та симптомів стресу та страху, змін у психофізіологічному функціонуванні та їх значень;

• натренованість у виявленні страху та стресу – запровадження відвертого спілкування про страх та стрес, як звичайні прояви психології людини, що сприятиме розвитку спроможності до виявлення таких ознак в собі та в інших, як фактор «свідомого зіткнення» та правомірного реагування вже на першій стадії його появи; впровадження процесу «вентиляції» (зменшення внутрішньої напруги шляхом вербалізації особистого досвіду та переживань), використання бойового досвіду ветеранів;

• опанування технік заспокоєння та саморегуляції – техніки дихання, тренування м'язової релаксації та техніки заспокоєння, які сприяють контролю за фізичними та психічними процесами, що має особливе значення безпосередньо перед бойовими діями.

Техніки заспокоєння є насправді техніками саморегуляції психофізичного стану, які опираються на теорію Джемса-Ланге [1] щодо взаємного функціонування – взаємодії трьох систем: поведінкової, когнітивної та фізіологічної. Відповідно до цієї моделі, зміни у фізіологічному стані, зокрема шляхом введення в організм хімічних препаратів, призведуть до зміни поведінки та когнітивного функціонування, у той же час, зміни когнітивної складової (наприклад, зміни у мисленні) діятимуть на фізіологічному та поведінковому рівні, а зміни поведінки відобразяться на когнітивному стані та фізіології. Іншими словами, модель Ланге встановлює, що за допомогою окремих дій (поведінка) чи роздумів (когнітивна складова) можна впливати на фізіологічне функціонування, зокрема, що можливо свідомими діями регулювати власні тілесні функції. На цих твердженнях розвинулися і сьогодні мають широке застосування техніки та процеси саморегуляції психофізичного стану, якими досягається реакція розслаблення (Бенсон, 1975) [2]. В багатьох сучасних арміях світу практичну користь підтвердили такі техніки: дихальні вправи, вправи прогресивної м'язової релаксації, техніки креативної візуалізації, автогенний тренінг та різноманітні медитативні техніки, якими через спрямування уваги на певну дію, емоцію чи думку можна досягти відчуття заспокоєння, зокрема зменшити відчуття тривоги та страху.

В процесі удосконалення порядку та методів проведення психологічної підготовки військовослужбовців доцільно використати аналогічний досвід, який впроваджено у багатьох арміях світу. Так, в армії США для адаптації новобранців застосовуються:

• використання віртуальної реальності (VR) та симуляторів з використанням технології віртуальної реальності для тренування в різних сценаріях, що допомагає звикнути до стресових ситуацій та приймати швидкі та правильні рішення;

• використання біометричних даних для оцінки стану психічного здоров'я та відслідковування індивідуальних реакцій на стресові ситуації;

• навчання новобранців різним стратегіям управління стресом, контролю емоцій та підвищення концентрації у стресових ситуаціях (методи когнітивно-поведінкової терапії);

• психологічна підтримка через технології зв'язку, групові тренінги та діалоги.

Показовим також може бути організація психологічної підготовки військовослужбовців та резервістів в армії Ізраїлю (ЦАХАЛ), ключовими аспектами якої є психологічне тестування, тренінги з управління стресом та адаптацією, комунікації та конфліктології та тренінги з розвитку психологічної міцності та психологічна підтримка.

Підсумовуючи вищенаведене, слід зазначити, що удосконалення психологічної підготовки та підтримки в Збройних Силах України в умовах триваючої війни, поряд із професійним навчанням, є ключовим для покращення бойової ефективності та морального духу військових. Ось кілька можливих шляхів удосконалення цієї сфери:

• ширше впровадження психологічних тренінгів з управління стресом та розвитку психологічної стійкості;

• інтеграція психологічної підтримки в усі аспекти військової служби (навчання, повсякденні обов'язки, бойова діяльність)

• розвиток програм для адаптації новобранців та мобілізованих осіб до військової служби (тренування з комунікації, лідерства, психологічного відновлення).

• невідкладне посилення ролі психологів у військових підрозділах.

Вказані заходи, наряду із підвищенням бойового та професійного навчання особового складу, підвищенням мотивації та іншими заходами морально-психологічного та матеріального плану можуть допомогти покращити психологічну підготовку в Збройних Силах України, забезпечуючи військовослужбовцям необхідні методики для успішної адаптації та виконання своїх обов'язків у складних умовах війни.

Список використаних джерел:

1. Cannon, Walter «The James-Lange Theory of Emotions: A Critical Examination and an Alternative Theory». The American Journal of Psychology.
2. Г. Бенсон. «Реакция Релаксации» («The Relaxation Response», 1975. ISBN 978-0-688-02955-5.

ПЕРЕМИБІДА І. В.,
старший викладач кафедри УПДВ та ТЗ,
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

ПЕРЕМИБІДА Д. О.,
начальник НДЛ СОП НДВ РПВ НЦ СВ,
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

ЦИФРОВІЗАЦІЯ ПІДГОТОВКИ КАДРІВ ДЛЯ ПОТРЕБ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ЯК ПРОГРЕСИВНА ІННОВАЦІЙНА ТЕНДЕНЦІЯ СИСТЕМИ ВІЙСЬКОВОЇ ОСВІТИ

Забезпечення національної безпеки та обороноздатності України залишається одним із найважливіших завдань державної політики, особливо в умовах зростання як реальних, так і потенційних загроз [3]. Це вимагає постійного пошуку ефективних шляхів і механізмів для своєчасного виявлення, попередження та нейтралізації деструктивних чинників, а також для підтримання належного рівня оборонного потенціалу держави, здатного гарантувати її військову безпеку. Одним із ключових напрямів розв'язання цих завдань є підвищення якості професійної підготовки фахівців сектору безпеки й оборони, спрямованої на формування високого рівня бойової готовності особового складу військових формувань і правоохоронних органів, а також їхньої спроможності ефективно виконувати службово-бойові завдання.

На сьогодні система підготовки кадрів для сектору безпеки та оборони України здійснюється переважно за загальними освітніми стандартами, які не враховують специфіку цього напряму діяльності [2]. Такий підхід позбавлений власних, чітко визначених критеріїв оцінювання якості професійного навчання, що істотно знижує його ефективність. Навчальні програми нерідко перевантажені другорядним теоретичним матеріалом і надмірним обсягом навчального часу, тоді як реальні потреби сил безпеки залишаються поза увагою.

За цих умов постає нагальна потреба перегляду підходів до формування системи підготовки кадрів у секторі безпеки й оборони, що передбачає створення цілісної, інтегрованої моделі освіти для персоналу. Її зміст має поєднувати принципи спеціалізації та індивідуалізації навчання, бути зорієнтованим на підвищення професійного рівня особового складу та розвиток нової культури безпеки, побудованої відповідно до стандартів і цінностей Європейського Союзу та НАТО. Отже, на перший план виходить завдання оптимізації освітньої діяльності у межах сектору безпеки й оборони – шляхом підвищення практичної спрямованості, інтенсифікації навчального процесу, посилення бойової

підготовки за натівськими стандартами та розширення можливостей професійного зростання персоналу. Такий підхід має стати підґрунтям для підвищення якості кадрового забезпечення державних інституцій безпеки, що, своєю чергою, сприятиме зміцненню обороноздатності країни загалом. Саме ці фактори визначають актуальність проведення наукового дослідження, спрямованого на пошук оптимальних моделей підготовки фахівців у даній сфері [1].

Варто наголосити, що сектор безпеки та оборони України є складною системою, яка включає низку державних інституцій і відомств. До його складу входять: Збройні Сили України, Національна поліція, Національна гвардія, Державна прикордонна служба, Державна міграційна служба, Державна служба з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони, Державна служба спеціального зв'язку та захисту інформації, Державна спеціальна служба транспорту, розвідувальні органи, Рада національної безпеки і оборони та інші. Вважали за доцільне зосередити увагу не на деталізації окремих аспектів, а на виявленні загальних тенденцій і закономірностей, притаманних процесу підготовки кадрів для всього сектору безпеки й оборони загалом. Такий підхід дозволяє розглянути систему в її цілісності, простежити спільні проблеми, окреслити напрями модернізації та визначити шляхи підвищення ефективності професійного навчання майбутніх фахівців цієї стратегічно важливої галузі.

З огляду на сучасні виклики до системи військової освіти, актуалізується потреба у вдосконаленні підходів до підготовки майбутніх офіцерів для структур сектору безпеки та оборони в напрямі використання сучасних цифрових технологій. Це зумовлює необхідність осмислення та узагальнення напрацювань українських науковців у цій сфері, а також урахування впливу глобалізаційних та інтеграційних процесів, які змінюють характер військової освіти у світі.

Особливого значення набуває вивчення зарубіжного досвіду професійної підготовки кадрів у країнах, що розвиваються, адже саме вони мають багато спільних рис з Україною у соціально-економічному та військово-політичному вимірах. Ці країни також стикаються з подібними загрозами для національної безпеки – прикордонними конфліктами, проявами тероризму, сепаратизмом, транскордонною злочинністю, збройною агресією, гібридними війнами, політичною нестабільністю тощо. Аналіз їхнього досвіду дозволяє визначити ефективні моделі та тенденції, які можуть бути адаптовані для підвищення результативності підготовки військових фахівців в Україні.

Військова освіта України має власну унікальність, що полягає у її тісній інтеграції в загальнодержавну освітню систему та регулюванні як загальними, так і спеціалізованими нормативно-правовими актами. Водночас, у контексті триваючої збройної агресії російської федерації та зростання гібридних загроз національному суверенітету, виникає нага-

льна потреба в оновленні засад державної політики у сфері військової освіти й професійної підготовки військовослужбовців.

Йдеться, передусім, про необхідність перегляду існуючих підходів до здобуття військовими вищих освітніх ступенів і рівнів кваліфікації, розширення спектра освітніх і професійних компетентностей, а також поступовий перехід на освітні програми, узгоджені з вимогами країн-членів НАТО та їх партнерів. Вектор сучасних реформ у галузі військової освіти спрямований на адаптацію національних стандартів до вимог Північноатлантичного альянсу, зокрема в частині взаємного визнання дипломів військових навчальних закладів і результатів навчання.

Процес трансформації системи військової освіти відповідно до стандартів НАТО передбачає розв'язання низки комплексних завдань. Серед них – створення єдиної, цілісної системи підготовки військових фахівців з урахуванням найкращих практик держав-членів Альянсу; розбудова ефективної інтегрованої моделі професійної освіти; підготовка кадрів оперативного та стратегічного рівнів; розвиток лідерського потенціалу військовослужбовців через курси професійної військової освіти; реалізація принципу «освіта протягом усієї службової кар'єри». Важливим аспектом є й запровадження чіткої системи забезпечення якості навчання, що відповідає стандартам НАТО, та створення передумов для взаємного визнання кваліфікацій, здобутих у військових навчальних закладах держав-партнерів.

Особливого значення набуває інтеграція інноваційних технологій у процес підготовки військових фахівців. Саме інноваційність визначає спроможність системи освіти забезпечувати підготовку військовослужбовців, здатних ефективно діяти в умовах сучасного, динамічного й високотехнологічного бойового середовища. Перехід до більш гнучкої, індивідуалізованої моделі навчання, заснованої на використанні цифрових платформ, симуляційних систем і дистанційних технологій, сприяє не лише підвищенню якості та доступності освіти, але й розвитку необхідних компетентностей, критичного мислення та адаптивності особового складу.

У сучасних умовах дедалі більшої уваги набуває ідея створення синтетичних освітніх середовищ, які поєднують реальні й віртуальні компоненти навчання. Такі середовища розглядаються у двох площинах: як віртуальні освітні простори, побудовані на цифрових технологіях, та як інтегровані системи, що поєднують фізичне середовище навчання з елементами симуляції, моделювання та віртуальної взаємодії. Саме така модель дозволяє максимально наблизити процес підготовки військовослужбовців до реалій сучасного бою, підвищуючи рівень їхньої готовності до виконання професійних завдань.

Цифровізація військової освіти сьогодні виступає одним із ключових напрямів її модернізації та ефективного розвитку. Вона не зводиться лише до технічного оновлення чи впровадження електронних

засобів навчання – йдеться про глибоку трансформацію всієї системи освіти, спрямовану на підвищення інтелектуального потенціалу учасників освітнього процесу. Цифрові технології стають інструментом розвитку аналітичного мислення, здатності до сприйняття, опрацювання та створення інформації, що є визначальним чинником якості сучасної військової освіти.

Інтеграція цифрових рішень у систему військової освіти не лише оптимізує навчальний процес і підвищує ефективність управління, а й сприяє формуванню ключових компетентностей військовослужбовців, необхідних для успішної адаптації до викликів інформаційного суспільства. Цифрові інструменти дозволяють створювати інтерактивне, динамічне середовище, у якому майбутні офіцери та фахівці сектору оборони здобувають знання в умовах, максимально наближених до реалій бойової діяльності. Система військової освіти як об'єкт цифровізації має низку унікальних характеристик, що зумовлюють складність та специфіку цього процесу. Її багаторівнева структура, велика кількість навчальних закладів і підрозділів, територіальна розосередженість, а також багатопрофільність підготовки фахівців різних освітньо-кваліфікаційних рівнів вимагають комплексного підходу до цифрової трансформації. Військова освіта потребує збереження балансу між неперервністю, цілісністю та гнучкістю освітнього процесу, що є важливою умовою її стабільного функціонування.

Цифровізація передбачає використання сучасних технологій для вдосконалення кожного етапу освітньої діяльності – від планування навчальних програм до контролю результатів навчання. Її особливостями є:

висока складність системи підготовки, яка потребує постійного оновлення змісту навчальних програм відповідно до змін стандартів і вимог НАТО;

необхідність моделювання та аналізу складних військово-спеціальних ситуацій із використанням спеціалізованих комп'ютерних технологій;

пріоритет інформаційних процесів над матеріальними, що зумовлює потребу у створенні безпечних, надійних систем збору, зберігання і передачі даних;

тривалі цикли підготовки, які вимагають запровадження нових, ефективних методів навчання для забезпечення глибокого засвоєння знань і формування професійних навичок;

постійне оновлення змісту освіти з урахуванням розвитку новітніх оборонних технологій та потреб військової практики.

Таким чином, цифровізація військової освіти є не лише технічним процесом, а стратегічним чинником її розвитку. Вона сприяє підвищенню якості підготовки фахівців, забезпечує адаптацію освітнього процесу до сучасних глобалізаційних тенденцій, підвищує гнучкість управлінських процесів і створює умови для ефективного використання інформаційних ресурсів у сфері оборони. У результаті цифрова

трансформація стає основою формування нової культури військової освіти – відкритої, технологічної, орієнтованої на результат і здатної швидко реагувати на виклики часу.

Список використаних джерел:

1. Вітер Д., Оліферук В., Мигун М. Доктринальне забезпечення розвитку системи військової освіти : методичні рекомендації. Київ : НУОУ, 2023. 128 с.
2. Красота-Мороз Г., Горбачевський С., Полторак М. Трансформація системи наукової та науково-технічної діяльності в системі Міністерства оборони України шляхом цифровізації. *Військова освіта*. № 2 (46), 2022 р. С. 150–161. DOI: https://doi.org/10.33099/2617- 1783/2022-46/150-160.
3. Мітягін О. Освіта та індивідуальна підготовка у країнах НАТО. *Збірник наукових праць «Військова освіта».* 2021. № 2 (44). С. 131–143. DOI: https://doi.org/10.33099/2617-1783/2021-44/131-143.
4. Полторак С. Т. Трансформація системи військової освіти України на шляху до досягнення стандартів НАТО. *Наука і оборона*. 2018. № 2. С. 3–10. DOI: https://doi.org/10.33099/2618-1614-2018-3-2-3-10.

ТРОБЮК Д. В.,
Національна академія Служби безпеки України

СУЧАСНА ВІЙСЬКОВА ОСВІТА І ФОРМУВАННЯ ПРОФЕСІЙНОЇ ВІДПОВІДАЛЬНОСТІ МАЙБУТНЬОГО ОФІЦЕРА: ПЕДАГОГІКО-ІНСТИТУЦІЙНИЙ ПІДХІД

Україна має тривалий досвід партнерства з Організацією Північноатлантичного договору, а посилення взаємодії та стратегічний курс на євроатлантичну інтеграцію стали одним із чинників ескалації російської агресії. Повномасштабне вторгнення рф порушило регіональну без пекову рівновагу та спричинило масштабну дестабілізацію без пекового середовища в Європі.

Однією з ключових умов набуття Україною членства в НАТО є досягнення стандартизації та взаємосумісності сектору безпеки і оборони з силами держав-членів Альянсу. Це завдання неможливо реалізувати без якісної підготовки військового персоналу, адже саме система військової освіти формує офіцерів, здатних діяти відповідно до натівських процедур, етичних норм та принципів відповідального лідерства.

У цьому контексті професійна відповідальність майбутнього офіцера виступає не лише складовою військової професії, а й ключовим показником готовності до дій в умовах ризику, невизначеності та морально-правової складності. Трансформація сектору безпеки і оборони України, орієнтована на інтеграцію зі стандартами НАТО, висуває формування відповідального офіцера як одне з пріоритетних завдань військової освіти. Сучасні дослідження військового лідерства та професійної військової освіти

підкреслюють, що розвиток відповідальності значною мірою зумовлений інституційним середовищем, застосовуваними освітніми технологіями та цілеспрямованим вихованням морально-етичних якостей курсанта [1; 4; 7].

У класичних моделях військової етики професійна відповідальність трактується як інтегративна якість, що охоплює моральну автономію, здатність до прийняття рішень у критичних ситуаціях, особисту дисциплінованість та усвідомлення наслідків власних дій [5]. Вітчизняні дослідники уточнюють її структуру, включаючи правову культуру, етичну поведінку, здатність діяти в умовах бойового стресу та рефлексивність [3; 7].

Вищі військові навчальні заклади відіграють роль інституцій формування «офіцерської ідентичності» – через нормативно-правові засади, ритуали, традиції, вимоги до поведінки, внутрішню культуру та професійну соціалізацію. У міжнародних дослідженнях професійної військової освіти підкреслюється, що саме інституційна культура визначає, наскільки успішно курсант засвоює норми відповідального лідерства [1; 2].

Аналіз наукових публікацій дозволяє виокремити низку актуальних проблем формування професійної відповідальності майбутнього офіцера:

розрив між задекларованими освітніми цілями та реальною практикою, де технічні та тактичні дисципліни часто домінують над гуманітарними та етичними складниками [3];

недостатня розробленість методик оцінювання поведінкових індикаторів відповідальності та брак інституційної підтримки цього процесу [1];

обмеженість застосування активних форм навчання – симуляцій, рольових ігор, кризового моделювання, аналізу морально-етичних дилем [2; 6];

дефіцит системних досліджень українського науковців та адаптації натівських підходів до умов українських військових навчальних закладів.

Ефективне формування професійної відповідальності майбутнього офіцера передбачає поєднання педагогічних та інституційних механізмів. Тому пріоритетними можна вважати такі напрямки:

1) Інституалізація принципів відповідального лідерства – створення етичних кодексів, включення компонентів відповідальності до освітніх стандартів, запровадження регулярного оцінювання морально-етичних проявів курсантів (оскільки у стандартах НАТО професійна відповідальність визначається як один із базових принципів військового лідерства [4]).

2) Використання активних методів навчання, здатних моделювати ситуації невизначеності: бойові симуляції, командні завдання в умовах

обмеженого часу, аналіз етичних дилем, структуровані після діяльнісні обговорення. Дослідження показують, що сааме такі методи сприяють розвитку моральної автономії та відповідального прийняття рішень [2; 6].

3) Наставництво та використання бойового досвіду інструкторів. У наукових роботах наголошується, що особистий приклад та професійна соціалізація є найбільш дієвими механізмами передачі норм відповідальної поведінки [6; 7].

4) Адаптація міжнародних процедур і стандартів, зокрема: NATO Decision-Making Process, Operational Planning Process, принципи військового етикету. Їх застосування забезпечує структурованість рішень, колективне обговорення ризиків, підвищення прозорості й персональної відповідальності командирів.

Отже, формування професійної відповідальності майбутнього офіцера є результатом взаємодії інституційної культури, освітніх технологій, нормативних вимог, наставництва та бойового досвіду. Досягнення оптимальних результатів вважаємо можливим лише за умови комплексного підходу, що поєднує компетентнісне навчання, морально-етичну підготовку, стандарти НАТО та зміцнення інституційної спроможності військової освіти.

Список використаних джерел:

1. Brooks D. Developing Ethical Leadership in Military Education. *Military Review*. 2019.
2. Czarnecki J. The Professional Military Leader’s Responsibility. *Journal of Military Learning. Army University Press*, 2018.
3. Demydenko V. Виховання морально-етичної відповідальності курсантів у процесі військово-професійної підготовки. *Збірник наукових праць Національної академії ДПСУ*. 2021.
4. NATO Standard AJP-01. NATO Leadership Doctrine. NATO Standardization Office, 2019.
5. Sarkesian A., Connor W. Military Ethics and Leadership Responsibility. *Oxford University Press*, 2020.
6. Snider D., Matthews L. Forging the Warrior’s Character: Moral Responsibility in Military Leadership. U.S. Army War College Press, 2017.
7. Суський О. Педагогічні умови формування професійної відповідальності майбутніх офіцерів. *Військова освіта*. 2022. № 2(46).
8. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 15.10.2025).
9. Про трансформацію системи військової освіти: Постанова Кабінету Міністрів України від 15 грудня 1997 р. № 1410. URL: https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text (дата звернення: 15.10.2025).
10. FM 6-22. Army Leadership and the Profession. U.S. Army, 2020.

ЧОРНОУС В. Д.,
кандидат психологічних наук, доцент,
Національна академія Служби безпеки України

ПСИХОЛОГІЧНА СКЛАДОВА ВОГНЕВОЇ ПІДГОТОВКИ ФАХІВЦІВ СИЛ БЕЗПЕКИ І СИЛ ОБОРОНИ В УМОВАХ ВОЄННОГО СТАНУ

В умовах тривалої широкомасштабної військової агресії російської федерації проти нашої держави доцільним і вагомим є об'єднання сил безпеки і сил оборони для стримування ворога й звільнення захопленої території нашої держави. Першочерговим завданням є захист національної безпеки, тобто захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства. Також ефективна взаємодія сприятиме своєчасному виявленню, запобіганню і нейтралізації реальних та потенційних загроз національним інтересам.

Теперішні події висувають оновлені вимоги до професійної підготовки військовослужбовців Збройних Сил, оперативного складу Служби безпеки, Національної гвардії, Державної прикордонної служби, поліцейських, рятувальників й інші співробітників оборонного та безпекового сектору, які щодня наближають нас до перемоги. У процесі оперативно-бойової діяльності вони досить часто зіштовхуються із необхідністю використовувати, а іноді й застосовувати вогнепальну зброю. Поряд із наявністю відповідних професійних знань та вмінь у фахівців сил безпеки і сил оборони мають бути розвинені стійкі навички застосування вогнепальної зброї та сформований високий рівень психологічної готовності до влучної стрільби. Зазначене сприятиме успішному вирішенню складних професійних завдань у будь-яких екстремальних ситуаціях за рахунок чітких й адекватні дії, здатності концентруватися на завданні, розвинених емоційно-вольових якостей, уміння керувати своїм емоційним станом під час застосування зброї.

Крім того, вплив психологічних особливостей екстремальних умов на особовий склад неоднаковий. У підготовлених осіб вони актуалізують: загострене почуття обов'язку, відповідальності та рішучості; мобілізацію сил і можливостей; підвищену енергійність та активність, наполегливість; зібраність та готовність до будь-яких неочікуваних ситуацій; швидку й адекватну реакцію на зміну обстановки; чіткість дій тощо. Разом з тим, поведінка непідготовленої особи в екстремальних умовах може супроводжуватись розгубленістю; нерішучістю; підвищеним рівнем тривожності; зниженням рівня уваги та спостережливості; проявами роздратованості й нестриманості; відмовою від виконання завдання тощо.

Загалом, реакції людей на екстремальні ситуації бувають досить

різними, проте для подолання дезорганізуючих станів, що виникають під дією стрес-факторів, найоптимальнішими є адекватні форми реагування зорієнтовані на подолання або мінімізацію впливу психотравмуючих чинників. Адекватна реакція супроводжується зростанням ролі психологічної готовності особистості до дій за таких умов. Загальновідомо, що навички влучної стрільби формуються у результаті правильно організованого навчання, тренувань і постійної практики. Однак, стрільба в бойових умовах вимагає врахування впливу екстремальних факторів на психіку людини. За даних умов дії фахівця сектору безпеки та результати його стрільби значною мірою залежать від емоційно-вольових якостей, підготовленості до дій в екстремальних умовах, здатності мобілізуватися та концентруватися на завданні, умінні керувати своїм емоційним станом під час виконання пострілу.

Таким чином, із вище викладеного слідує, що психологічна складова посідає важливе місце у підготовці фахівців сектору безпеки і сил оборони до влучної стрільби, оскільки застосування ними зброї реалізується за екстремальних умов, яким притаманні: дефіцит часу та інформації; високий ступінь особистого ризику та небезпеки для життя; вплив на особистість сильних подразників та домінування негативних емоцій; високий рівень психічної напруги; підвищена відповідальність при прийнятті рішень.

Результатом вогневої підготовки фахівців сектору безпеки і сил оборони має стати розвинена психологічна готовність до влучної стрільби, що включає: стійкість до стресу, високий рівень само-контролю емоцій та поведінки; здатність до збереження працездатності у критичних ситуаціях, а також до швидкого її відновлення; розвинені адаптивні властивості, що дають змогу зберігати на необхідному ріні працездатність у стані стомлення, здатність адекватно реагувати на різні події.

Наявність у фахівців сектору безпеки і сил оборони розвиненої психологічної готовності до влучної стрільби дасть їм змогу: успішно долати негативні психічні стани (страх, фрустрацію, паніку, конфлікт, кризу), що виникають у процесі стрільби, а також успішно діяти в напружених стресових ситуаціях, оскільки нездатність витримувати довготривалу емоційну напругу може призвести до неадекватних реакцій, імпульсивних дій, зміни значущості мотивів, що загалом свідчить про нераціональну поведінку та намагання активно протистояти зовнішнім впливам екстремальних умов; знизити рівень тривожності, тобто схильності відчувати занепокоєння в різних життєвих ситуаціях, у тому числі і тих, об’єктивні характеристики яких до цього не спонукають; підвищити адаптивні можливості фахівців сектору безпеки завдяки формуванню стійкості до тривалого напруження, небезпеки та ризику; здатність до оптимальної мобілізації можливостей організму та набуття досвіду подолання перешкод в екстремальних умовах.

ШВИДЕНКО Є. Ю.,
кандидат юридичних наук,
Національна академія Служби безпеки України

ПІДГОТОВКА КАДРІВ ДЛЯ ПОТРЕБ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В СУЧАСНИХ УМОВАХ

Якісна підготовка кадрів сил сектору безпеки і оборони (СБО) є критично важливою для забезпечення національної безпеки держави [5, с. 210]. Сили СБО включають Збройні Сили України (ЗСУ), інші військові формування, а також правоохоронні та спеціальні органи, які виконують завдання у сфері оборони і безпеки. В сучасних умовах, особливо в умовах воєнного стану та відбиття широкомасштабної збройної агресії, потреба у висококваліфікованих, навчених кадрах різко зросла. Виклики гібридної війни, масового застосування сучасних озброєнь, кіберзагроз та інформаційних атак вимагають від персоналу сектору нових підходів до навчання та тренувань [6, с. 68–69]. Відповідно, підготовка кадрів для потреб сил СБО перетворилася на один із пріоритетних напрямів державної політики і військового будівництва [5, с. 212].

Тривалий час система підготовки кадрів у секторі безпеки і оборони мала суттєві недоліки. Дослідження свідчать, що навчання здійснювалося за загальноосвітніми стандартами без належної спеціалізації під реальні потреби сил оборони, не існувало ефективної системи оцінювання якості професійної підготовки, а навчальні програми були перевантажені теоретичним матеріалом [6, с. 67–70]. Головним недоліком залишалася невідповідність змісту підготовки реальним потребам сил безпеки України.

З початком повномасштабної війни ці проблеми стали особливо відчутними. Аналіз бойових дій 2022–2024 рр. виявив низку проблем в організації оперативної та бойової підготовки військ, що призвело до розриву між необхідним і фактичним рівнем навченості підрозділів, дефіциту спроможностей і зниження боєздатності. Однією з ключових причин цього стала недостатня ефективність функціонування існуючої системи підготовки ЗСУ в умовах воєнного стану [1, с. 234]. Таким чином, на початку особливого періоду стало очевидно, що система підготовки кадрів потребує негайного реформування та адаптації до сучасних викликів.

В умовах активних бойових дій та стрімкого розвитку технологій відбувається трансформація підходів до навчання військових і фахівців безпеки. Серед ключових сучасних тенденцій підготовки персоналу СБО доцільно виокремити такі напрями.

Акцент робиться на освоєнні новітніх військових технологій, зокрема безпілотних літальних апаратів, автоматизованих систем управління військами та засобів радіоелектронної боротьби. Майбутні офіцери та військовослужбовці повинні вміти ефективно застосовувати безпілотні системи та протидіяти аналогічним засобам противника, оскільки характер

бойових дій дедалі більше залежить від цифрових технологій [2, с. 30]. Важливою складовою є також підготовка до ведення мережево-центричних операцій із використанням сучасних систем зв'язку та управління [2, с. 33].

З урахуванням досвіду бойових дій відбувається відхід від шаблонних підходів до тактики. Натомість впроваджуються динамічна оборона, гнучкі контратаки та дії малими тактичними групами. Особовий склад навчається діяти автономно, швидко маневрувати та використовувати фактор раптовості, що підвищує живучість військ і вимагає високого рівня командирської підготовки [1, с. 235].

Ворог активно застосовує інформаційно-психологічний вплив з метою підриву морального стану військовослужбовців і суспільства. У зв'язку з цим програми підготовки включають формування у командирів компетентностей з розпізнавання та нейтралізації дезінформації, а також навичок інформаційної стійкості та управління моральним станом підрозділів [2, с. 35].

Значні санітарні втрати в умовах сучасного бою зумовили підвищену увагу до навчання навичок домедичної допомоги, організації евакуації поранених та медичного забезпечення бойових дій. Тактична медицина стала обов'язковим елементом підготовки як рядового складу, так і командирів підрозділів [6, с. 71].

Важливим пріоритетом є розвиток лідерських якостей, здатності діяти в умовах невизначеності та зберігати психологічну стійкість. Постійні стресові фактори війни вимагають системної психологічної підготовки, розвитку навичок саморегуляції та підтримки бойового духу особового складу [2, с. 37].

Український сектор безпеки і оборони активно адаптує стандарти НАТО у сфері управління, організації та підготовки кадрів. Участь у міжнародних навчаннях, обмін інструкторами та стандартизація процедур сприяють підвищенню взаємосумісності та ефективності підготовки особового складу [6, с. 72].

Для реалізації зазначених пріоритетів держава здійснює комплексну модернізацію системи підготовки кадрів СБО. Впроваджується інтегрована міжвідомча система освіти, що поєднує військову, спеціальну та вищу освіту, забезпечуючи узгодженість підготовки персоналу різних складових сектору безпеки [5, с. 216].

Державна політика у сфері кадрового забезпечення відображена в Концепції військової кадрової політики до 2028 року, яка передбачає перехід до професійної моделі комплектування, розвиток системи рекрутингу, кар'єрного зростання та цифровізацію управління персоналом [3]. Паралельно Стратегія розвитку людського капіталу сил оборони до 2027 року спрямована на формування цілісної системи підготовки, мотивації та утримання персоналу в умовах воєнного і післявоєнного періодів [4]. Впровадження положень цих стратегічних документів дозволяє забезпечити прогнозованість кадрових процесів і підвищити стійкість системи управління персоналом у Збройних Силах України.

Важливим аспектом є поєднання професійної підготовки з належним рівнем соціального захисту військовослужбовців, що позитивно впливає на мотивацію до проходження служби та зменшує плинність кадрів. Окрему роль відіграє розвиток сучасних електронних систем військового обліку й управління кар'єрою, які забезпечують прозорість кадрових рішень і підвищують ефективність планування. Крім того, розширення міжнародного військово-освітнього співробітництва сприяє впровадженню кращих практик підготовки та управління персоналом відповідно до стандартів НАТО. У сукупності зазначені заходи формують передумови для створення професійної, адаптивної та стійкої системи кадрового забезпечення сил сектору безпеки і оборони.

Висновок. Отже, У сучасних умовах воєнного стану підготовка кадрів для сил сектору безпеки і оборони набуває стратегічного значення та потребує системного, науково обґрунтованого оновлення. Проведений аналіз засвідчує, що традиційна система підготовки не повною мірою відповідала викликам сучасної війни, що зумовило необхідність її глибокої трансформації з урахуванням бойового досвіду та нових форм збройної боротьби Впровадження новітніх технологій, розвиток адаптивної тактики, посилення практичної та медичної складових навчання, а також формування психологічної стійкості особового складу сприяють підвищенню рівня боєздатності підрозділів і якості виконання оперативно-бойових завдань.

Важливою умовою ефективної підготовки кадрів є інтеграція освітніх, тренувальних і управлінських компонентів у межах єдиної міжвідомчої системи, що забезпечує узгодженість підготовки та наступність професійного розвитку військовослужбовців. Реалізація положень Концепції військової кадрової політики та Стратегії розвитку людського капіталу сил оборони створює передумови для формування професійної, мотивованої та соціально захищеної армії в умовах воєнного і післявоєнного періодів. У підсумку формування сучасної системи підготовки кадрів сил сектору безпеки і оборони є ключовим чинником зміцнення обороноздатності держави, її інтеграції до євроатлантичного безпекового простору та гарантією здатності ефективно реагувати на поточні й майбутні загрози національній безпеці.

Список використаних джерел:

1. Годзь С. В., Василенко С. С., Швець Т. М., Біляков І. В. Методичні аспекти обґрунтування перспективної системи підготовки Збройних Сил України в умовах воєнного стану. *Military Science*. 2025. Т. 2, № 4. С. 229–240.
2. Діденко О. М., Сніца Т. Є., Дем'янюк Ю. В., Андрощук О. В., Корчев В. М. Тенденції професійної підготовки офіцерських кадрів сил сектору безпеки і оборони України в умовах правового режиму воєнного стану. *Збірник наукових праць НАДПСУ*. 2025. Т. 40, № 1. С. 23–41.
3. Про затвердження Концепції військової кадрової політики в системі Міністерства оборони України на період до 2028 року : наказ Міністерства оборони України від 27.10.2023 № 637/нм.

4. Про затвердження Стратегії залучення, розвитку та утримання людського капіталу в Силах оборони України на період до 2027 року : наказ Міністерства оборони України від 29.12.2024 № 862/нм.
5. Сокуренко В. В. Підготовка кадрів для сектору безпеки і оборони як передумова забезпечення національної безпеки України. *Право і безпека*. 2021. № 3(82). С. 209–218.
6. Сьомін С. В., Резнікова О. О. Проблеми реформування системи підготовки кадрів для сектору безпеки і оборони України. *Стратегічна панорама*. 2017. № 1. С. 67–73.

ШОВКУН В. М.,
Національна академія Служби безпеки України

СУЧАСНІ ТЕНДЕНЦІЇ ТА ТЕХНОЛОГІЇ У ВОГНЕВІЙ ПІДГОТОВЦІ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Система вогневої підготовки сил сектору безпеки і оборони України перебуває в стадії глибокої трансформації через потребу адаптації до гібридного характеру бойових дій. Традиційна модель – орієнтована на нормативно-фізичні показники та полігонні вправи з бойовими боєприпасами – виявляє низьку ефективність в умовах високої маневровості противника, поширення БПЛА та застосування розвідувально-ударних комплексів.

Наявний дисбаланс між оперативними потребами і технікометодичним рівнем підготовки зумовлений кількома ключовими проблемами: застаріла навчально-матеріальна база, що не забезпечує адекватної імітації бойових сценаріїв; дефіцит кваліфікованих інструкторів, здатних інтегрувати сучасні технології; обмеженість полігонного ресурсу; фрагментарність нормативно-правового регулювання, яка ускладнює стандартизацію вимог між відомствами [1, с. 53].

Порівняльний аналіз із практиками провідних країн (США, Великобританія, Польща, Ізраїль) виявляє принципову різницю: там вогнева підготовка є інтегрованою складовою бойового навчання, з модульними курсами, багаторівневою симуляцією та цифровою аналітикою, що забезпечує адаптивність, персоналізацію та постійний зворотний зв’язок. Для України імплементація таких підходів потребує не лише технічної модернізації інфраструктури, але й методологічного переформатування на компетентнісно-операційну модель, де стрілець – носій інтегрованих когнітивних, психофізіологічних і технічних компетенцій [2].

В умовах безперервних бойових завдань критично необхідно систематизувати технологічні підходи, оцінити їхню практичну ефективність і розробити поетапну методологію інтеграції інновацій у навчальні цикли з урахуванням логістичних, безпекових і ресурсних обмежень.

Удосконалення методик вогневої підготовки дедалі більше набуває рис техніко-технологічної інженерії навчального процесу: відходить підхід дискретних вправ на користь синтезованих, багаторівневих тренувальних екосистем, що поєднують ергономічну фізіологію, кібернетичні симуляції та алгоритмічну оцінку поведінкових патернів. Це дозволяє розглядати формування вмінь як динамічну адаптивну систему, керовану даними й валідацією результатів. VR та AR створюють континуум «реальне-віртуальне», де сценарії з керованою складністю й стрес-індукцією реплікують візуально-аудіальні та фізіологічні тригери; LVC-архітектури забезпечують зв'язок реальних підрозділів із віртуальними агентами для підвищеної репрезентативності за мінімальних витрат [3, с. 2011].

Симуляційні комплекси – від цифрових тирів до тактичних тренажерів із імітацією віддачі – реалізують force-on-force взаємодію через апаратно-програмні модулі, що відтворюють баллістику, звук і тактичну динаміку; уніфікація інтерфейсів (MILES, SAAB BT – 46) вимагає відкритих протоколів обміну й часової синхронізації телеметрії. Рухомі та сценарно-адаптивні роботизовані мішені підвищують реалізм за допомогою стохастичних траєкторій і поведінкових алгоритмів, що дозволяє кількісно вимірювати точність, час захоплення цілі та ефективність вогню в русі, за умови застосування надійних систем навігації, локалізації й дистанційного управління [4, с. 27].

Лазерні тренажери та інтерактивні полігони покривають безпечне, економічно ефективне і повторюване відпрацювання з високою роздільною телеметрією, що формує цифровий слід для модульного аналізу поведінкових показників. Інтеграція аналітики та ШІ – від часових моделей до класифікації помилок і біомеханічного аналізу на основі інерційних сенсорів – дозволяє прогнозувати траєкторії навчального прогресу, формувати адаптивні навчальні криві та встановлювати порогові значення придатності за допомогою байєсівської валідації. Синергетична інтеграція цих технологій трансформує індивідуальні вміння в колективну бойову компетентність, вимагаючи уніфікації даних, стандартів інтероперабельності та формалізації кількісних критеріїв ефективності [5, с. 146].

Узагальнений методично-організаційний каркас вогневої підготовки має базуватися на принципах адаптивності, вимірюваності та інтегрованості, що передбачає перехід від нормативно-орієнтованих сценаріїв до компетентнісно-орієнтованих навчальних траєкторій.

Адаптивні навчальні програми слід проєктувати як ієрархічно структуровані модулі, що забезпечують персоналізацію процесу на основі діагностики компетенцій, динамічного моніторингу і прогнозної аналітики. Це включає формалізацію компетентнісних профілів із чіткими критеріями оцінювання, впровадження алгоритмів формування навчальних маршрутів, які в режимі реального часу коригують склад і інтенсивність вправ за телеметрією та результатами симуляцій, а також інтеграцію модульного контенту (базові навички → тактичні сценарії →

командна взаємодія) з механізмами персистентного навчання для консолідації навичок.

Система KPI має бути багаторівневою – тактичні (індивідуальні: точність, час реакції, критичні помилки), оперативні (підрозділові: синхронність дій, комунікації, час виконання задачі) і стратегічні (масштаб підготовки: досягнення цілей, ресурсна інтенсивність, індекс бойової готовності). Цифрові індикатори повинні формуватися з агрегованих датасетів (телеметрія, відеоаналіз, біометрія), проходити статистичну валідацію і відображатися в єдиному dashboard з історизацією; впровадження вимагає регламентації порогових значень, калібрування сенсорів і гарантії цілісності даних.

Синхронізація тренувального процесу з реальними бойовими сценаріями базується на сценарній матриці з варіативністю параметрів (ландшафт, освітленість, ЕМ-перешкоди, мобільні цілі), впровадженні LVC-архітектури для комбінованого відпрацювання з реальними та віртуальними агентами та інтеграції спеціалізованих модулів (нічні приціли, RCIED / РЕБ-імітація, контр-БПЛА). Ключовим є цикл «тренування – оцінка – корекція», що забезпечує оновлення програм, корекцію KPI та оптимізацію ресурсів за умови міжвідомчої координації та гнучкого планування полігонів і цифрових активів [1, с. 57].

Політика безпеки навчального процесу повинна спиратися на концепцію safety-by-design: тренажерні технології дозволяють знизити ризики інцидентів, реплікативно відпрацьовувати ризикові сценарії та проводити стрес-індуковані тренінги без загрози для МТБ. Економічний ефект проявляється у зменшенні витрат (боєприпаси, паливо, амортизація) і підвищенні інтенсивності використання ресурсів, проте потребує капітальних інвестицій і моделювання TCO / ROI на життєвому циклі обладнання.

Стандартизація й сертифікація нових систем є критичною для інтероперабельності й валідності результатів: необхідні формалізовані технічні специфікації (інтерфейсні протоколи, синхронізація, формати телеметрії), критерії валідації баллістики й тактичного моделювання, процедури калібрування сенсорів та методики кореляції тренажерних і полігонних показників. Стандарти мають супроводжуватися механізмами акредитації постачальників, сертифікації комплексів і нормативною інкорпорацією цифрових метрик у офіційні критерії бойової придатності [2].

Важливо звернути увагу на те, що підготовка, орієнтована лише на техніко-тактичні компетенції, ігнорує психофізіологічні чинники, критично важливі для бойової діяльності. Симуляційні технології дають змогу моделювати контрольовані, але стресові умови, що сприяють розвитку стресостійкості через десенситизацію реакцій і формування компенсаторних стратегій поведінки. Це передбачає використання квазіекспериментальних протоколів із варіюванням рівнів стимулу, моні-

торингом вегетативних (ЧСС, ВСР, шкірно-гальванічна реакція) і когнітивних показників (швидкість прийняття рішень, точність розпізнавання, ситуативна обізнаність).

Тренування психологічної готовності до ведення вогню по реальній цілі має спиратися на етичні та правові засади – навчання ідентифікації цілей, оцінки пропорційності застосування сили, управління післястріляльними діями. Доцільним є впровадження модульних програм розвитку морально-етичних компетенцій, сценаріїв прийняття рішень у неоднозначних ситуаціях і вправ із деескалації та психологічної саморегуляції. Такий підхід знижує ризик посттравматичних розладів і підвищує стійкість особового складу в бойових умовах.

Ключову роль відіграють командири та інструктори, які виступають фасилітаторами навчання і менеджерами стресових навантажень. Їх підготовка має включати педагогічні, психологічні й аналітичні компетенції для інтерпретації біометричних даних, корекції навантажень і проведення якісного дебрифінгу. Зворотний зв'язок має бути багаторівневим: оперативним (миттєві підказки), корективним (індивідуальні рекомендації) і рефлексивним (аналіз поведінкових та психологічних аспектів). Комплексна психофізіологічна підготовка забезпечує ефективний трансфер навичок у бойові умови, знижує кризові реакції та підвищує стійкість підрозділів [6].

Інституційно-стратегічна модернізація тренувальної бази потребує державних програм довгострокового планування, стандартизації інтероперабельності, сертифікації засобів навчання та емпіричної валідації їх ефективності. Необхідно забезпечити фінансову сталість через державно-приватне партнерство, грантові механізми та підтримку НДДКР. Такі ініціативи мають формувати не лише технічну, а й знаннєву екосистему, що сприяє підготовці кадрів та трансферу технологій [4, с. 29].

Залучення приватного сектора і наукових установ створює синергію: промисловість відповідає за інженерні рішення, наука – за дослідження, тестування та валідацію моделей. Важливими є податкові стимули для R&D, програми акселерації стартапів і відкриті стандарти інтеграції модулів. Це забезпечує розвиток вітчизняних технологій і потенціал їхнього експорту.

Міжнародна військово-технічна співпраця сприяє адаптації стандартів НАТО, сумісності протоколів LVC-архітектури, створенню спільних навчальних і дослідницьких центрів. Вона стимулює технологічний розвиток, але потребує контролю ризиків залежності та локалізації критичних компонентів. Стратегічна мета – створення стійкої, модульної та інтероперабельної системи вогневої підготовки, здатної адаптуватися до змін характеру сучасної війни [6].

Отже, сучасна система вогневої підготовки сил сектору безпеки і оборони України перебуває у фазі комплексної технологічної та методологічної модернізації, спрямованої на відповідність умовам гібридної війни. Її ефективність нині визначається рівнем інтеграції інноваційних тренувальних технологій – VR / AR-середовищ, симуляційних комплексів, роботизованих мішеней, аналітики даних і систем штучного інтелекту – у єдину адаптивну освітньо-тренувальну екосистему. Ключовими орієнтирами розвитку виступають персоналізація навчання, цифрова вимірюваність результатів, психофізіологічна стійкість військовослужбовців і стандартизація безпекових процедур. Подальше вдосконалення вогневої підготовки потребує державної підтримки, державно-приватного партнерства, залучення наукових установ і міжнародної співпраці, що дозволить сформувати стійку, інтероперабельну та науково обґрунтовану систему підготовки, здатну забезпечити високу боєздатність підрозділів у реаліях сучасного збройного протистояння.

Список використаних джерел:

1. Пурнак В., Мартинов І., Солоненко В. Основні тенденції застосування сучасного озброєння та військової техніки суб'єктами сектору безпеки та оборони під час виконання службово-бойових (бойових) завдань. *Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки.* 2025. №2 (99). С. 52–59. DOI: https: // doi.org / 10.32453 / 3. v99i2.1877.
2. Negi P., Pathani A., Bhatt B. C. et al. Integration of Industry 4.0 Technologies in Fire and Safety Management. 2024. Fire. № 7 (10). DOI: https: // doi.org / 10.3390 / fire7100335.
3. Kaya R. D, Hastilow K., Owen K. M. et al. An Augmented Reality Rifle Qualification Test for Return-to-Duty Assessment in Service Members, *Military Medicine.* 2024. Vol. 189. Is. 9–10. P. 2009–2015. DOI: https: // doi.org / 10.1093 / milmed / usae028.
4. Мазуренко Л. Використання технологій віртуальної реальності у військовій освіті. *Збірник наукових праць Уманського державного педагогічного університету.* 2024. Вип. 3. С. 26–32. DOI: https: // doi.org / 10.31499 / 2307–4906.3.2024.312954.
5. Зеленський Є. О., Задорожня Р. В., Фісун Н. О. Використання інтерактивних методів навчання під час проведення практичних занять з вогневої підготовки. *Науковий вісник Ужгородського університету. Сер.: Право.* Ужгород, 2023. Т. 2. Вип. 80. С. 144–148.
6. O'Hagan Ch. J., Mitchell P., Paffenroth N., Hendrick A. Tactical UAS: Three-Tiered UAS Manning for Increased Lethality and Situational Awareness: веб-сайт. URL: https: // www. lineofdeparture. army. mil / Journals / Infantry / Infantry-Archive / Winter – 2024–2025 / Three-Tiered-UAS-Manning/ (дата звернення: 25.10.2025).

2 МІЖВІДОМЧА ВЗАЄМОДІЯ У РАМКАХ РЕАЛІЗАЦІЇ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ

БИЧЕНКО С. М.,
кандидат історичних наук, доцент,
провідний науковий співробітник
науково-дослідної лабораторії
з дослідження проблем управління
у сфері цивільного захисту,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

МІЖВІДОМЧА ВЗАЄМОДІЯ У РАМКАХ РЕАЛІЗАЦІЇ ЗАХОДІВ З ЕВАКУАЦІЇ НАСЕЛЕННЯ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ (2022–2025 РР.)

Повномасштабне вторгнення російської федерації в Україну у лютому 2022 року спричинило безпрецедентні виклики для системи цивільного захисту. Евакуація населення з небезпечних територій стала одним із пріоритетних завдань держави. У цьому контексті міжвідомча взаємодія набула критичного значення, забезпечуючи оперативність, безпеку та ефективність евакуаційних заходів. Вивчення досвіду 2022–2025 років дозволяє окреслити тенденції, проблеми та перспективи вдосконалення евакуаційної політики в умовах воєнного стану.

До реалізації евакуаційних заходів були залучені різні державні структури, кожна з яких виконувала визначені функції. Державна служба України з надзвичайних ситуацій (ДСНС) виступала координатором евакуаційних процесів, відповідала за планування, оповіщення, логістику та розгортання пунктів прийому. Збройні Сили України забезпечували безпеку маршрутів, супровід колон та розвідку загроз. Національна поліція та Національна гвардія України здійснювали охорону громадського порядку, контроль на пунктах евакуації та супровід транспорту. Органи місцевого самоврядування формували списки евакуйованих, забезпечували транспорт, розміщення та соціальну підтримку. Міністерства охорони здоров’я, соціальної політики та інфраструктури відповідали за медичне забезпечення, психологічну допомогу та транспортну логістику.

У 2022–2025 роках було оновлено та адаптовано низку нормативних актів, що регламентували евакуаційні заходи. Зокрема, постанови Кабінету Міністрів України визначали порядок організації евакуації, накази МВС та ДСНС регламентували створення координаційних штабів, а методичні рекомендації ДСНС містили алгоритми дій, моделі координації та типові схеми оповіщення. Важливим

нововведенням стало впровадження цифрових платформ, таких як «єДопомога» та «Трембіта», які забезпечували реєстрацію та моніторинг евакуйованих осіб [1, 2, 3].

У 2022 році відбувалася евакуація населення з Київської, Чернігівської та Харківської областей, що супроводжувалась формуванням перших координаційних штабів. У 2023 році масштабна евакуація охопила Донеччину та Херсонщину, а також було впроваджено цифрові реєстри для обліку переміщених осіб. У 2024 році відбулося удосконалення нормативної бази та інтеграція волонтерських структур у систему реагування. У 2025 році розпочалася планова евакуація з зон потенційної ескалації, що супроводжувалась розширенням міжвідомчих протоколів та впровадженням нових механізмів координації [7, 8, 9].

Ефективна міжвідомча взаємодія забезпечувалась через створення регіональних та місцевих штабів з евакуації, використання єдиних інформаційних платформ для обміну даними, проведення спільних навчань та тренувань, а також активне залучення волонтерських організацій та міжнародних партнерів. Така модель дозволила забезпечити гнучкість, адаптивність та оперативність реагування на зміну безпекової ситуації.

Серед основних проблем, що виникали у процесі реалізації евакуаційних заходів, слід відзначити нестачу транспорту, пального та персоналу, відсутність єдиної системи обліку евакуйованих на початкових етапах, психологічну напругу серед населення та служб, а також потребу в адаптації нормативної бази до умов воєнного часу. Ці виклики вимагали постійного вдосконалення механізмів взаємодії та управління.

Подальший розвиток міжвідомчої взаємодії у сфері евакуації населення передбачає розробку національної стратегії евакуації з урахуванням воєнних ризиків, інституціоналізацію міжвідомчих штабів як постійних структур, впровадження системи моніторингу евакуаційних процесів у реальному часі, а також підвищення кваліфікації персоналу через навчальні програми.

Висновки. Міжвідомча взаємодія в умовах воєнного стану стала основою ефективної евакуації населення. Її розвиток у 2022–2025 роках демонструє здатність українських інституцій до адаптації, координації та інноваційного управління в умовах кризи. Подальше вдосконалення цієї взаємодії є запорукою безпеки громадян та стійкості держави.

Список використаних джерел:

1. Кодекс цивільного захисту України від 02 жовтня 2012 року № 5403-VI (Відомості Верховної Ради (ВВР), 2013, № 34-35, ст. 458). URL: https://zakon.rada.gov.ua/ laws/show/5403-17#Text (дата звернення: 21.10.2025).
2. «Про затвердження Порядку проведення евакуації у разі загрози виникнення або виникнення надзвичайних ситуацій». Постанова Кабінету Міністрів України від 30.10.2013 № 841 (зі змінами) . Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/841-2013-%D0%BF#Text (дата звернення: 21.10.2025).

3. «Про утворення Координаційного штабу з проведення евакуаційних заходів та ефективного реагування на масове переміщення населення». Постанова Кабінету Міністрів України від 29.07.2022 № 854 (зі змінами). Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/854-2022-п#Text (дата звернення: 21.10.2025).
4. «Про затвердження Методичних рекомендацій щодо планування і порядку проведення евакуації населення» Наказ МНС України від 07.09.2004 № 44 (зі змінами). Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/rada/show/v0044512-04#Text (дата звернення: 21.10.2025).
5. Платформа «єДопомога». Міністерство соціальної політики України. URL: https://edopomoga.gov.ua.
6. Портал «Трембіта». Міністерство цифрової трансформації України. URL: https://trembita.gov.ua.
7. Матеріали ДСНС України щодо евакуації дітей з Донеччини.
8. Офіційні повідомлення військових адміністрацій Харківської та Херсонської областей.
9. Аналітичні звіти UNHCR та IOM щодо внутрішнього переміщення в Україні. (дата звернення: 20.10.2025).

ГАЄВСЬКИЙ Є. О.,
курсант, Харківський національний інститут внутрішніх справ

МЕТОДИ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД DDOS-АТАК

У сучасному світі, який дедалі більше переходить у цифровий формат, питання кібербезпеки стають надзвичайно важливими. Сьогодні практично кожна людина, організація чи держава залежать від інформаційних технологій, адже саме через них здійснюється обмін даними, фінансові операції, комунікація, керування бізнес-процесами та навіть функціонування державних структур. У такому середовищі будь-яка вразливість у системах безпеки може мати серйозні наслідки.

Щодня фіксуються тисячі спроб несанкціонованого доступу, зараження шкідливими програмами або кібератак різного масштабу. Однією з найнебезпечніших серед них вважається DDoS-атака – це один із найпоширеніших способів вивести з ладу веб-ресурси, сервери або навіть цілі мережі. Наслідки таких атак можуть бути катастрофічними: вони здатні паралізувати роботу компаній, призвести до фінансових збитків, втрати довіри клієнтів і навіть поставити під загрозу національну безпеку.

Тому розуміння суті DDoS-атак, їхніх механізмів, методів реалізації та можливостей захисту є важливою складовою сучасної кіберосвіти.

Що таке DDoS-атака

DDoS (Distributed Denial of Service) – це тип кібератаки, спрямований на перевантаження інформаційних ресурсів, зокрема серверів, мереж або веб-додатків, шляхом масового надсилання великої кількості запитів із різних джерел. Головна мета такої атаки – зробити ресурс недоступним для звичайних користувачів.

Для здійснення DDoS-атаки зазвичай використовується ботнет – це мережа заражених пристроїв (комп'ютерів, смартфонів, маршрутизаторів, IoT-пристроїв), які підконтрольні зловмиснику. Власники таких пристроїв найчастіше навіть не підозрюють, що їхні комп'ютери беруть участь у кібератаці.

Основна відмінність DDoS від DoS (Denial of Service) полягає в масштабі. Якщо DoS-атака здійснюється з одного джерела, то DDoS використовує велику кількість пристроїв, розподілених по всьому світу. Це робить її більш потужною, ефективною та значно складнішою для виявлення і блокування.

Як працює DDoS-атака

Механізм дії таких атак можна описати поетапно.

1. Створення ботнету. Зловмисник поширює шкідливе програмне забезпечення через фішингові листи, заражені вебсайти або шкідливі файли. Після зараження пристрої жертви приєднуються до ботнету.
2. Керування ботами. Через спеціальні сервери управління хакер може віддавати команди всім зараженим пристроям одночасно.
3. Початок атаки. У визначений момент усі боти починають генерувати величезну кількість запитів до цільового сервера. Це спричиняє перевантаження каналів зв'язку, процесорних ресурсів або баз даних, через що сайт перестає відповідати на запити легітимних користувачів.
4. Масштабування. У разі потреби зловмисники підключають ще більше заражених пристроїв, посилюючи потужність атаки.

Основні типи DDoS-атак

Існує кілька видів DDoS-атак, які відрізняються своїми механізмами впливу:

- Об'ємні атаки – спрямовані на перевантаження пропускної здатності мережі. Зазвичай це UDP-флуд, ICMP-флуд або SYN-флуд, коли величезна кількість запитів надсилається одночасно.
- Атаки на рівні протоколів – використовують недоліки в мережевих протоколах, наприклад, DNS або NTP-ампліфікації.
- Атаки прикладного рівня – орієнтовані на конкретні веб-додатки чи служби, наприклад, HTTP-флуд або атаки типу Slowloris.

Іноді хакери комбінують кілька типів атак, щоб зробити їх ефективнішими та ускладнити виявлення.

Цілі та мотиви зловмисників

Мотиви здійснення DDoS-атак можуть бути найрізноманітнішими:

- Політичні. Хакери атакують державні сайти, ЗМІ або організації для того, щоб висловити протест чи тиск на владу.
- Фінансові. Деякі групи вимагають викуп за припинення атаки або намагаються паралізувати роботу конкурентів.
- Саботаж. Конкуренти можуть замовляти DDoS-атаки, щоб зірвати роботу бізнесу.
- Кібервандалізм. Дії без конкретної мети, просто заради розваги або демонстрації власних можливостей.
- Кібервійна. У сучасних геополітичних умовах атаки можуть бути елементом міждержавного протистояння.

Приклади відомих DDoS-атак

- WikiLeaks (2010). Після публікації секретних документів сайт зазнав потужної DDoS-атаки, через що став тимчасово недоступним.
- GitHub (2018). Один із найпотужніших випадків в історії, коли обсяг шкідливого трафіку перевищив 1,3 терабайта на секунду.
- Банки США (2012). Серія атак на провідні фінансові установи призвела до порушення роботи онлайн-банкінгу.

Ці приклади демонструють, що DDoS-атаки можуть мати різну природу, масштаб і мотиви, але завжди завдають значної шкоди.

Захист від DDoS-атак

Ефективний захист вимагає комплексного підходу, який включає технічні, організаційні та освітні заходи.

1. Фільтрація трафіку. На рівні маршрутизаторів і міжмережевих екранів можна блокувати підозрілий трафік.
2. Використання CDN. Контент-мережі допомагають розподіляти навантаження між серверами по всьому світу.
3. Системи виявлення вторгнень (IDS/IPS). Такі рішення аналізують трафік і автоматично блокують підозрілі запити.
4. Розподілений захист. Поєднання локальних і хмарних систем безпеки дозволяє швидше виявляти та реагувати на атаки.

Рекомендації:

- Створюйте резервну інфраструктуру.
- Плануйте алгоритм дій під час атаки.
- Регулярно оновлюйте програмне забезпечення.
- Проводьте навчання персоналу.
- Використовуйте багатофакторну автентифікацію та надійні паролі.

Інструменти для моніторингу та аналізу

Серед популярних засобів моніторингу трафіку можна виділити:

- Snort – система для виявлення вторгнень, що аналізує пакети даних у реальному часі.
- Suricata – глибоко перевіряє мережеві потоки та дозволяє виявляти аномалії.
- Wireshark – дає змогу досліджувати деталі трафіку на низькому рівні.

- Firewalls і DDoS Protection Appliances – спеціалізовані пристрої для блокування атак.

Сьогодні також широко застосовуються хмарні сервіси захисту (DDoS Protection as a Service), які можуть автоматично масштабувати ресурси для нейтралізації атак у режимі реального часу.

Майбутнє DDoS-атак

Технологічний прогрес несе не лише нові можливості, але й нові ризики. Потужність DDoS-атак зростатиме разом із розвитком штучного інтелекту, машинного навчання та Інтернету речей (IoT). Багато IoT-пристроїв мають слабкий захист, тому вони часто стають частиною ботнетів.

У майбутньому очікується також поява DDoS-атак, які зможуть адаптуватися до захисних систем у реальному часі. Це означає, що захист теж має стати «розумним» – використовувати аналітику, штучний інтелект і автоматичне реагування на загрози.

Висновок

DDoS-атаки є однією з найсерйозніших загроз у кіберпросторі. Вони можуть паралізувати роботу компаній, знищити репутацію бренду та спричинити мільйонні збитки. Тому боротьба з ними – це не одноразова дія, а постійний процес, який включає навчання, модернізацію інфраструктури, аналіз ризиків і впровадження новітніх технологій.

Розуміння принципів роботи DDoS-атак і застосування сучасних методів протидії дозволяють суттєво підвищити рівень безпеки інформаційних систем. Адже в умовах цифрової епохи лише той, хто готовий до нових викликів, може зберегти свої дані та забезпечити стабільність роботи своїх сервісів.

Список використаних джерел:

1. URL: https://foxminded.ua/ddos-ataka/.
2. URL: https://iitd.ua/najkrashhi-metodi-zapobigannya-ta-zahistu-vid-ddos-atak/.

ІГНАТЬЄВ А. М.,
кандидат наук з державного управління,
Національний університет оборони України

ВИЗНАЧЕННЯ СТАНУ ВОЄННОЇ БЕЗПЕКИ НА ЗАСАДАХ ВИКОРИСТАННЯ ЙМОВІРНІСНОЇ МОДЕЛІ РЕАЛІЗАЦІЇ НАЦІОНАЛЬНОГО ІНТЕРЕСУ

Аналіз відомих досліджень і публікацій, свідчить що у світовій та вітчизняній науковій думці і практиці питання реалізації національних інтересів, визначення їх методології та політико-правових засад є предметом дослідження таких вчених як Г. Моргентау, Дж. Розенау,

В. П. Горбулін, А. Б. Качинський, А. Кузьменко, Ф. Медвідь, В. О. Саламатов та інші. Проблематику геополітичного іміджу у своїх наукових розвідках розглядали Е. А. Галумов, К. С. Гаджиев, Д. Е. Замятин. Разом із тим, на теперішній час комплексних досліджень та отриманих результатів щодо розробки теоретичної моделі реалізації національного інтересу не існує і не проводяться, що обґрунтовує актуальність мети такого дослідження.

У виступі обґрунтовано, що на теперішній час проблема визначення стану та рівня воєнної безпеки держави у цілому з урахуванням усіх національних інтересів у сфері воєнної безпеки є актуальним науковим питанням.

Головна ідея запропонованого автором дослідження ґрунтується на реалізації чотирьох етапів: формуванні повного переліку (множини) національних інтересів у сфері воєнної безпеки; визначення переліку небезпек і загроз для кожної системи реалізації; формуванні системи реалізації кожного національного інтересу; визначення ступеню впливу небезпек, загроз на кожну систему реалізації національного інтересу з урахування ступеня захищеності останньої системою забезпечення воєнної безпеки держави .

Ґрунтуючись на зазначеній головній ідеї, в доповіді розкрито авторський підхід щодо формування моделі реалізації національного інтересу особливістю якої є спроможність враховувати стан системи реалізації кожного національного інтересу в контексті впливу на неї загрози (загроз) та/або відсутності цього впливу з одночасним врахуванням різноманітності структури системи реалізації кожного національного інтересу та ступеня захищеності системою забезпечення воєнної безпеки держави.

Визначення стану воєнної безпеки у дослідженні запропоновано на основі ймовірнісної моделі реалізації національного інтересу. Запропонована модель надає можливість враховувати різноманітності структури системи реалізації кожного національного інтересу, визначати здатність блоку нормативно-правових актів забезпечувати процедурне функціонування підсистеми реалізації національного інтересу та виконувати комплекс заходів щодо збереження структури системи реалізації національного інтересу. Врахування зазначених чинників дозволяє адекватно та достатньо глибоко описати процес реалізації кожного (будь-якого) національного інтересу. Додатково модель надає можливість виявляти ступінь зменшення впливу загрози на систему реалізації національного інтересу в результаті адекватного реагуванням системи забезпечення воєнної безпеки держави, що максимально наближає імовірнісну модель реалізації національного інтересу до реального стану воєнної безпеки.

НЕКЛОНСЬКИЙ І. М.,
кандидат військових наук,
старший викладач кафедри
організації і проведення
аварійно-рятувальних робіт,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

СТРУКТУРНО-ФУНКЦІОНАЛЬНА МОДЕЛЬ МІЖВІДОМЧОЇ ВЗАЄМОДІЇ

В умовах збройної агресії рф зростає значимість взаємодії різнорідних сил (сили цивільного захисту, сили сектору безпеки і оборони, міжнародні організації тощо) під час реалізації заходів із забезпечення національної безпеки. Це потребує системного підходу щодо дослідження взаємодії з урахуванням сучасних еволюційних процесів розвитку форм і способів застосування відповідних формувань [1]. Крім того, введення в дію Доктрини «Цивільно-військове співробітництво» (2020 р.), потребує дослідження шляхів та механізмів її реалізації [2].

За визначенням «взаємодія – це заздалегідь узгоджені дії, що ведуться кожним із суб'єктів взаємодії з метою виконання свого завдання з урахуванням дій протилежних суб'єктів взаємодії, з витратою частини власних ресурсів для виконання завдань взаємодіючих сторін та з відповідною витратою ними частини своїх ресурсів для інших суб'єктів взаємодії у своїх інтересах». Суть взаємодії полягає в діях та заходах взаємодіючих суб'єктів, які базуються на відповідних нормативно-правових домовленостях і координуються на всіх рівнях під час виконання відповідних завдань.

Для дослідженні системи управління, як правило, використовуються мультиагентна [3,4] або структурно-функціональна [5] концепції. З урахуванням відповідних концепцій структурно-функціональну модель взаємодії можна представити у вигляді сукупності шести множин (двох суб'єктів взаємодії (СбВ)), де елементи двох СбВ пов'язані структурно-функціональними базисами взаємодії:

– множина структурних елементів СбВ1 – $S_i = \{u_1\}$, де $u_1 = 1,..., r_1$ – номер структурного елемента СбВ1;

– множина структурних елементів СбВ2 – $S_j = \{u_2\}$, де $u_2 = 1,..., r_2$ – номер структурного елемента СбВ2;

– множина функціональних елементів СбВ1 – $F_i = \{k_1\}$, де $k_1 = 1,..., p_1$ – номер функціонального елемента СбВ1;

– множина функціональних елементів СбВ2 – $F_j = \{k_2\}$, де $k_2 = 1,..., p_2$ – номер функціонального елемента СбВ2;

– множина завдань СбВ1 – $G_i = \{g_i\}$, де $i = 1,...,m$ – номер завдання СбВ1 під час реалізації заходів із забезпечення національної безпеки;

– множина завдань СбВ2 – $G_j = \{g_j\}$, де $j = 1,...,n$ – номер завдання СбВ2 під час реалізації заходів із забезпечення національної безпеки.

Під варіантом взаємодії будемо розуміти одне з можливих поєднань двох структурно-функціональних елементів, між якими може бути налагоджена взаємодія при вирішенні певних завдань.

Сформована структурно-функціональна модель взаємодії може бути представлена у вигляді неорієнтованого графа $G = (V, E)$ (рис. 1), де V – множина вершин графа, що відповідає кількості елементів системи, E – множина ребер, що відповідає кількості відносин між елементами системи.

Введення елементів теорії графів дозволяє відобразити структурність формальної моделі, наочним чином представити встановлені зв'язки між учасниками. Апарат графів дає можливість описувати варіанти взаємодії за допомогою матриць суміжності. Матрицею суміжності A графа G будемо вважати квадратну $n \times n$ - матрицю, в якій елемент a_{ij} i-го рядка та j-го стовпчика дорівнює 1, якщо вершини v_i та v_j з номерами i та j суміжні, і дорівнює 0 в іншому разі. Таким чином отримаємо матриці суміжності графів, що можуть бути побудовані на основі моделі рис. 1. Елементарними перетвореннями над рядками і стовпцями матриці шляхом викреслювання нульового рядка і стовпця отримаємо необхідні алгебраїчні аналоги відповідних графів, де $a_{ij} = 1$, якщо взаємодії має бути відпрацьована, $a_{ij} = 0$, якщо взаємодія не потрібна.

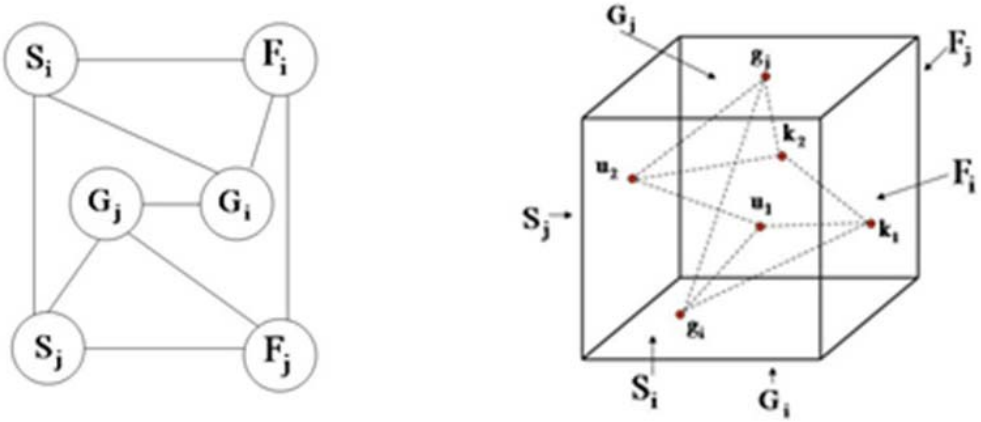

Рисунок 1 – Граф структурно-функціональної моделі взаємодії: S_i – множина структурних елементів СбВ1 (r_1); S_j – множина структурних елементів СбВ2 (r_2); F_i – множина функціональних елементів СбВ1 (p_1); F_j – множина функціональних елементів СбВ2 (p_2); G_i – множина завдань СбВ1 (m); G_j – множина завдань СбВ2 (n)

Список використаних джерел:

1. Семененко О., Митченко С., Добровольський Ю., Ремез А., Ярмольчик М., Твердохліб Є. Еволюція форм і способів застосування угруповань військ (сил): тенденції збройної боротьби. Social Development and Security. 2024. 14(3). С. 33–52. URL: https://doi.org/10.33445/ sds.2024.14.3.3.
2. Цивільно-військове співробітництво у захисті населення під час війни в Україні. Аналітична доповідь Центра Разумкова. Київ, 2023. 73 с. URL: https://razumkov.org.ua/images/2024/02/2024-Sunhurovskyi-CIVIL-WAR-1-F.pdf.
3. Будур І. М., Бойко С. А. Мультиагентна модель системи підтримки прийняття рішення по управлінню розподіленими об’єктами. Системи озброєння і військова техніка. 2020. № 3 (63). С. 54–61. DOI: https://doi.org/10.30748/soivt.2020.63.08.
4. Коноваленко О. Є., Брусенцев В. О. Мультиагентні системи управління та підтримки прийняття рішень Вісник Національного технічного університету «ХПІ». Серія: Машинознавство та САПР. 2019. № 1. С. 18–27. DOI: https://doi.org/10.20998/2079-0775.2019.1.03.
5. Гута С.С. Структурно-функціональна модель системи державного управління в умовах кризових ситуацій, зумовлених воєнно-політичними чинниками. Державне управління: удосконалення та розвиток. 2020. № 2. URL: http://www.dy.nayka.com.ua/?op=1&z=1578 (дата звернення: 29.10.2025). DOI: 10.32702/2307-2156-2020.2.100.

ТИЩЕНКО Є. О.,
доктор технічних наук, професор,
професор кафедри автоматичних систем
безпеки та електроустановок,
Навчально-науковий інститут пожежної
та техногенної безпеки
Національного університету
цивільного захисту України

КОТЛЯР Д. О.,
ад’юнкт докторантури-ад’юнктури,
Національний університет
цивільного захисту України

АНАЛІЗ НЕБЕЗПЕК ДЛЯ РЯТУВАЛЬНИКІВ ПРИ ЛІКВІДАЦІЇ НАДЗВИЧАЙНИХ СИТУАЦІЙ НА ОБ’ЄКТАХ ЗІ ЗРУЙНОВАНОЮ ЧИ ПОШКОДЖЕНОЮ СИСТЕМОЮ БЛИСКАВКОЗАХИСТУ

Сучасні виклики у сфері ліквідації наслідків надзвичайних ситуацій (НС) актуалізують важливу проблему, що стосується діяльності рятувальних підрозділів на об’єктах із пошкодженими або зруйнованими системами блискавкозахисту (БЗ) [1].

Актуальність теми зумовлена рядом важливих факторів. По-перше, метеорологічні спостереження та аналітичні дані служб цивільного захисту, як в Україні, так і у світі, свідчать про зростання інтенсивності та частоти грозових явищ. Це безпосередньо підвищує ризик ураження інфраструктурних об’єктів блискавкою, а відтак, суттєво збільшує

небезпеку для рятувальників, які працюють у зонах надзвичайних ситуацій, особливо під час грозової активності [6]. По-друге, руйнування або пошкодження систем блискавкозахисту внаслідок бойових дій, пожеж, вибухів чи стихійних лих створює надзвичайно небезпечне середовище [3]. У таких умовах різко зростає ймовірність ураження електричним струмом через неконтрольоване розповсюдження струму блискавки, а також через вторинні ефекти − сплески напруги чи крокову напругу. Крім того, підвищується ризик виникнення вторинних надзвичайних подій − пожеж, вибухів або коротких замикань, зумовлених небезпечними електричними розрядами, особливо за наявності пошкоджених комунікацій або вибухонебезпечних матеріалів.

До основних небезпек, що загрожують рятувальникам, під час ліквідації надзвичайних ситуацій на об'єктах зі зруйнованою чи пошкодженою системою блискавкозахисту належать такі фактори:

а) пряме ураження блискавкою під час активної грози – рятувальники, що працюють на відкритих або частково пошкоджених конструкціях під час грози, ризикують бути у зоні повторних ударів;

б) несподівані струмові шляхи через пошкоджені елементи LPS (ринги, струмоводи, заземлювачі) якщо громовідвідні елементи деформовані або переломані, струм блискавки (або залишковий потенціал після розряду) може проходити через металеві конструкції, арматуру, покрівельні елементи, труби, крани, обладнання − тобто через те, що рятувальники можуть торкатися. Через це підвищується ризик отримати електротравму при контакті з ураженими поверхнями; в) небезпека від замикань і перенапруг у електромережах/обладнанні − це прямий або близький удар може спричинити замикання, пошкодження ізоляції й створити напругу на корпусах обладнання. Пошкоджена система блискавкозахисту знизить контрольований відвід струму в землю;

г) пожежі, спалахи та вибухи − індустріальні об'єкти (резервуари, легкозаймисті рідини, газо-повітряні суміші) підвищують ризик вторинних пожеж і вибухів при ураженні блискавкою. Пошкоджений LPS може не відвести імпульсний струм, що підвищує шанс займання;

д) структурні ушкодження й нестабільність − удар блискавки та супутні пожежі можуть порушити несучу здатність конструкцій; рятувальники ризикують впасти або бути травмованими уламками;

е) ризики при наданні допомоги постраждалим під час грози − торкання потерпілого без оцінки безпеки довкола може поставити рятувальника під ризик, хоча надання першої допомоги після стихання грози є безпечним за рекомендаціями медичних позицій [4, 5].

Система блискавкозахисту (LPS) призначена для безпечного відведення струму блискавки в землю через спеціальні струмовідводи та заземлювачі [1]. Коли окремі її елементи зруйновані або пошкоджені, струм розряду шукає альтернативні шляхи через металеві конструкції, комунікації або обладнання будівлі. Це призводить до появи небезпечних потенціалів на поверхнях, до яких може торкатися людина. Крім

того, пошкодження або корозія заземлювальної системи підвищує її опір, що спричиняє локальне накопичення високих напруг у ґрунті навколо точки розряду. У результаті навіть короткочасний контакт із металевими елементами чи перебування поруч може призвести до ураження електричним струмом [1].

Комплекс заходів щодо забезпечення електробезпеки рятувальників і захисту технічних засобів від впливу блискавки під час аварійно-рятувальних операцій:

1. Оцінка метеоумов. Перед початком робіт необхідно здійснити оцінку погодних умов та визначити наявність активної грозової діяльності. У разі триваючої грози або високої ймовірності ударів блискавки слід утриматися від виконання робіт на відкритих або висотних ділянках. Персонал має бути своєчасно евакуйований до безпечних укриттів.

2. Ізоляція та деенергізація електромереж. За можливості слід відключити або ізолювати джерела електроживлення, припинивши подачу напруги на пошкоджене обладнання. Координацію таких дій необхідно проводити спільно з персоналом електротехнічного обслуговування або операторами об’єкта. Незважаючи на імпульсний характер струму блискавки, своєчасне відключення живлення дозволяє запобігти вторинним замиканням у мережі та ураженню електричним струмом.

3. Уникнення контакту з провідними елементами. Рятувальникам слід утримуватися від дотику до металевих конструкцій, комунікацій та елементів обладнання, які потенційно можуть залишатися під напругою, особливо після нещодавнього удару блискавки. Перед початком робіт необхідно переконатися у безпечному потенціалі таких елементів. Рекомендується створювати безпечні робочі зони та застосовувати принципи рівноважної потенціальної зони − зокрема, здійснювати попереднє з’єднання (бондінг) металевих частин, що можуть бути під різними потенціалами. Застосування засобів індивідуального захисту та спеціального інструменту. Під час проведення робіт необхідно використовувати діелектричні рукавички, ізолюючі матеріали, інструменти з ізольованими ручками, а також засоби захисту при роботі на висоті. Звичайні робочі рукавиці не забезпечують належного рівня електробезпеки у разі наявності залишкових потенціалів.

4. Контроль стану заземлення та вимірювання потенціалів. Перед початком робіт рекомендується перевірити ефективність заземлення об’єкта та здійснити вимірювання потенціалів за допомогою електронних тестерів або вольтметрів із високим вхідним імпедансом. Це дозволяє виявити небезпечні напруги дотику та кроку.

5. Координація дій із власником або оператором об’єкта. Перед початком робіт рятувальники повинні отримати технічну інформацію − плани системи блискавкозахисту (LPS), схеми заземлення, а також дані щодо потенційно небезпечних зон (резервуарів, сховищ легкозаймистих речовин тощо).

6. Документування стану системи блискавкозахисту. У процесі ліквідації наслідків надзвичайної ситуації необхідно фіксувати наявні пошкодження елементів LPS. Такі відомості мають бути внесені до оперативних звітів для подальшого аналізу, планування ремонтних робіт та запобігання повторним ризикам у майбутньому [7, с. 120].

Тактичні підходи під час робіт на різних типах об’єктів:

а) промислові та нафтогазові підприємства. Першочергово необхідно перевіряти наявність легкозаймистих парів у повітрі, оскільки навіть незначна іскра від пошкодженого обладнання може призвести до вибуху. Дії рятувальників мають бути скоординовані з інженерно-технічним персоналом об’єкта: слід перекрити клапани, зупинити технологічні процеси та організувати охолоджувальні бар’єри для запобігання займанням;

б) висотні споруди та покрівлі. Під час грози необхідно утримуватися від виконання робіт на дахах. Перед початком дій потрібно перевірити справність систем відведення струму блискавки, а також виявити металеві елементи або арматуру, які можуть перебувати під напругою;

в) електроустановки та трансформаторні підстанції. На таких об’єктах існує високий ризик пошкодження обладнання та наявності залишкової напруги. Вхід рятувальників дозволяється лише після офіційного підтвердження енергопостачальної організації про повне відключення електроживлення [3, 5]. Ключові рекомендації на рівні підготовки персоналу: інтеграція оцінки систем блискавкозахисту (LPS) у стандартні процедури розвідки місця події та післяінцидентні звіти; розроблення навчальних програм для рятувальників, які охоплюватимуть основи електробезпеки: поняття потенціалу дотику і крокового потенціалу, принципи еквіпотенціального вирівнювання та базові методи перевірки заземлення; посилення взаємодії з інженерно-технічними службами об’єктів для забезпечення своєчасного доступу до схем систем блискавкозахисту та планів заземлення ще до початку аварійно-рятувальних робіт [6, с. 48].

Можна говорити про те, що проведений аналіз засвідчує, що пошкодження або руйнування систем блискавкозахисту створює значні ризики для рятувальників під час ліквідації наслідків надзвичайних ситуацій, особливо в умовах грозової активності. Забезпечення електробезпеки особового складу вимагає комплексного підходу − від технічного контролю стану LPS до впровадження спеціалізованих навчальних програм і чіткої координації дій з інженерними службами. Реалізація таких заходів сприятиме мінімізації ризиків ураження електричним струмом і підвищить загальну ефективність аварійно-рятувальних операцій.

Список використаних джерел:

1. ДСТУ EN 62305-1:2012 Захист від блискавки. Частина 1. Загальні принципи (EN 62305-1:2011, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=29300.
2. ДСТУ EN 62305-2:2022 Захист від блискавки. Частина 2. Управління ризиками (EN 62305-2:2012, IDT; IEC 62305-2:2010, MOD). URL: https:// online.budstandart.com/ua/catalog/doc-page.html?id_doc=107970.
3. ДСТУ EN 62305-3:2021 Блискавкозахист. Частина 3. Фізичні пошкодження будівель (споруд) та небезпека для життя (EN 62305-3:2011, IDT; IEC 62305-3:2010, MOD). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=96752.
4. ДСТУ EN 62305-4:2012 Захист від блискавки. Частина 4. Електричні та електронні системи, розташовані в будинках і спорудах (EN 62305-4:2011, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=29303.
5. НПАОП 40.1-1.32-01 (ДНАОП 0.00-1.32-01) Правила будови електроустановок. Електрообладнання спеціальних установок. URL: https://zakon.rada.gov.ua/rada/show/ v0272203-01#Text.
6. Ковальчук В. М., Бондаренко І. В. *Електробезпека в надзвичайних ситуаціях: навчальний посібник.* Київ : ІДУЦЗ, 2020.
7. Мартинюк В. Ф. *Електротехнічна безпека: теорія, практика, стандарти.* Київ : Техніка, 2019.

ФОРНОЛЯК В. М.,
кандидат психологічних наук,
Національна академія Служби безпеки України

МІЖВІДОМЧА ВЗАЄМОДІЯ СУБ'ЄКТІВ БОРОТЬБИ З ТЕРОРИЗМОМ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

У сучасному інформаційно-глобалізованому середовищі загрози тероризму стають багатовимірними, вони охоплюють не лише військові чи правоохоронні аспекти, а й соціально-політичні, інформаційні, кібернетичні. У зв'язку з цим ефективна протидія таким загрозам неможлива виключно силами лише однієї державної структури, тут необхідна скоординована діяльність різних суб'єктів, що реалізують заходи з національної безпеки.

Зазначимо, що поняття «міжвідомчої взаємодії» у цьому контексті означає систему організаційних, правових та процедурних механізмів, які забезпечують узгоджене виконання завдань різними органами державної влади та силовими структурами з метою запобігання, виявлення та нейтралізація терористичної діяльності та пов'язаних із нею загроз. Водночас відмітимо, що зазначена взаємодія передбачає, що різні державні суб'єкти (зокрема, Служба безпеки України (СБУ), Міністерство внутрішніх справ України (МВС), Державна прикордонна служба України (ДПСУ), Збройні сили України (ЗСУ), Державна служба

України з надзвичайних ситуацій (ДСНС) тощо) об'єднують свої повноваження, ресурси, інформацію й координаційні заходи задля спільної відповіді на загрозу.

В Україні правове регулювання взаємодії суб'єктів у сфері боротьби з тероризмом базується на низці законодавчих актів та міжнародних угод. Зауважимо, що згідно зі статтею 26 Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV [1], Україна здійснює міжнародне співробітництво з іноземними державами, правоохоронними органами та міжнародними організаціями у боротьбі з тероризмом. Окрім того, нормативно-правове поле включає акти щодо єдиної державної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків [2]. Міжнародно-правові інструменти також відіграють ключову роль: Організація Об'єднаних Націй (ООН) надає перелік правових актів, спрямованих на боротьбу з тероризмом [3], що встановлюють механізми співпраці держав-учасниць, екстрадиції, правової допомоги тощо.

До суб'єктів боротьби з тероризмом належать державні органи, які визначені статтею 4 Закону України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV [1] та здійснюють профілактичну, оперативно-розшукову, антитерористичну та кризову діяльність. У межах міжвідомчої взаємодії вони виконують різні функції: збір та аналіз інформації, превенція та профілактика, реагування на загрозу, забезпечення правопорядку, координація дій у кризових ситуаціях. Організація такої взаємодії передбачає створення координаційних механізмів (наприклад, співпраця між регіональними підрозділами, обмін інформацією, проведення спільних навчань). У законодавстві України чітко зазначено, що суб'єктами боротьби з тероризмом є відповідні органи, які мають повноваження щодо виявлення, припинення, розслідування терористичних проявів.

Можемо стверджувати, що міжвідомча взаємодія має суттєве значення у контексті національної безпеки та оборони, оскільки: забезпечує цілісність державної відповіді на терористичні загрози, уникаючи дублювання функцій та «вузького» підходу; підвищує швидкість реагування та ефективність дій в умовах кризових ситуацій; сприяє оптимальному використанню ресурсів силових структур, інформаційних систем, аналітики; зміцнює довіру громадськості до державних інституцій завдяки погодженій та однозначній комунікації; забезпечує сумісність з міжнародними партнерами та включає Україну у глобальні/регіональні механізми боротьби з тероризмом.

Міжвідомча взаємодія у сфері боротьби з тероризмом ґрунтується на чітко визначених організаційних і функціональних механізмах, що забезпечують ефективну координацію діяльності силових структур, органів державного управління, правоохоронних органів і військових формувань України. Її системоутворюючим елементом виступає Антитерористичний центр при Службі безпеки України (АТЦ при СБУ), який

є координуючим органом у межах єдиної державної системи боротьби з тероризмом [1].

АТЦ при СБУ здійснює загальне керівництво організацією та проведенням антитерористичних операцій, координує діяльність суб'єктів боротьби з тероризмом, забезпечує обмін інформацією між ними та розробляє методичні рекомендації щодо дій у кризових ситуаціях [4]. До складу координаційної групи при АТЦ входять представники Міністерства внутрішніх справ України, Міністерства оборони, Державної прикордонної служби, Національної поліції, ДСНС, Офісу Генерального прокурора, місцевих органів влади тощо.

Завдяки цьому створюється механізм єдиного управління під час проведення антитерористичних операцій, що дає змогу оперативно реагувати на загрози, уникати дублювання функцій і мінімізувати людські та матеріальні втрати.

Ключовим напрямом міжвідомчої взаємодії є обмін розвідувальною, оперативною та аналітичною інформацією. У межах виконання завдань із виявлення та нейтралізації терористичних загроз використовуються спільні інформаційно-аналітичні бази даних, механізми міжвідомчого запиту та інтегровані комунікаційні системи [5]. Зокрема, підрозділи СБУ тісно співпрацюють із МВС і Національною поліцією щодо ідентифікації осіб, причетних до терористичної діяльності, відстеження каналів фінансування тероризму, а також із Збройними силами України у питаннях ліквідації терористичних груп у зоні бойових дій.

Формами практичної взаємодії є проведення спільних оперативно-профілактичних заходів, антитерористичних навчань і тренувань із відпрацювання алгоритмів спільних дій у разі терористичного акту. Такі заходи підвищують узгодженість дій, інформаційну сумісність і рівень готовності до кризових сценаріїв [6].

Важливим елементом організаційної взаємодії є узгодження діяльності суб'єктів боротьби з тероризмом у системі національної безпеки та оборони. Відповідно до положень Стратегії національної безпеки України (Указ Президента № 392/2020) [7], боротьба з тероризмом розглядається як міжвідомчий процес, що вимагає спільного планування, управління й контролю. При цьому координація забезпечується через Раду національної безпеки і оборони України (РНБО), Кабінет Міністрів України, а також міжвідомчі робочі групи при СБУ та МВС. Особливу увагу приділено забезпеченню інформаційної сумісності та захисту комунікаційних каналів, оскільки обмін інформацією між різними структурами має стратегічне значення в умовах гібридної війни та кібератак.

Разом з тим, слід відзначити, що Україна активно співпрацює з міжнародними партнерами, зокрема Європейським Союзом, НАТО, ОБСЄ, Інтерполом та ООН у межах спільних програм із протидії тероризму, відмиванню коштів і незаконному обігу зброї [8]. СБУ як

головний координатор взаємодіє з відповідними органами держав-партнерів, отримує аналітичні матеріали та бере участь у програмах обміну досвідом, зокрема у межах Програми НАТО «Партнерство заради миру» [9]. Такі міжнародні комунікації зміцнюють міжвідомчі зв'язки й сприяють імплементації європейських стандартів у національну систему протидії тероризму.

Попри нормативно визначені засади координації діяльності суб'єктів боротьби з тероризмом, сучасна практика виявляє низку проблемних аспектів, що ускладнюють ефективність взаємодії. Однією з ключових проблем є фрагментарність інформаційних потоків між державними структурами, зокрема відомча закритість, різні протоколи обміну даними та відсутність єдиних стандартів комунікації часто призводять до втрати оперативності під час реагування на терористичні загрози. Другою значущою проблемою є недостатній рівень координації під час планування та реалізації спільних антитерористичних операцій. Деякі дослідники зазначають, що міжвідомчі органи іноді діють за відомчими інтересами, що створює ризики дублювання функцій або суперечностей у прийнятті рішень [10]. Суттєвим викликом залишається правове та організаційне забезпечення міжвідомчого обміну інформацією у сфері кібербезпеки, оскільки зростання кількості кібертерористичних проявів вимагає спільного реагування СБУ, Держспецзв'язку, Національної поліції та Збройних сил України.

Крім того, вплив зовнішніх гібридних загроз зумовлює потребу в посиленні стратегічних комунікацій між силовими структурами та органами державної влади, а також у виробленні єдиного наративу державної інформаційної політики у сфері національної безпеки.

Хочеться акцентувати увагу на тому, що удосконалення міжвідомчої взаємодії в сфері боротьбі з тероризмом має ґрунтуватися на принципах інституційної єдності, прозорості та оперативної координації. Одним із перспективних напрямів є створення інтегрованої системи управління безпековими процесами з використанням сучасних цифрових технологій і аналітичних платформ обміну даними між суб'єктами антитерористичної діяльності [11]. Важливим кроком є посилення ролі Антитерористичного центру при Службі безпеки України як координатора міжвідомчої взаємодії, зокрема у питаннях спільного планування, навчань і оцінки ефективності антитерористичних заходів.

Підвищення ефективності, на нашу думку, можливо досягти через удосконалення нормативно-правового забезпечення – гармонізацію українського законодавства з європейськими стандартами у сфері безпеки, що сприятиме поглибленню міжнародного співробітництва. Окремо варто наголосити на необхідності розвитку системи професійної підготовки кадрів, які мають бути компетентними у сфері кризового управління, стратегічних комунікацій, аналізу ризиків та міжвідомчої координації.

Таким чином, міжвідомча взаємодія суб'єктів боротьби з тероризмом є невід'ємною складовою системи забезпечення національної безпеки та оборони України, яка передбачає узгодженість дій, спільну відповідальність і високий рівень координації між усіма структурами сектору безпеки.

У сучасних умовах гібридних загроз та ескалації терористичних ризиків, ефективність цієї взаємодії безпосередньо визначає результативність державної політики у сфері протидії тероризму. Вона має базуватись на принципах єдності стратегічного управління, інтегрованості інформаційних ресурсів, оперативності прийняття рішень та комунікаційної узгодженості між суб'єктами системи. Ключовими чинниками підвищення ефективності міжвідомчої взаємодії виступають: цифровізація управлінських і аналітичних процесів, що забезпечує швидкий обмін інформацією та прогнозування загроз; розвиток культури спільного реагування, заснованої на довірі, професійній компетентності та взаємній відповідальності між органами безпеки; формування єдиного стратегічного наративу у сфері комунікацій, що дозволяє узгодити дії всіх державних структур у контексті інформаційної безпеки; адаптація української практики міжвідомчої координації до стандартів ЄС і НАТО, що сприятиме посиленню інтеграційних можливостей держави у міжнародній системі безпеки.

Отже, подальший розвиток системи міжвідомчої взаємодії у боротьбі з тероризмом має відбуватись у напрямі створення інтегрованого національного безпекового простору, заснованого на технологічній взаємодії, правовій узгодженості та спільній підготовці кадрів. Реалізація цих завдань забезпечить підвищення стійкості держави до терористичних та гібридних загроз, а також сприятиме формуванню ефективної, проактивної та скоординованої системи національної безпеки України.

Список використаних джерел:

1. Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV. Відомості Верховної Ради України. 2003. № 25. Ст. 180. URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 27.10.2025).
2. Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків : Постанова Кабінету Міністрів України від 18.02.2016 № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF (дата звернення: 27.10.2025).
3. United Nations. International legal instruments to counter terrorism. URL: https://www.un.org/counterterrorism/ru/international-legal-instruments (дата звернення: 27.10.2025).
4. Служба безпеки України. Антитерористичний центр при СБУ : офіційний сайт. URL: https://atc.ssu.gov.ua/ (дата звернення: 27.10.2025).
5. Герасименко О. М., Сірий О. В. Нормативно-правове забезпечення міжнародного співробітництва СБУ під час протидії кримінальним правопорушенням на об'єктах критичної інфраструктури. Аналітично-порівняльне правознавство.

2025. № 3. URL: https://journal-app.uzhnu.edu.ua/article/view/335211 (дата звернення: 27.10.2025).
6. Служба безпеки України. Звіт про діяльність у сфері протидії тероризму, 2024 р. URL: https://ssu.gov.ua/terrorism (дата звернення: 27.10.2025).
7. Про Стратегію національної безпеки України : Указ Президента України № 392/2020. Офіційний вісник Президента України. 2020. № 7. Ст. 234. URL: https://zakon.rada.gov.ua/laws/show/392/2020 (дата звернення: 27.10.2025).
8. European External Action Service (EEAS). EU–Ukraine cooperation in counter-terrorism. URL: https://www.eeas.europa.eu/ (дата звернення: 27.10.2025).
9. NATO. Counter-terrorism cooperation with Ukraine. URL: https://www.nato.int/ (дата звернення: 27.10.2025).
10. Кононенко С. В. Координаційні механізми діяльності суб'єктів боротьби з тероризмом. Право і безпека, 2022. № 3. С. 45–52. URL: https://pb.univd.edu.ua/ (дата звернення: 27.10.2025).
11. Кузьменко, О. В. Сучасні підходи до цифрової трансформації системи національної безпеки України. Вісник НАДУ, 2023. № 2. С. 73–81. URL: https://vadnd.org.ua/ (дата звернення: 27.10.2025).

ЯВОРСЬКИЙ А. О.,
курсант, Харківський національний університет внутрішніх справ

ВАЛЕРСЬКИЙ Н. С.,
курсант, Харківський національний університет внутрішніх справ

КІРІКА Д. В.,
кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ (науковий керівник)

ШЛЯХИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ ВЗАЄМОДІЇ СИЛ ОБОРОНИ ТА ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ У ПЕРІОД ЗБРОЙНОЇ АГРЕСІЇ

В умовах збройної агресії російської федерації забезпечення національної безпеки України стало особливо актуальним завданням державних органів. Ефективність протидії загрозам значною мірою залежить від координації дій сил оборони та правоохоронних органів, що здійснюють контроль, охорону та оборону критично важливих об'єктів і територій. Організаційні механізми взаємодії забезпечують оперативне реагування на загрози, обмін інформацією та злагодженість дій у реальному часі, а правове регулювання визначає повноваження, відповідальність і межі діяльності кожного суб'єкта сектору безпеки. Аналіз правових та організаційних аспектів такої взаємодії має ключове значення для підвищення обороноздатності та стабільності держави.

Взаємодія Сил оборони України та правоохоронних органів під час збройної агресії є складною системою організаційних і правових відносин, які регулюються як національним законодавством, так і підзаконними нормативними актами, наказами та інструкціями відповідних органів. Основою такої взаємодії є Конституція України, яка визначає права та обов'язки держави щодо забезпечення національної безпеки та оборони, гарантує верховенство закону і встановлює правові рамки діяльності збройних сил та правоохоронних органів [1].

Одним із ключових законодавчих актів, що регламентує координацію діяльності Сил сектору безпеки, є Закон України «Про національну безпеку України» [2], який визначає принципи взаємодії органів виконавчої влади, зокрема Міністерства оборони, Служби безпеки України, Національної поліції, Державної прикордонної служби та інших суб'єктів сектору безпеки. Цей закон передбачає, що під час загроз національній безпеці органи повинні діяти узгоджено, дотримуючись законності та конституційних норм, що дозволяє забезпечити ефективну координацію оперативних і оборонних заходів. Додатково, взаємодія регламентується спеціальними законами, такими як «Про Збройні Сили України» [3], «Про Службу безпеки України» [4], «Про Національну поліцію» [5], «Про Державну прикордонну службу України» [6], які визначають повноваження органів у мирний та воєнний час, порядок застосування сил, участь у забезпеченні громадського порядку та охороні критичної інфраструктури. Ці нормативні акти встановлюють також правила обміну інформацією, порядок залучення ресурсів та взаємну відповідальність за невиконання покладених завдань.

Особливе значення у законодавчому регулюванні взаємодії має положення про правовий режим воєнного стану, який визначає специфіку дій як Сил оборони, так і правоохоронних органів України. У період введення воєнного стану органи влади мають право застосовувати спеціальні заходи, що включають блокування комунікацій, контроль за переміщенням осіб та транспортних засобів, організацію оборонних операцій, координацію дій із забезпечення безпеки держави та цивільного населення. Водночас законодавство передбачає контроль за дотриманням прав і свобод людини навіть у надзвичайних умовах, що зумовлює необхідність чіткого правового регулювання взаємодії органів влади.

На практиці нормативно-правова база взаємодії посилюється підзаконними актами: наказами Міністерства оборони, СБУ, Нацполіції та інших відомств, інструкціями щодо координації дій під час оперативно-бойових завдань та захисту критично важливих об'єктів. Вони деталізують порядок взаємодії підрозділів, умови застосування сил, процедури обміну інформацією, алгоритми реагування на надзвичайні ситуації та кібератаки.

Таким чином, нормативно-правова база взаємодії Сил оборони та правоохоронних органів України під час збройної агресії складається з

конституційних положень, законів України, спеціальних законодавчих актів та підзаконних нормативних документів, які забезпечують правову визначеність, координацію дій та ефективне виконання завдань із захисту національної безпеки. У сучасних умовах агресії така база постійно удосконалюється, що дозволяє оперативно реагувати на загрози, забезпечувати захист держави та її громадян і підвищувати ефективність взаємодії між силами оборони та правоохоронними органами.

Законодавчо-організаційні заходи повинні:

- привести в єдину систему законодавчі акти, що визначають повноваження Збройних Сил України, Національної поліції України, Державної прикордонної служби України, Служби безпеки України, Державної служби з надзвичайних ситуацій у воєнний час;
- визначити чіткі тригери для передачі та координації повноважень (оголошення воєнного стану, активні бойові дії у регіоні тощо);
- нормувати підстави для формування оперативних координаційних штабів на державному, регіональному та районному рівнях з чітким переліком повноважень, ланцюгом підпорядкування та відповідальністю;
- врегулювати порядок притягнення до відповідальності військовослужбовців та правоохоронців у зонах бойових дій; уніфікувати процедури розслідування злочинів, пов’язаних із конфліктом.

Ефективна взаємодія Сил оборони України та правоохоронних органів у період збройної агресії потребує чітко налагодженої системи організаційних механізмів, що забезпечують координацію дій, оперативний обмін інформацією та оперативне реагування на загрози національній безпеці. До таких механізмів належать як структурні форми взаємодії, так і процедурні та функціональні інструменти управління. До структурних форм можна віднести центри управління, координаційні штаби та міжвідомчі робочі групи, які створюються на різних рівнях: від центрального до регіонального. Наприклад, у період ведення воєнних дій при Кабінеті Міністрів України та в межах регіональних адміністрацій діють оперативні штаби, що об’єднують представників Міністерства оборони, Служби безпеки України, Національної поліції, Державної прикордонної служби та інших органів сектору безпеки. Такі штаби забезпечують своєчасний обмін розвідувальною та оперативною інформацією, планування спільних заходів і контроль за їх виконанням. Процедурні механізми взаємодії включають регламентовані алгоритми прийняття рішень, узгодження дій та обміну інформацією. Це можуть бути стандартизовані накази, протоколи координаційних нарад, планування спільних навчань і тренувань, визначення відповідальних осіб за окремі напрями діяльності. Важливу роль відіграють також системи інформаційного обміну, що дозволяють оперативно передавати

дані про загрози, пересування сил противника, стан критичної інфраструктури та потреби в ресурсах [7].

Функціональні інструменти включають визначення чітких повноважень, зон відповідальності та процедур взаємодії підрозділів, що дозволяє уникати дублювання функцій і забезпечує єдність дій у кризових ситуаціях. Одним із важливих аспектів є планування спільних дій за сценаріями надзвичайних ситуацій, включно з блокуванням комунікацій, охороною об'єктів критичної інфраструктури, реагуванням на кібератаки та підтримкою громадського порядку. Організаційні механізми також передбачають регулярний контроль та моніторинг результатів взаємодії, що дозволяє своєчасно виявляти проблеми та коригувати стратегії.

Незважаючи на наявність нормативно-правової бази та структурних механізмів, у діяльності сил сектору безпеки та оборони існує ряд проблем, що ускладнюють ефективну взаємодію. Однією з головних є недостатня чіткість законодавчих норм, які визначають межі повноважень органів у період воєнного стану. Часто виникають ситуації, коли повноваження різних відомств перекриваються або не узгоджені, що створює ризики дублювання дій або, навпаки, уповільнює реакцію на загрозу [8].

Шляхи вдосконалення правового та організаційного регулювання взаємодії сил оборони та правоохоронних органів включають:

- уточнення та гармонізація законодавчих норм, що визначають повноваження різних органів сектору безпеки, зокрема в умовах воєнного стану, для чіткого розмежування компетенції та відповідальності;
- створення інтегрованих систем обміну інформацією та централізованих платформ управління, які дозволять забезпечити оперативну координацію дій у режимі реального часу;
- підвищення рівня професійної та психологічної підготовки персоналу, організація спільних навчань, тренувань та навчальних програм, спрямованих на розвиток навичок міжвідомчої взаємодії;
- розробка стандартних процедур координації та планів спільних дій, що включають алгоритми реагування на загрози та надзвичайні ситуації, а також систему контролю за виконанням поставлених завдань;
- моніторинг на постійній основі та оцінка ефективності взаємодії, що дозволяє своєчасно виявляти слабкі місця, коригувати стратегії та вдосконалювати організаційні механізми.

У підсумку, вдосконалення організаційних, правових та процедурних механізмів взаємодії сил оборони та правоохоронних органів дозволяє не лише підвищити оперативну спроможність держави в умовах збройної агресії, а й забезпечити захист громадян, критично важливих об'єктів та стабільність національної безпеки держави. Основними цілями та пріоритетами такої взаємодії є: узгоджене та законне застосування сил у зоні бойових дій та при загрозі безпеці держави;

мінімізація конфліктів повноважень та дублювання дій; забезпечення ефективного обміну інформацією, спільний контроль кордонів, захист цивільного населення та безперебійне забезпечення логістики; підтримка верховенства права та захисту прав людини під час застосування військових і правоохоронних засобів. Уніфікація нормативної бази, створення законодавчих положень про спільне командування в кризові періоди, регламенти щодо юрисдикції та кримінальної відповідальності – це ті законодавчо-організаційні заходи, що здатні окреслити системний підхід удосконалення нормативно-правової бази та стати ключем ефективного функціонування сектору безпеки та оборони України в сучасних умовах.

Список використаних джерел:

1. Конституція України : затв. Верховною Радою України 28 червня 1996 р. № 254к/96-ВР. Київ, 1996. 80 с. URL: https://zakon.rada.gov.ua/go/254к/96-ВР (дата звернення: 21.10.2025).
2. Закон України «Про національну безпеку України» : від 21 червня 2018 р. № 2469-VIII. Відомості Верховної Ради України, 2018, № 45, ст. 234. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 21.10.2025).
3. Закон України «Про Збройні Сили України» : від 6 грудня 1991 р. № 1934-XII. Відомості Верховної Ради України, 1991, № 52, ст. 512. URL: https://zakon.rada.gov.ua/go/1934-12 (дата звернення: 21.10.2025).
4. Закон України «Про Службу безпеки України» : від 25 березня 1992 р. № 2229-XII. Відомості Верховної Ради України, 1992, № 19, ст. 176. URL: https://zakon.rada.gov.ua/go/2229-12 (дата звернення: 21.10.2025).
5. Закон України «Про Національну поліцію» : від 2 липня 2015 р. № 580-VIII. Відомості Верховної Ради України, 2015, № 42, ст. 335. URL: https://zakon.rada.gov.ua/go/580-19 (дата звернення: 21.10.2025).
6. Закон України «Про Державну прикордонну службу України» : від 12 листопада 2003 р. № 661-IV. Відомості Верховної Ради України, 2003, № 45, ст. 314. URL: https://zakon.rada.gov.ua/go/661-15 (дата звернення: 21.10.2025).
7. Про правовий режим воєнного стану в Україні : Указ Президента України від 26 листопада 2018 р. № 393/2018. Офіційний портал Верховної Ради України. URL: https://www.president.gov.ua/documents/3932018-25594 (дата звернення: 21.10.2025).
8. Накази та інструкції Міністерства оборони України, Служби безпеки України, Національної поліції України щодо координації дій у період воєнного стану. Київ, 2022–2024. URL: https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakazi-ministerstva-oboroni-ukraini-za-2022-rik (дата звернення: 21.10.2025).

3 БЕЗПЕКА ТА ЗАХИСТ ОБ'ЄКТІВ НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

PEDAN A. V.,
Student of Bachelor's degree of specialty 183
«Environmental Protection Technologies»,
National University of Civil Protection
of Ukraine of SES of Ukraine

KONDRATENKO O. M.,
DSc(Engineering), Professor, Professor of the
Department of Fire and Technogenic Safety
of Objects and Technologies, Educational and
Scientific Institute of Fire
and Technogenic Safety,
National University of Civil Protection
of Ukraine of SES of Ukraine

ANALYSIS OF ENVIRONMENTAL COMPONENTS POLLUTION FROM HEAT-AND-ELECTRIC POWER PLANT AS THE OBJECT OF THE NATIONAL CRITICAL INFRASTRUCTURE

Annotation. The study comprehensively analyzed the legislative aspects of the relevance of its topic, taking into account the industry, departmental, and geographical aspects of training applicants in specialty 183, and provided the results of the analysis of aspects of the negative technogenic impact on the environmental components of the operation of heat-and-electric power plants in one of the eastern regions of Ukraine.

Key words: Ecological Safety, Environment Protection Technologies, Pollutiants Emission, Heat-and-Electric Power Plant

1. INTRODUCTION

Relevance of the study topic is due to the following components. Compliance with:

– the Order of the State Emergency Service of Ukraine № 618 dated 20.09.2013 «On approval of the Regulations on the organization of environmental support of the State Emergency Service of Ukraine» (https://zakon.rada.gov.ua/rada/show/v0618388-13#Text), namely: the results of research allow achieving the goal of environmental support of the SES of Ukraine as a set of organizational and technical measures, carried out, including by higher educational institutions, namely, achieving environmental safety of all types of activities of bodies and units of the SES of Ukraine, protection of personnel and employees, material and technical means under the influence of environmentally unfavorable anthropogenic and natural

factors, as well as environmental protection in the places of deployment and location of bodies and units of the SES of Ukraine, in terms of fulfilling the task of scientific support of the main tasks of environmental support of the SES of Ukraine, providing an assessment of environmental damage from the activities of bodies and units of the SES of Ukraine, implementing measures to restore the environment, complying with maximum permissible standards for emissions of harmful substances into the atmosphere, implementing measures to reduce them, reducing the toxicity of exhaust gases from equipment;

– the Decree of the President of Ukraine № 722/2019 dated 30.09.2019 «On the Sustainable Development Goals of Ukraine for the period until 2030» (https://zakon.rada.gov.ua/laws/show/722/2019#Text), namely: the results of research correspond to Goal № 3 «Ensure healthy lives and promote well-being for all at all ages», Goal № 7 «Ensure access to affordable, reliable, sustainable and modern energy for all», Goal № 11 «Ensure inclusive, safe, liveable and environmentally sustainable cities and other human settlements», Goal № 13 «Take urgent action to combat climate change and its impacts»;

– the Resolution of the Cabinet of Ministers of Ukraine № 476 dated 04/30/2024 «On approval of the list of priority thematic areas of scientific research and scientific and technical developments for the period until December 31 of the year following the termination or abolition of martial law in Ukraine» (https://zakon.rada.gov.ua/laws/show/476-2024-%D0%BF#Text), namely: the results of research correspond to the direction of «Rational Environmental Management», namely «Modeling and Forecasting of the State of the Natural Environment, Technologies for Overcoming Negative Impacts on It», the section «Energy and Energy Efficiency», namely «Systems for Generating and Transporting Electric and Thermal Energy» and «Technologies for Developing and Using New Types of Fuel, Renewable and Alternative Energy Sources and Types of Fuel», the section «National Security and Defense», namely «Ecologically Balanced Energy Security» and «Intelligent Information and Control Technologies for Diagnostics, Operation and Repair of Military and Special Equipment»;

– the Specialty Passport of 21.06.01 «Ecological Safety», approved by Resolution of the Presidium of the Higher Attestation Commission of Ukraine № 33-07/7 dated 04.07.2001 (https://zakon.rada.gov.ua/rada/show/va7_7330-01#Text), namely: the results of research correspond to the directions of «Development of scientific methods for research of complex assessment and forecasting of the impact of technogenic pollution on the environment and humans» and «Improvement of existing, creation of new, environmentally safe technological processes and equipment that ensure the rational use of natural resources, compliance with the standards of harmful impacts on the environment. Environmental audit, environmental management»;

– the Law of Ukraine № 3769-IX dated 04.06.2024 «On Amendments to Some Laws of Ukraine Regarding the Mandatory Use of Liquid Biofuels (Biocomponents) in the Transport Sector» (https://zakon.rada.gov.ua/laws/show/3769-20#Text), namely: in Article 1, part «sustainability criteria –

requirements that liquid biofuels (biocomponents) and biogas intended for use in the transport sector meet, in particular indicators of greenhouse gas emission reduction from the use of these types of biofuels and the prohibition of the use of certain land plots to obtain raw materials necessary for the production of such types of biofuels» and Section II «Liquid biofuels (biocomponents), which are taken into account to comply with the regulatory mandatory share in the sales of automotive gasoline in the customs territory of Ukraine, must meet sustainability criteria from June 1, 2025»;

– the Standard of Higher Education in Specialty 183 «Environmental Protection Technologies» of the Third (Educational and Scientific) Level in the Field of Knowledge 18 «Production and Technologies», approved by Order of the Ministry of Education and Science of Ukraine № 1427 dated 23.12.2021 (https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2021/12/24/183-Tekhn.zakh.navk.seredovyshcha-dokt.filos. pdf.), namely: the Integral Competence «The ability to produce new ideas, solve complex problems in the field of research and innovation in the field of environmental protection technologies, which provides for a deep rethinking of existing and creation of new holistic knowledge and/or professional practice, to carry out own scientific research, the results of which have scientific novelty, theoretical and practical significance; to apply modern methodologies of scientific and scientific-pedagogical activity» and Special Competence «SC03. Ability to identify weaknesses and shortcomings in environmental protection systems, set appropriate scientific tasks and solve them using engineering, modeling, statistical, expert and other scientific research methods» and also Program Education Result «PER07. Develop, implement and evaluate the effectiveness of innovative environmental technologies and equipment in production to reduce the man-made burden on the environment and improve the ecological state of industrial regions»;

– the Topics of Scientific Research and Scientific and Technical (Experimental) Developments for 2025-2029, approved by Order of the Ministry of Internal Affairs of Ukraine № 326 dated 21.05.2024 (https://mvs.gov.ua/normativno-pravovi-akti/nakaz-mvs-vid-21052024-326-pro-zatverdzennia-tematiki-naukovix-doslidzen-i-naukovo-texnicnix-eksperimentalnix-rozrobok-na-2025-2029-roki), namely: in the Point 25 in part «Modeling and forecasting the state of the natural environment, technologies for overcoming negative impacts on it» and the Point 27 «Development of aviation, water and other types of transport of bodies and units of the Ministry of Internal Affairs system under the legal regime of martial law and the post-war period»;

– the Civil Protection Code of Ukraine in its current version dated 12.09.2025, Article 108 «Civil Defense Service Oath» (https://zakon.rada.gov.ua/laws/show/5403-17#Text), namely: «I swear to courageously and resolutely protect the lives and health of citizens, the property of Ukraine, and its natural environment from emergencies».

Purpose of the study. To analyze aspects of pollution of environmental

components from a heat-and-electric power plant as the object of the national critical infrastructure.

Object of the study. Negative technogenic impact on environmental components from a heat-and-electric power plant as the object of the national critical infrastructure.

Subject of the study. Qualitative and quantitative indicators characterizing the object of the study.

2. RESULTS OF THE STUDY

Kharkiv region, as a region with developed industry and heat and power industry, faces significant environmental challenges associated with pollution of all components of the environment. The largest sources of pollution are enterprises of the heat and power industry, oil and gas and mining sectors. It has been established that H&E PP emit sulfur oxides, nitrogen oxides, carbon monoxide, heavy metals, as well as products of incomplete combustion, including soot and benzopyrene, into the air, which have a negative impact on human health, cause respiratory diseases, destroy infrastructure, cause acid rain and reduce the transparency of the atmosphere [1, 2].

Such energy-generating facilities are included in the list of critical infrastructure facilities, the aspects of ensuring their protection are regulated [3-7]:

– Law of Ukraine № 1882-IX in the current version dated 21.09.2024 «On Critical Infrastructure»;

– Resolution of the Cabinet of Ministers of Ukraine № 1109 of September 09.09.2020 «Some issues of critical infrastructure facilities» (as amended by Resolution of the Cabinet of Ministers of Ukraine № 48 of 16.01.2024);

– Law of Ukraine № 389-VIII in the current version dated 14.05.2025 «On the legal regime of martial law»;

– Law of Ukraine № 1550-III in the current version dated 18.05.2024 «On the legal regime of the state of emergency»;

– Law of Ukraine № 1932-XII in the current version dated 09.07.2025 «On the Defense of Ukraine».

In addition, the introduction of modern technologies, such as reheating of steam, regenerative heating, the use of scrubbers to capture sulfur oxides and reduce the formation of nitrogen oxides through optimization of the combustion process, allows to significantly reduce the negative impact on the environment. Particular attention should be paid to the situation that has developed as a result of a full-scale war. The destruction of industrial facilities, a decrease in production volumes and the relocation of enterprises led to a temporary decrease in the level of industrial pollution. However, explosions, fires and shelling caused new environmental threats, including air pollution by combustion products and the destruction of infrastructure. Under

martial law, assessing the real level of pollution is complicated by the limited ability to monitor and provide official reporting.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

This study analyzed qualitative and quantitative indicators characterizing the negative technogenic impact on environmental components from a heat-&-electric power plant as the object of the national critical infrastructure.

ACKNOWLEDGMENTS

In this study the materials from the VCU library system have been used, including electronic versions of journals and other materials, databases, interlibrary subscription as part of participation in Non-Resident Academic Associates program co-sponsored by the College of Humanities and Sciences at Virginia Commonwealth University (VCU) and the Davis Center for Eurasian Studies at Harvard University in 2024–2025 academic year.

References:

1. Research of Properties and Rational Composition of Ecosafe Building Materials with Ash-and-Slag Waste from Masute Fuel And Coal Combustion / O. Kondratenko, V. Koloskov, H. Koloskova, V. Babakin // Key Engineering Materials. 2023. Vol. 935, pp. 85–97. DOI: 10.4028/p-RwzP9p.
2. Research of Technical and Economic Properties of Material of Porous Fuel Briquettes from the Solid Combustible Waste Impregnated with Liquid Combustible Waste / O. Kondratenko, V. Koloskov, S. Kovalenko, Y. Derkach // Materials Science Forum, 2021, № 1038, pp. 303–314. DOI: https://doi.org/10.4028/www.scientific.net/msf.1038.303.
3. Law of Ukraine № 1882-IX in the current version dated 21.09.2024 «On Critical Infrastructure». URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
4. Resolution of the Cabinet of Ministers of Ukraine № 1109 of September 09.09.2020 «Some issues of critical infrastructure facilities» (as amended by Resolution of the Cabinet of Ministers of Ukraine № 48 of 16.01.2024). URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF.
5. Law of Ukraine № 389-VIII in the current version dated 14.05.2025 «On the legal regime of martial law». URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.
6. Law of Ukraine № 1550-III in the current version dated 18.05.2024 «On the legal regime of the state of emergency». URL: https://zakon.rada.gov.ua/laws/show/1550-14.
7. Law of Ukraine № 1932-XII in the current version dated 09.07.2025 «On the Defense of Ukraine». URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

БОГДАН Д. М.,
доктор філософії,
старший консультант,
Штаб Антитерористичного центру
при Службі безпеки України

СЕЛІНА М. Б.,
кандидат юридичних наук,
консультант-експерт,
Штаб Антитерористичного центру
при Службі безпеки України

ОРГАНІЗАЦІЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД ТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ

Система забезпечення національної безпеки України потребує якісного переосмислення підходів до захисту критичної інфраструктури як однієї з ключових умов стабільності держави та життєздатності суспільства. У сучасних умовах воєнного стану, гібридної війни та зростання кількості терористичних загроз держава стикається з необхідністю системного оновлення механізмів протидії цим викликам.

Особливу небезпеку становить діяльність Російської Федерації, яка цілеспрямовано застосовує елементи терору у поєднанні з широким застосуванням збройних сил проти України, деструктивною дипломатичною діяльністю, економічним тиском, інформаційно-психологічними та кібернетичними операціями. Розширюється також використання безпілотних авіаційних комплексів, ракетного озброєння різного базування, а також методів кібератак проти енергетичних, транспортних, комунікаційних та фінансових систем України. Усе це створює комплексну терористичну загрозу для об'єктів критичної інфраструктури, які мають стратегічне значення для держави.

Відповідно до підходів Європейського Союзу, визначених у Стратегії боротьби з тероризмом ЄС (2005 р.) [1] та Директиви Європейського Парламенту і Ради 2022/2557 від 14 грудня 2022 року про стійкість критично важливих суб'єктів [2], документі НАТО «Оцінка інфраструктури в оперативному середовищі НАТО» [3], система забезпечення стійкості критично важливих суб'єктів повинна ґрунтуватися на оцінюванні ризиків, прогнозуванні загроз та інтегрованому управлінні антитерористичною безпекою. Україна, орієнтуючись на європейські стандарти, має розбудовувати власну модель антитерористичного захисту, що поєднує ризик-орієнтований підхід, технологічну модернізацію, міжвідомчу координацію та гармонізацію законодавства у сфері боротьби з тероризмом з acquis ЄС.

Оновлена Концепція боротьби з тероризмом в Україні (далі – Концепція), яка підготовлена експертами Штабу Антитерористичного центру при СБ України, базується на чотирьох взаємопов'язаних

пріоритетах – «Запобігання», «Захист», «Реагування» та «Переслідування». Серед них саме пріоритет «Захист» відіграє ключову роль у забезпеченні стабільності функціонування об'єктів критичних інфраструктури (ОКІ).

Зокрема, в оновленій Концепції реалізація пріоритету «Захист від терористичної діяльності» має здійснюватися шляхом:

формування моделі прогнозованої загрози, виявлення та усунення потенційних терористичних загроз;

розробки ефективних механізмів захисту об'єктів критичної інфраструктури і ланцюгів постачання від безпілотних систем, крилатих, балістичних та інших ракет і засобів ураження;

посилення фізичного захисту, спрямованого на зниження уразливості об'єктів критичної інфраструктури і ланцюгів постачання, удосконалення систем охорони, контролю доступу та забезпечення безпеки транспорту і місць масового перебування людей;

зміцнення кіберзахисту, забезпечення сталого функціонування об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів (кіберстійкості);

модернізації технічних засобів охорони та впровадження новітніх систем відеоспостереження, сигналізації, моніторингу, контролю доступу та інших інженерно-технічних засобів безпеки об'єктів критичної інфраструктури, органів державної влади та управління, військових об'єктів, місць масового перебування людей;

оптимізації державних систем фізичного захисту транспортної системи (автомобільного транспорту (мости, тунелі), залізничної інфраструктури, забезпечення безпеки повітряного простору), морської безпеки;

удосконалення системи підготовки персоналу об'єктів критичної інфраструктури з метою підвищення їх професійного рівня з питань протидії терористичним загрозам;

удосконалення системи забезпечення хімічної безпеки та управління хімічною продукцією, оптимізації механізмів, спрямованих на недопущення незаконного виготовлення вибухових речовин;

розробки ефективних механізмів контролю у сфері використання безпілотних літальних апаратів та інших безпілотних систем;

протидії незаконному поводженню з радіоактивними, хімічними, біологічними та ядерними матеріалами і речовинами;

недопущення потрапляння у незаконний обіг вогнепальної зброї, боєприпасів та вибухових речовин і пристроїв [4].

Отже, організація захисту ОКІ передбачає реалізацію комплексу заходів, спрямованих на зниження вразливості таких об'єктів до терористичних впливів, диверсій, кіберзагроз і фізичного ураження. У межах цього напряму держава має забезпечити формування системи прогнозування і моделювання можливих загроз, визначення найбільш уразливих елементів, розробку заходів їх інженерно-технічного

укріплення та створення механізмів постійного моніторингу безпекового середовища. Захист критичної інфраструктури повинен реалізовуватись на основі сучасних технологій, зокрема, автоматизованих систем відеоспостереження, сигналізації, контролю доступу, засобів кіберзахисту, систем раннього виявлення атак.

Особливої уваги потребує забезпечення кіберстійкості об'єктів інформаційної та комунікаційної інфраструктури. Кібератаки можуть мати руйнівний ефект, зупиняючи роботу енергетичних систем, транспортних вузлів або органів управління. Тому необхідно створити багаторівневу систему кіберзахисту, що включатиме постійний моніторинг мереж, шифрування даних, резервне зберігання інформації та застосування національних стандартів безпеки інформаційних систем. Важливим елементом є координація між органами державної влади, операторами ОКІ та приватним сектором, адже саме взаємодія дає змогу забезпечити комплексну стійкість до терористичних атак [5].

Одним із пріоритетних напрямів є підготовка персоналу, відповідального за безпеку ОКІ. Працівники мають володіти практичними навичками реагування на терористичні загрози, знанням алгоритмів евакуації, локалізації небезпеки, застосування технічних засобів безпеки та комунікації з правоохоронними структурами. Необхідно впровадити систему спеціалізованого навчання, регулярних тренувань і перевірок готовності персоналу до дій у надзвичайних ситуаціях. Це дасть змогу оперативно мінімізувати наслідки можливих терористичних атак.

Важливе місце у системі захисту посідає вдосконалення нормативно-правової бази. Україна має гармонізувати своє законодавство із законодавством ЄС, у тому числі щодо регулювання використання безпілотних систем, обігу вибухових речовин, захисту транспортної інфраструктури, а також уніфікації термінології у сфері протидії тероризму. Це створить єдине правове поле для взаємодії суб'єктів безпеки та спростить інформаційний обмін про терористичні загрози та загалом міжнародне співробітництво у сфері боротьби з тероризмом.

Не менш важливим є запровадження державного моніторингу стану захищеності об'єктів критичної інфраструктури. Систематична оцінка рівня безпеки, ідентифікація вразливих ланок, а також постійне оновлення планів реагування дадуть змогу своєчасно виявляти потенційні ризики. Додатково слід передбачити створення єдиної бази даних ОКІ, із зазначенням ступеня їх уразливості та планів інженерного укріплення.

Сучасні терористичні загрози характеризуються широким використанням технологічних інновацій – від дронів до штучного інтелекту. Тому важливо не лише протидіяти цим загрозам, але й використовувати такі технології для моніторингу, прогнозування, виявлення ризиків і автоматизації процесів управління антитерористичною безпекою. Використання

великих даних, систем машинного навчання та аналізу патернів діяльності терористичних організацій та поведінки окремих терористів дасть змогу суб'єктам боротьби з тероризмом своєчасно визначати підозрілі активності у кіберпросторі, а також всередині та навколо ОКІ.

Отже, організація захисту об'єктів критичної інфраструктури має розглядатись як один із пріоритетів державної політики у сфері боротьби з тероризмом. Її основою повинна бути інтегрована модель безпеки, яка включає правові, технічні, кадрові та технологічні компоненти. Захист критичної інфраструктури має здійснюватися не лише на рівні фізичного укріплення об'єктів, а й через розвиток інтелектуальних систем управління ризиками, створення єдиної інформаційної платформи обміну даними між суб'єктами безпеки та підвищення культури безпеки у суспільстві.

Висновки: організація захисту об'єктів критичної інфраструктури від терористичних загроз вимагає системного підходу, який охоплює оцінювання ризиків, постійний моніторинг, удосконалення нормативно-правового регулювання, підвищення кіберстійкості та розвиток людського потенціалу. Основним завданням є інтеграція сучасних технологій у систему безпеки, забезпечення міжвідомчої координації та впровадження ризик-орієнтованої моделі управління. Лише за умови комплексного виконання цих заходів можливо гарантувати безпеку громадян, належний рівень захисту об'єктів критичної інфраструктури та стійкість держави до терористичних загроз.

Список використаних джерел:

1. The European Union Counter-Terrorism Strategy: Strategy of 30.11.2005. URL: https://www.refworld.org/policy/legalguidance/council/2005/en/61243 (дата звернення: 24.10.2025).
2. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333/164, 27.12.2022.
3. NATO Allied Command Operations Directive 084-002 «Infrastructure Assessment in the NATO Operating Environment», 17.10.2019.
4. Проєкт оновленої Концепції боротьби з тероризмом в Україні.
5. Стратегія кібербезпеки України : Указ Президента України від 26 серпня 2021 року № 447/2021. *Урядовий кур'єр*, від 28.08.2021 № 165.

БОРИСОВА Л. В.,
кандидат юридичних наук, доцент,
доцент кафедри,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

ДЕНДАРЕНКО В. Ю.,
кандидат технічних наук, доцент,
начальник кафедри,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

ІНСТРУМЕНТИ ТА СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ ТА ФІЗИЧНОЇ БЕЗПЕКИ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ДЕРЖАВИ

Національна критична інфраструктура (НКІ) – це сукупність об'єктів, систем і мереж, які мають вирішальне значення для функціонування держави, економіки, безпеки, охорони якої є запорукою стабільності держави, а будь-які порушення у функціонуванні, спричиненні зростанням кількості гібридних загроз, кібератак, диверсій і терористичних дій, спрямованих на об'єкти критичної інфраструктури України, особливо в умовах воєнного стану, можуть призвести до масштабних криз.

Нормативно-правове забезпечення безпеки НКІ формується Законами України «Про основні засади забезпечення кібербезпеки України» (2017), «Про критичну інфраструктуру» (2021), «Про національну безпеку України» (2018), Постановою Кабінету Міністрів України № 1109 від 09.10.2022 р. «Про затвердження Порядку формування переліку об'єктів критичної інфраструктури», Стратегією кібербезпеки України на 2021–2025 роки (2021), що визначають процедури ідентифікації об'єктів, вимоги до оцінки ризиків і планів безпеки, вимоги до їх захисту, порядок взаємодії між суб'єктами безпеки та відповідальність за порушення режиму захищеності.

Проте на практиці існує низка проблем, пов'язаних з відсутністю деталізованих механізмів взаємодії між державними і приватними структурами, нестача стандартів фізичного й кіберзахисту, неузгодженість термінології з європейським законодавством (зокрема з NIS2 Directive), обмежена реалізація системи державного моніторингу безпеки.

Стаття 21 Закону України «Про критичну інфраструктуру» визначає, що суб'єкти критичної інфраструктури зобов'язані забезпечувати:

захист об’єктів критичної інфраструктури шляхом створення та підтримання систем фізичної безпеки, операційної безпеки та кібербезпеки;

розробляти, оновлювати й виконувати плани безпеки, управління ризиками, ліквідації наслідків аварій і заходів кіберзахисту;

інформувати уповноважені державні органи (зокрема СБУ, Національну поліцію, Нацгвардію) про інциденти, загрози, диверсії, терористичні акти, кібератаки та інші небезпечні події;

захищати інформацію про системи управління, зв’язку, фізичну безпеку й кібербезпеку, забезпечуючи конфіденційність даних відповідно до законодавства.

Разом з тим, серед основних проблем у сфері захисту НКІ виділяють недостатню координацію між державними структурами та відсутність єдиного центру управління ризиками, недосконаліть класифікації об’єктів – відомства застосовують різні критерії віднесення до критичних, обмежене фінансування програм модернізації технічних систем, кадровий дефіцит у сфері кіберзахисту та кризового менеджменту, високий рівень кіберзагроз з боку держав-агресорів, що атакують енергетику, транспорт і зв’язок, недостатню готовність до кризових ситуацій і відсутність ефективних механізмів реагування.

Аналіз міжнародних підходів до захисту критичної інфраструктури вказав на правові і технічні інструменти, концентрацію на аналітиці, спрямованість на технічні методи, поєднання аналітичних та інноваційних рішень. Наприклад, Велика Британія та США (NIST) мають сильні правові та нормативні рамки, RAND (США) – стратегічний «think-tank» із розгорнутою аналітикою, міжнародні дослідження (PenTest, 2024, AI) – драйвери технічних та інноваційних рішень.

На основі міжнародних підходів пропонуємо такі рекомендації щодо захисту критичної інфраструктури для України.

Враховуючи досвід Великої Британії прийняти законодавчу модель Cyber Security and Resilience Bill як основу для кіберзахисту критичної інфраструктури (CNI), інтегрувати кібер- та фізичну безпеку для енергетики, транспорту, військових об’єктів та практику регулярних симуляцій гібридних атак, створити єдиний центр управління кібер- та фізичними ризиками, поєднаного з системою ЦЗ (ЄДС ЦЗ).

Зважаючи на практику США перейняти структурований підхід до кібербезпеки (Identify, Protect, Detect, Respond, Recover) з використання Profiles для адаптації під різні сектори (енергетика, транспорт, зв’язок, охорона здоров’я) та запровадження Tiers для оцінки зрілості кіберзахисту організацій.

Адаптувати аналітичні підходи до оцінки ризиків, готовності й відновлення після катастроф, сценарне планування і моделювання для стратегічної підготовки RAND Corporation, що сприятиме створенню аналітичного центру CIP у партнерстві з науковими установами та міжнародними think-tank.

Враховуючи актуальність міжнародних досліджень на прикладі Penetration testing (2024), важливо включити penetration testing у регулярний аудит державних і приватних операторів CNI, а також використання exploit development для прогнозування реальних атак із створенням для України програми обов'язкового «червоного командування» (red teaming) для об'єктів критичної інфраструктури.

Застосовувати інноваційний підхід до автоматизації кіберзахисту за допомогою LLM (моделі ШІ) для суттєвого покращення сканування та фільтрації вразливостей у кібербезпеці, запити на пошук загроз, виявлення генеративного ШІ-тексту в атаках, генерації та передачі коду безпеки.

Використання ШІ для аналізу аномалій, прогнозування атак і швидкого реагування, тобто циклічна модель «аналіз → застосування → оновлення» як пілотні проєкти з використання AI для кіберзахисту енергосистем, зв'язку та медицини важливі для України.

Безпека національної критичної інфраструктури є ключовим елементом національної безпеки України. В умовах гібридних загроз і воєнних ризиків держава має забезпечити комплексний підхід, що поєднує правові, організаційні, технічні й кадрові заходи. Розвиток системи управління ризиками, гармонізувати українське законодавство з директивами ЄС (зокрема NIS2) щодо кібер- і фізичного захисту, використовувати стандарти ISO 27001 і ISO 31000 у системі управління ризиками та міжнародна координація становлять основу підвищення стійкості держави до зовнішніх і внутрішніх загроз.

Список використаних джерел:

1. Річний звіт про кібербезпеку в Україні / Державна служба спеціального зв'язку та захисту інформації України. 2023.
2. Закон України «Про критичну інфраструктуру» : № 1882-IX від 16.11.2021 // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20.
3. Закон України «Про кібербезпеку» : № 2163-VIII від 05.10.2017 // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
4. Закон України «Про національну безпеку України» : № 2469-VIII від 21.06.2018 // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
5. Національна стратегія кібербезпеки України. 2021. Кабінет Міністрів України.
6. Онищук В. Правові механізми забезпечення захисту критичної інфраструктури України // Журнал досліджень національної безпеки. 2022. Т. 5, № 2. С. 45–53.
7. Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 р. про заходи для забезпечення високого спільного рівня кібербезпеки в усьому Союзі (Директива NIS2).
8. ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Міжнародна організація зі стандартизації, 2022.
9. Гарагуц К. Захист інформаційної інфраструктури держави в умовах кіберзагроз // Інформаційна безпека. 2021. № 3. С. 12–20.
10. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис на основі еліптичних кривих. Київ : ДЕРЖСПОЖИВСТАНДАРТ України, 2002.

11. Методичні рекомендації щодо впровадження системи управління кібербезпекою об’єктів критичної інфраструктури / Міністерство цифрової трансформації України. Київ, 2022.
12. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report. 2023.
13. Кузьменко О. Система реагування на кіберінциденти та обмін інформацією між суб’єктами критичної інфраструктури // Кібербезпека: освіта, наука, техніка. 2022. № 4. С. 28–36.
14. IT Specialist. (2023, 27 червня). *5 способів покращити кібербезпеку за допомогою ChatGPT та LLM.* URL: https://my-itspecialist.com/5-ways-chatgpt-and-llm-can-improve-cyber-security (дата звернення: 21.10.2025).

ВЛАСКО Д. Є.,
курсант, Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

ЛУЧИК В. Є.,
доктор економічних наук,
професор кафедри протидії кіберзлочинності,
Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

ПОРІВНЯЛЬНИЙ АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ КІБЕРБЕЗПЕКИ ДЛЯ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У сучасних умовах цифровізації суспільства кібербезпека стала ключовим елементом національної безпеки. Особливої уваги потребує захист об’єктів критичної інфраструктури, від стабільної роботи яких залежить функціонування енергетичної, транспортної, фінансової та інформаційної систем держави. Зростання кількості кіберзагроз вимагає впровадження ефективних міжнародних підходів до управління безпекою.

Серед найвідоміших світових моделей кіберзахисту – NIST Cybersecurity Framework, ISO/IEC 27001, CIS Controls та ENISA Guidelines, які відрізняються принципами побудови, структурою та рівнем практичної застосовності. Порівняння цих стандартів дозволяє визначити, який з них є найбільш придатним для використання в Україні [1].

Критична інфраструктура посідає центральне місце в системі національної безпеки, оскільки від її стабільного функціонування залежить безперервність основних суспільних процесів, економічна стійкість та обороноздатність держави. До складу критичної інфраструктури належать об’єкти енергетичного, транспортного, фінансового, інформаційно-комунікаційного та інших секторів, порушення діяльності

яких може призвести до масштабних негативних наслідків для суспільства [2].

Кібератаки на об’єкти критичної інфраструктури становлять серйозну небезпеку, оскільки можуть спричинити не лише фінансові збитки, а й дестабілізацію окремих секторів економіки або навіть держави в цілому.

Кібербезпека критичної інфраструктури є комплексом організаційних, технічних і правових заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також на стійке функціонування систем управління технологічними процесами. Основним завданням кіберзахисту є мінімізація ризиків, запобігання інцидентам та оперативне відновлення працездатності систем після можливих атак [3].

В Україні питання кібербезпеки регулюються Законом «Про основні засади забезпечення кібербезпеки України», проте національна система захисту критичної інфраструктури перебуває у процесі вдосконалення [4].

Міжнародні стандарти кібербезпеки формують основу ефективного управління ризиками та захисту критичної інфраструктури.

NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США, орієнтований на управління кіберризиками через п’ять основних функцій: ідентифікацію, захист, виявлення, реагування та відновлення. Його перевагою є гнучкість – організації можуть адаптувати Framework до власних потреб, не порушуючи основних принципів безпеки. Цей стандарт особливо ефективний для великих інфраструктурних об’єктів, оскільки забезпечує чітку послідовність дій та дає змогу оцінювати рівень зрілості системи кіберзахисту [5].

ISO/IEC 27001 – міжнародний стандарт системи управління інформаційною безпекою, який встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення політики безпеки. Його ключова особливість полягає у фокусі на безперервному вдосконаленні процесів (модель PDCA – Plan-Do-Check-Act), що сприяє системному підходу до захисту інформаційних активів. ISO/IEC 27001 має високу міжнародну визнаність і може бути офіційно сертифікований, що робить його привабливим для організацій, які прагнуть підтвердити відповідність світовим вимогам [6].

CIS Controls – це набір із 18 практичних рекомендацій, розроблених Центром Інтернет-безпеки (Center for Internet Security). Вони зорієнтовані на конкретні технічні дії для запобігання найпоширенішим типам атак. Цей підхід відрізняється прикладним характером, оскільки забезпечує швидке підвищення рівня кіберзахисту навіть за обмежених ресурсів. CIS Controls добре підходить для малих і середніх підприємств, а також для державних установ, які прагнуть впровадити базовий рівень безпеки без надмірної бюрократизації [7].

ENISA Guidelines, розроблені Європейським агентством з кібербезпеки, зосереджені на гармонізації підходів до кіберзахисту в межах Європейського Союзу. Вони охоплюють рекомендації щодо оцінки ризиків, управління інцидентами, обміну інформацією між суб'єктами критичної інфраструктури та впровадження найкращих практик. Ці настанови відзначаються орієнтацією на співпрацю між державним і приватним секторами, що відповідає сучасним тенденціям кіберзахисту в ЄС [8].

Порівняльна таблиця та аналіз міжнародних стандартів кібербезпеки для об'єктів критичної інфраструктури наведено у табл. 1 і на рис. 1.

Таблиця 1

Порівняльна таблиця міжнародних стандартів кібербезпеки для об'єктів критичної інфраструктури

Критерій	NIST Cybersecurity Framework (CSF)	ISO/IEC 27001	CIS Controls v8	ENISA Guidelines
Цілі та принципи	Управління кіберризиками через 5 функцій: Identify, Protect, Detect, Respond, Recover; гнучкість та адаптивність до контексту організації.	Створення та підтримка системи управління інформаційною безпекою (ISMS); принцип безперервного вдосконалення (PDCA).	Забезпечення базового рівня безпеки через пріоритетні технічні заходи; практичність і швидкість реалізації.	Гармонізація підходів у межах ЄС; координація між секторами; акцент на обмін інформацією та спільне реагування.
Підхід до управління ризиками	Ризикоорієнтований, з інструментами для оцінки, пріоритезації та контролю ризиків.	Формалізований процес оцінки, обробки та моніторингу ризиків у рамках ISMS.	Непряме зниження ризиків через реалізацію технічних заходів без формальної методики оцінки.	Враховує міжсекторну взаємодію та національні ризики; підтримує методи оцінки, сумісні з європейськими директивами.
Практичність впровадження	Висока гнучкість, але потребує підготовлених фахівців для адаптації.	Потребує значних організаційних ресурсів; підходить для формалізованих структур.	Легко впроваджується; орієнтований на швидкий результат навіть за обмежених ресурсів.	Залежить від політики держави; підходить для інтеграції у національні та галузеві стратегії.

Джерело: [5,6,7,8]

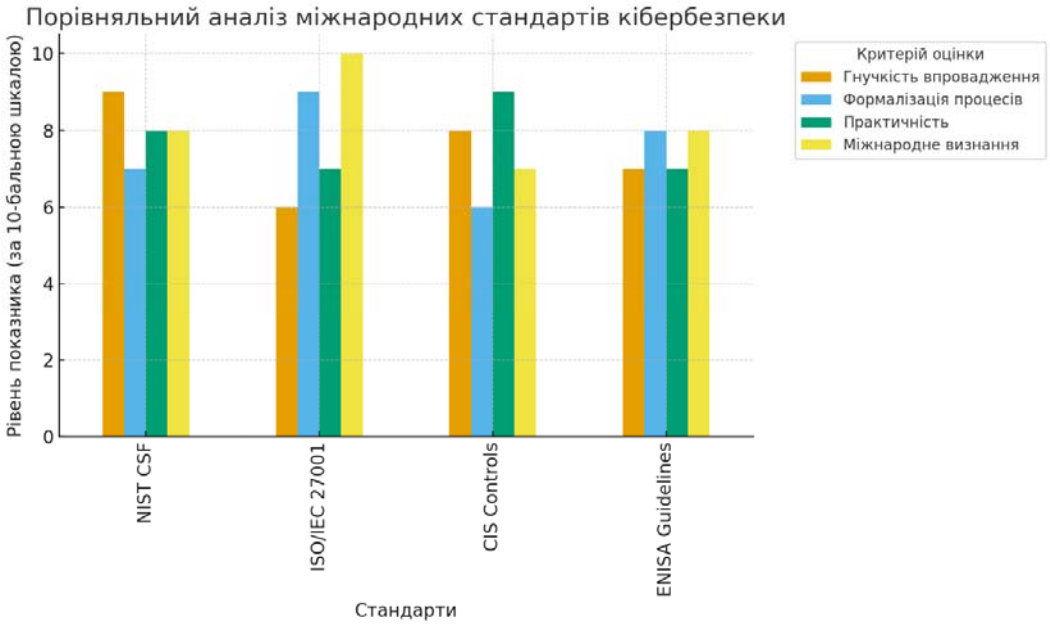

Рисунок 1 – Порівняльний аналіз міжнародних стандартів кібербезпеки для об’єктів критичної інфраструктури

Джерело: [1, 3]

Проведений порівняльний аналіз міжнародних стандартів кібербезпеки для об’єктів критичної інфраструктури засвідчив, що кожен із них має власні переваги та сферу ефективного застосування. Стандарт NIST Cybersecurity Framework відзначається високою гнучкістю та орієнтацією на ризики, ISO/IEC 27001 забезпечує формалізований підхід і можливість сертифікації, CIS Controls вирізняється практичністю та простотою впровадження, а ENISA Guidelines сприяють гармонізації політики кіберзахисту на рівні ЄС. Для України доцільним є поєднання підходів NIST і ISO/IEC 27001 із використанням практичних рекомендацій CIS та ENISA. Такий комплексний підхід дозволить створити ефективну, адаптовану до національних умов систему кіберзахисту критичної інфраструктури, яка відповідатиме міжнародним стандартам та сприятиме зміцненню національної безпеки у цифровому просторі.

Список використаних джерел:

1. NIST CSF vs ISO 27001 vs CIS Control Cybersecurity Frameworks. TekClarion. URL: https://www.tekclarion.com/cyber-security/cybersecurity-frameworks-nist-csf-vs-iso-27001-vs-cis-controls/ (дата звернення: 22.10.2025).
2. Національний координаційний центр кібербезпеки при РНБО України. Аналітична доповідь «Стан кіберзахисту об’єктів критичної інфраструктури в Україні». 14 с. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/analityka.pdf (дата звернення: 22.10.2025).
3. Gnatyuk, S., Berdibayev , R., Sydorenko, V., Zhyharevych, O., & Smirnova, T. (2023). СИСТЕМА КОРЕЛЮВАННЯ ПОДІЙ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ. Електронне

фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 176–196. https://doi.org/10.28925/2663-4023.2023.19.176196
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 22.10.2025).
5. Cybersecurity Framework. NIST. URL: https://www.nist.gov/cyberframework (дата звернення: 23.10.2025).
6. ISO/IEC 27001:2022, 2013. Система Менеджменту Інформаційної Безпеки Юнісерт Україна Міжнародна сертифікація ISO 27001 Україна. System Management Міжнародна сертифікація ISO 9001, ISO 14001, OHSAS 18001, ISO 22000, ISO 50001, ISO 27001, ISO 17100, ISO 13485. URL: https://certification.com.ua/iso27001?gad_source=1&gad_campaignid=22638344346&gbraid=0AAAAAo4yQR3sS-m60nP8HEW7Xj36XxYp9&gclid=CjwKCAjwpOfHBhAxEiwAm1SwEp-dIbzFN5UHKPqk5G6eDmn2nnAFgqv6PiNOB58VL64mdK9C3DLGHRoCdjQQAvD_BwE (дата звернення: 23.10.2025).
7. CIS Controls. CIS. URL: https://www.cisecurity.org/controls (дата звернення: 23.10.2025).
8. Guideline on Security Measures under the EECC ENISA. Home ENISA. URL: https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc (дата звернення: 23.10.2025).

ВОРОБЕЙ Ю. В.,
Національна академія Служби безпеки України

СЛОНЬ А. Г.,
Національна академія Служби безпеки України

БЕЗПЕКА ТА ЗАХИСТ ОБ'ЄКТІВ НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Критична інфраструктура − це об'єкти, які є надзвичайно важливими для функціонування суспільства та економіки країни, до яких передусім належать об'єкти оборони, а також ті, що забезпечують життєво важливі послуги й комунікацію [1].

За належністю до певного сектору (галузі) економіки та/або спільною функціональною спрямованістю об'єкти критичної структури поділяють на такі сектори:

енергетика та паливно-енергетичний комплекс – електростанції, мережі передачі електроенергії, газопроводи, нафтопроводи, які забезпечують життєдіяльність усіх інших систем;

телекомунікації та інформаційні технології − мобільний зв'язок, інтернет-провайдери, центри обробки даних, державні реєстри, що становлять основу сучасного управління та комунікації;

фінансовий сектор − національний банк, комерційні банки, платіжні системи, які відповідають за забезпечення економічної стабільності й безперебійності розрахунків;

життєзабезпечення (вода, тепло) − водоканали, системи очищення води, тепломережі, критично важливі для здоров'я та комфорту населення;

транспортна інфраструктура − залізниця, аеропорти, порти, ключові автомобільні шляхи та мости, критично необхідні для логістики, оборони та економічного обігу;

охорона здоров'я − ключові медичні установи, системи управління медичними даними, які забезпечують безперервне надання медичних послуг.

Безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечуються її функціональність, безперервність роботи, відновлюваність, цілісність і стійкість. Захист критичної інфраструктури включає види діяльності, що виконуються перед або під час створення, функціонування, відновлення й реорганізації об'єктів критичної інфраструктури та спрямовані на своєчасне виявлення, запобігання, нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [2].

Визначають такі **основні загрози критичній інфраструктурі:**

кібератаки – зараження систем, крадіжка даних, DDoS-атаки;

фізичні загрози – теракти, обстріли, диверсії;

природні катастрофи – повені, землетруси, пожежі;

техногенні аварії – вибухи, радіаційні витоки, виведення з ладу обладнання.

Україна, перебуваючи в стані війни, стала полігоном для тестування найагресивніших методів впливу на критичну інфраструктуру. Ці інциденти підкреслюють необхідність постійної модернізації захисту.

Наведемо лише кілька з наймасштабніших із них.

Вірус NotPetya. У червні 2017 року вірус NotPetya стрімко поширився світом, спричинивши мільярдні збитки країнам Європи, Азії та Америки. У перший же день він уразив дві тисячі організацій, 75 % жертв припало на Україну. Постраждали українські міністерства, поліція, банки, ЗМІ, мобільні оператори, медичні компанії, аеропорт «Бориспіль», київський метрополітен. Вірус блокував комп'ютери й вимагав гроші в обмін на відновлення доступу до заблокованих програм [3].

Служба безпеки України й американська компанія FireEye небезпідставно вважають, що за вірусом NotPetya стоять російські спецслужби. У НАТО також убачають «російський слід» у цій атаці, яка найбільше вдарила по Україні [4].

Атака на енергетику. 23 листопада 2022 року російські війська завдали п'ятого масованого ракетного удару по енергетичній інфраструктурі України. Росіяни застосували крилаті ракети повітряного й морського базування. Уперше в історії одночасно зупинилися всі чотири діючі українські АЕС. Через обстріли світло навіть зникло в сусідній

Молдові. Менше ніж за добу електричний струм подали до всіх областей, хоча екстрені відключення тривали ще тиждень, зокрема в столиці [5].

Кібератака на ПрАТ «Київстар». Наприкінці 2023 року внаслідок «безпрецедентної кібератаки» проти української телекомунікаційної компанії «Київстар» росіяни зруйнували 70 % віртуальної інфраструктури – хакерського втручання зазнали 4,8 тис. віртуальних серверів із 5 тис. загалом [6].

Позаяк успішна атака на об'єкт критичної інфраструктури завжди має каскадний ефект, який виходить далеко за межі пошкодженого об'єкта, уражаючи всі аспекти життя суспільства.

Наслідки таких атак:

економічні збитки – прямі витрати на відновлення обладнання, мільярдні втрати від простою виробництв, порушення експортних/імпортних операцій та інвестиційна непривабливість;

соціальна дестабілізація – паніка серед населення, недовіра до влади, проблеми з доступом до базових послуг (зв'язок, тепло), зростання рівня злочинності в умовах блекауту;

загроза життю та здоров'ю людей – збої в роботі лікарень (операційні, життєзабезпечення), припинення водопостачання, перебої з опаленням взимку, що безпосередньо загрожує життю найбільш вразливих груп населення;

втрата керованості – порушення роботи державних реєстрів, систем оповіщення, органів місцевого самоврядування та військового командування через відсутність зв'язку;

екологічні катастрофи – викиди небезпечних речовин через збої на промислових об'єктах або зупинку систем очищення води, що може мати довгострокові наслідки.

Наразі до найбільш дієвих технологічних рішень для захисту критичної інфраструктури належать:

1. Кібербезпека.

Захист цифрових систем і мереж. Використовуються міжмережеві екрани, системи виявлення вторгнень, шифрування, багатофакторна автентифікація, резервне копіювання, моніторинг у режимі реального часу та регулярне оновлення програмного забезпечення. Важливо ізолювати виробничі мережі (SCADA) від офісних.

2. Фізичний захист.

Охоплює охорону об'єктів, відеоспостереження, системи контролю доступу, сигналізацію, протидію дронам, протипожежні системи та інженерні укриття. Мета – унеможливити проникнення, диверсії чи пошкодження обладнання.

3. Резервування.

Забезпечує безперервність роботи навіть під час аварій або атак. Використовуються резервні джерела живлення (UPS, генератори), дубльовані сервери та канали зв'язку, географічно віддалені дата-центри й регулярне тестування планів відновлення.

Усі три напрями мають застосовуватися одночасно, в комплексі: кіберзахист оберігає інформацію, фізичний – захищає об'єкти, а резервування гарантує стабільність системи.

Загрози критичній інфраструктурі часто є транскордонними, що робить міжнародну співпрацю в цьому напрямі абсолютно необхідною. Україна бере активну участь у такій співпраці, передаючи свій унікальний досвід гібридної війни. При цьому спільна робота дає змогу:

обмінюватися досвідом і технологіями у сфері кіберзахисту, реагування на інциденти та відновлення систем;

отримувати допомогу від партнерів-членів ЄС, НАТО, зокрема через навчальні програми, спільні тренування й проєкти кіберстійкості;

підвищувати рівень підготовки фахівців під час міжнародних навчань, симуляції кібератак та обміну експертами;

удосконалювати законодавство й стандарти відповідно до європейських і міжнародних норм (наприклад, директива NIS2, стандарти ISO/IEC);

розвивати раннє попередження й обмін даними про загрози через мережі CERT, ENISA, NATO CCDCOE та інші міжнародні платформи.

Завдяки такій взаємодії Україна зміцнює свій кіберімунітет, покращує захист енергетики, зв'язку, транспорту й інших критичних секторів, а також робить внесок у безпеку європейського кіберпростору загалом.

Ефективний захист критичної інфраструктури можливий лише за комплексного підходу, що поєднує кібербезпеку, фізичний захист і резервування. Важливу роль відіграє міжнародна співпраця, яка забезпечує обмін досвідом, технологіями й підтримку в протидії сучасним загрозам. Україна, зміцнюючи власну стійкість, робить вагомий внесок у безпеку європейського та світового простору.

Отже, безпека й захист критичної інфраструктури – це одна з ключових передумов стабільного функціонування будь-якої держави. В умовах сучасних гібридних загроз, воєнних дій та кібератак критична інфраструктура стає головною мішенню противника, адже її пошкодження або знищення може паралізувати роботу секторів економіки, спричинити гуманітарну кризу та підірвати довіру до державних інституцій. Україна, маючи безпрецедентний досвід ведення війни в цифрову добу, стала прикладом того, як поєднання фізичного, кібернетичного та організаційного захисту може забезпечити стійкість навіть у найскладніших умовах.

Після масових атак вірусів BlackEnergy, NotPetya та Industroyer, а також ракетних ударів по енергосистемі у 2022–2024 роках держава значно зміцнила систему реагування. Була створена відповідна нормативна база, визначені категорії критичних об'єктів, сформована структура управління ризиками й реагування на надзвичайні ситуації. Проте виклики залишаються значними. Суттєва частина енергетичної та транспортної інфраструктури України побудована ще в радянський

період і потребує глибокої модернізації. Тому пріоритетом має стати поступовий перехід до стійких, розподілених систем, здатних функціонувати автономно в разі часткових пошкоджень. Майбутнє безпеки критичної інфраструктури полягає в комплексному підході, який поєднуватиме технології, управління ризиками, кадрову підготовку, правове забезпечення та міжнародну взаємодію. Захищена інфраструктура – це не лише питання національної безпеки, а й запорука економічного розвитку, довіри громадян до влади та спроможності держави протистояти будь-яким загрозам у XXI столітті.

Список використаних джерел:

1. Все, що ви повинні знати про об'єкти критичної інфраструктури в Україні. URL: https://share.google/kdmoTi1KKmYWOHKLu.
2. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: https://share.google/yc4k0dOOyb4cdz6Z0.
3. РНБО звинуватила Росію в хакерській атаці на Україну. URL: https://www.bbc.com/ukrainian/news-56179424.
4. Він вам не Petya: чи довели російський слід вірусу. URL: https://www.bbc.com/ukrainian/features-40528599.
5. Масований ракетний обстріл України 23 листопада 2022 – Вікіпедія. URL: https://share.google/mY7edNOqQCIlGkT7G.
6. Президент «Київстару»: Внаслідок кібератаки наприкінці 2023 року росіяни знищили 70 % віртуальної інфраструктури компанії ms.detector.media. URL:https://share.google/uD2fVlcgYTd7vKa5P.

ГРИЦИНА І. М.,
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

КОНЦЕПТУАЛЬНІ ЗАСАДИ ВИКОРИСТАННЯ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ТА РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ДЛЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ВІД ПОВІТРЯНИХ ЗАГРОЗ

Повномасштабна збройна агресія проти України актуалізувала проблему захисту критичної інфраструктури (КІ) як складової національної безпеки. Системність та інтенсивність повітряних атак, свідчать про необхідність переосмислення концепції оборони життєвоважливих об'єктів. Ураження енергетичних, транспортних, телекомунікаційних, інформаційних та промислових систем не лише створює короткочасні перебої у функціонуванні держави, а й спричиняє деградацію економіки та зниження обороноздатності.

Принципи державної політики у сфері захисту КІ, засади функціонування національної системи безпеки та коло суб'єктів, відповідальних за її реалізацію визначається в Законі України «Про критичну інфраструктуру» [1]. Документ запроваджує підхід до КІ як до цілісного комплексу взаємозалежних об'єктів і послуг, порушення яких може мати суттєвий негативний вплив на економіку, державне управління та життєзабезпечення населення. Відповідно до [1] виділяють чотири категорії критичності: 1 – об'єкти, що мають високу важливість для держави в цілому і здатні суттєво впливати на інші об'єкти КІ. Якщо їхня робота буде порушена, виникне кризова ситуація державного значення; 2 – об'єкти, що є життєво важливими, а припинення чи порушення їх роботи спричинить кризову ситуацію регіонального значення; 3 – важливі об'єкти, порушення чи припинення роботи яких спричинить кризову ситуацію місцевого значення; 4 – необхідні об'єкти, порушення чи припинення роботи яких спричинить кризову ситуацію локального значення. Саме категорія об'єктів критичної інфраструктури є вихідним етапом для планування оборони об'єктів.

Динаміка атак має хвильовий характер. Перша хвиля, що тривала з березня до жовтня 2022 року, характеризувалася ураженням транспортної, комунальної та логістичної інфраструктури, метою якої було дестабілізувати систему постачань і внутрішні комунікації. Друга хвиля (жовтень 2022 – березень 2023 рр.) стала початком системних атак на енергетику: у цей період обстрілам піддавалися трансформаторні підстанції, об'єкти генерації та розподільчі вузли. Третя хвиля (осінь 2023 – зима 2024 рр.) засвідчила перехід до комплексних дій, коли одночасно уражалися енергетичні та телекомунікаційні мережі, що мало на меті зірвати координацію реагування. Поточна, четверта хвиля поєднує комбіновані ракетно-дронові удари по розподільчим мережам, об'єктам генерації електроенергії та тепла, об'єктам видобутку та зберігання природного газу.

Статистичний аналіз свідчить про постійне зростання складності та інтенсивності ударів, що підтверджує потребу в інтегрованих системах раннього попередження, здатних поєднувати класичні методи протиповітряної оборони з можливостями електронного моніторингу та протидії.

Радіоелектронна розвідка (РЕР) виконує функцію оперативного контролю електромагнітного спектра, забезпечуючи виявлення, класифікацію й відстеження джерел випромінювання, що потенційно належать до систем управління безпілотних літаючих апаратів (БпЛА) або навігаційних каналів ракетного озброєння. Своєчасне виявлення таких сигналів дозволяє формувати інформаційно-аналітичну картину повітряного простору, ідентифікувати напрямки можливих атак і завчасно координувати роботу сил протиповітряної оборони та інших служб реагування. РЕР є також невід'ємним елементом зворотного зв'язку у системі оцінювання ефективності оборонних дій.

Засоби радіоелектронної боротьби (РЕБ), у свою чергу, застосовуються для створення перешкод каналам управління противника, дезорганізації його навігаційних і комунікаційних систем, а також для захисту власних каналів зв'язку. Використання РЕБ має оборонний характер і спрямоване на зниження точності наведення та ефективності застосування засобів ураження противника. У практиці захисту об'єктів КІ така діяльність полягає у створенні контрольованих зон електромагнітного впливу навколо найважливіших об'єктів, де відбувається приглушення або спотворення сигналів керування БпЛА, обмеження роботи систем позиціонування та передачі даних. Інтеграція РЕР і РЕБ із засобами протиповітряної оборони забезпечує багатошарову архітектуру безпеки.

На першому рівні відбувається електронне виявлення і класифікація загрози, на другому – її технічна нейтралізація засобами РЕБ, на третьому – кінетичне перехоплення. Такий підхід дозволяє мінімізувати ймовірність прориву атакуючих систем до критичних об'єктів і зменшити матеріальні збитки навіть у разі часткового ураження.

Серед перспективних і вже задіяних у практиці рішень для охорони окремих критичних об'єктів доцільно виділити кілька категорій обладнання, кожна з яких виконує певну функціональну роль у єдиному контурі захисту. Пасивні системи дальнього виявлення, представлені прикладами типу «Kolchuga», забезпечують національний або регіональний рівень моніторингу електромагнітного простору; їхня інтеграція з центрами ситуаційного аналізу дозволяє формувати широку оперативну картину й видавати пріоритети для подальшого розгортання локальних ресурсів. Тактичні модульні комплекси, типу «ETER», придатні для пеленгування та оперативної локалізації джерел підозрілої активності навколо об'єкта. Системи класу «Bukovel-AD» та інші застосовуються як локальний шар захисту й призначені для зниження ефективності групових дронових атак на невеликі й середні за площею об'єкти шляхом обмеження каналів управління і навігації противника. Для об'єктів КІ це забезпечує тимчасове зменшення ризику фізичного ураження критичних вузлів. Мережеві архітектури, представлені проектами типу «Atlas», що дозволяє масштабувати захист і оперативно перерозподіляти ресурси для захисту інфраструктурних об'єктів.

Разом із тим, аналіз практики функціонування показує, що чинна нормативна база потребує подальшої конкретизації щодо правового режиму застосування РЕБ у межах території України, зокрема у цивільному секторі, де наявність джерел радіочастотного випромінювання може впливати на безпеку цивільних систем зв'язку. Необхідне також чітке врегулювання питань взаємодії між військовими та цивільними структурами у разі використання спільних частотних діапазонів під час ліквідації наслідків повітряних атак [2].

Сучасні умови диктують потребу у створенні комплексної національної системи електронного моніторингу й протидії, здатної забезпечувати своєчасне виявлення загроз та інтеграцію з існуючими мережами спостереження. Така система має ґрунтуватися на поєднанні стаціонарних і мобільних засобів РЕР, розташованих у безпосередній близькості до стратегічних об'єктів енергетики, транспорту та зв'язку, а також на розгортанні центрів ситуаційного аналізу, що опрацьовують дані з різних джерел у режимі реального часу. Ефективність цього підходу залежить від рівня автоматизації, надійності каналів обміну інформацією та підготовленості персоналу. Підвищення стійкості КІ вимагає постійного удосконалення процедур реагування, передбачених регламентами. Регулярні міжвідомчі навчання з моделювання масованих атак, відпрацювання алгоритмів взаємодії та перевірки каналів комунікації дозволяють скоротити час реагування й відновлення після інцидентів. Водночас доцільним є створення системи обов'язкової сертифікації технічних засобів, що використовуються для захисту КІ, з урахуванням вимог електромагнітної сумісності та інформаційної безпеки.

Таким чином, аналіз розвитку воєнних подій і характеру атак на об'єкти критичної інфраструктури України свідчить про еволюцію загроз. Інтеграція систем радіоелектронної розвідки та боротьби в єдину архітектуру оборони є необхідною умовою забезпечення ефективного захисту КІ. Законодавча база України закладає основи для такої інтеграції, проте потребує подальшого розвитку з урахуванням сучасних технологічних реалій. Зміцнення взаємодії між державними структурами, приватними операторами інфраструктури та науковими установами створить умови для сталого функціонування критичних систем навіть у ситуації постійного зовнішнього тиску та збройної агресії.

Список використаних джерел:

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX : станом на 21.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 27.10.2025).
2. Про реалізацію експериментального проекту щодо нарощування спроможностей радіоелектронного прикриття об'єктів критичної інфраструктури : Постанова Кабінету міністрів України від 15 липня 2025 р. № 881 : станом на 15.07.2025. URL: https://zakon.rada.gov.ua/laws/main/881-2025-%D0%BF?utm_source=chatgpt.com#Text (дата звернення: 27.10.2025).

ЗОЗУЛЯ І. В.,
доктор юридичних наук, професор,
професор кафедри,
Навчально-науковий інститут № 1
Харківського національного університету
внутрішніх справ

БЕЗПЕКА ТА ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВОЄННИХ РУЙНУВАНЬ

Воєнна агресія проти України перетворила питання безпеки та стійкості національної критичної інфраструктури (КІ) на один із ключових елементів державної політики у сфері національної безпеки. Збройні атаки на енергетичні об'єкти, транспортні вузли, телекомунікаційні системи, об'єкти водо- та теплопостачання засвідчили масштаб вразливості стратегічних ресурсів держави [1]. В умовах тривалого воєнного стану проблема переходу від реактивної до превентивної моделі забезпечення безпеки набуває першочергового значення, оскільки збереження функціональності інфраструктурних систем є передумовою обороноздатності, економічної стабільності та життєздатності суспільства [2].

Захист критичної інфраструктури України сьогодні формується на перетині правових, організаційних, технічних і криміналістичних підходів. З одного боку, необхідне вдосконалення державної системи безпеки, а з іншого – створення дієвих механізмів виявлення, запобігання та розслідування злочинів, спрямованих проти об'єктів КІ. У цьому контексті криміналістика та судово-експертна діяльність виступають не лише реактивним інструментом фіксації наслідків атак, але й важливим аналітичним та прогностичним ресурсом для розроблення заходів превенції [3].

Сучасна модель захисту критичної інфраструктури України спирається на концепцію національної стійкості, що охоплює енергетичну, транспортну, інформаційну, фінансову та оборонну підсистеми. Проте війна продемонструвала, що навіть найкращі адміністративні регламенти не забезпечують ефективного функціонування без комплексної координації дій державних органів.

Ключову роль у цьому напрямі відіграє **Служба безпеки України (СБУ)**, яка здійснює оперативно-розшукову та контррозвідувальну діяльність, спрямовану на запобігання диверсіям, терористичним актам і кіберзагрозам проти об'єктів критичної інфраструктури [4]. Вона виступає центральною ланкою у системі захисту національних інтересів у сфері енергетичної, інформаційної та економічної безпеки. Зокрема,

СБУ координує міжвідомчі заходи із виявлення ризиків, що можуть призвести до втрати функціональності або контролю над об'єктами КІ, забезпечує обмін інформацією між суб'єктами безпеки та проводить експертно-аналітичну оцінку потенційних загроз.

Законодавчою основою системи захисту КІ є Закон України «Про критичну інфраструктуру» [1], який визначає її категорії, принципи управління ризиками та порядок взаємодії суб'єктів. Водночас воєнні події актуалізували необхідність постійного оновлення правових норм – з урахуванням кібервоєн, гібридних загроз і безпрецедентної інтенсивності фізичних атак на інфраструктуру.

Важливим є усвідомлення того, що правові механізми самі по собі не можуть забезпечити повноцінний захист критичних об'єктів без ефективного залучення криміналістичних і судово-експертних інструментів. Саме їх інтеграція у систему національної безпеки дозволяє не тільки реагувати на наслідки руйнувань, але й формувати превентивні механізми виявлення, документування та аналізу загроз.

Так, судово-експертна діяльність посідає центральне місце у структурі захисту критичної інфраструктури у секторі безпеки та оборони України [3]. Зокрема, експертиза об'єктів, що постраждали внаслідок ракетних ударів, диверсій чи техногенних катастроф, дозволяє встановити не лише причини руйнувань, а й виявити закономірності впливу воєнних дій на функціонування КІ. Це створює науково обґрунтовану основу для підвищення стійкості систем і визначення пріоритетів їх відновлення.

Криміналістика в умовах війни виходить за межі традиційного доказового аналізу. Вона формує аналітичну та прогностичну основу для оцінки загроз – як внутрішніх, так і зовнішніх [5]. Вивчення механізмів руйнування об'єктів, характеру пошкоджень, застосованих технічних засобів або методів диверсії дозволяє прогнозувати нові ризики та розробляти профілактичні заходи на випередження.

При цьому, питання ліквідації наслідків воєнних руйнувань інфраструктури потребують чіткої правової організації та скоординованої міжвідомчої взаємодії. Це включає залучення фахівців ДСНС, СБУ, Національної поліції, військових підрозділів, а також експертних установ, що здійснюють оцінку технічного стану об'єктів і визначають обсяг збитків. Таким чином, судово-експертна діяльність є не лише доказовою, а й безпековою складовою державного управління.

Одним із головних напрямів розвитку системи безпеки КІ є впровадження **превентивної моделі управління ризиками**, що ґрунтується на аналітичних даних і прогнозах. Криміналістичні методи – моделювання подій, трасологічний аналіз, криміналістична експертиза пошкоджень, аналіз цифрових доказів – можуть бути застосовані не

лише після інцидентів, а й для передбачення потенційних сценаріїв атак. Це відповідає концепції проактивної безпеки, за якої правоохоронні та експертні інституції працюють на випередження.

Ефективна превенція потребує інтеграції криміналістичних знань у діяльність суб'єктів критичної інфраструктури, зокрема операторів енергетичних систем, транспортних мереж, телекомунікацій та об'єктів оборонної промисловості [6]. Така інтеграція передбачає створення єдиної інформаційно-аналітичної бази ризиків, систему раннього попередження та проведення спільних тренувань із реагування на загрози.

В умовах воєнного стану координація дій між державними структурами має вирішальне значення. СБУ, МВС, ДСНС, Міноборони та оператори КІ повинні діяти в єдиному інформаційному полі, що базується на принципах оперативного обміну, достовірності та кіберзахищеності даних. Аналітична платформа має забезпечувати виявлення слабких місць у системах енергетичного та цифрового забезпечення, прогнозування наслідків атак і планування відновлення.

Важливим інструментом стають **аналітичні центри безпеки (Security Operation Centers)**, які здійснюють моніторинг інформаційних систем у реальному часі, фіксують аномалії та співпрацюють із правоохоронними органами. У контексті криміналістики це формує новий рівень доказового аналізу – цифрові відбитки атак, лог-файли та метадані стають ключовими доказами у справах про кіберзлочини.

Таким чином, безпека та захист об'єктів національної критичної інфраструктури України в умовах воєнних руйнувань – це не лише питання технічного зміцнення або правового регулювання, а цілісна система міждисциплінарної взаємодії. Криміналістика, судово-експертна діяльність і робота Служби безпеки України формують основу для створення адаптивної моделі безпеки, що поєднує аналітику, превенцію та відновлення.

Перехід до превентивної моделі управління ризиками дозволяє підвищити стійкість держави перед воєнними загрозами, а також забезпечити доказову підтримку процесів відбудови та міжнародного правового захисту. Український досвід у цій сфері може стати прикладом ефективного поєднання безпеки, криміналістики та експертизи у системі національної стійкості.

Список використаних джерел:

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 15.10.2025).
2. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : Указ Президента

України від 27.09.2021 № 479/2021. URL: https://www.president.gov.ua/documents/4792021-40181 (дата звернення: 15.10.2025).
3. Зозуля І. Судово-експертна діяльність як ключовий елемент захисту критичної інфраструктури у секторі безпеки та оборони України. *Актуальні питання розвитку українського простору судово-експертної діяльності : матеріали доповідей Міжнародної наук.-практ. конф.* (м. Київ, 31 січня 2025 р.). Львів-Торунь : Liha-Pres, 2025. С. 92–99.
4. Служба безпеки України. Звіт за перше півріччя 2024 року. Заходи з реалізації засад загальної відомчої політики, виконання антикорупційної стратегії та державної антикорупційної програми. URL: https://antycorportal.nazk.gov.ua/uploads/uo/00034074/report-977/nacp-report-977.pdf (дата звернення: 15.10.2025).
5. Зозуля І. В. Правові підходи до організації ліквідації наслідків спричиненого воєнними діями руйнування інфраструктури та її відновлення. *Форум Права.* 2024. № 80(3). С. 91–109. DOI: http://doi.org/10.5281/zenodo.12591874 (дата звернення: 15.10.2025).
6. Міністерство енергетики України. Нова енергетична стратегія України до 2035 року: «Безпека, енергоефективність, конкурентоспроможність». URL: https://www.rada.gov.ua/uploads/documents/41771.pdf (дата звернення: 15.10.2025).

ЗЮБАНОВА Е. Я.,
здобувачка вищої освіти,
Національний університет
цивільного захисту України

КАЛЬЧЕНКО Я. Ю.,
доктор філософії,
доцент кафедри,
Навчально-науковий інститут
пожежної і техногенної безпеки
Національного університету
цивільного захисту України

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ЕНЕРГЕТИЧНОГО КОМПЛЕКСУ УКРАЇНИ ВІД ОБСТРІЛІВ

Проблема захисту енергетичної інфраструктури України є найгострішою оперативною задачею держави та суспільства, перейшовши з розряду планового обслуговування у статус критичного фронту війни, оскільки російська агресія використовує енергетику як ключовий інструмент терору та примусу до капітуляції, реалізуючи стратегію «випаленої землі» щодо критичної інфраструктури. Актуальність аналізу методів захисту досягла критичного, життєво важливого рівня, оскільки ворог перейшов до цілеспрямованого знищення самої генерації, а не лише розподільчих мереж. Такий перехід призвів до безпрецедентних наслідків:

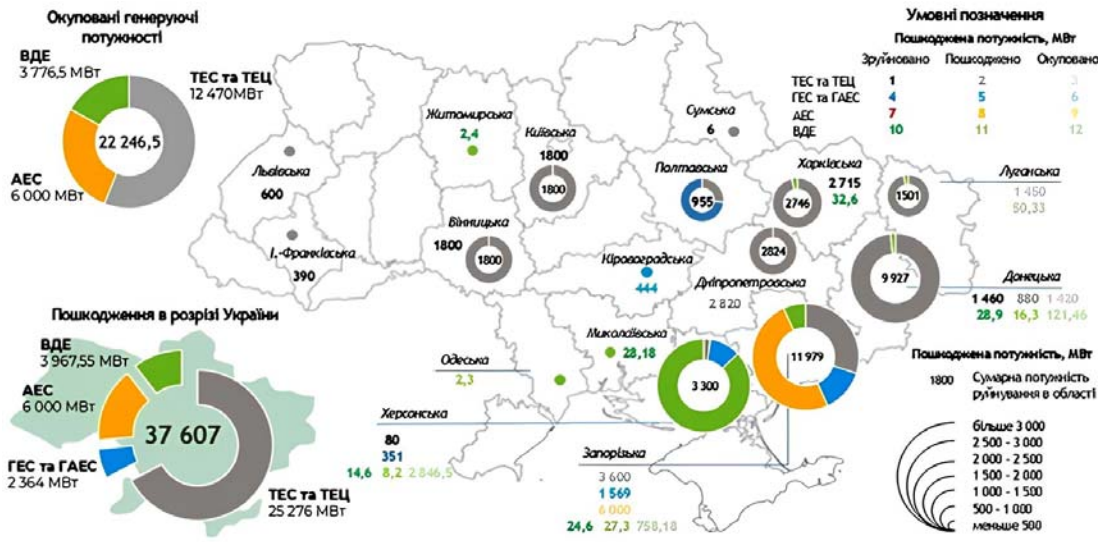

Рисунок 1 – Масштаб втрат енергосистеми України

Аналіз методів захисту енергетичного комплексу України від обстрілів доцільно розділити на три взаємопов’язані стратегічні напрямки: активний захист, пасивний (фізичний) захист та архітектуро-технологічна стійкість (децентралізація).

Активний захист залишається найбільш пріоритетним методом, оскільки лише він здатний повністю запобігти влучанню. Максимальне насичення території навколо критичних енергооб’єктів засобами ППО, включаючи системи середнього та малого радіусу дії для боротьби з дронами-камікадзе та крилатими ракетами. Ефективність прямо залежить від безперебійного постачання зброї та боєприпасів від міжнародних партнерів. У 2024 році ППО стало ключовим фактором захисту, але його покриття не є ідеальним, особливо проти балістичних ракет та високоточних гіперзвукових систем, що вимагає впровадження фізичного захисту [1].

Пасивний (фізичний) захист є страхуванням на випадок прориву ППО і має на меті мінімізувати руйнування від уламків, ударної хвилі або прямого, але менш потужного влучання. Урядом та Генштабом ЗСУ було розроблено три рівні захисту: перший рівень (захист від уламків та ударної хвилі) захищає від вторинних уражень, спричинених падінням уламків збитих ракет, дронів-камікадзе або дронів оперативно-технічного рівня, використовуються прості та швидкозведені захисті споруди такі як габіони (металеві сітчасті контейнери, наповнені камінням або щебенем); біг-беги (великі м’які контейнери, наповнені піском, ґрунтом або іншими сипучими матеріалами. Ці конструкції встановлюються безпосередньо навколо обладнання і здатні поглинати енергію вибуху невеликих боєприпасів, уламків або запобігати швидкому розливу та загорянню оливи при пошкодженні трансформатора. Це найпоширеніший та найшвидший у реалізації рівень захисту, впроваджений на десятках об’єктів [2].

Другий рівень (захист від прямих влучань БПЛА) забезпечує стійкість ключових елементів системи передачі до прямого влучання БПЛА ударного типу, які несуть значно потужніший заряд. Зводять капітальні, масивні, бетонні або залізобетонні конструкції, спеціальні захисні кожухи або бокси з товстого бетону, що оточують обладнання з усіх боків, крім повітряних вводів, також захисні ангари/завіси над обладнанням. Такі споруди призначені для прийому критичної та фугасної енергії вибуху дрона. Застосування цього рівня дозволяє зберегти працездатність дороговартісних та унікальних велико-габаритних трансформаторів. Готовність споруд цього рівня все що потребує прискорення, проте вона вища, ніж у третього рівня .

Третій рівень (захист від прямих влучань ракет) – це максимальний захист найбільш критичних, стратегічно важливих і незамінних вузлів генерації та передачі прямого влучання потужних ракет. Це найбільш складні та капіталомісткі інженерні проєкти, які часто передбачають перенесення життєво важливого обладнання під землю у спеціально збудовані бункери. Будівництво капітальних фортифікаційних споруд із багатошарових, особливо витримати значну енергію влучання. Такий рівень є останньою групою оборони і покликаний уберегти систему від повного колапсу. Реалізація третього рівня просувається найповільніше: готовність цих найважливіших протиракетних споруд становить менше ніж чверть від запланованого, що є найбільшою системною проблемою в пасивному захисті .

Архітектурно-технологічна стійкість – це стратегічний довго-строковий метод, що забезпечує безперебійність системи. Перехід від централізованої системи (великі ТЕС/ГЕС/АЕС) до розподіленої генерації. Це включає встановлення великої кількості малих генеруючих потужностей (газопоршневі, газотурбінні установки, когенерація) ближче до споживачів, також активний розвиток мікромережі та накопичувачів енергії. Хоча ідея децентралізації підтримується на рівні громад та бізнесу її впровадження на державному рівні сповільнюється через бюрократичні перешкоди, боргові проблеми на ринку електро-енергії та брак інвестиційного клімату [3].

Аналіз підтверджує, що ефективність захист енергетичного комплексу вимагає синхронізації трьох напрямків: активне посилення ППО, прискорення та усунення управлінських прогалин у фізичному захисті, негайне усунення регуляторних перешкод для децентралізації. При цьому лише спільна робота за цими напрямками може забезпечити Україні стійкість в умовах триваючої енергетичної війни.

Список використаних джерел:

1. Аналіз методів захисту енергетичного комплексу України від обстрілів розділено на три стратегічні напрямки. URL: https://www.rbc.ua/rus/news/shmigal-zahist-energoob-ektiv-e-tri-rivni-1724751478.html.
2. Енергооб’єкти в Україні отримали три рівні захисту від ракет і дронів. URL:

https://suspilne.media/621497-energoobekti-v-ukraini-otrimali-tri-rivni-zahistu-vid-raket-i-droniv.
3. Розвиток розподіленої генерації електроенергії в Україні. URL: https://epravda.com.ua/energetika/maybutnye-rozpodilenoji-generaciji-v-ukrajini-vikliki-mozhlivosti-ta-perspektivi-804835.

ІШУ В. В.,
курсант, Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

ЛИТВИНЕНКО Р. Г.,
курсант, Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

ЛУЧИК С. Д.,
доктор економічних наук, професор,
професор кафедри
інформаційних систем та технологій,
Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ
(науковий керівник)

БЕЗПЕКА ТА ЗАХИСТ ОБ'ЄКТІВ НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ФІЗИЧНИЙ ТА ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ АСПЕКТИ

Національна критична інфраструктура (НКІ) є основою стабільності та функціонування держави, адже забезпечує енергетичну безпеку, транспортне сполучення, комунікації, фінансову діяльність, охорону здоров'я та обороноздатність країни. Порушення її роботи може спричинити значні соціально-економічні наслідки, дестабілізувати суспільство й поставити під загрозу національну безпеку.

Метою системи захисту критичної інфраструктури є забезпечення її стійкості до внутрішніх і зовнішніх загроз, мінімізація ризиків виникнення надзвичайних ситуацій і збереження безперервної функціонування держави. У сучасних умовах це стає одним із ключових напрямів державної політики безпеки.

Захист критичної інфраструктури передбачає реалізацію комплексу заходів, спрямованих на забезпечення їхньої стійкості, безперервності функціонування та мінімізацію наслідків можливих загроз. У сучасних умовах, коли держава стикається з гібридними, кібернетичними та терористичними викликами, питання ефективної системи безпеки набуває особливої актуальності. до фізичної безпеки належать: фізичний

захист, кіберзахист, техногенно-екологічний захист та інформаційно-аналітичний захист.

Обговоримо аспекти фізичного та інформаційно-аналітичного захисту критичної інфраструктури. Почнемо з фізичного захисту.

Фізичний захист передбачає запобігання несанкціонованому доступу до об'єктів НКІ та мінімізацію ризиків фізичного знищення чи пошкодження. До основних заходів відносять:

1. охорона території, пропускний режим;
2. системи відеоспостереження, сигналізації, контролю доступу;
3. інженерно-технічні бар'єри, укриття, резервні джерела живлення;
4. протидія терористичним і диверсійним загрозам.

Розглянемо більш детально.

1. Охорона території та пропускний режим:

Це базовий елемент фізичної безпеки, спрямований на запобігання несанкціонованому проникненню осіб, транспорту чи вантажів на територію об'єкта. До заходів належать: організація постів охорони, патрулювання та цілодобове чергування, облаштування огорож, воріт і контрольних пунктів в'їзду/виїзду, ведення журналів відвідування, електронна реєстрація персоналу та відвідувачів, використання перепусток, електронних карт або біометричних систем доступу. Такі заходи дозволяють своєчасно виявити підозрілих осіб, запобігти незаконному доступу й підтримувати контроль над усіма переміщеннями на об'єкті.

2. Системи відеоспостереження, сигналізації та контролю доступу:

Ці технічні засоби формують ядро сучасної системи безпеки. Відеоспостереження забезпечує цілодобовий моніторинг ключових зон (входи, периметр, склади, технічні приміщення). Камери з функцією нічного бачення та автоматичного розпізнавання обличчя дозволяють швидко реагувати на інциденти. Сигналізаційні системи подають сповіщення у випадку спроби вторгнення, пошкодження об'єкта або несанкціонованого відкриття дверей. Системи контролю доступу (СКД) дозволяють обмежувати доступ до окремих приміщень за рівнями допуску, фіксують усі входи та виходи, інтегруються з базами даних персоналу.

У комплексі ці системи забезпечують автоматизований контроль безпеки й дають змогу швидко реагувати на потенційні загрози.

3. Інженерно-технічні бар'єри, укриття та резервні джерела живлення:

Цей напрям спрямований на підвищення фізичної стійкості об'єкта до зовнішніх впливів. Інженерно-технічні бар'єри (металеві огорожі, блокпости, турнікети, бетонні блоки, сейф-двері, броньовані вікна) ускладнюють фізичне проникнення зловмисників або транспортних засобів. Укриття призначені для захисту персоналу та технічних систем під час надзвичайних ситуацій (вибухів, обстрілів, пожеж, аварій).

Резервні джерела живлення – генератори, акумуляторні станції, автономні енергетичні системи – забезпечують безперебійну роботу критичних об'єктів у разі знеструмлення чи аварії в енергомережі.

Такі засоби суттєво підвищують надійність і живучість інфраструктури в кризових умовах.

4. Протидія терористичним і диверсійним загрозам:

Заходи запобігання будь-яким навмисним діям, спрямованим на знищення, пошкодження або дестабілізацію роботи об'єкта включають: розроблення планів реагування на теракти чи диверсії, перевірку персоналу (background check) і контроль за доступом до чутливих зон, співпрацю з правоохоронними органами, СБУ та Національною поліцією для обміну інформацією про потенційні загрози, проведення навчань і тренувань персоналу щодо дій у разі нападу або евакуації, встановлення систем виявлення вибухових і небезпечних речовин. Завдяки цим заходам знижується ймовірність успішної атаки та мінімізуються можливі наслідки.

Інформаційно-аналітичний захист є ключовим елементом системи безпеки національної критичної інфраструктури, оскільки забезпечує своєчасне виявлення, прогнозування та попередження загроз, що можуть вплинути на стабільність функціонування об'єктів. Його головно. Метою є створення ефективної системи збору, обробки, аналізу та обміну інформацією про потенційні ризики, інциденти й вразливості.

Основу цього виду захисту становить аналітична діяльність, яка передбачає безперервний моніторинг стану інфраструктурних систем, відстеження подій у кіберпросторі, економічних і соціально-політичних процесів, що можуть мати вплив на безпеку. Зібрані дані обробляються за допомогою спеціалізованих інформаційних платформ і баз даних, що дозволяє формувати актуальні профілі ризиків та визначати пріоритети реагування.

Важливою складовою є створення аналітичних центрів моніторингу, таких як ситуаційні або кризові центри, які здійснюють оперативне спостереження за станом НКІ та координують дії у разі загроз. У межах таких структур використовуються системи раннього попередження, що аналізують великі обсяги даних у реальному часі, застосовують методи штучного інтелекту та аналітику великих даних (Big Data) для виявлення аномалій або підозрілої активності.

Не менш важливим напрямом є інформаційна взаємодія між державними органами, підприємствами та службами безпеки. Ефективний обмін даними дає змогу швидко реагувати на інциденти, координувати дії між різними суб'єктами критичної інфраструктури та запобігати поширенню загроз. В Україні цю функцію частково виконує Національний координаційний центр кібербезпеки при РНБО, який здійснює аналіз ситуації у сфері захисту інформаційного простору.

Крім того, інформаційно-аналітичний захист включає оцінку ризиків та прогнозування кризових ситуацій. За результатами

аналітичних досліджень розробляються сценарії можливих подій, плани реагування, а також рекомендації щодо модернізації систем безпеки та мінімізації наслідків надзвичайних ситуацій.

Таким чином, інформаційно-аналітичний захист відіграє стратегічну роль у забезпеченні безперервності роботи критичної інфраструктури. Його ефективність визначається рівнем інтеграції інформаційних систем, якістю аналітики, своєчасністю передачі даних та здатністю органів влади оперативно приймати рішення на основі достовірної інформації.

Фізичний та інформаційно-аналітичний захист є взаємодоповнюючими складовими системи безпеки об'єктів критичної інфраструктури. Фізичний захист забезпечує недопущення несанкціонованого доступу, пошкодження або знищення важливих об'єктів шляхом впровадження інженерно-технічних засобів, охорони, контролю доступу та відеоспостереження. Водночас інформаційно-аналітичний захист спрямований на моніторинг кіберзагроз, аналіз ризиків, виявлення підозрілої активності та прийняття своєчасних управлінських рішень.

Комплексне поєднання цих напрямів створює багаторівневу систему безпеки, здатну ефективно реагувати на сучасні загрози – від фізичних атак до кібератак, забезпечуючи стійке функціонування критичної інфраструктури держави.

Список використаних джерел:

1. Cybersecurity and Infrastructure Security Agency (CISA) – "Protected Critical Infrastructure Information (PCII) Program". cisa.gov.
2. CISA – "Critical Infrastructure Assessments". cisa.gov.
3. National Council of ISACs – інформація про Information Sharing and Analysis Centers (ISACs). natlcouncilofisacs.
4. United States Department of Homeland Security – сторінка "Information Analytics" (стосується аналітики ризиків в інфраструктурі). dhs.gov.
5. Звіт «Cyber Threat Activity Related to the Russian Invasion of Ukraine» – приклад сучасної кіберзагрози для критичної інфраструктури. Canadian Centre for Cyber Security.
6. KPMG International – "Ukraine conflict: Cyber considerations" – приклад глобального контексту кіберзахисту. assets.kpmg.com.

КОХАН С. О.,
старший викладач кафедри
тактико-спеціальних дисциплін,
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

МЕЛЬНИК В. В.,
доктор філософії,
старший викладач кафедри
тактико-спеціальних дисциплін,
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

ВИКОРИСТАННЯ ГЕЛІКОПТЕРІВ АРМІЙСЬКОЇ АВІАЦІЇ ДЛЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ХОДІ РОСІЙСЬКОЇ ЗБРОЙНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

З початком повномасштабної збройної агресії російської федерації проти України у лютому 2022 року питання захисту об'єктів критичної інфраструктури (КІ) стало одним із ключових аспектів забезпечення національної безпеки. Об'єкти енергетики, транспорту, зв'язку, оборонної промисловості та державного управління стали основними цілями для масованих повітряних і ракетних ударів противника [1].

У цих умовах гелікоптери армійської авіації (АА) відіграли важливу роль у системі оперативного реагування, розвідки, протидії диверсійно-розвідувальним групам (ДРГ), евакуації персоналу та матеріальних цінностей, а також у безпосередньому прикритті важливих об'єктів. Досвід бойових дій 2022–2025 років продемонстрував необхідність інтеграції армійської авіації у комплексну систему оборони критичної інфраструктури [3].

Згідно з доктринальними документами Збройних Сил України та досвідом сучасних конфліктів [2; 5], основними завданнями армійської авіації у забезпеченні оборони об'єктів КІ є:

1. повітряна розвідка та моніторинг районів розташування об'єктів, особливо в зонах підвищеної терористичної загрози;
2. чергування сил швидкого реагування для виявлення та нейтралізації ДРГ;
3. вогнева підтримка підрозділів охорони у разі спроби прориву або нападу на об'єкт;
4. доставка сил підкріплення, боєприпасів і технічних засобів у випадку обстрілів або руйнування транспортної інфраструктури;
5. евакуація постраждалого персоналу та проведення пошуково-рятувальних операцій.

Тому армійська авіація стала мобільним компонентом, який забезпечує оперативне реагування у найкоротші терміни, що особливо

важливо при одночасних атаках по кількох об’єктах критичної інфраструктури [4].

Практичний досвід застосування авіаційної складової сухопутних військ по захисту раніше зазначених об’єктів показав, що під час активної фази бойових дій (2022–2023 рр.) гелікоптери Мі-8, Мі-24 та Мі-2МСБ виконували низку завдань з прикриття енергетичних об’єктів у Київській, Дніпропетровській, Миколаївській та Харківській областях. Особовий склад АА здійснював патрулювання у районах теплових та гідроелектростанцій, підстанцій і транспортних вузлів [3]. У листопаді 2022 року підрозділи армійської авіації успішно провели операцію з евакуації персоналу після ракетного удару по Кременчуцькій ТЕС. Гелікоптери Мі-8 здійснили понад 10 вильотів під загрозою повторних ударів, забезпечивши транспортування постраждалих у безпечні райони [6]. Під час зимової кампанії 2022–2023 рр., коли російська федерація здійснила масовані атаки по енергосистемі України, гелікоптери виконували завдання з доставки ремонтних бригад, енергетичного обладнання та медичної евакуації. Зокрема, екіпажі 16-ї окремої бригади армійської авіації забезпечили прикриття об’єктів «Укренерго» у центральному регіоні України [3; 4]. У 2024 році, з появою сучасних засобів ППО та БпЛА противника, акцент було зміщено на високоманеврові дії малими групами. Гелікоптери типу Мі-2МСБ-В та H145M здійснювали розвідку й моніторинг районів промислових підприємств, нафтобаз та складів боєприпасів [5]. Водночас упроваджувалися елементи спільних операцій гелікоптерів і безпілотників (Manned–Unmanned Teaming), що дозволило підвищити точність виявлення загроз [7].

У ході аналізу досвіду застосування АА по захисту об’єктів КІ слід відмітити і тісну взаємодію з іншими підрозділами Сил оборони. Тому що якість виконання завдань значною мірою залежала від координації з підрозділами СБУ, Національної гвардії, Сил територіальної оборони та ППО. Зокрема, у ході відбиття атак на об’єкти «Укрзалізниці» у 2023 р. було створено єдину систему реагування, де гелікоптери здійснювали розвідку з повітря, а наземні групи – ліквідацію наслідків [6].

У рамках спільних дій з підрозділами СБУ на Дніпровському напрямку екіпажі армійської авіації використовували нічні прилади спостереження для виявлення руху ДРГ поблизу об’єктів енергетики. Цей досвід став основою для розроблення нових тактичних прийомів нічних бойових вильотів у межах програми підготовки льотного складу [2; 7].

Поряд з цим, практичний досвід застосування виявив і ряд суттєвих проблем, що впливали на ефективність виконання завдань зокрема:

- висока насиченість району бойових дій засобами ППО противника, що обмежувало висоту і тривалість польотів;

- застарілий парк гелікоптерів, частина яких мала вичерпаний ресурс;
- нестача сучасних засобів зв'язку та навігації, які ускладнювали взаємодію з підрозділами ППО та БпЛА;
- потреба в додатковій підготовці екіпажів для дій у нічних і складних метеоумовах [2; 5].

Для подолання цих проблем у майбутньому потрібний подальший розвиток способів та методів використання гелікоптерів армійської авіації у сфері захисту критичної інфраструктури. Це передбачає комплексний підхід, який охоплює технічні, тактичні та організаційні напрями.

1. Технічний напрям – передбачає модернізацію гелікоптерів за стандартами НАТО (установлення систем нічного бачення, GPS/INS-навігації, засобів РЕБ, теплових пасток, бронювання кабін), зокрема заходи з модернізації гелікоптерів Мі-8МСБ-В, оснащення їх комплексами РЕБ та системами попередження про радіолокаційне опромінення [5].
2. Тактичний напрям – розроблення єдиної доктрини повітряного реагування на загрози критичним об'єктам, включно з алгоритмами взаємодії з БпЛА, підрозділами СБУ, ППО та Силами територіальної оборони. Відповідно до стратегічних документів Міністерства оборони України, до 2030 року передбачається створення єдиної авіаційної мережі реагування для всіх видів Збройних Сил [6; 7].
3. Організаційний напрям – створення алгоритмів автоматизованого обміну даними між авіаційними підрозділами та центрами управління критичною інфраструктурою, здатних у реальному часі виявляти загрози та спрямовувати екіпажі гелікоптерів у зони небезпеки. До цього можна віднести упровадження інтегрованої системи аерокосмічного моніторингу об'єктів КІ, що об'єднуватиме інформацію від супутників, безпілотників і гелікоптерів у єдиному аналітичному просторі [1; 4].

Також велике значення у вирішенні цих питанн відіграють роль наші Міжнародні партнери, зокрема США, Польща та Велика Британія, які вже підтримують Україну у створенні сучасної системи повітряного реагування на загрози енергетичним та транспортним об'єктам, з урахуванням досвіду НАТО [5]. Така співпраця сприятиме підвищенню сумісності систем управління, навігації та зв'язку.

Отже досвід бойового застосування гелікоптерів армійської авіації у 2022–2025 роках підтвердив їхню ключову роль у системі захисту критичної інфраструктури держави. Висока мобільність, універсальність та здатність діяти в умовах інтенсивного вогневого впливу роблять ці підрозділи незамінними у протидії гібридним загрозам.

Подальший розвиток цієї складової оборонної системи України має ґрунтуватися на модернізації авіаційної техніки, інтеграції з безпілотними платформами та впровадженні єдиної системи управління обороною критичних об’єктів. Врахування досвіду, здобутого у 2022–2025 роках, дозволить сформувати ефективну модель авіаційного прикриття КІ, здатну забезпечити безпеку енергетичної, транспортної та промислової інфраструктури України в умовах тривалого протистояння.

Список використаних джерел:

1. Міністерство оборони України. Біла книга 2023: Збройні Сили України. Київ : МОУ, 2024. 150 с.
2. Горбулін В. П., Ланде Д. В. Війна майбутнього: концепти, технології, перспективи. Київ : НІСД, 2023. 312 с.
3. АрміяInform. Роль армійської авіації у захисті об’єктів критичної інфраструктури URL: https://armyinform.com.ua.
4. The Military Balance 2025. London: International Institute for Strategic Studies, 2025. 560 p.
5. NATO Standardization Office. ATP-49. Air Operations in Support of Land Forces. Brussels : NSO, 2022. 210 p.
6. Командування Сухопутних військ ЗСУ. Аналіз бойового застосування авіаційних підрозділів у ході оборони об’єктів критичної інфраструктури 2022–2024 рр. Київ : НУОУ, 2025. 52 с.
7. Jane’s Defence Weekly. Protecting Energy and Transport Infrastructure : Lessons from Ukraine. London, 2024.

КОЧКІН В. Г.,
Національна академія Служби безпеки України

ЗАХИСТ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

В умовах сучасних загроз національній безпеці України особливе значення набуває захист об’єктів критичної інфраструктури. Ці об’єкти є стратегічно важливими для життєдіяльності суспільства, оскільки будь-яке порушення їх функціонування може призвести до серйозних соціально-економічних та екологічних наслідків. Гібридні загрози, які поєднують військові дії, кібератаки, диверсійні операції та інформаційний вплив, ставлять перед державними та приватними структурами завдання підвищення рівня захисту та стійкості критичних об’єктів. Метою дослідження є аналіз сучасних підходів до захисту критичних об’єктів, оцінка їх вразливості та визначення ефективних заходів щодо підвищення безпеки в умовах гібридної війни. Особлива увага приділяється об’єктам хімічної промисловості, де порушення технологічних процесів може призвести до масштабних аварій, витоків токсичних речовин та загрози життю населення.

Критична інфраструктура охоплює енергетичні системи, транспортні вузли, об'єкти комунального господарства, промислові комплекси, включаючи хімічні підприємства. Основні фактори вразливості таких об'єктів включають залежність від цифрових технологій, високу концентрацію небезпечних речовин та соціально-економічну значимість. Автоматизовані системи управління технологічними процесами роблять об'єкти вразливими до кібератак, а порушення безпеки на хімічних підприємствах може спричинити витоки аміаку, хлору чи інших токсичних речовин. Крім того, стратегічне значення об'єктів критичної інфраструктури робить їх потенційними цілями для диверсій та саботажу, що у поєднанні з інформаційним впливом створює комплексну загрозу національній безпеці.

Гібридна війна поєднує різні методи тиску та руйнування, включаючи кібератаки на системи управління технологічними процесами, саботаж на об'єктах, дезінформаційні кампанії та психологічний тиск на населення. Такі загрози можуть носити як прямий характер, безпосередньо порушуючи роботу об'єктів, так і непрямий, створюючи хаос через поширення паніки та невірної інформації. Практичний аналіз показує, що навіть локальні втручання в роботу промислових об'єктів можуть спричинити серйозні наслідки для економіки та безпеки. В умовах гібридної війни ключовим завданням стає прогнозування ризиків та розробка комплексних систем захисту об'єктів, здатних швидко реагувати на будь-які загрози.

Захист критичних об'єктів передбачає комплекс технічних, організаційних та кадрових заходів. До технічних заходів належать системи відеоспостереження та контролю доступу, автоматизовані системи моніторингу технологічних процесів, протипожежні та аварійні системи, а також кіберзахист промислових мереж. Організаційні заходи включають розробку регламентів реагування на кризові ситуації, плани евакуації, координацію з підрозділами СБУ та Національної поліції, проведення навчальних операцій та тренувань персоналу. Кадрові заходи передбачають підготовку фахівців з охорони та реагування на надзвичайні ситуації, навчання методам стресостійкості та командної взаємодії, застосування симуляційних тренажерів та навчальних кейсів. Крім того, важливим аспектом є дотримання законодавчих та нормативних вимог, стандартів європейської хімічної промисловості та інтеграція міжнародних рекомендацій у систему управління ризиками.

Для підвищення ефективності захисту рекомендується впровадження сучасних інформаційних систем раннього виявлення загроз, цифрових тренажерів для моделювання аварійних ситуацій, розробка планів превентивного реагування та координація з державними органами. Використання штучного інтелекту для прогнозування ризиків дозволяє визначити пріоритетні об'єкти та сценарії, що потребують особливої уваги. Забезпечення комунікаційної готовності сприяє швид-

кому інформуванню персоналу та населення у разі загрози або аварійної ситуації.

Таким чином, захист об’єктів критичної інфраструктури в умовах гібридної війни є комплексним стратегічним завданням для національної безпеки. Інтегрований підхід, що поєднує технічні, організаційні, кадрові та законодавчі заходи, дозволяє підвищити стійкість об’єктів, забезпечити ефективне реагування на загрози та мінімізувати негативні наслідки для економіки та населення. Системна підготовка персоналу, включаючи психологічну стійкість, знання кіберзахисту та навички реагування на кризові ситуації, є ключовим фактором забезпечення національної безпеки та збереження функціонування критично важливих об’єктів у складних умовах сучасних загроз.

Список використаних джерел:

1. Білокінь С. М. Критична інфраструктура України: оцінка загроз та методи захисту. Київ : НА СБУ, 2022.
2. Кузьменко О. В., Рибак П. А. Гібридні загрози та їх вплив на промислові об’єкти. Вісник національної безпеки, 2023.
3. NATO. Critical Infrastructure Protection Guidelines. Brussels : NATO, 2021.
4. European Chemical Industry Council. Safety Management in Chemical Plants. Brussels, 2020.
5. АрміяInform. Захист критичної інфраструктури України у умовах війни, 2023.
6. Романенко С. В., Петров В. М. Кібербезпека промислових систем. Київ : НА СБУ, 2021.

МИРОШНИК О. М.,
доктор технічних наук, професор,
професор кафедри цивільного захисту
та інформаційних технологій,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

ПОДЛЕСНА В. І.,
викладач кафедри,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

OPTIMISATION OF CIVIL PROTECTION UNITS’ ACTIONS IN RESPONDING TO EMERGENCIES AT THERMAL POWER FACILITIES

The thermal energy sector is a critical component of national energy security, ensuring a stable supply of electricity and heat to industry and the

population. However, thermal power plants (TPPs), boiler houses, and combined heat and power plants (CHPs) are classified as high-risk facilities where accidents can cause severe consequences for people, the environment, and the economy. The most common emergencies include boiler room fires, fuel system explosions, releases of combustion products, hazardous substance leaks, and the destruction of pressurised equipment.

The effectiveness of civil protection units in such situations depends on their level of training, access to modern technical equipment, operational coordination, and the optimal use of tactical methods. Practice shows that response operations at thermal power facilities are complicated by factors such as large production areas, high equipment temperatures, rapid fire spread due to flammable materials, and the risk of secondary explosions.

Optimisation of emergency response should combine organisational, technical, and innovative approaches. A key direction involves the development and application of mathematical models that can predict the progression of accidents and identify the most effective response strategies. For instance, fire spread modelling in boiler rooms–considering temperature dynamics and air flow–helps determine optimal deployment of resources for fire containment.

Decision support systems (DSS) for emergency managers are another essential component. These systems enable real-time data analysis on facility conditions, event intensity, and potential secondary hazards, offering tactical recommendations. This is particularly vital at thermal power facilities, where even short delays can lead to equipment failure and production losses.

Technical enhancement of civil protection units is also critical. The use of mobile foam systems, firefighting robots for hard-to-reach areas, thermal imagers, and drones for reconnaissance significantly improves operational efficiency. Combining traditional firefighting methods with innovative technologies reduces risks to personnel and shortens response time. Furthermore, the introduction of advanced communication technologies–such as integrated command-and-control platforms–can facilitate information exchange between on-site responders and central coordination centres, ensuring situational awareness and prompt decision-making.

Organisational preparedness is equally important. Regular training and simulation drills at power facilities involving emergency units help refine coordination procedures, update Emergency Response and Elimination Plans (EREPs), and familiarise personnel with site-specific characteristics. Such exercises enable faster decision-making in real emergencies. Training should also incorporate elements of scenario-based learning and virtual reality simulations, allowing personnel to practise responding to complex multi-factor incidents in a risk-free environment. This approach not only strengthens individual skills but also develops teamwork and leadership under stress.

The integration of information technologies into civil protection activities enhances monitoring and forecasting of man-made threats, enabling early detection of hazards and risk assessment at energy enterprises. This contributes not only to effective mitigation but also to prevention of emergencies. Equally important is the creation of unified data platforms that consolidate information from energy operators, meteorological services, and emergency departments, providing a comprehensive view of potential threats.

Coordination among the State Emergency Service, facility administrations, and other stakeholders (medical, law enforcement, environmental) must also be strengthened. Optimisation in this area involves adopting unified management standards aligned with international frameworks such as ISO 22320:2018 and NFPA 1600:2019, which regulate emergency response procedures. In the longer term, interagency cooperation should be developed into a full-fledged strategic partnership model that includes joint planning, shared resource pools, and collective risk assessment mechanisms. Such coordination enhances resilience not only at the facility level but across the entire energy infrastructure of the state.

In conclusion, optimising the actions of civil protection units at thermal power facilities is a complex, multi-dimensional process. It encompasses the use of predictive modelling and decision support systems, modern technical means, continuous organisational training, and international management standards. Implementing these measures will enhance the efficiency and safety of emergency response while minimising harm to the population, the environment, and the economy.

References:

1. Кодекс цивільного захисту України : Закон України від 2 жовт. 2012 р. № 5403-VI // Відомості Верховної Ради України. 2013. № 34–35. Ст. 458.
2. ДСТУ ISO 22320:2022. Безпека та адаптивність. Управління в надзвичайних ситуаціях. Настанови щодо управління інцидентами (ISO 22320:2018, IDT). Київ : ДП «УкрНДНЦ», 2022. 30 с.
3. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). Київ : ДП «УкрНДНЦ», 2019. 34 с.
4. Мирошник О., Землянський О., Дендаренко В., Зажома В. Оцінка ефективності системи цивільного захисту з попередження та ліквідації наслідків надзвичайних ситуацій у прикордонних районах України // *Надзвичайні ситуації: попередження та ліквідація*. 2025. № 1. С. 105–114.
5. Мирошник О. М. Технологія експертного визначення рівня техногенної безпеки житла у будинках підвищеної поверховості // Вісник Черкаського державного технологічного університету. 2018. № 1. С. 136–141.

ПОМАЗА-ПОНОМАРЕНКО А. Л.,
доктор наук з державного управління, професор,
завідувач науково-дослідної лабораторії
з дослідження проблем управління
у сфері цивільного захисту,
Національний університет
цивільного захисту України

ТАРАДУДА Д. В.,
кандидат технічних наук, доцент,
професор кафедри управління діяльністю
підрозділів цивільного захисту інституту
післядипломної освіти,
Львівський державний університет
безпеки життєдіяльності

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стійкість функціонування об'єктів критичної інфраструктури (КІ) є визначальною умовою національної безпеки, економічної стабільності та життєдіяльності суспільства. В умовах воєнного стану, масштабних гібридних загроз, кібератак та терористичних ризиків, питання забезпечення безперервності роботи критичної інфраструктури (далі – КІ) стає одним із головних напрямів державної політики безпеки. Для України, яка зазнала руйнувань енергетичної, транспортної, комунікаційної інфраструктури внаслідок воєнних дій, формування системи стійкості КІ означає не лише відновлення, а й створення нової архітектури безпеки, заснованої на принципах адаптивності, цифрової інтегрованості та взаємодії секторів.

У науковій літературі поняття resilience (стійкість, життєздатність) розглядається як здатність системи передбачати, поглинати, адаптуватися та швидко відновлюватися після деструктивних впливів. Стійкість критичної інфраструктури включає три основні рівні:

1. Технічна стійкість – здатність інженерних систем зберігати функціональність у разі фізичного чи кібернетичного ураження.
2. Організаційна стійкість – ефективність управління кризами, координація суб'єктів безпеки.
3. Соціальна стійкість – готовність населення та персоналу до дій у надзвичайних ситуаціях.

Методологічно концепція стійкості КІ [1] базується на моделі адаптивного управління (adaptive management), ризик-орієнтований підхід, а також принципи управління безперервністю бізнесу (Business Continuity Management).

Державна політика України у сфері забезпечення стійкості КІ регулюється низкою документів, а саме: Закон України «Про критичну

інфраструктуру», що визначає правові основи функціонування, захисту та відновлення КІ; Постанова КМУ «Про затвердження Порядку формування переліку об'єктів критичної інфраструктури»; Стратегія забезпечення кібербезпеки України (на 2021–2025 роки); Стратегія національної безпеки України (2020 р.), що закріплює принципи захисту КІ як складової безпекової політики [2]. Однак практична реалізація цих документів стикається з такими проблемами: відсутністю інтегрованої інформаційної системи моніторингу стану КІ, фрагментарністю управлінських повноважень й обмеженими ресурсами для модернізації об'єктів.

Серед основних проблем забезпечення стійкості КІ можна виокремити такі:

1. Високий рівень фізичних загроз – цілеспрямовані обстріли енергетичних, транспортних, об'єктів ЖКГ та ін. під час війни.

2. Кібератаки на енергетичні системи (наприклад, атака на «Укренерго» (грудень 2022 р.), коли відбулася спроба порушити енергопостачання через шкідливе ПЗ.

3. Нестача резервних потужностей і децентралізованих елементів інфраструктури.

4. Недостатній рівень міжвідомчої координації через інституційне дублювання функцій (між Міноборони, НКЦК при РНБО, Держспецзв'язку та Міненерго, СБУ, ДСНС тощо).

5. Відсутність системи аудиту стійкості (відсутні стандарти оцінки ризиків для об'єктів різних секторів КІ (енергетичного, транспортного, ІТ).

6. Залежність від імпортних технологій у галузях енергетики, зв'язку, хімічної промисловості, що ускладнює самостійне відновлення після руйнувань.

Щодо ключових напрямів державної політики щодо забезпечення стійкості КІ, то серед них можна визначити такі:

1. Розвиток системи оцінки ризиків на об'єктах КІ. Упровадження інтегрованої системи Risk Assessment & Management System для всіх секторів КІ, що забезпечує прогнозування наслідків і сценарне моделювання криз.

2. Забезпечення кіберстійклості КІ, що передбачає розгортання національної мережі центрів реагування на кіберінциденти (CERT-UA, SOC у відомствах), а також створення системи сертифікації ІТ-продуктів, що використовуються на об'єктах КІ.

3. Розвиток локальних енергетичних систем, мікромереж, відновлюваних джерел енергії, які підвищують автономність об'єктів КІ у кризових ситуаціях.

4. Підвищення результативності інституціональної взаємодії шляхом упровадження моделі мережевого врядування (network governance), що поєднує державні, приватні та громадські структури у спільному забезпеченні безпеки КІ.

5. Забезпечення накопичення та повноцінної реалізації людського капіталу. Це вимагає оперативного навчання необхідних кадрів з управління кризами та безперервності діяльності, підвищення кваліфікації персоналу КІ у сфері безпеки, кіберзахисту та протидії гібридним загрозам.

Європейський Союз у межах Директиви (EU) 2022/2557 про стійкість критичних суб'єктів запровадив принцип «all-hazards approach», що передбачає застосування комплексного підходу до управління всіма типами ризиків. США реалізують концепцію Critical Infrastructure Security and Resilience (CISR), що передбачає тісну співпрацю між державою та приватним сектором через Агентство з кібербезпеки та безпеки інфраструктури (CISA). Ізраїль формує багаторівневу модель захисту з інтеграцією елементів цивільної оборони, кіберзахисту і локальної самоврядності [4; 5].

Для України адаптація таких практик може базуватися на створенні Національної ради з питань стійкості КІ при РНБО, а також публічно-приватного партнерства у сфері модернізації критичної інфраструктури. У цьому контексті доцільно розглянути технологічні аспекти стійкості КІ, що забезпечується за рахунок: 1) систем моніторингу і раннього виявлення інцидентів (Early Warning Systems); 2) резервного копіювання і дублювання критичних елементів (redundancy & backup); 3) технології штучного інтелекту для прогнозування пошкоджень; 4) інтернет речей (IoT) у системах управління ресурсами; 5) блокчейн-технологій для забезпечення цілісності критичних даних.

Важливим компонентом стійкості КІ є готовність населення до кризових ситуацій, формування культури безпеки, довіри до державних інститутів, ефективна інформаційна політика, що запобігає панічним настроям під час криз.

Отже, стійкість критичної інфраструктури – це не лише технічне завдання, а системна державна стратегія, що охоплює правові, інституційні, кадрові, технологічні та соціальні компоненти. Її забезпечення можливе лише за умов інтеграції принципів resilience governance у політику національної безпеки, розбудови міжсекторної співпраці, переходу від реактивного до проактивного управління ризиками, залучення громадянського суспільства до моніторингу та контролю у сфері безпеки КІ. Стійкість критичної інфраструктури – це стратегічний ресурс держави, що визначає її здатність не лише виживати, а й розвиватися в умовах багатовимірних криз.

Список використаних джерел:

1. Лазор О. Я., Юник І. Г., Чемерпільська А. М. Організаційно-правові засади забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури України: формування та розвиток // Державне управління: удосконалення та розвиток. 2024. № 5. URL: https://www.nayka.com.ua/index.php/dy/article/view/3677/3712.

2. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1030-2022-%D0%BF#Text.
3. Помаза-Пономаренко А. Л., Тарадуда Д. В. Застосування цифрових технологій у сфері критичної інфраструктури для забезпечення цивільної безпеки // Матеріали Науково-практичної конференції «Інноваційні підходи до розвитку технологій та економіки» (27.06.2024 р., м. Свалява). 2024. С. 248–251.
4. Помаза-Пономаренко А. Л., Тарадуда Д. В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). URL: https://www.inter-nauka.com/issues/administration2024/3/9732.
5. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Vol. 14. Issue 1. Pp. 216–220.

РЕМІННИЙ О. В.,
курсант, Національний університет
цивільного захисту України

БОРСУК О. В.,
кандидат технічних наук,
викладач кафедри,
Навчально-науковий інститут пожежної
та техногенної безпеки
Національного університету
цивільного захисту України

ВПЛИВ БОЙОВИХ ДІЙ НА СТІЙКІСТЬ ЕНЕРГЕТИЧНИХ СИСТЕМ ТА ВИНИКНЕННЯ АВАРІЙНИХ РЕЖИМІВ КОРОТКОГО ЗАМИКАННЯ

Об'єкти енергетики є пріоритетними цілями під час воєнної агресії рф, адже їх ураження призводить до масштабних порушень у роботі енергосистеми, відключення електропостачання об'єктів критичної та цивільної інфраструктури. Руйнування підстанцій, ліній електропередач і трансформаторів безпосередньо впливає на стійкість електромережі та створює умови для виникнення аварійних режимів, найпоширенішими з яких є короткі замикання [1].

Ударні хвилі вибухів і прямі обстріли можуть пошкоджувати ізоляцію та контакти обладнання, порушувати цілісність обмоток трансформаторів, що призводить до електричних пробоїв і коротких замикань. Такі аварії здатні спричинити відключення великих ділянок мережі та порушити безперебійне електропостачання [1].

Пошкодження енергетичних об'єктів можна класифікувати як: **прямі** – фізичне руйнування унаслідок обстрілів чи вибухів і **побічні або вторинні** – пошкодження, що виникають через аварійні режимів та нестабільність електричних систем, що сприяють підвищенню

температури, імпульсним перенапруги, пробоям ізоляції, утворенню коротких замикань.

При дії на енергоустановку вражаючих факторів вибухів можливі утворення аварійного режиму короткого замикання, що виникає в результаті безпосереднього контакту фаз між собою або між фазою та землею, унаслідок чого протікає великий струм, який пошкоджує електрообладнання.

Іншим руйнівним вторинним фактором є ізоляційні пошкодження, що виникають у разі великих теплових впливів та можуть спричинити руйнування або зниження опору ізоляційних матеріалів, що спричиняє пробої й зменшення електричної міцності системи.

Також відслідковуються випадки короткочасних електричних пробоїв, викликані дією вибухових хвиль, електромагнітних імпульсів чи перенапруг, які можуть спричиняти виникнення коротких замикань, навіть без прямого контакту провідників [2].

Аналіз сучасних існуючих заходів щодо запобігання аварійних режимів направлена на впровадження дистанційних датчиків контролю параметрів навантаження та потужності електромереж, своєчасне відключення та повідомлення про відхилення від нормального режиму роботи. Завдяки впровадженню систем датчиків, що фіксують початкові ознаки несправностей та формують запит на зміну конфігурацій параметрів мережі, здійснюється попередження перевантаження обладнання та пошкодження ізоляції трансформаторів унаслідок перегріву. Завдяки елементам постійному моніторингу та контролю параметрів можна відстежувати зміни енергетичних потоків і ефективніше розподіляти навантаження між компонентами енергосистем [3].

Важливість роботи енергосистем та їх пріоритетність як цілі військової агресії вказують на вразливість енергооб’єктів та необхідність захисту, як від прямого – фізичного знищення, так і в забезпеченні подальшої стабільної роботи. В умовах сьогодення України для підвищення стійкості енергосистем і зменшення ризику вторинних пошкоджень необхідно застосовувати комплекс превентивних заходів: захисні конструкції енергоустановок, захист ліній електропередач, використання броньованої та високоякісної ізоляції, надійного заземлення, впровадження систем контролю та автоматичного відключення пошкоджених ділянок, захисту від імпульсних перенапруг систем мережі. Виконання цих заходів підвищує надійність і стійкість енергосистеми, зменшує масштаби аварій і забезпечує стабільне електропостачання критично важливих об’єктів за складних умовах воєнного часу.

Список використаних джерел:

1. Сіренко Ю. В., Вольвач Т. С., Савойський О. Ю., Козін В. М. Аналіз стану енергетичної системи України та заходи щодо покращення ситуації. Вісник Херсонського національного технічного університету 1(2(93)) : 229–237. URL: https://www.researchgate.net/publication/394961246.

2. ДСТУ EN 50160-2023. Характеристики напруги електропостачання в електричних мережах загальної призначеності (EN 50160:2022, IDT). [Чинний від 08.12.2023]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023. 32 с.
3. Остренко Д.О. Дослідження роботи штучної нейронної мережі, яка працює в енергосистемі з метою запобігання аварійних режимів. URL: https://web.archive.org/web/20220309054028id_/http://elen.donntu.edu.ua/2074-2630-2020-1-48-54.pdf.

ТАРАНОВ Д. В.,
Національна академія Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ФІЗИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У сучасних умовах збройної агресії російської федерації проти України питання забезпечення фізичного захисту об'єктів критичної інфраструктури (далі – ОКІ) набуває стратегічного значення. Критична інфраструктура охоплює галузі енергетики, транспорту, зв'язку, водопостачання, охорони здоров'я, фінансів, оборони тощо, які є життєво необхідними для стабільного функціонування держави та суспільства [1]. Зростання кількості диверсій, терористичних загроз та кібератак актуалізує необхідність формування цілісної системи захисту ОКІ, інтегрованої в загальнодержавну систему безпеки.

Метою даного дослідження є визначення основних напрямів і механізмів забезпечення фізичної безпеки об'єктів критичної інфраструктури в контексті національної безпеки України.

Слід зазначити, що згідно з підходами ЄС та НАТО, захист критичної інфраструктури (Critical Infrastructure Protection, CIP) – це комплекс превентивних, технічних, організаційних та правових заходів, спрямованих на зниження ризиків впливу деструктивних факторів на функціонування життєво важливих об'єктів [2].

В українському законодавстві поняття «критична інфраструктура» визначене у Законі України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX, де під нею розуміють сукупність об'єктів, систем, мереж та процесів, порушення функціонування яких може мати негативні наслідки для національної безпеки [1].

Фізичний захист ОКІ передбачає використання технічних засобів охорони, пропускного контролю, відеоспостереження, сигналізації, систем реагування та протидиверсійних заходів. Водночас ефективність фізичного захисту неможлива без його інтеграції з кібербезпекою, аналітикою ризиків і системою стратегічних комунікацій [3].

Нормативно-правова база України у сфері захисту ОКІ формується на засадах національної безпеки, державного управління, оборонного

планування та євроатлантичної інтеграції. Її основою є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII, який визначає правові та організаційні засади забезпечення безпеки кіберпростору, зокрема і в частині критичної інфраструктури [4].

Визначення, ідентифікацію та категоризацію ОКІ регламентує Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Про затвердження Порядку визначення об'єктів критичної інфраструктури» [5]. Документом установлено алгоритм відбору об'єктів за критеріями життєво важливості, міжгалузевого впливу та потенційних наслідків їх дестабілізації.

Важливе значення має також Закон України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII, який визначає критичну інфраструктуру складовою сектору безпеки та оборони [6]. У розвиток його положень прийнято Стратегію кібербезпеки України на 2021–2025 роки, затверджену Указом Президента України від 26 серпня 2021 р. № 447/2021, де окремо визначено напрями зміцнення фізичного та інформаційного захисту ОКІ [7].

На рівні підзаконних актів діють відомчі нормативи, зокрема накази Служби безпеки України щодо охорони державної таємниці, інструкції МВС з організації охорони об'єктів, а також державні стандарти ДСТУ ISO/IEC 27001 та ДСТУ ISO 28000:2008, які встановлюють вимоги до систем управління безпекою ланцюгів постачання.

Міжнародно-правовими орієнтирами виступають Директива ЄС 2008/114/ЕС про ідентифікацію та охорону європейських критичних інфраструктур, а також NATO Security Investment Programme (NSIP), де акцентується важливість інтеграції фізичного та кіберзахисту. Україна поступово гармонізує свої підходи з цими стандартами в межах Угоди про асоціацію з ЄС.

Отже, нормативно-правова база фізичного захисту ОКІ в Україні має багаторівневу структуру, однак потребує подальшої систематизації, усунення колізій та узгодження між відомствами, насамперед між СБУ, МВС, Міноборони, ДСНС і Мінцифри.

Водночас зазначимо, що система фізичного захисту ОКІ – це комплекс організаційно-технічних, інженерних та правових заходів, спрямованих на запобігання несанкціонованому доступу, диверсіям, терористичним актам та іншим загрозам функціонуванню критичних об'єктів [8]. Її основу становлять три взаємопов'язані рівні:

1. Організаційний – розроблення політик безпеки, планів реагування, інструкцій дій персоналу, координація з органами СБУ, МВС та ДСНС.

2. Технічний – використання сучасних систем відеоспостереження, сигналізації, контролю доступу, біометричних ідентифікаторів, датчиків руху, систем аналітики подій.

3. Інженерно-технологічний – укріплення периметрів, створення багаторівневих зон безпеки, резервне енергозабезпечення, протипожежні системи, укриття та бар'єрні споруди.

При цьому особлива увага приділяється інтеграції фізичного та кіберзахисту, адже більшість критичних систем є автоматизованими й підключеними до мережі. Тому сучасні стратегії безпеки впроваджують концепцію «Security by Design», тобто – безпека закладається в архітектуру системи ще на етапі проєктування [9].

Важливим елементом є ризик-менеджмент, що передбачає ідентифікацію потенційних загроз, оцінку вразливостей, формування планів реагування та навчання персоналу. Приклади ефективних практик можна спостерігати в енергетичній галузі, де оператори систем передачі (НЕК «Укренерго») впроваджують багаторівневий моніторинг стану мереж і взаємодіють із СБУ та кіберполіцією для запобігання диверсіям.

У структурі системи фізичного захисту ОКІ важливою є також підготовка персоналу, створення аварійно-рятувальних підрозділів та проведення спільних міжвідомчих навчань. Успішна реалізація цих заходів можлива лише за умови достатнього фінансування, міжгалузевої координації та державного контролю ефективності впроваджених систем.

Незважаючи на нормативне забезпечення, система фізичного захисту ОКІ стикається з рядом проблем:

− нерівномірність рівня захищеності об'єктів у різних галузях;

− застарілі технічні засоби охорони та низький рівень автоматизації процесів;

− недостатнє фінансування безпекових заходів, особливо у комунальній інфраструктурі;

− обмежена міжвідомча координація між СБУ, МВС, Міноборони, ДСНС;

− недосконалість системи підготовки персоналу з питань безпеки [10].

Зовнішнім викликом є гібридний характер загроз, який поєднує кібератаки, інформаційний вплив, диверсії та саботаж, що вимагає комплексного підходу до фізичного й кіберзахисту.

Враховуючи викладене, зазначимо, що підвищення ефективності фізичного захисту критичної інфраструктури можливе за рахунок: упровадження ризик-орієнтованого підходу до планування безпеки; розвитку державно-приватного партнерства у сфері безпеки (взаємодія держави з операторами критичної інфраструктури); інтеграції фізичного та кіберзахисту через створення єдиних центрів моніторингу подій безпеки; запровадження міжнародних стандартів (ISO 28000, IEC 62443, NIST SP 800-82); навчання та сертифікації персоналу, створення системи постійного професійного розвитку у сфері безпеки критичних об'єктів.

Також перспективним є застосування штучного інтелекту для прогнозування загроз, автоматичного виявлення порушень і управління кризовими ситуаціями.

Фізичний захист об'єктів критичної інфраструктури є фундаментом стійкості національної безпеки України, адже порушення їх функціонування може мати катастрофічні соціально-економічні наслідки. Забезпечення належного рівня безпеки вимагає комплексного підходу, що поєднує інженерно-технічні, правові, інформаційно-аналітичні та організаційні заходи.

В умовах триваючої агресії російської федерації необхідно посилити міжвідомчу координацію, підвищити технологічну оснащеність об'єктів, розвивати партнерство держави й бізнесу, а також формувати культуру безпеки на всіх рівнях управління.

Реалізація цих напрямів сприятиме підвищенню операційної стійкості критичної інфраструктури, мінімізації ризиків терористичних і диверсійних загроз та зміцненню обороноздатності держави.

Список використаних джерел:

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 23.10.2025).
2. European Commission. EU Programme for European Critical Infrastructure Protection (EPCIP). URL: https://home-affairs.ec.europa.eu (дата звернення: 23.10.2025).
3. Служба безпеки України. Аналітична доповідь «Захист критичної інфраструктури в умовах гібридних загроз», 2023. URL: https://ssu.gov.ua (дата звернення: 23.10.2025).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 23.10.2025).
5. Про затвердження Порядку визначення об'єктів критичної інфраструктури : Постанова КМУ № 1109 від 09.10.2020. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF (дата звернення: 23.10.2025).
6. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 23.10.2025).
7. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021(дата звернення: 23.10.2025).
8. Служба безпеки України. «Забезпечення безпеки критичної інфраструктури: основні підходи». URL: https://ssu.gov.ua (дата звернення: 23.10.2025).
9. NATO Cooperative Cyber Defence Centre of Excellence. «Critical Infrastructure Protection and Cyber Security». URL: https://ccdcoe.org (дата звернення: 23.10.2025).
10. UNIDIR. Critical Infrastructure Protection: Policy and Technology Trends, 2023. URL: https://unidir.org (дата звернення: 23.10.2025).

ХАРЧЕНКО С. О.,
старший викладач кафедри,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

БАС О. В.,
кандидат технічних наук,
доцент кафедри,
Навчально-науковий інститут
цивільного захисту
Національного університету
цивільного захисту України

ПРОБЛЕМИ ЗАХИСТУ ТА БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ТЕРИТОРІЇ УКРАЇНИ

Об'єкти критичної інфраструктури являються сукупністю об'єктів, систем і мереж, порушення функціонування яких може спричинити значну шкоду для національної безпеки, економіки, здоров'я населення, порушення нормальних умов життя та діяльності людей та може паралізувати цілі регіони або державу [1].

У сучасних умовах війни, кіберзагроз і терористичних актів питання безпеки та захисту критичної інфраструктури набуває першочергового значення для кожної держави, зокрема – для України яка перебуває в стані війни.

До таких об'єктів критичної інфраструктури належать сектори, такі як:

– енергетика (електростанції, газо та нафтопроводи);
– транспорт (аеропорти, залізничні вузли, мости);
– водопостачання і водовідведення;
– телекомунікації і зв'язок;
– охорона здоров'я (лікарні, лабораторії);
– державне управління (державні інформаційні системи);
– фінансовий сектор (банки, біржі);
– оборонно-промисловий комплекс.

Після початку війни в Україні питання захисту критичної інфраструктури стало пріоритетом, і було запроваджено ряд заходів які направлені на питання покращення безпеки, а саме:

– створено Національну систему захисту критичної інфраструктури;
– прийнято закон «Про критичну інфраструктуру» (2021);
– визначено відповідальні органи – РНБО, СБУ, МВС, ДСНС, Міністерство енергетики та інші;
– посилено міжнародну співпрацю з НАТО, ЄС, США в питаннях кібербезпеки [2] та обміну інформацією;

– впроваджуються стандарти NIST, ISO 27001, розробляються національні регламенти.

Особливо важливими стали дії з:

– фізичної охорони об’єктів (укріплення, охоронні системи);

– резервування систем управління та енергоживлення;

– розгортання кіберцентрів моніторингу (SOC);

– навчання персоналу і проведення тренувань щодо дій в умовах надзвичайних ситуацій.

В зв’язку із атаками на об’єкти критичної інфраструктури було виокремлено вразливі сторони деяких напрямків та заходи підвищення рівня безпеки, які було відображено в таблиці 1.1:

Таблиця 1.1 Виявлених недоліків та заходів підвищення безпеки

Сторона (аспект безпеки)	Виявлені недоліки / вразливості	Заходи підвищення безпеки
1. Кібер-вразливості	- Застаріле ПЗ та ОС (особливо SCADA/ICS) - Недостатня сегментація мереж (доступ IT → промислові мережі) - Відсутність оновлень та патч-менеджменту - Слабка аутентифікація і контроль привілеїв - Незашифровані канали зв’язку - Вразливі сторонні компоненти та прошивки (supply chain)	- Регулярні патчі та віртуальні патчі - Сегментація мереж (air gap або firewall) - Багатофакторна автентифікація - Моніторинг аномалій - Менеджмент постачання та аудит компонентів
2. Фізичні вразливості	- Недостатній контроль доступу (КПП, охорона) - Вразливі точки енергопостачання, вентиляції, комунікацій - Незахищені критичні вузли (підстанції, насосні станції)	- Контроль доступу, відеоспостереження - Резервне живлення - Фізична стійкість до підривів/пожеж - Регулярні аудити - Фізичний захист (огорожі, бетонні стіни) - Засоби колективного та індивідуального захисту персоналу
3. Інсайдерські загрози і людський фактор	- Помилки операторів, відсутність навчання - Корупція або зловмисні дії співробітників - Недостатнє управління змінами	- Навчання з безпеки - Політика доступу «потрібно знати» - Моніторинг дій користувачів - Перевірка персоналу та аудит дій
4. Взаємо-залежності та ланцюги постачання	- Залежність від зовнішніх постачальників енергії, IT, комплектуючих - Ланцюговий ефект при відмові одного елемента	- Картографування залежностей - Резервні постачальники - Контракти з вимогами безпеки - Плани відновлення критичних процесів

5. Природні загрози та кліматичні ризики	- Повені, бурі, землетруси, пожежі, екстремальні температури - Зношені елементи інфраструктури	- Аналіз і моделювання ризиків за сценаріями - Інженерне укріплення об’єктів - Плани евакуації - Страхування - Моніторинг погодних ризиків
6. Організаційні / процесні вразливості	- Відсутність або застарілі плани реагування - Недостатня координація між відомствами - Нестача бюджетів і кваліфікованого персоналу	- Розробка і тестування планів реагування - Міжвідомча координація - Регулярні тренування (tabletop, full-scale)
7. Законодавчі та нормативні прогалини	- Недостатні вимоги або їх невиконання - Невпроваджені стандарти чи слабкий нагляд	- Відповідність міжнародним і національним стандартам (NIST, ISO) - Участь у галузевих ініціативах - Регулярний аудит відповідності

Захист об’єктів критичної інфраструктури – це питання не лише технічне, а й стратегічне, яке потребує системного підходу, державної політики та широкої міжвідомчої взаємодії. Для України, яка перебуває у стані війни, це питання виживання. Інвестиції в безпеку критичних об’єктів – це запорука стабільності, стійкості та розвитку держави в майбутньому.

Список використаних джерел:

1. Закон України «Про критичну інфраструктуру» (2021).
2. Закон України «Про основні засади забезпечення кібербезпеки України» (2017).

ЧЕРНОВОЛ Є. О.,
Національна академія Служби безпеки України

ІНЖЕНЕРНИЙ ЗАХИСТ ВІД ПОВІТРЯНИХ ЗАГРОЗ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

Повномасштабна збройна агресія російської федерації проти України докорінно змінила підходи до забезпечення безпеки держави та її критично важливих об’єктів. Особливого значення в умовах війни набуває захист об’єктів критичної інфраструктури, які систематично зазнають ракетних, авіаційних та безпілотних ударів. Енергетика, транспорт, зв’язок, водопостачання та паливно-енергетичний комплекс стали ключовими цілями противника.

Ураження таких об’єктів має не лише локальні наслідки, а й спричиняє масштабні каскадні ефекти, що впливають на економіку, обороноздатність і соціальну стабільність держави. У цьому контексті інженерний захист виступає одним із базових елементів комплексної системи національної безпеки.

Закон України «Про критичну інфраструктуру» визначає коло об’єктів, порушення функціонування яких створює загрозу національній безпеці [1]. У воєнний час зазначені положення набувають практичного значення, оскільки потребують адаптації до умов постійної повітряної загрози та обмежених ресурсів.

Сучасні доктринальні документи у сфері безпеки передбачають необхідність поєднання інженерних, організаційних та інформаційних заходів, спрямованих на зменшення вразливості критичних об’єктів та підвищення їх стійкості до ураження.

Повітряні загрози сучасного конфлікту характеризуються різноманітністю засобів ураження та високою інтенсивністю застосування. Противник активно використовує крилаті та балістичні ракети, ударні безпілотні авіаційні системи та комплекси, керовані та некеровані авіаційні боєприпаси, а також комбіновані схеми атак.

Особливу небезпеку становлять масовані комбіновані удари, які спрямовані на перевантаження систем протиповітряної оборони та ураження об’єктів із різних напрямків. Це значно ускладнює завдання захисту та вимагає застосування багаторівневих інженерних рішень.

Аналіз практики бойових дій дозволяє виокремити типові вразливості об’єктів критичної інфраструктури. До них належать відкритість технологічного обладнання, відсутність захисних укриттів, недостатній рівень резервування систем життєзабезпечення, а також залежність від єдиних вузлів управління.

Ураження таких елементів призводить до тривалих відключень електроенергії, порушення водопостачання, втрати зв’язку та блокування транспортних шляхів, що має безпосередній вплив на цивільне населення і оборонний потенціал держави.

Ефективна система інженерного захисту повинна будуватися на принципах багаторівневості, пріоритетності, модульності та стійкості. Багаторівневий підхід передбачає поєднання заходів раннього виявлення загроз, пасивного та активного захисту, а також швидкого відновлення функціонування об’єктів.

Пріоритетність дозволяє зосереджувати ресурси на найбільш критичних елементах інфраструктури, а модульність забезпечує можливість швидкої адаптації захисних конструкцій до змін характеру загроз.

Інженерні засоби захисту умовно поділяються на пасивні, активні та інтелектуальні. Пасивний захист включає укриття, захисні бар’єри, габіонні конструкції та броньовані елементи. Активні засоби передбачають використання систем радіоелектронної боротьби та інших

технічних рішень, спрямованих на протидію повітряним загрозам. Інтелектуальні системи базуються на використанні сенсорних мереж, автоматизованих систем оповіщення та аналітичних платформ для прогнозування атак і підтримки прийняття рішень.

Досвід впровадження інженерних рішень на об’єктах енергетики та зв’язку свідчить про суттєве зниження рівня ризику ураження. Використання укриттів, розосередження обладнання та резервування систем живлення дозволяє зменшити наслідки атак і скоротити час відновлення.

Застосування комплексного підходу до захисту підтверджує доцільність поєднання інженерних заходів із засобами протиповітряної оборони та інформаційно-аналітичними системами.

Інженерний захист об’єктів критичної інфраструктури є невід’ємною складовою системи національної безпеки України в умовах війни. Найвищу ефективність демонструє багаторівневий комбінований підхід, що дозволяє знизити ризики ураження та забезпечити стійкість функціонування критичних об’єктів.

Перспективним напрямом подальших досліджень є розробка єдиного національного стандарту інженерного захисту та впровадження інтелектуальних систем підтримки прийняття рішень.

Список використаних джерел:

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 29.10.2025).

4 ДОСВІД БОЙОВОГО ЗАСТОСУВАННЯ СИЛ ОБОРОНИ ПРИ ВІДСІЧІ ЗБРОЙНОЇ АГРЕСІЇ РФ

БАШТОВА О. Г.,
доктор філософії,
старший викладач кафедри
вогневої підготовки,
Навчально-науковий інститут
поліцейської діяльності
Національної академії внутрішніх справ

БЕЗПАЛИЙ С. М.,
кандидат наук, доцент,
професор кафедри
вогневої підготовки,
Навчально-науковий інститут
поліцейської діяльності
Національної академії внутрішніх справ

ДОСВІД БОЙОВОГО ЗАСТОСУВАННЯ СИЛ ОБОРОНИ ПРИ ВІДСІЧІ ЗБРОЙНОЇ АГРЕСІЇ РФ

Сили оборони України в умовах відбиття збройної агресії РФ виконують низку ключових завдань, а саме: стримування агресії, її відсіч, охорону повітряного та територіального морського простору, а також участь у заходах боротьби з тероризмом. Це безпосереднє протистояння російській агресії, яка розпочалася в 2014 році з окупації Криму та подальших бойових дій на сході України.

Основним елементом системи забезпечення воєнної безпеки безумовно є сектор безпеки і оборони України. Сектор безпеки і оборони – система органів державної влади, Збройних сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України, діяльність яких перебуває під демократичним цивільним контролем і, відповідно до Конституції та законів України, за функціональним призначенням спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки України [1].

Стримування в контексті всеохоплюючої оборони України передбачає готовність сил оборони України, національної економіки, населення та всієї держави до надання відсічі збройній агресії проти України, нарощування спроможностей системи протиповітряної оборони, створення цілісної системи територіальної оборони, вжиття

превентивних заходів щодо протидії воєнним загрозам, досягнення та підтримання спроможностей завдати противнику неприйнятних політичних, економічних, воєнних та інших втрат, з огляду на які він буде змушений відмовитися від ескалації або припинити збройну агресію проти України.

Стійкість у ході всеохоплюючої оборони України досягається здатністю системи управління державою, сил оборони, національної економіки, інфраструктури та суспільства швидко відновлюватися та адаптуватися до змін у безпековому середовищі й до тривалого протистояння в наданні відсічі і стримування збройної агресії проти України, підтриманням спроможностей до здійснення стратегічного розгортання, територіальної оборони України, руху опору, ведення операцій (бойових, спеціальних, стабілізаційних дій), налагодженням надійних каналів комунікації з населенням та підтриманням його життєдіяльності [2].

Основними завдання Сил оборони є стримування та відсіч агресії, тобто забезпечення обороноздатності країни та протидія зовнішній агресії; охорона повітряного простору України; охорона територіального моря, забезпечує захист морського простору України у межах, визначених законом; участь у боротьбі з тероризмом, залучення до заходів, спрямованих на протидію терористичній діяльності.

Повномасштабне вторгнення росії в Україну у лютому 2022 року стало каталізатором швидкої еволюції сучасних бойових підходів і тактик. Цей конфлікт поєднав ознаки маневреної війни, позиційних конфліктів та інтенсивного використання вогневих і інформаційних засобів, а також продемонстрував значення гнучкості на тактичному та оперативному рівнях. Для держав з обмеженими ресурсами вивчення та імплементація набутих уроків є критичною задачею.

Артилерія залишилась визначальним фактором на стратегічному й тактичному рівнях: той бік, який мав стійкий постачальний ланцюг боєприпасів і здатність масовано застосовувати вогонь, отримував перевагу. Брак боєприпасів і скорочення темпів вогневого навантаження критично впливали на здатність наступати або утримувати позиції.

Широке використання БпЛА для розвідки, коригування вогню та ударів по цілям стало однією з визначальних ознак конфлікту. Масове впровадження комерційних і промислових дронів призвело до необхідності нових заходів ПРО/РЕБ та тактик інтегрованої оборони.

Ефективніші операції демонстрували підрозділи, які інтегрували піхоту, артилерію, ССО, ППО/ПРО та розвідку в єдину систему дії з гнучким командуванням і швидким обміном даних. Там, де координація була слабшою – оборонні успіхи були локально обмежені.

Конфлікт підтвердив, що стійка логістика (паливо, боєприпаси, запчастини, ремонтні потужності) – визначальна умова тривалої операційної стійкості. Розриви в постачанні швидко трансформувалися у вогневі та маневрені обмеження.

Швидка мобілізація людських ресурсів і організація територіальної оборони продемонстрували високу роль місцевих резервів у затриманні противника та захисті інфраструктури. Це також підкреслило потребу у стандартизованій підготовці й інтеграції ТрО до загальної системи оборони.

Успіх операцій залежав від здатності комунікаційних мереж працювати в умовах інтенсивного РЕБ і кіберзагроз. Децентралізоване прийняття рішень, резервні канали зв'язку та стійкі системи обміну ситуаційною інформацією підвищували оперативну гнучкість.

Можемо виокремити декілька основних чинників Сил оборони:

Адаптивність доктрини. Конфлікт показав, що доктринальні рамки повинні бути гнучкими та орієнтованими на швидку імплементацію тактичних інновацій, зокрема щодо використання БпЛА, інтегрованих датчиків та розподіленого управління.

Пріоритет забезпечення боєприпасами. Об'єктивна потреба у політиці запасів, локальному виробництві та диверсифікованих ланцюгах постачання – ключова для збереження вогневої переваги в середньостроковій перспективі.

Технологічні контрзаходи. Зростання ролі дронів диктує розвиток засобів ППО малого радіусу дії, РЕБ та алгоритмів оперативної інтеграції даних. Але технологічні рішення повинні поєднуватись із тактичними процедурами.

Чисельні та людські чинники. Навіть за високотехнологічного оснащення ключову роль відіграє підготовка особового складу, лідерство на тактичному рівні та психологічна стійкість.

Рекомендації для посилення ефективності збройній відсічі рф:

1. Підсилення логістики: створення регіональних складів боєприпасів, ремонтних майстерень та резервних маршрутів постачання.
2. Інтеграція БпЛА в розвідувально-ударні схеми: розвиток тактичних процедур інтеграції дронів з артилерією та коригуванням вогню (без вказівки специфічних тактик).
3. Розвиток стійких каналів зв'язку: багаторівнева система комунікацій з резервами на випадок РЕБ-ударів і кіберзагроз.
4. Підготовка та навчання: стандартизація підготовки для ТрО, нарощування практики комбінованих дій та міжвузлової координації.
5. Доктринальна гнучкість: регулярні процедури зворотного зв'язку між підрозділами фронту й структурами прийняття рішень для швидкої адаптації до тактичних нововведень.

Досвід Сил оборони в умовах відбиття збройної агресії РФ показав, що сучасний бій визначається не лише технічними засобами, але й здатністю гнучко організувати вогневі, розвідувальні й логістичні потужності в єдину систему дій. Забезпечення вогневої переваги, стійка логістика, інтеграція БпЛА та надійні канали управління – ключові

складові обороноздатності на сучасному етапі. Імплементація цих висновків у доктрину, структуру підготовки та систему забезпечення – пріоритет для підвищення ефективності оборонних сил.

Список використаних джерел:

1. Про національну безпеку України : Закон України від 21.06.2018 року № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text.
2. Стратегія воєнної безпеки України : затверджена Указом Президента України від 25.03.2021 р. № 121/2021. URL : https://www.president.gov.ua/documents/1212021-37661 (дата звернення: 27.07.2024).

МЕЛЬНИК В. В.,
доктор філософії,
старший викладач кафедри
тактико-спеціальних дисциплін,
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

ДОСВІД БОЙОВОГО ЗАСТОСУВАННЯ ПІДРОЗДІЛІВ АРМІЙСЬКОЇ АВІАЦІЇ ПРИ ВІДСІЧІ ЗБРОЙНОЇ АГРЕСІЇ РФ (2022–2025 рр.)

Повномасштабна збройна агресія російської федерації проти України, що розпочалася 24 лютого 2022 року, стала наймасштабнішим воєнним конфліктом у Європі після Другої світової війни [1, с. 3]. У ході бойових дій армійська авіація Сухопутних військ Збройних Сил України (далі – АА ЗСУ) набула безпрецедентного досвіду виконання бойових завдань в умовах інтенсивного протиповітряного протиборства, нестачі матеріальних ресурсів та необхідності інтеграції з безпілотними системами [3].

Аналіз бойового застосування підрозділів АА ЗСУ в ході протистояння російській агресії дає можливість визначити основні його етапи, та надати їм коротку характеристику:

На першому етапі (лютий–червень 2022 р.) основна увага приділялася виконанню завдань у тилу противника – доставці вантажів, евакуації та підтримці підрозділів, що діяли в оточенні (зокрема в районах Києва, Чернігова, Маріуполя). В умовах переваги противника в повітрі українські екіпажі здійснювали польоти на гранично малих висотах, переважно в нічний час, використовуючи рельєф місцевості для укриття [3].

На другому етапі (літо 2022 – кінець 2023 рр.) армійська авіація активно залучалася до вогневої підтримки наступальних дій Сил оборони на Харківському, Херсонському та Бахмутському напрямках. Застосування гелікоптерів Мі-8 та Мі-24 у форматі «удар–відхід» дозволяло наносити точкові удари НАР та протитанковими ракетами. Водночас

удосконалювалася система планування бойових вильотів, що базувалася на розвідданих БпЛА та супутникових знімках [6].

Третій етап (2024–2025 рр.) характеризується поступовою інтеграцією армійської авіації у систему об'єднаних повітряно-наземних операцій. З'явилися елементи скоординованого управління із залученням безпілотників-розвідників, засобів РЕБ і точного озброєння. Успішним прикладом стала взаємодія гелікоптерних підрозділів з ударними БпЛА під час оборони Куп'янського та Сіверського напрямків у 2024 р., що дало змогу знищити кілька колон противника без втрат власних літальних апаратів [4; 7].

Попри високу ефективність в ході відбиття збройної агресії рф на початковому етапі, АА ЗСУ зазнала і відчутних втрат у техніці та особовому складі через недостатню кількість засобів ППО, відсутність сучасних систем нічного бачення, засобів РЕБ і радіоелектронного маскування, все це було обумовлено тим, що значна частина гелікоптерного парку була виготовлена ще в радянський період, що обмежувало їх бойові можливості [2, с. 25].

Тому починаючи з 2023 року Україна отримала значну допомогу від країн-партнерів НАТО – зокрема, постачання гелікоптерів Мі-17, Black Hawk та Sea King [4]. Вони використовуються для виконання завдань евакуації, транспортування вантажів і спеціальних операцій. Окрім технічної підтримки, партнери надали можливість підготовки екіпажів у тренувальних центрах Польщі, США та Великої Британії, де застосовуються стандарти НАТО у плануванні повітряно-наземних операцій [5].

Крім того, до 2030 року заплановано реалізацію комплексної програми «Армійська авіація – 2030», що передбачає:

1. оновлення парку літальних апаратів за рахунок закупівлі H145M, AH-1Z Viper та UH-60 Black Hawk;
2. створення єдиної системи управління повітряно-наземними операціями на основі стандартів ATP-49 (NATO) [5];
3. удосконалення системи технічного обслуговування та логістичного забезпечення;
4. впровадження цифрових систем навігації, зв'язку та РЕБ, які забезпечують сумісність з авіацією союзників;
5. розвиток навчально-тренувальної бази для підготовки льотного складу з використанням VR/AR-технологій та симуляторів бойових дій.

Також перспективним і залишається напрям розвитку армійської авіації України, який полягає у переході до концепції "Manned–Unmanned Teaming (MUM-T)", що передбачає взаємодію пілотованих гелікоптерів з безпілотними платформами. Такі системи вже довели свою ефективність у країнах-членах НАТО [7].

Таким чином досвід бойового застосування армійської авіації у 2022–2025 рр. довів її стратегічну роль у забезпеченні мобільності, вогневої підтримки та управління військами в умовах високо-

технологічної війни [1; 4]. Водночас отриманий досвід засвідчує необхідність подальшого розвитку даного роду сухопутних військ, який має ґрунтуватися на поєднанні вітчизняного інноваційного потенціалу та міжнародної інтеграції у систему колективної безпеки НАТО.

Завдяки міжнародній підтримці, технологічним інноваціям і високому професіоналізму екіпажів гелікоптерів, армійська авіація Збройних Сил України поступово перетворюється на сучасний, мобільний і високоефективний компонент оборонної системи держави.

Список використаних джерел:

1. Міністерство оборони України. Біла книга 2023: Збройні Сили України. Київ : МОУ, 2024. 150 с.
2. Горбулін В. П., Ланде Д. В. Війна майбутнього: концепти, технології, перспективи. Київ : НІСД, 2023. 312 с.
3. АрміяInform. Досвід застосування армійської авіації у ході бойових дій 2022–2024 років. URL: https://armyinform.com.ua.
4. The Military Balance 2025. London: International Institute for Strategic Studies, 2025. 560 p.
5. NATO Standardization Office. ATP-49. Air Operations in Support of Land Forces. Brussels : NSO, 2022. 210 p.
6. Командування Сухопутних військ ЗСУ. Аналіз бойового застосування авіаційних підрозділів у ході оборонних операцій 2022–2024 рр. Київ : НУОУ, 2025. 48 с.
7. Jane’s Defence Weekly. Army Aviation in Ukraine: Lessons from the Battlefield. London, 2024.

ТОНКОНОГ І. О.,
Національна академія Служби безпеки України

СУПРОВІД ПОШУКУ І ЗНЕШКОДЖЕННЯ ДРГ ПРОТИВНИКА

Четвертий рік поспіль точаться бої з російською ордою по всій лінії бойового зіткнення. Не зважаючи на масований натиск ворога вже зараз здійснюється звільнення певних ділянок тимчасово окупованих територій країни на яких проводяться силові та режимно-обмежувальні заходи силами підрозділів суб’єктів безпеки та оборони України. Здійснюється постійна боротьба як проти регулярних військ країни-агресора, так і проти його диверсійно-розвідувальних груп (далі –ДРГ).

Способи проведення режимно-обмежувальних та силових заходів під час організації оперативно процесуальних дій, частиною, чи метою яких є проведення пошуку і знешкодження ДРГ противника або незаконних збройних формувань (далі – НЗФ) залежить від умов оперативної і тактичної обстановки, наявності сил і засобів ЗСУ, НГУ, НП, СБУ, добровольчих формувань територіальних громад тощо, а також характеру місцевості та пори року [1].

На нашу думку, і це доводить практика, режимно-обмежувальні та силові заходи можуть проводитися такими способами: блокуванням;

пошуком; оточенням; переслідуванням; розосередженням. Розглянемо деякі з них.

Блокування – це заходи суб'єктів сектору безпеки та оборони України, направлені на ізоляцію визначеного району (об'єкта), з метою недопущення виходу злочинців за його межі. Воно може бути суцільним або за напрямком руху злочинців.

Мета блокування – ізоляція певного району, забезпечення вдалого ведення пошуку або затримання противника. При цьому також необхідно дотримуватися правил, що запобігають втратам особового складу. Блокування ДРГ противника (озброєних злочинців) необхідно проводити у безпечному місці, за межами населеного пункту (станції, порту). Щільність блокування залежить від умов місцевості та оперативного значення ділянок, що оточуються. При розрахунку сил для оточення місцевості керуються такими критеріями: наряд із 2–3 співробітників може перекрити рубіж на відстані 75 м на закритій та до 150 м – на відкритій місцевості за допомогою кінологів. Блокування розташовується від об'єкта (місця блокування) на відстані яка відповідає тактичному розрахунку. Проводиться як відомчим підрозділом (в даному випадку СБ України), так і підрозділами інших суб'єктів сектору безпеки та оборони України, які залучаються до забезпечення заходу (спецоперації) після попереднього інструктування.

Пошук – це дії суб'єктів сектору безпеки та оборони (суб'єктів боротьби з тероризмом) України, що направлені на виявлення, затримання або знешкодження ДРГ противника або незаконних збройних формувань, а також вилучення речей і предметів (матеріального та нематеріального характеру (інформація)), що належать їм та можуть служити в якості речових доказів. Пошук може проводитися в блокованому або в неблокованому районі (населеному пункті), з одного або декількох напрямків, з використанням БПЛА та/або авіації.

Переслідування – це спосіб силових дій, який застосовується рухомими спеціальними військовими нарядами оперативних або оперативно-бойових груп (ОГ, ОБГ) СБ України з метою затримання або знешкодження злочинців, котрі намагаються вийти (зникнути) з району проведення СО.

Оточення – це дії суб'єктів сектору безпеки та оборони України з ізоляції району проведення антитерористичної або контрдиверсійної операції (заходів), масових заворушень у населеному пункті, місць великих катастроф, пожеж, стихійного лиха, з метою недопущення входу (виходу) в район проведення спецоперації сторонніх осіб [2].

Пропонуємо розглянути один з варіантів комплексу дій оперативного та оперативно-бойового підрозділу (груп) з пошуку та знешкодження ДРГ (НЗФ).

1. Отримання від джерела (декількох джерел) інформації про появу ДРГ в районі відповідальності.

2. Перевірка та уточнення інформації по декільком каналам. Вивчення інформації, її аналіз і висновки по ній.

3. Встановлення радіоконтролю в районі відповідальності підрозділу СБУ, з метою виявлення і фіксації раптових короткочасних радіопередач (миттєвих радіоімпульсів) в районі можливих дій ДРГ. Контроль оперативно-технічного підрозділу за телефонними і СМС повідомленнями тощо.

4. Приховане підвищення боєготовності підрозділів охорони і безпеки на особливо важливих об'єктах і комунікаціях, розташованих в районі.

5. Націлення наявної агентури на добування інформації щодо дій противника (ДРГ, НЗФ), виявлення осіб, які розносять чутки та плітки про перебіг бойових дій, стан справ в країні тощо.

6. Перевірка і підтвердження інформації з різних джерел щодо наявності та дій ДРГ (НЗФ) в районі.

7. Організація взаємодії з органами, частинами і підрозділами ЗСУ, НП і НГУ, з метою уточнення, узагальнення, аналізу, та обміну інформації щодо дій ДРГ противника (НЗФ) в районі відповідальності.

8. Активізація роботи радіо і радіоелектронної розвідки наших сил в районі, з метою перехоплення повідомлень до та від ДРГ противника.

9. Визначення районів (місць) виходу в ефір радіостанцій противника.

10. Встановлення (уточнення) членів ДРГ (НЗФ).

11. Виявлення та встановлення посібників противника.

12. Посилення охорони та оборони особливо важливих обєктів та інфраструктури.

13. Ведення спостереження за встановленими адресами переміщених осіб з тимчасово окупованих районів та районів ведення бойових дій.

14. Ведення спостереження за встановленими адресами посібників противника. Активне проведення оперативно-технічних заходів.

15. Попередня розробка плану взаємодії органів і підрозділів суб'єктів безпеки та оборони України з одночасного захоплення противника.

16. Узгодження та затвердження плану проведення спеціальних контрдиверсійних заходів (далі – СКДЗ) складається з:

− розрахунку задіяних сил і засобів (ЗСУ, ССО, МВС, СБУ тощо);

− визначення рубежів блокування району проведення СКДЗ, час їх зайняття, якими силами і від кого вони призначені;

− вивчення і затвердження маршрутів і часу висування підрозділів на рубежі, встановлення сигналів управління;

− розрахунку часу (підйом по тривозі задіяних сил і засобів, висування на визначені рубежі та розгортання підрозділів);

− встановлення сигналів і знаків взаємного розпізнавання своїх сил та засобів (форма одягу, паролі, робочі радіочастоти, переговорні таблиці, кодування карт і схем району проведення операції (по квадратах));

− визначення початкових та кінцевих рубежів прочісування, перевірки і вирівнювання підрозділів та часу їх роботи;

− уточнення дій залучених підрозділів у випадку збройного опору противника.

Визначають місця для збору «200» і «300», надання первинної медичної допомоги, порядок відправлення постраждалих в медичні установи; розташування фільтраційних пунктів; маршрути доставки полонених до місць їх подальшого утримання та склад конвойних команд.

17. Здійснення попередньої рекогносцировки (дорозвідки) місцевості, а також відпрацювання дій підрозділів на мапах (схемах, фотоматеріалах отриманих з БПЛА) [3].

18. Оповіщення і задіяння представників місцевих органів самоврядування та МВС здійснюється в останню чергу, з метою зменшення можливості витоку інформації.

19. Перевірка документів на стаціонарних і тимчасових (пересувних) блокпостах, поза межами району проведення СКДЗ здійснюється представниками НП та НГ України із залученням оперативних співробітників СБУ.

Для проведення пошуку в блокованому або в неблокованому районі можуть залучатися як окремі оперативно-бойові підрозділи ЦСО «А» або ДКР СБУ, так і спільні (змішані) групи у складі співробітників СБУ та військовослужбовців ЗСУ (ССО). Пошук в районі може бути одностороннім, двох і трьох сторонніх.

В цьому випадку завчасно відпрацьовуються питання легендованого виходу задіяних сил в район; знаки і сигнали взаємного розпізнавання; порядок виходу на зв’язок і радіочастоти; виклик підкріплення; виклик і наведення ударів армійської авіації та артилерії по визначеним рубежам й виявленим цілям тощо. Слід зазначити, що це тільки частина завдань, які потрібно буде вирішувати підрозділам СБ України під час організації та проведення контрдиверсійних заходів [4, 5].

Таким чином одним з основних завдань і проблем в організації контрдиверсійних заходів було і є підготовка особового складу підрозділів Національної Гвардії та Національної поліції України до виконання завдань на пересіченій місцевості та в населених пунктах (особливо в зруйнованих). Ці підрозділи потрібно завчасно готувати до дій з блокування та пошуку слідів наявності ДРГ або НЗФ та їх ліквідації. На це піде не один навчальний день. Особовий склад повинен бути навчений орієнтуванню на місцевості, ведення спостереження, знати ознаки встановлення мінно-вибухових приладів (загороджень), ведення вогневого бою на коротких і середніх дистанціях, вміти

застосовувати БПЛА та коректувати вогонь артилерії, надавати долікарську медичну допомогу постраждалим та багато ще чого.

Список використаних джерел:

1. Про основи національного спротиву : Закон України від 16 вересня 2021 р. Відомості Верховної Ради України. 2021. № 11. С. 339. [із змінами і доповненнями].
2. «Інструкція з організації та проведення антитерористичних та контрдиверсійних заходів (кодова назва «Промінь-Україна»)» затверджена спільним наказом СБУ, МВС, ЗСУ № 33/1-5190ві від 05.11.2022.
3. Бойовий Статут механізованих і танкових військ СВ ЗСУ. Частина ІІ (батальйон, рота). Київ : Вид-во «Центр учбової літератури», 2022.Тактика легкої піхоти для малих підрозділів. К. Е. Ларсен. Електронна версія 1.0. URL: nashformat.ua/products/ taktika-legkoi-pehoti-dlya-malih-pidrozdiliv (дата звернення: 13.10.2025).
4. Тактика легкої піхоти для малих підрозділів. К. Е. Ларсен. Електронна версія 1.0. URL: nashformat.ua/products/taktika-legkoi-pehoti-dlya-malih-pidrozdiliv (дата звернення: 13.10.2025).
5. Мала війна. Організація і тактика бойових дій малих підрозділів : хрестоматія / Склав. А. Тарас. Київ : Вид-во Варта, 2005. 510 с.

ШЕВЧЕНКО С. В.,
Національна академія Служби безпеки України

ГАЛАГАН В. В.,
доктор філософії,
Національна академія Служби безпеки України

ПРОТИДІЯ СБУ ДИВЕРСІЙНО-РОЗВІДУВАЛЬНИМ ГРУПАМ РФ У ПРИФРОНТОВИХ РАЙОНАХ: ВИКЛИКИ, ПРОБЛЕМИ, ПЕРСПЕКТИВИ

Сучасна гібридна війна РФ проти України супроводжується активним залученням диверсійно-розвідувальних груп (ДРГ), які несуть багатоаспектні загрози державній безпеці. Діяльність ДРГ РФ спрямована на фізичне знищення об’єктів інфраструктури, підрив економіки, дез-організацію системи управління військами та проведення інформаційно-психологічних операцій, що створюють паніку в суспільстві. Особливо небезпечним є дія ДРГ у прифронтових зонах, де обмежені можливості контролю та швидкого реагування. Відповідно, завдання СБУ виявляти та нейтралізовувати такі групи, блокувати агентурні мережі і коригувати удари ворога. З початку повномасштабного вторгнення 2022 року СБУ неодноразово повідомляла про успішне викриття ДРГ на прифронтових територіях та в тилу. Водночас для системного аналізу діяльності ДРГ слід виділити основні напрями їх впливу: фізичний, інформаційний, соціальний

та економічний, а також особливості роботи сил спецоперацій СБУ, що координувались з підрозділами ЗСУ під час оборони ключових напрямків.

Правова база щодо ДРГ значною мірою фрагментована. Існуючий Закон України «Про боротьбу з тероризмом» делегує СБУ координацію антитерористичних заходів, але чітких положень саме щодо ДРГ у ньому немає. РНБО України ініціювано законопроєкт «Про протидію диверсійно-розвідувальним групам», проте станом на 2025 рік він не ухвалений, що створює правовий вакуум. Через це підрозділи СБУ та ЗСУ часто діють на підставі тимчасових директив, що не сприяє впровадженню системного підходу з протидії діяльності ДРГ, сповільнює реакцію цих підрозділів на диверсійно-розвідувальні загрози та обмежує їх оперативно-бойові можливості. Відсутність чіткого правового механізму застосування сили у мирний час і неврегульованість діяльності з протидії ДРГ ускладнюють застосування оперативно-бойової компоненти в прифронтових районах.

На практиці відсутність єдиного міжвідомчого органу ускладнює взаємодію суб'єктів сектору безпеки та оборони. Хоча Антитерористичний центр при СБУ формально координує діяльність всіх суб'єктів боротьби з тероризмом (антитерористичні (контрдиверсійні) заходи), наявні суттєві прогалини в обміні інформацією та плануванні операцій. Наприклад, у разі проникнення диверсантів оперативні дані військової розвідки можуть передаватися СБУ із затримкою, що зменшує шанси на їх швидке блокування. Відсутність єдиного центру управління операціями на рівні РНБО України часто призводить до дублювання дій різними підрозділами чи конфліктів між ними. Так, у 2022 році в Маріуполі підрозділ НГУ вступив у бій із підрозділом СБУ через різні плани операції. Також завдання з протидії ДРГ закріплені за різними відомствами: СБУ зосереджується на контррозвідці і виявленні агентурних мереж, тоді як фізична ліквідація ДРГ залишається в компетенції ЗСУ/НГУ, що вимагає чіткішого розмежування повноважень і швидкого обміну оперативною інформацією. Неврегульований розподіл функцій без спільного управління загрожує втратами часу в кризових ситуаціях.

Різні суб'єкти сектору безпеки і оборони України мають різні банки даних (інформаційно-аналітичні системи) і канали зв'язку, які не інтегровані в єдину систему. Це ускладнює ідентифікацію членів ДРГ, які, як свідчить практика, діють під прикриттям мирного населення. До прикладу, у 2023 році СБУ не своєчасно отримала від місцевого населення інформацію про підготовку диверсій під Донецьком, оскільки не було налагоджено оперативного каналу зв'язку з Силами оборони України. Затримка в обміні даними створює ризики зриву контрзаходів і додаткове навантаження на розвідувальні органи та підрозділи. Загалом слабка інтеграція інформаційних ресурсів СБУ і ЗСУ унеможливлює швидкий доступ до даних про ворога.

Підрозділи ЦСО «А» СБУ на початковому етапі війни мали обмежені засоби зв'язку і технічного спостереження. Як свідчить практика участі підрозділів ЦСО «А» у відбитті збройної агресії в

лютому-квітні 2022 року, під час оборони Києва ними використовувалися лише радіостанції і рідко супутниковий зв'язок. Відсутність сучасних БПЛА, засобів радіоелектронної боротьби та єдиного каналу зв'язку відразу після широкомасштабного вторгнення суттєво знижувала оперативно-бойові можливості підрозділів ЦСО «А». Згодом СБУ спільно з партнерами значно розширили технічне забезпечення національної спецслужб: на сьогодні активно застосовуються БПЛА для розвідки та коригування дій у протидії ворожим ДРГ. Втім, забезпечення новітніми засобами все ще залишається викликом, зокрема, посилення потребує централізований облік і оперативна подача техніки в прифронтові райони та безпосередньо на лінію бойового зіткнення. Також ускладнює роботу дефіцит кваліфікованих кадрів та висока завантаженість діючих співробітників національної спецслужби в умовах воєнного стану.

Ворожі ДРГ активно використовують замасковані схеми дій – залучають до конфіденційного співробітництва осіб з числа місцевого населення, а останнім часом під час переміщення маскують діяльність під цивільних.

Для підвищення ефективності протидії ДРГ необхідно впроваджувати комплексний підхід: він має поєднувати вдосконалення правової основи, яка регулює діяльність всіх суб'єктів сектору безпеки та оборони України; посилення координації їх діяльності та покращення технологічного оснащення.

По-перше, вважаємо за необхідне прийняти Закон України «Про протидію диверсійно-розвідувальним групам», який має визначити поняття ДРГ, їх статус, права та обов'язки суб'єктів їх виявлення та нейтралізації, механізми реалізації оперативно-бойових заходів, а також порядок взаємодії і координації.

По-друге, доцільно створити єдиний міжвідомчий Ситуаційний центр наприклад, ОЦКБ під керівництвом РНБО України, який забезпечуватиме координацію дій, оперативний обмін інформацією та спільне управління операціями СБУ, ЗСУ, Нацгвардії і Державної прикордонної служби України в реальному часі. Такий штаб повинен мати повноваження швидко приймати рішення і прямий зв'язок між підрозділами різних відомств. Інтеграція баз даних та введення єдиної комунікаційної мережі сприятиме швидшому виявленню ДРГ і уникненню «двійного контакту» силових структур на полі бою.

По-третє, потрібно суттєво оновити матеріально-технічну базу контрдиверсійних підрозділів. Особливу увагу слід приділити оснащенню суб'єктів контрдиверсійної діяльності сучасними БПЛА та системами радіоелектронної боротьби, що дозволить краще виявляти та придушувати дистанційне керування ДРГ і зброю противника. Надалі варто нарощувати оперативну та аналітичну компоненту спрямовану на виявлення диверсійно-розвідувальної діяльності на ранніх стадіях і запобігання підготовці терористичних актів та диверсій.

Таким чином, ефективна протидія ДРГ потребує комплексного підходу поєднання законодавчих змін, удосконалення міжвідомчої взаємодії та потужного технічного забезпечення всіх суб'єктів контр-диверсійної діяльності. Реалізація цих заходів дозволить посилити обороноздатність країни та забезпечити швидке реагування на загрози ДРГ у прифронтових районах.

Одним із важливих елементів ефективної протидії ДРГ є системна робота з місцевим населенням у прифронтових районах. СБУ організовує інформаційно-роз'яснювальні заходи серед місцевих жителів, формує канали конфіденційного зв'язку та взаємодії. Це дозволяє своєчасно отримувати оперативну інформацію про підозрілих осіб, негласну активність, порушення режиму або об'єкти, які можуть бути використані ворогом [2, с. 45].

Паралельно з цим активно застосовуються контрольно-перевірочні контррозвідувальні заходи на деокупованих територіях. СБУ, спільно з військовими адміністраціями, перевіряє осіб на можливу причетність до співпраці з ворогом. Досвід деокупації частини Харківської області показав, що такі перевірки дозволяють виявити до 40 % осіб уже в перші тижні після деокупації [4, с. 56]. Мобільні контрдиверсійні групи СБУ, до складу яких входять співробітники підрозділів контррозвідки, вибухотехніки та кінологи, здійснюють патрулювання у тактичній зоні та проводять верифікацію осіб, що потрапили в поле зору контррозвідки. Вони здійснюють свою діяльність переважно в умовах оперативного ризику, часто в нічний час або в районах із відсутністю комунікаційного покриття [7, с. 38].

Особливої уваги заслуговує врахування досвіду оперативно-бойового застосування підрозділів ЦСО «А», зокрема, успішних бойових операцій з ліквідації ДРГ, штурму будівель із озброєними диверсантами та забезпечення безпеки в умовах загрози терористичних актів та диверсій. До таких операцій варто віднести контрдиверсійні дії ЦСО «А» під час звільнення Бучі, Ізюма та Красногорівки [9, с. 211].

У межах міжнародного співробітництва СБУ бере участь у спільних навчаннях із країнами НАТО, особливо у сфері виявлення та нейтралізації ДРГ в урбанізованому середовищі. Практики країн Балтії, Польщі та Ізраїлю щодо виявлення терористичних осередків були частково адаптовані вітчизняною спецслужбою та успішно інтегровані в оперативно-бойову практику [5, с. 164]. Значну роль відіграє також аналітична діяльність, зокрема, прогнозування напрямів застосування противником ДРГ на основі даних радіоелектронної розвідки, аналізу відкритих джерел і поведінкової аналітики. Це дозволяє моделювати зони потенційної загрози та вчасно пере-дислоковувати ресурси СОУ [6, с. 59].

З 2022 по 2025 роки структура та методи протидії ДРГ суттєво трансформувались. Якщо на початку війни акцент робився на реагуванні, то згодом він змістився на реалізацію комплексу упереджувальних заходів. Зокрема, велику роль почали відігравати заходи спрямовані на своєчасне виявлення диверсантів в разі можливої їх перевірки під час

контрольно-перевірочних контррозвідувальних заходів, зокрема, під час перевірки їх мобільних терміналів, соціальних мереж, контрозвідувальних опитувань. Активно впроваджується в практику розробка психологічних портретів диверсантів тощо [8, с. 41].

Нарешті, важливим напрямом є гарантування безпеки у звільнених районах. СБУ, разом з іншими структурами, розробляє стратегії стабілізації: контрольно-перевірочні контррозвідувальні заходи, виявлення прихованих схронів (тайників), профілактика колабораційної діяльності та психологічна реабілітація населення. Цей напрям має бути пріоритетом після перемоги [1, с. 128].

Висновок. Отже, у контексті сучасної повномасштабної війни проти України ДРГ рф залишаються однією з найнебезпечніших загроз у прифронтових районах. Їхня діяльність спрямована на дестабілізацію тилу, зрив мобілізаційних та логістичних процесів, деморалізацію населення і дискредитацію органів державної влади. Служба безпеки України, діючи в умовах постійної зміни тактики діяльності ворожих спецслужб, демонструє здатність до адаптації, посилення оперативно-бойових можливостей та удосконалення міжвідомчої взаємодії.

Незважаючи на низку об’єктивних проблем таких як нормативна фрагментарність, нестача та низька підготовка кадрів, обмеженість технічного ресурсу, СБУ сформувала ефективну систему контрдиверсійних заходів. До ключових напрямів такої діяльності належать: виявлення агентурних мереж ворожих спецслужб, проведення контрольно-перевірочних контррозвідувальних заходів, мобільне патрулювання тактичної смуги, інтеграція з іншими суб’єктами сектору безпеки і оборони, аналітична розвідка та інформаційна робота з населенням. Практика довела, що поєднання превентивних, технічних і оперативно-бойових заходів дає змогу локалізувати загрозу ще до реалізації диверсійних планів.

Перспективним є подальше зміцнення законодавчої бази, формування єдиного ситуаційного центру при РНБО України, забезпечення СБУ сучасними контрдиверсійними засобами, а також імплементація сучасного міжнародного досвіду країн НАТО. Окрему увагу слід приділяти формуванню довіри з боку населення в прифронтових районах, яке має стати основою своєчасного виявлення спроб проникнення ДРГ.

Таким чином, боротьба з диверсійно-розвідувальними групами рф багатовекторне завдання, яке потребує стратегічного мислення, системності, високого рівня професійної підготовки, тісної взаємодії СБУ з іншими складовими сектору безпеки й оборони та глибокого розуміння природи сучасного воєнного конфлікту.

Список використаних джерел:

1. Андрушко, О. С. Стабілізаційні заходи на деокупованих територіях / О. С. Андрушко. *Вісник КНУВС.* 2025. № 1. С. 125–130.
2. Білоус, П. І. Диверсійна загроза у прифронтовій зоні: концептуальні засади реагування / П. І. Білоус. *Вісник Національної академії СБУ.* 2023. № 1. С. 41–50.
3. Гуменюк, І. П. Кримінальні провадження проти диверсантів: практика документування / І. П. Гуменюк. *Юридичний журнал.* 2024. №3. С. 74–81.
4. Ковальчук, В. І. Практика фільтраційних заходів на звільнених територіях / В. І. Ковальчук. *Збірник наукових праць НДІ проблем воєнної безпеки.* 2023. Т. 4, № 2. С. 55–61.
5. Литвин, А. Г. Міжнародний досвід боротьби з ДРГ / А. Г. Литвин. *Зовнішні справи.* 2023. № 5. С. 162–169.
6. Марченко, Ю. І. Аналітичні методи прогнозування загроз ДРГ / Ю. І. Марченко. *Збірник наукових праць ЦДССУ.* 2024. № 2. С. 57–65.
7. Мельник, С. В. Контрдиверсійні мобільні групи в умовах гібридної війни / С. В. Мельник. *Право і безпека.* 2024. № 2. С. 35–43.
8. Орел, В. В. Психологічний портрет диверсанта: ознаки та моделі / В. В. Орел. Психологія і суспільство. 2023. № 4. С. 39–45.
9. Сіроштан, Л. М. Спецпідрозділи СБУ в зоні бойових дій: оперативний аналіз / Л. М. Сіроштан. *Військова освіта.* 2024. № 1. С. 210–217.
10. Шевченко, І. В. Агентурні мережі РФ на Сході України: досвід виявлення / І. В. Шевченко. *Схід.* 2023. № 6 (194). С. 108–112.

5 ПИТАННЯ ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВОСЛУЖБОВЦІВ ПРИ ВИКОНАННІ ОПЕРАТИВНО-БОЙОВИХ ЗАВДАНЬ В РАЙОНІ ПРОВЕДЕННЯ БОЙОВИХ ДІЙ

НЕДУЖА І. Л.,
Національна академія Служби безпеки України

ОПАНАСЕНКО Т. А.,
Національна академія Служби безпеки України

ПСИХОЛОГІЧНА ГОТОВНІСТЬ ВІЙСЬКОВОСЛУЖБОВЦІВ ДО НАДАННЯ ПЕРШОЇ ДОМЕДИЧНОЇ ДОПОМОГИ В БОЙОВИХ УМОВАХ

У сучасних бойових умовах здатність військовослужбовця надати першу домедичну допомогу часто визначає шанс на виживання для пораненого побратима. Проте ефективність таких дій залежить не лише від рівня знань і навичок, а й, насамперед, від психологічної готовності діяти в умовах ризику, страху, болю та стресу. Перша домедична допомога – це невідкладні дії, які виконуються на місці події до прибуття медичних працівників з метою порятунку життя, запобігання ускладненням і підтримання життєвих функцій постраждалого.

В умовах війни вона є першою ланкою системи виживання (так званий ланцюг порятунку). Без якісного виконання першої ланки інші етапи часто втрачають сенс, бо поранений може загинути ще до прибуття медиків. На полі бою або під час обстрілів медики не завжди можуть одразу дістатися постраждалого. Саме побратими або сам постраждалий (самодопомога) стають тими, хто реально рятує життя в перші хвилини [1].

У травматології є поняття «золота година» – перша година після поранення, коли ймовірність виживання найвища. Домедична допомога забезпечує ефективне використання цієї години та зумовлює зниження бойових втрат.

Разом з тим, тривале перебування військовослужбовців у небуденній обстановці, та ще й із підвищеною загрозою для життя і здоров’я, зумовлює відповідне незвичне реагування психіки на дію психотравмуючих чинників. У психологічно підготовлених військовослужбовців це, як правило, загострене почуття обов’язку, повна мобілізація сил і можливостей, зібраність та постійна готовність до будь-яких неочікуваних ситуацій, швидка реакція на зміну обстановки, підвищення чіткості дій та успішності вирішення завдань тощо. Поведінка непідготовлених, у свою чергу, може супроводжуватись низкою негативних фізіологічних та емоційних проявів, розгубленістю. Результатом такої підготовки є психологічна готовність –

цілісний стан мобілізованості особистості, що забезпечує здатність швидко, свідомо й упевнено діяти в екстремальній ситуації, зберігаючи самоконтроль і ефективність поведінки [2].

Отже, формування у військовослужбовців психологічної готовності до надання домедичної допомоги в умовах стресу, небезпеки, крові, втрат і невизначеності є вкрай актуальним сьогодні. У межах зазначеного важливим є:

– розвиток стійкої мотивації до надання допомоги як до морального обов'язку;

– формування стресостійкості та високого рівня самоконтролю у критичних ситуаціях;

– відпрацювання до автоматизму дій у стані бойового стресу;

– забезпечення адекватних дій та рішучості при оцінці ризиків і прийнятті рішень;

– розвиток здатності до успішної взаємодопомогу в групі.

Загалом уміння діяти в екстремальній ситуації знижує страх і безпорадність, натомість підвищуючи впевненість у власних силах. Це підтримує моральний дух підрозділу і відчуття взаємної підтримки та здатності виявляти людяність навіть у нелюдських умовах. Кожен підготовлений військовослужбовець – це потенційно врятоване життя.

Навички домедичної допомоги без психологічної готовності – лише теорія. Тому особлива увага має приділятися розвиту такої готовності.

До змістових компонентів психологічної готовності до надання першої домедичної допомоги, насамперед відносять такі [3; 4]:

мотиваційний – усвідомлення значення допомоги, цінність життя, почуття обов'язку;

когнітивний – знання алгоритмів, розуміння пріоритетів у дії, оцінка ризиків;

емоційно-вольовий – контроль емоцій, подолання страху, стресостійкість;

операційний (поведінковий) – здатність діяти автоматично, швидко, без паніки.

Також виокремлюють психологічні чинники, що впливають на готовність, а саме:

– рівень тривожності та страху смерті;

– попередній бойовий досвід;

– психологічна стабільність та самоконтроль;

– командна підтримка й соціально-психологічний клімат підрозділу;

– регулярність тренувань у стресових умовах (стрес-інокуляція).

Технологія розвитку психологічної готовності військовослужбовців до надання домедичної допомоги розглядається як цілісна система психолого-педагогічних засобів, форм, методів і прийомів, спрямованих на формування в особистості стійкого емоційно-вольового

стану, здатності діяти впевнено, швидко й адекватно під час надання допомоги пораненим у бойових умовах.

Метою застосування цієї технології є розвиток у військовослужбовців здатності до ефективного виконання завдань із порятунку життя побратимів в умовах стресу, ризику, поранень і смертельної небезпеки. Тож до завдань технології відносять такі:

– сформувати мотиваційно-ціннісне ставлення до надання першої допомоги як до морального й професійного обов'язку військовослужбовця;

– розвинути емоційну стійкість, самоконтроль та вольову регуляцію в умовах бойового стресу;

– сформувати знання та когнітивні стратегії ефективних дій у критичних ситуаціях;

– відпрацювати поведінкові навички до рівня автоматизму;

– забезпечити формування командної взаємопідтримки та психологічної взаємодопомоги.

До того ж, застосування згаданої технології має спиратися на низку принципів, які відображають психолого-педагогічні закономірності підготовки військовослужбовців, зокрема:

принцип реалістичного моделювання – навчальні ситуації максимально наближені до реальних бойових умов (шум, кров, крики, вибухи);

принцип поступовості – поетапне ускладнення завдань і підвищення рівня стресового впливу;

принцип інтеграції – поєднання медичних, психологічних і тактичних компонентів підготовки;

принцип рефлексії – усвідомлення власних емоційних реакцій, помилок і шляхів їх корекції;

принцип командності – розвиток довіри, взаємопідтримки й почуття відповідальності за побратима.

Також важливим є і визначення змісту п'яти основних етапів реалізації зазначеної технології.

Перший етап – діагностико-мотиваційний. На цьому початковому етапі проводиться психодіагностика вихідного рівня готовності, виявлення індивідуальних особливостей стресостійкості, самоконтролю, емоційної врівноваженості.

Здійснюється мотиваційне налаштування через обговорення бойових ситуацій, аналіз прикладів героїзму, демонстрацію відеоматеріалів. Формується установка: «Я здатен діяти впевнено й ефективно навіть у критичній ситуації».

Другий етап – когнітивно-підготовчий. Основна мета цього етапу – передати знання про психологію екстремальних станів і навчити способів їх подолання.

Військовослужбовці отримують інформацію про закономірності поведінки людини під стресом, механізми емоційного шоку, особливості сприйняття часу, простору та небезпеки в бою.

Використовуються методи когнітивного програвання ситуацій, обговорення типових помилок і правильних алгоритмів дій («що робитиму, якщо...»).

Третій етап – емоційно-стресовий (тренувальний). Центральний етап технології, спрямований на практичне формування емоційної стійкості та психологічної витривалості.

Здійснюються стресові симуляційні тренінги, де створюються умови, наближені до бойових (імітація звуків пострілів, обмежена видимість, тиск часу, «поранені» актори).

Військовослужбовці виконують дії з надання домедичної допомоги під контролем інструкторів, одночасно навчаючись застосовувати техніки саморегуляції – дихальні вправи, внутрішній самонаказ, короткочасну релаксацію.

Використовується метод стрес-інокуляції (за Мейхенбаумом), який полягає у поступовому привчанні до стресу шляхом послідовного збільшення інтенсивності подразників.

Четвертий етап – рефлексивно-корекційний. Після кожного тренування проводиться психологічна рефлексія: учасники аналізують свої відчуття, емоційні реакції, причини помилок і засоби їх подолання.

Використовуються групові обговорення, індивідуальні консультації, вправи з відновлення емоційної рівноваги (релаксація, техніки усвідомленого дихання, коротка медитація).

Цей етап сприяє закріпленню адаптивних моделей поведінки і формує готовність до саморегуляції в реальних умовах.

П’ятий етап – закріплювально-практичний. На завершальному етапі здійснюється практичне відпрацювання навичок у комплексних тактичних навчаннях, де перевіряється рівень сформованості психологічної готовності.

Військовослужбовці діють у складі підрозділу, надаючи допомогу в умовах обмеженого часу, загрози обстрілу, наявності втрат.

Проводиться самооцінка і взаємооцінка готовності, що сприяє розвитку впевненості, бойового братерства та внутрішньої підтримки.

Крім того, до м*етодів та засобів реалізації технології розвитку психологічної готовності до надання першої домедичної допомоги відносять:*

- психотренінги емоційно-вольової регуляції;
- рольові ігри та ситуаційні вправи з моделювання реальних бойових подій. відпрацювання алгоритмів допомоги у реалістичних сценаріях;
- методи десенсибілізації – поступове звикання до травмуючих стимулів (вид крові, крики, шум);
- когнітивно-поведінкові методи – заміна деструктивних думок на адаптивні;
- тренінги командної взаємодії та взаємної підтримки;

- рефлексивні групи для обговорення досвіду та емоційних реакцій.

Реалізація зазначеної технології сприяє:

- підвищенню рівня емоційної стабільності та стресостійкості;
- формуванню швидкої, впевненої реакції у критичних ситуаціях;
- зменшенню проявів дезорганізації, паніки, ступору;
- розвитку самоконтролю, внутрішньої мобілізації та рішучості;
- зміцненню взаємопідтримки і почуття відповідальності в колективі;
- формуванню автоматизованих дій під час надання допомоги, що підвищує шанси на порятунок життя.

Таким чином, домедична допомога в умовах війни – це не просто набір дій, а комплекс життєво важливих умінь, які: зберігають життя, підтримують моральну стійкість, зміцнюють бойову спроможність, формують гуманність у найскладніших умовах. Головний сенс – «врятуй того, хто поруч, і врятуєш частину країни». У свою чергу, психологічна готовність до надання домедичної допомоги є важливим елементом бойової ефективності військовослужбовця. Вона формується у процесі системної підготовки, що поєднує професійну компетентність, емоційну стабільність і моральну відповідальність.

Розвиток цієї готовності потребує цілеспрямованої роботи психологів підрозділів, командирів і медичних інструкторів, що забезпечує збереження життя та морально-психологічну стійкість військових у бою.

Технологія розвитку психологічної готовності військовослужбовців до надання першої домедичної допомоги в бойових умовах є системним, поетапним процесом, що охоплює діагностику, навчання, тренування, рефлексію та практичне закріплення набутих умінь. Її ефективність забезпечується поєднанням психологічних, медичних і тактичних компонентів підготовки, а також створенням умов, максимально наближених до реальних бойових ситуацій.

Розвинена психологічна готовність є запорукою не лише професійної ефективності військовослужбовця, а й збереження життя побратимів та самого воїна.

Список використаних джерел:

1. Долікарська медична допомога : навч. посіб. / А. М. Ляшевич та ін. Житомир : Вид-во ЖДУ ім. І. Франка, 2021. 224 с.
2. Іванова Н. Г., Андрусишин Ю. І. Психологічні детермінанти стресостійкості військовослужбовців в умовах впливу психотравмуючих чинників. *Вісник Національного університету оборони України.* 2023. № 1 (71). С. 72–78.
3. Іванова Н. Г. Формування психологічної готовності правоохоронців до діяльності в екстремальних умовах. *Вісник Національного університету оборони України.* 2014. № 6(43). С. 294–299.
4. Психологічне забезпечення професійної діяльності фахівців сектору безпеки : навч. посіб. / Н. Г. Іванова та ін. Київ : Нац. акад. СБУ, 2019. 244 с.

ПЛАТОНОВ В. М.,
доктор філософії (Ph.D.) з психології,
науковий співробітник навчально-наукової
лабораторії екстремальної та кризової психології,
Навчально-науковий інститут
оперативно-рятувальних сил
Національного університету
цивільного захисту України

ОСОБЛИВОСТІ ПРОФЕСІЙНО-ПСИХОЛОГІЧНИХ ЯКОСТЕЙ ОПЕРАТОРІВ БЕЗПІЛОТНИХ СИСТЕМ ДСНС УКРАЇНИ

Розвиток та впровадження безпілотних систем у сегменті вирішення завдань з цивільного захисту населення сьогодні набуває значного поширення. Їх застосування дозволяє виконувати надскладні та ризиковані завдання з метою мінімізації людських втрат та забезпечити можливість залучення більшої кількості ресурсів для ліквідації надзвичайної ситуації, зокрема шляхом доставки більшого обсягу води або речовин для гасіння осередку пожежі, де робота рятувальників може бути надмірно ризикованою або пройти більшу кількість замінованої території. В умовах застосування безпілотних систем різних типів ключовою ланкою в системі «людина–машина–середовище» залишається оператор.

У сучасних наукових дослідженнях психологами-науковцями підіймається питання щодо визначення та оцінки впливу людського фактора на якість виконання завдань за допомогою безпілотних систем. У нещодавніх наукових публікаціях неодноразово наголошується на важливості створення професіографічних профілів фахівців-операторів безпілотних систем різних типів. Найбільшого поширення цей напрям досліджень набув серед науковців військового профілю, що зумовлено значним поширенням застосування комплексів безпілотних систем саме у військовій практиці. Аналіз наявних робіт свідчить про значний перелік як професійних, так і психологічних вимог, яким повинні відповідати кандидати на посаду операторів безпілотних систем. Так, Ю. Широбоков, В. Пасічник та О. Савчук наводять значний перелік професійних вимог до операторів військових безпілотних комплексів: точність виконання дій та наказів, швидке ухвалення рішень, уміння швидко адаптуватися до керування дроном у різних режимах, значна відповідальність як за виконання завдання, так і за сам дрон та його корисне навантаження, тривале перебування в статичних положеннях тіла з можливістю швидко змінити своє положення, що згодом веде до відчуття втоми, а разом із цим – до погіршення атенційних якостей, зниження швидкості прийняття рішень, зменшення якості результатів інтелектуальної діяльності та виникнення нервово-психічних перевантажень. Натомість авторами визначено орієнтовний перелік професійно важливих психологічних якостей, а саме: для успішного здійснення

професійних функцій операторам безпілотних систем необхідні зібраність, постійна включеність у процес прийняття рішень, спостережливість, нервово-психічна стійкість, швидка адаптація до складних та часто змінних умов виконання завдань, моральна нормативність поведінки, високий рівень військово-професійної спрямованості, психологічної та фізичної підготовленості тощо [2, с. 117].

У дослідженні В. Медведєва та С. Коропа наголошується не тільки на професійно важливих психологічних якостях, а й на психофізіологічних функціях. Авторами виділено, що значного впливу на операторів безпілотних систем спричиняє інформаційне перевантаження. При цьому оператор, окрім врахування даних про сам дрон, повинен аналізувати інформацію та ситуацію, у якій перебуває дрон, щоб ухвалити найбільш «вигідне» рішення для керування ним, його подальшого застосування й повернення. Оператору доводиться аналізувати значний обсяг інформації, який надходить переважно на одну групу аналізаторів; у більшості випадків це інформація, що надходить на дисплей або до спеціальних окулярів. У цьому ж дослідженні автори також виділяють набір основних підсистем професійно важливих якостей, до яких відносять: швидке й точне реагування на зовнішні стимули, мнемічні властивості, добре розвинену уяву, когнітивні процеси у контексті творчого та оперативного мислення, вольові якості у контексті цілеспрямованості, наполегливості, рішучості та стресостійкості [3].

У дослідженні С. Коропа, присвяченому визначенню професійно важливих психологічних якостей операторів безпілотних систем, автором відзначено відмінності професійно-психологічних характеристик між операторами безпілотних систем тактичних класів та коптерного типу [1].

Враховуючи сучасні тенденції поширення безпілотних систем, Державна служба України з надзвичайних ситуацій активно використовує їх у напрямках діяльності з гуманітарного розмінування територій, гасіння пожеж великих масштабів, оцінки наслідків надзвичайних ситуацій, розвідки та пошуку зниклих людей [4]. Хоча оператори безпілотних систем виконують функції з керування дроном, варто зазначити, що ця категорія фахівців має певні особливості. З огляду на приклади, наведені вище, доцільно розділити операторів безпілотних систем різних напрямів діяльності ДСНС України, наприклад:

– для операторів безпілотних систем, які використовуються в гуманітарному розмінуванні, професійно важливими якостями є висока відповідальність, чітке слідування правилам, терпіння, збереження спокою та високий рівень адаптації;

– для операторів безпілотних систем, що застосовуються для пожежогасіння, важливими є професійно-психологічні якості: точність виконання інструкцій, висока відповідальність, розвинені інтелектуальні здібності в аспекті аналізу та прогнозування розвитку надзвичайної ситуації, високий рівень технічної підготовки;

– для операторів безпілотних авіаційних систем можна розглядати ті якості, які вже виділені науковцями та наведені вище;

– оператори безпілотних систем підводного розмінування повинні мати високий рівень технічної грамотності, уважність до деталей і добре розвинене просторове мислення. Така діяльність вимагає аналітичного мислення, стресостійкості, відповідальності та здатності швидко приймати рішення в екстремальних умовах. Важливими є також комунікабельність, самоконтроль і дотримання правил безпеки під час виконання гуманітарних завдань.

Таким чином, розвиток і впровадження безпілотних систем у сфері цивільного захисту населення відкриває нові можливості для підвищення ефективності та безпеки виконання завдань рятувальниками. Аналіз наукових джерел свідчить, що головним чинником успішності роботи таких систем залишається людський фактор – професійна підготовка, психологічна стійкість та технічна компетентність оператора. Для різних напрямів діяльності операторів дронів у ДСНС України важливо сформувати перелік специфічних професійно важливих якостей. Подальший розвиток дослідження цієї тематики полягає у чіткому визначенні переліку професійно важливих якостей операторів безпілотних систем, а також у розробленні відповідного психодіагностичного інструментарію для відбору кандидатів на навчання за спеціальністю оператора безпілотних систем в ДСНС України.

Список використаних джерел:

1. Korop S. V. MILITARY AND PROFESSIONAL ACTIVITIES OF OPERATORS OF UNMANNED AERIAL VEHICLES OF THE COPTER TYPE: PSYCHOLOGICAL FEATURES. Habitus. 2024. № 67. С. 243–247. URL: https://doi.org/10.32782/2663-5208.2024.67.40.
2. Pasichnyk V., Shyrobokov Y., Savchuk O. PSYCHOLOGICAL FEATURES OF THE ACTIVITY OF OPERATORS OF UNMANNED AERIAL SYSTEMS OF TACTICAL CLASSES AND THEIR CONSIDERATION IN THE PRACTICE OF PROFESSIONAL TRAINING OF THESE MILITARY SPECIALISTS. The scientific journal of the National Academy of National Guard "Honor and Law". 2023. Vol. 4, no. 87. P. 113–120. URL: https://doi.org/10.33405/2078-7480/2023/4/87/295206.
3. Короп, С., Медведєв, В. Психофізіологічні особливості операційно-інструментальної діяльності оператора безпілотного авіаційного комплексу мультироторного типу (і класу). Повітряна міць України, 2(7). 2024. 73–79. https://doi.org/10.33099/2786-7714-2024-2-7-73-79.
4. Кушнір А., Альфавіцька Г. Аналіз можливостей застосування безпілотних літальних апаратів у діяльності ДСНС України. Проблеми та перспективи розвитку системи безпеки життєдіяльності : Зб. наук. праць XX Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів. Львів : ЛДУ БЖД, 2025. С. 152–154.

СОЛОНЕНКО А. С.,
викладач кафедри психології та педагогіки,
Навчально-науковий інститут роботи з персоналом
Національної академії
Національної гвардії України

ПИТАННЯ ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВОСЛУЖБОВЦІВ ПРИ ВИКОНАННІ ОПЕРАТИВНО-БОЙОВИХ ЗАВДАНЬ В РАЙОНІ ПРОВЕДЕННЯ БОЙОВИХ ДІЙ: РЕАЛІЇ ТА ПРІОРИТЕТИ

В умовах постійної напруги на фронті тема психологічного забезпечення має не теоретичне, а цілком практичне, життєво важливе значення. Сучасна війна – це жорсткий психологічний тиск. З мого досвіду, якщо в бійця «зламаний» дух, його зброя не стріляє. Без стійкої психіки навіть найкраще озброєння «не відпрацює». Головна мета військового психолога та командира – не допустити «зламу» і зберегти боєздатність. Ми розглядаємо психологічне забезпечення як безперервний «цикл» роботи. У цій доповіді я хочу зосередитися на ключових проблемах та практичних інструментах, які ми використовуємо в районі боїв.

1. Першочергові виклики та фактори дезадаптації особового складу

На практиці ми стикаємося з тим, що є кілька основних факторів, які «б'ють» по психіці бійців і призводять до дезадаптації:

Хронічний стрес і втома. Постійні «прильоти», недосипання, неможливість нормально «перезавантажитися» (навіть у тилу його немає) призводять до вигорання. Через це падає концентрація, швидкість реакції, і підрозділ «сиплеться».

Вплив високоінтенсивних боїв. Це не лише фізичні травми, а й контузії, які завжди мають психологічний наслідок, а також переживання втрат побратимів. Це – каталізатор для гострої реакції на стрес (ГРС). Тому ми мусимо бути напоготові [1, 3].

Ізоляція та невизначеність. Обмежений зв'язок із домом і нерозуміння термінів ротації посилюють тривожність. Ми бачимо, що це прямо впливає на морально-психологічний стан (МПС) бійця.

Вважаю, що наша робота полягає в тому, щоб вчасно «зчитати» ці сигнали і не дати їм перерости у серйозну проблему.

2. Пріоритетні напрями психологічного забезпечення у бойових умовах

Ефективне забезпечення відпрацьовує на двох ключових рівнях: індивідуальному та груповому. Ми починаємо з того, що готуємо людей ще в тилу, але основна робота відбувається вже «на нулі».

2.1. Екстрена та кризова допомога «на нулі»

Це перша лінія психологічного захисту. Вона має бути швидкою і чіткою, як медична допомога [2]:

Дебрифінг після бою. Необхідно відразу «знімати» накопичену напругу, щойно підрозділ «вийшов» із контакту. Це може бути розмова, обмін досвідом, «скидання» негативу.

Робота з ГРС. Якщо бачимо паніку, ступор чи неконтрольовану агресію, психолог або навчений парамедик має стабілізувати бійця. Зокрема, використовуються дихальні техніки та повернення до реальності (орієнтація). Це дозволяє бійцю відновити боєздатність і відпрацювати до кінця зміни.

Психологічна розвідка. Командири та психологи повинні постійно вести спостереження за МПС, виявляючи тих, хто «сиплеться», ще до того, як ситуація загостриться [4].

2.2. Психологічна згуртованість підрозділу

Ми знаємо, що найкращий психолог для бійця – це його побратим. Через це велику увагу ми приділяємо створенню стійких зв'язків та довіри. Підрозділ повинен «відпрацювати» як єдиний організм. Якщо боєць довіряє своєму командиру і товаришу, його психологічна стійкість зростає в рази. Це досягається через спільне виконання складних завдань, де кожен відчуває плече напарника [1, 3].

3. Трансформація ролі командира та перспективи

Я стикався з тим, що часто командири недооцінюють психологію. Це помилка. У сучасній війні командир є основним психологом. Його стиль, тон наказу, вміння слухати – все це формує МПС.

3.1. Командир як ключовий фактор

Мотивація та інформування. Бійці повинні чітко розуміти мету, навіть якщо задача – просто «тримати опорник». Командир має грамотно подати інформацію, пояснюючи, чому їхня робота важлива.

Децентралізація відповідальності. Командир повинен делегувати повноваження на нижчі ланки. Це підвищує відчуття контролю у бійців. В результаті, зменшується відчуття безпорадності, яке є коренем багатьох психологічних проблем [4].

3.2. Необхідність впровадження інновацій

Вважаю, що ми повинні активніше впроваджувати сучасні технології:

Телемедицина. Вивести психолога на «нуль» завжди складно. Тому захищені канали зв'язку для дистанційних консультацій – це пріоритет.

Чітка ротація та реабілітація. Потрібен чіткий графік, щоб бійці могли «скинути» бойовий стрес у центрах відновлення, перш ніж повертатися на фронт [5]. Це необхідно для довгострокової стійкості.

Висновки

Підсумовуючи, можна сказати, що психологічне забезпечення – це не просто додаткова опція, а критичний елемент боєздатності. Ці дії реально працюють у бойових умовах, коли вони є системою, а не разовою акцією.

Для ефективної роботи необхідно:

Забезпечити безперервність психологічної розвідки та екстреної допомоги безпосередньо в зоні боїв.

Зміцнювати довіру та згуртованість підрозділів, бо побратимство – найкращий захист від стресу.

Трансформувати роль командира і активно впроваджувати дистанційні технології підтримки.

Успіх у війні залежить від міцності духу, і це завдання ми зобов'язані відпрацювати на найвищому рівні.

Список використаних джерел:

1. Кривоконь М. В. Психологічне забезпечення бойової діяльності військовослужбовців у зоні АТО/ООС. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Психологія»*. 2018. № 1. С. 98–105.
2. Морозов О. В., Кудрявцев В. В. Особливості надання першої психологічної допомоги військовослужбовцям в умовах бойових дій. *Збірник наукових праць Національної академії сухопутних військ імені гетьмана Петра Сагайдачного*. 2020. № 1(57). С. 147–153.
3. Тимченко О. В., Пащенко В. В. Психологічна стійкість військовослужбовців як фактор збереження боєздатності. *Науковий вісник Львівського державного університету внутрішніх справ*. 2021. № 2. С. 182–190.
4. Ярошенко В. П. Роль командира у психологічному забезпеченні підрозділу в бойових умовах. *Військово-науковий вісник*. 2019. № 32. С. 101–108.
5. Центр психічного здоров'я та реабілітації ветеранів. *Методичні рекомендації щодо психологічної реабілітації*. Київ, 2022. 120 с.

ЧЕРНЕНКО Т. В.,
кандидат філософських наук,
Національна академія Служби безпеки України

ВПЛИВ КОМАНДИРСЬКОЇ РИТОРИКИ ТА МОТИВАЦІЙНИХ НАРАТИВІВ НА МОРАЛЬНО-ПСИХОЛОГІЧНИЙ СТАН ОСОБОВОГО СКЛАДУ В БОЙОВИХ УМОВАХ

У сучасних бойових умовах ефективність військових підрозділів дедалі більше залежить не лише від рівня підготовки чи технічного забезпечення, а від мотиваційного стану особового складу. Досвід останніх років засвідчує, що саме морально-психологічна стійкість, внутрішня переконаність у справедливості боротьби та довіра до командирів стають визначальними чинниками успішного виконання завдань [1]. Водночас поширення негативних наративів – як зовнішніх, створених противником, так і внутрішніх, що виникають через неефективну комунікацію командирів, – призводить до демотивації, втрати ініціативи та зниження згуртованості, і як наслідок, ефективності підрозділів [2]. Командирська риторика і мотиваційні наративи є критичними чинниками, що формують бойову готовність, довіру до командування й відчуття справедливості боротьби. В умовах війни рф

проти України питання морально-психологічного забезпечення набуває екзистенційного характеру, адже від нього залежить виживання підрозділів і їхня здатність до тривалого опору.

Попри формальну наявність у структурах сектору безпеки і оборони систем морально-психологічного забезпечення (МПЗ), комунікаційна складова діяльності командира часто не розглядається як окремий елемент бойової готовності. Проблема ефективної командирської риторики має історичний вимір – від промов полководців античності до сучасних підходів стратегічних комунікацій. В умовах війни рф проти України саме якість внутрішньої комунікації визначає моральну стійкість підрозділів. На жаль, часто риторика командирів не відповідає ситуаційним потребам – домінує наказово-контрольна модель, а не мотиваційно-виховна. Проблема ускладнюється інформаційним фоном, у якому бійці отримують суперечливі повідомлення – від офіційних звітів до неформальних телеграм-каналів і приватних коментарів контраверсій них новин. Цю ситуацію системно описують українські фахівці, які доводять, що словесне приниження, прилюдне висміювання чи ігнорування скарг мають прямі наслідки у вигляді дезорганізації та демотивації. Українські дослідники, зокрема Мамедов Р. Ч., Немінський І. В., Лесюк О. М., Олійник В. О., Мась Н. М., Рой О. Б., Капінус О. С., Лук'яненко В. В., Весер В. В., Нечитайло Ю. В., Можарівський В. В., Магола С. І.; Урсол А. О.; Черевичний С. В., Пшенишнюк Г. О., Заріцький Т. Б.; Сидоренко А. В., Бродська Л. А.; Возніцина К. Б., Стасюк В. В., Крук В. П., Романенко О. Г. [3–5], підкреслюють, що гуманістична риторика командира зміцнює дисципліну й довіру, тоді як словесне приниження руйнує бойовий дух. Натомість визнання внеску конкретного бійця, пояснення не лише «що робимо», але й «навіщо» – підвищує готовність діяти без примусу. Таким чином, проблема має не лише психологічний, а й стратегічний вимір: мовлення командира є елементом обороноздатності.

Історично питання командирської риторики та морально-психологічного забезпечення супроводжує армійські практики від давніх часів: від ритуалізованих промов воєначальників у доіндустріальну епоху до сучасних масових медіа- та інформаційних кампаній. Протягом XX століття дослідники військового лідерства підкреслювали роль мовлення командира у формуванні бойового духу, одночасно вказуючи на ризики авторитарних практик, що демобілізують ініціативу. Свого часу проблему досліджували як військові соціологи, так і фахівці з психології лідерства та стратегічних комунікацій. Серед авторів, чиї роботи становлять корисну основу для аналізу, можна виокремити праці D. Grossman (комбатологія та психологія вбивства), S. Tatham і P. Taylor (поведінкова складова конфліктів), а також дослідження центрів стратегічних комунікацій і наукових інституцій NATO SCOE. Сучасна агресивна війна рф проти України поставила питання комунікаційної якості та мотиваційних наративів на новий, кризовий порядок денний:

під постійним вогнем інформаційної та психологічної війни відсутність злагодженої риторики може мати катастрофічні операційні наслідки.

Метою дослідження є визначення ролі командирської риторики та мотиваційних наративів у підтриманні морально-психологічного стану особового складу, а також розроблення практичних рекомендацій щодо удосконалення внутрішніх комунікацій у бойових підрозділах.

Мотиваційні наративи – смислові конструкції, що формують у свідомості військовослужбовців відчуття мети, значущості служби й причетності до спільної справи. У практиці підрозділів виділяються три основні групи наративів: патріотично-ціннісні, колективно-відповідальні та місійні (екзистенційні) [4]. Але самі по собі наративи не працюють автоматично: вирішальним є їхня трансляція через командирську риторику, яка повинна адаптувати загальні смисли до умов конкретного бою. Мотиваційні наративи – це внутрішня логіка служби, яку командир пропонує особовому складу. В українській практиці виділяють три типи таких наративів: патріотично-ціннісні, колективно-відповідальні та екзистенційні. Вони ефективні лише тоді, коли слова командира підкріплені конкретними діями – турботою про бійців, справедливим розподілом навантаження, своєчасною ротацією [4].

По-перше, важливим елементом є послідовність і сталість повідомлень. Коли командири постійно змінюють тон або меседжі не узгоджуються зі штабними інструкціями, у підлеглих виникає відчуття невизначеності і подвійних стандартів. Це знижує довіру і стимулює інформаційний хаос на рівні підрозділу.

По-друге, необхідна емоційна щирість у комунікації. Формальні, клішовані звернення не створюють почуття причетності; натомість, чесні, конкретні пояснення ситуації, визнання труднощів та реальні дії із забезпечення безпеки і побуту створюють основу для довіри.

По-третє, командирська риторика мусить бути цілеспрямованою і практичною: підкреслення конкретних завдань, досягнень підрозділу та зрозумілих критеріїв успіху сприяє мотивації, оскільки солдат розуміє, навіщо і в яких межах очікується його внесок.

По-четверте, слід враховувати вплив зовнішніх інформаційних чинників: медійні повідомлення, чутки у соцмережах і публічні дискусії можуть спричиняти різноспрямований вплив на розуміння особовим складом тих чи інших подій, призводити до де мотивації військово-службовців бойових підрозділів. Командири, які ігнорують ці впливи, залишають поле діяльності інформаційним опонентам. Натомість активне пояснення та контраргументація з боку командирів зменшують курс дезінформації і зберігають бойову мотивацію.

По-п’яте, важлива так звана «зворотна комунікація»: наявність каналів, через які підлеглі можуть висловити проблеми, пропозиції або побоювання, дозволяє командирові своєчасно реагувати і демонструвати готовність до змін. Відсутність таких каналів породжує накопичення незадоволення і підсилює відчуття відчуженості.

Успішним прикладом інтеграції мотиваційних комунікацій у систему оборони є досвід Ізраїлю. У структурах IDF (Israel Defense Forces) від початку 2000-х років функціонують підрозділи морально-психологічної підтримки (Heb. – Yahash, від Yechidat HaHizuk HaRuach – «Підрозділ зміцнення духу»), які входять до складу військових округів. Їхнє завдання – постійна присутність поруч із бойовими командирами, оперативний аналіз морального стану, корекція риторики та контрнаративів. Згідно з дослідженнями RAND Israel Reports [7] і публікаціями у Military Psychology Review , ефективна комунікація командира в IDF базується на трьох принципах: 1. чесність у повідомленнях («ніяких прикрас – лише правда про ситуацію»); 2. визнання помилок як частини командирської зрілості; 3. щоденна комунікаційна взаємодія – короткі 5-хвилинні брифінги для підтримки відчуття спільної мети.

За даними ізраїльського психолога A. Ben-Dor [6], підрозділи, де командири регулярно проводили такі сесії, демонстрували на 30 % вищу стабільність морального стану під час тривалих операцій у секторі Газа.

Війна рф проти України продемонструвала обидва полюси командирської риторики. Таким негативним прикладом можна визнати те, що у низці підрозділів подекуди спостерігалися випадки, коли командири реагували на втрати агресивно або зневажливо. За словами одного з військовослужбовців, оприлюдненими у Hromadske.ua (липень 2023 р.), «нас відчитали за втрату техніки, навіть не вислухавши, як вона була втрачена під обстрілом. Після цього мотивація служити зникла на тиждень».

Проте є й позитивні приклади: низка підрозділів Сил оборони України відзначається впровадженням структурованих внутрішніх комунікаційних практик – регулярні брифінги, короткі морально-мотиваційні наради, peer-to-peer підтримка, системи визнання досягнень та чіткі процедури ротації, що дозволяють розвантажити бойовий персонал. Ці практики пов’язані з поліпшенням матеріально-побутових умов, підвищенням рівня професійної підготовки командирів, а також із залученням психологів і офіцерів морально-психологічного забезпечення до регулярної роботи в підрозділах. Зокрема, у 2023–2024 рр. одні з найбільш ефективних підрозділів Сил оборони України, зокрема бригади «Азов», 93-тя ОМБр «Холодний Яр» запровадили практику коротких вечірніх зібрань для підбиття підсумків і моральної підтримки. Командири успішно застосовують принцип «відкритої комунікації» – чесно говорять про втрати, але акцентують на спільній меті. Як зазначив один із ротних командирів у коментарі для ArmyInform (травень 2024 р.): «Мені не треба, щоб ви були героями. Мені треба, щоб ви були живі й готові до завтрашнього шикування». Така риторика, за оцінкою військового психолога Романенка О. Г., «перемикає мислення бійця з патетики на відповідальність, що і є ядром стійкої мотивації». Як наслідок, за внутрішніми звітами психологічних служб (НА СБУ,

2024 р.), підрозділи, які впровадили подібну практику, демонструють зниження конфліктності на 25 % і зменшення випадків емоційного виснаження серед особового складу.

Війна рф проти України загострила значущість цих комунікаційних механізмів. Наслідки неефективної командирської риторики на полі бою можуть бути драматичними: зниження ініціативи та ініціативності, підвищення числа внутрішніх інцидентів і конфліктів, зростання сепаративних або дезертирських настроїв, погіршення координації дій під час масштабного наступу чи відступу, а також зниження оперативної готовності підрозділу. У крайніх випадках – це втрата позицій, підвищені бойові втрати або системний колапс морального клімату.

З впровадженням стандартизованих модулів комунікацій у навчальні програми командирів та розвитком системи моніторингу внутрішнього інформаційного середовища можна масштабувати позитивні практики на більшу кількість підрозділів. Ключові кроки для масштабування включають: розроблення шаблонів коротких щоденних брифінгів, навчальні кейси для командирів із прикладами «що говорити і як», створення простих інструментів збору зворотного зв’язку та забезпечення наявності офіцерів морально-психологічного забезпечення в безпосередньому складі батальйонів.

Висновки та рекомендації

1. Командирська риторика має бути усвідомленим інструментом мотиваційного впливу, що базується на послідовності, щирості та практичності.
2. Необхідна нагальна розробка коротких стандартизованих модулів внутрішніх комунікацій у підрозділах для використання в умовах бойових дій.
3. Вкрай актуальною є необхідність інтегрувати комунікаційну підготовку у систему службової освіти командирів на всіх рівнях.
4. Необхідно впровадити регулярний моніторинг внутрішнього інформаційного середовища підрозділів і механізми швидкого реагування на демотивуючі сигнали.
5. Вкрай актуальним також є необхідність масштабувати позитивні практики через тренінги, навчальні кейси та обмін успішними прикладами між підрозділами.
6. Досвід Збройних сил Ізраїлю підтверджує: морально-психологічна стійкість особового складу є продуктом не стільки пропаганди, скільки чесного, регулярного діалогу командира з підлеглими. Україні доцільно розглянути створення штатних груп мотиваційно-психологічного супроводу підрозділів за зразком Yahash, інтегрованих у структуру МПЗ Сил безпеки.

Список використаних джерел:

1. Hunter G. Military Leadership and Learning: A Guide for Training and Motivation. Routledge, 2020. URL: https://www.researchgate.net/publication/233021225_Leadership_and_Team_Dynamics_for_Dangerous_Military_Contexts (дата звернення: 26.10.2025).
2. NATO Strategic Communications Centre of Excellence. Psychological Resilience in the Armed Forces. Riga, 2023. URL: https://stratcomcoe.org/publications/defence-strategic-communications-volume-12-spring-2023/283 (дата звернення: 27.10.2025).
3. Психологічне забезпечення Збройних Сил України : навч.-метод. посіб. / за заг. ред. генерал-майора В. Клочкова. Київ : НДЦ ГП ЗС України, 2024. 293 с.
4. Крук В. П. Лідерство і морально-психологічна готовність військовослужбовців у бойових умовах. // Вісник НУОУ, № 3, 2023. С. 45–53.
5. Романенко О. Г. Проблеми комунікативної взаємодії в системі військового управління. // Збірник наукових праць НА СБУ, № 2, 2024. С. 87–94.
6 Ben-Dor A. Motivational Communication in the IDF: Psychological Perspectives. // Military Psychology Review, Vol. 14(2), 2020. URL: https://doi.org/10.1080/08995605.2022.2127986 (дата звернення: 28.10.2025).
7 RAND Corporation. Building Resilient Morale in the Israel Defense Forces. RAND Israel Reports, 2021. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3400/RRA3486-1/RAND_RRA3486-1.pdf (дата звернення: 28.10.2025).
8 ArmyInform. Командирська риторика як фактор мотивації бійців. URL: https://armyinform.com.ua/2023/02/06/horosha-motyvacziya-plyus-horosha-pidgotovka-dorivnyuye-mozhlyvosti-nashyh-cyl-oborony-povernuty-ukrayini-svoye-prezydent/ (дата звернення: 28.10.2025).

6 ЗАСТОСУВАННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У ДІЯЛЬНОСТІ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ (ЦИВІЛЬНО-ВІЙСЬКОВЕ СПІВРОБІТНИЦТВО, ІНФОРМАЦІЙНІ ТА ПСИХОЛОГІЧНІ ОПЕРАЦІЇ)

БАФЯН Г. М.,
головний спеціаліст 2 відділу
3 служби УРОС СБ України
(аспірант, Національна академія
Служби безпеки України)

ВНУТРІШНІ КОМУНІКАЦІЇ – ДІЄВИЙ МЕХАНІЗМ В СИСТЕМІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Виклики гібридної війни проти України вимагають ефективного управління інформаційним простором не менше ніж військової сили. Тому ключовим інструментом забезпечення національної безпеки стають стратегічні комунікації (далі – СтратКом).

СтратКом – це діяльність державних інституцій, яка цілеспрямовано та скоординовано фокусується на формування сприятливого інформаційного середовища, зміцнення довіри до держави, а також забезпечення єдності дій у внутрішньому та зовнішньому фокусі. Це інформаційна зброя держави, яка дозволяє формувати інформаційну перевагу, невід'ємна складова оперативного управління сектору безпеки. У Воєнній доктрині зустрічається поняття СтратКом, як скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків із громадськістю, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [1].

Виокремлюють такі основні концептуальні характеристики стратегічних комунікацій: формування інформаційного середовища; інформаційна підтримка та забезпечення інформацією суспільства; тлумачення дій як інформації; вплив на цільову аудиторію, формування довірливих стосунків та підтримка зворотного зв'язку; здатність враховувати потреби аудиторії та досліджувати реакції на різні події та повідомлення; налагодження діяльності та координація комунікації між суб'єктами державних та корпоративних інституцій з метою посилення стратегічного ефекту; визначення та досягнення інтересів держави на національному та міжнародному рівнях; формування стійкого політичного іміджу держави; ефективна взаємодія між політиками з метою досягнення спільних (культурних, соціальних, економічних, політичних та ін.) цілей; налагодження структурної взаємодії в галузі

стратегічних комунікацій шляхом запровадження дієвих комунікативних механізмів тощо [3].

В часи, коли країна мусить протистояти ворогу, в обличчі рф, забезпечення ефективної системи СтратКому – надзвичайно важлива місія. Основними напрямками застосування якої є інформаційна безпека та протидія ІПсО. Скоординовані дії допомагають гідно відповідати на інформаційні атаки ворога, розпізнавати можливі маніпуляції та чітко реагувати в медіапросторі. Не менш важливими є напрямки кризових комунікацій та внутрішніх комунікацій. Узгоджене, достовірне, чітке інформування під час бойових дій – запорука успіху та збереження людського капіталу сил безпеки і оборони. А формування корпоративної культури, довіри та командної взаємодіє в середині тилових структур сектору безпеки і оборони – це інструмент успішної реалізації СтратКому.

Ефективна система внутрішніх комунікацій, як невід'ємна складова СтратКому – це обмін інформацією на вертикальному та горизонтальному рівнях всередині підрозділів сектору безпеки і оборони, спрямований на забезпечення налагодженої взаємодії між керівниками та підлеглими, що включають в себе формальні канали комунікації: наради, накази, розпорядження та неформальні: підтримка командного духу та неформальне спілкування. Чіткий обмін інформацією всередині підрозділів допомагає уникнути непорозумінь, прискорити процес прийняття рішень, у тому числі управлінських, підвищити залученість та продуктивність фахівців сектору безпеки і оборони, підвищити моральних дух та стійкість серед особового складу.

За стандартами НАТО [6] внутрішні комунікації – один із важливих компонентів системи стратегічних комунікацій. Внутрішні комунікації розглядаються як напрям інформаційно-пропагандистського забезпечення військових частин (підрозділів), військових навчальних закладів, установ і організацій ЗС України, що здійснюється в системі інформаційної роботи посадових осіб органів військового управління, командирів (начальників) через сукупність дій, зв'язаних з обробкою і передачею інформації до особового складу через спілкування [4].

Налагоджена система внутрішніх комунікацій серед фахівців сектору безпеки і оборони як складова ефективної управлінської діяльності та лідерства керівників усіх рівнів забезпечить досягнення належного рівня мотивації та лояльності особового складу, який сприяє виконанню підрозділами завдань за призначенням.

Проте, в контексті реалізації СтратКому варто зауважити, що ключовими проблемами розбудови системи стратегічних комунікацій в Україні можуть стати проблеми налагодження дієвої та ефективної координації, вироблення узгодженого бачення концепції стратегічних комунікацій, створення повноцінного та довгострокового механізму підготовки фахівців зі стратегічних комунікацій в Україні, а також розвиток ефективного наукового супроводу стратегічних комунікацій через

розбудову їх чіткої та дієвої концепції для практичного використання державними органами в інтересах національної безпеки [2].

Як висновок, задля досягнення стратегічних комунікацій варто фокусуватися на виконанні основних практичних дій: постійно боротися за сприйняття своїх дій як легітимних, таких що варті довіри та підтримки, забезпечувати потрібний вплив, діяти активно, на випередження і швидко; розуміти оперативне середовище, у якому відбуваються дії, аудиторію та зміст керівних вказівок вищого командування, підтримувати дії інструментами внутрішніх комунікацій; визначити відповідальний особовий склад для допомоги командиру в розробленні комунікаційної стратегії, синхронізації діяльності зі стратегічних комунікацій для досягнення синергії цих зусиль; використати можливості навчань з питань внутрішніх комунікацій, інформування та впливу не тільки на тих, хто безпосередньо займається комунікаціями, інформаційними операціями, а й тими, хто застосовує сили і засоби проти противника; постійно проводити уточнення і аналіз оперативного середовища, важливих аудиторій для правильності та ефективності внутрішніх комунікацій [5].

Список використаних джерел:

1. Дубов Дмитро Володимирович, доктор політичних наук, старший науковий співробітник, Стратегічні комунікації: проблеми концептуалізації та практичної реалізації 1, Стратегічні пріоритети № 4 (41). 2016. С. 19.
2. Дубов Дмитро Володимирович, доктор політичних наук, старший науковий співробітник, Стратегічні комунікації: проблеми концептуалізації та практичної реалізації 1, Стратегічні пріоритети № 4 (41). 2016. С. 20.
3. Ліна Стороженко, Світлана Петькун, Стратегічні комунікації: концептуальні підходи та базові принципи. Society. Document. Communication (2021) Ed. 11. 386 – 403/. DOI https://doi.org/10.31470/2518-7600-2021-11-386-403.
4. Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України : наказ Генерального штабу Збройних Сил України від 04.01.2017 р. № 4. Київ, 2017. 25 с.
5. Семененко В. М. Організація внутрішніх комунікацій в Об’єднаних силах // Філософсько-соціологічні та психолого-педагогічні проблеми підготовки особистості до виконання завдань в особливих умовах : збірник тез доповідей науково-практичної конференції (м. Київ 31 жовтня 2019 р). Київ, 2019.
6. NATO Strategic Communications Handbook: Draft for Use Ver 9.1.21–31 March 2015. Norfolk, VA: Supreme Allied Command Transformation HQ. 2015. 86 p.

ГАЛАГАН Г. А.,
Національна академія Служби безпеки України

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК ІНСТРУМЕНТ АНТИТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Сучасні безпекові виклики, спричинені поширенням терористичних загроз, гібридних воєн та інформаційно-психологічних операцій, зумовлюють необхідність оновлення підходів до антитерористичної діяльності нашої держави. В умовах триваючої збройної агресії російської федерації проти України стратегічні комунікації стають ключовим інструментом формування суспільної стійкості, довіри до силових структур і координації між владою, громадянами та міжнародними партнерами.

Особливу роль у цьому процесі відіграє Служба безпеки України (далі – СБУ), яка здійснює комплекс заходів щодо запобігання, виявлення та нейтралізації терористичних загроз. Слід зазначити, що ефективне використання стратегічних комунікацій у діяльності СБУ забезпечує не лише інформаційну протидію деструктивним впливам, а й сприяє формуванню позитивного іміджу державних інституцій, підвищенню рівня громадської довіри та мобілізації суспільства у протидії тероризму [1].

Метою нашого дослідження є визначення сутності стратегічних комунікацій та обґрунтування їхнього значення у підвищенні ефективності антитерористичної діяльності Служби безпеки України.

Варто відзначити, що у науковій літературі стратегічні комунікації розглядаються як системна, цілеспрямована діяльність органів державної влади, спрямована на формування, підтримання та просування наративів, що відповідають національним інтересам і забезпечують довіру суспільства [2]. Вони охоплюють такі складові, як публічна дипломатія, комунікаційний менеджмент у кризових ситуаціях, взаємодія з медіа, інформаційні операції, а також соціальна реклама та роз'яснювальні кампанії [3].

Європейські підходи до стратегічних комунікацій базуються на принципах прозорості, достовірності, відкритості та координації між урядовими структурами. В Україні концепція стратегічних комунікацій закріплена у Доктрині інформаційної безпеки України (2017) та Стратегії комунікацій у сфері євроатлантичної інтеграції України на 2018–2025 роки, де визначено, що ефективна комунікаційна політика є складовою національної безпеки [4].

Зауважимо, що у контексті антитерористичної діяльності стратегічні комунікації виступають інструментом протидії дезінформації, запобігання панічним настроям у суспільстві та забезпечення узгодженості дій силових структур із громадськістю. Вони, у свою чергу, дозволяють координувати інформаційні повідомлення під час кризових

ситуацій, налагоджувати міжвідомчу взаємодію та зміцнювати стійкість суспільства до ворожих інформаційних впливів.

Таким чином, стратегічні комунікації виступають невід'ємним елементом сучасної системи державного управління у сфері національної безпеки, забезпечуючи інформаційне підґрунтя для ефективної реалізації антитерористичних заходів.

Служба безпеки України є центральним органом, уповноваженим на реалізацію державної політики у сфері протидії тероризму. Одним із важливих напрямів її діяльності є інформаційно-комунікаційна взаємодія із суспільством, що спрямована на формування довіри громадян до дій силових структур, забезпечення інформаційної відкритості та запобігання поширенню деструктивних наративів

Відповідно до Закону України «Про боротьбу з тероризмом» (2003 р.), СБУ зобов'язана не лише здійснювати оперативно-розшукові заходи, а й проводити роз'яснювальну роботу серед населення з метою попередження терористичних проявів та підвищення рівня обізнаності громадян щодо загроз національній безпеці [5]. У цьому контексті стратегічні комунікації виступають не допоміжним, а системоутворювальним елементом антитерористичної політики.

З огляду на виклики гібридної війни, СБУ активно використовує інструменти стратегічних комунікацій для інформаційної протидії дезінформаційним кампаніям противника, поширення достовірних повідомлень про результати антитерористичної діяльності та формування єдиного державного наративу у сфері безпеки. Наприклад, офіційні публікації та відеоматеріали СБУ в соціальних мережах і на офіційному вебсайті регулярно інформують суспільство про викриття агентурних мереж, попередження терактів та протидію диверсійним групам, що зміцнює інформаційний і морально-психологічний захист населення [1].

Окремий напрям діяльності СБУ полягає у взаємодії з медіа та громадськістю під час кризових ситуацій. Зокрема, комунікаційні підрозділи Служби оперативно реагують на фейки та інформаційні провокації, забезпечуючи публічне роз'яснення офіційної позиції. Такий підхід відповідає міжнародним стандартам кризових комунікацій, коли достовірна, своєчасна та прозора інформація знижує ризик паніки та недовіри [3]. Окрім того, СБУ проводить освітньо-профілактичні інформаційні кампанії спільно з закладами освіти, місцевими органами влади та громадськими організаціями. Ці заходи спрямовані на підвищення рівня кіберграмотності громадян, розпізнавання інформаційних маніпуляцій, а також попередження радикалізації молоді [2].

Застосування стратегічних комунікацій у діяльності СБУ є свідченням переходу від реактивної до проактивної моделі інформаційної безпеки, коли держава не лише реагує на загрози, а й формує власні безпекові наративи, спрямовані на консолідацію суспільства та підтримку національної стійкості. Таким чином, стратегічні комунікації виступають інтегрованим механізмом

забезпечення ефективності антитерористичної діяльності, оскільки вони поєднують аналітичну, інформаційну, освітню та іміджеву складові у межах єдиної державної політики безпеки. Водночас варто й зазначити, що попри зростання ролі стратегічних комунікацій у забезпеченні національної безпеки, процес їхнього впровадження у практичну діяльність Служби безпеки України стикається з низкою організаційних, кадрових, технологічних та нормативно-правових труднощів [2].

Однією з ключових проблем є відсутність цілісної комунікаційної стратегії у сфері антитерористичної діяльності, що ускладнює координацію між центральним апаратом СБУ, регіональними управліннями та іншими державними інституціями. Незважаючи на існування загальнодержавних документів стратегічного рівня – таких як Доктрина інформаційної безпеки України (2017) [4], їх імплементація у відомчі стандарти СБУ залишається недостатньою.

Кадровим викликом є нестача підготовлених фахівців зі стратегічних комунікацій, які б володіли досконалими знаннями у галузі психологічних операцій, кризового менеджменту, кіберкомунікацій і медіааналітики [6]. У більшості випадків комунікаційні функції виконують пресслужби, що обмежує можливості для довгострокового планування та стратегічного аналізу інформаційного середовища.

Технологічний аспект проблеми полягає у недостатньому рівні цифрової інфраструктури та аналітичних інструментів моніторингу інформаційного простору. У сучасних умовах, коли терористичні угруповання активно використовують соціальні мережі, месенджери та онлайн-платформи для вербування, координації дій і пропаганди, СБУ потребує системного впровадження технологій OSINT (Open Source Intelligence) та систем автоматичного аналізу інформаційних потоків [1].

Іншим викликом залишається інформаційна протидія іноземним впливам. російська федерація системно здійснює інформаційно-психологічні операції, спрямовані на дискредитацію СБУ, поширення фейків і підрив довіри до державних інституцій. Це вимагає постійного удосконалення механізмів інформаційного реагування та підвищення швидкості офіційних комунікацій у кризових ситуаціях. Також актуальною є потреба у зміцненні партнерських відносин із громадянським суспільством і медіа, які можуть стати провідниками достовірної інформації серед населення. Формування єдиної комунікаційної екосистеми «держава – суспільство – медіа» сприяє підвищенню інформаційної стійкості та протидії радикалізації.

Отже, подолання означених викликів потребує комплексного підходу, що включає: розроблення відомчої стратегії стратегічних комунікацій СБУ; впровадження освітніх програм підготовки комунікаційних фахівців у сфері безпеки; розвиток аналітичних платформ для моніторингу та прогнозування інформаційних загроз; посилення міжнародної співпраці у сфері інформаційної безпеки та обміну досвідом.

Таким чином, проведений аналіз засвідчує, що стратегічні комунікації є невід'ємною складовою сучасної системи забезпечення національної безпеки та виступають ефективним інструментом у реалізації антитерористичної політики держави. У діяльності Служби безпеки України вони забезпечують не лише оперативну взаємодію з громадськістю, але й формують інформаційну стійкість суспільства, сприяють зміцненню довіри до державних інституцій та консолідації громадян у протидії терористичним загрозам. Використання стратегічних комунікацій дозволяє СБУ своєчасно реагувати на інформаційно-психологічні атаки, запобігати поширенню фейкових повідомлень і формувати позитивний імідж Служби як гаранта національної безпеки. Завдяки системному застосуванню публічних комунікацій, інформаційних кампаній та кризового інформування, підвищується ефективність антитерористичної діяльності на всіх рівнях від профілактики радикалізації до оперативного реагування на загрози.

Водночас ефективність стратегічних комунікацій у СБУ стримується низкою організаційно-кадрових і технологічних проблем, серед яких: недостатня інтеграція комунікаційної політики у структуру безпекового менеджменту, обмеженість аналітичних інструментів моніторингу інформаційного простору, а також дефіцит підготовлених фахівців із кризових та безпекових комунікацій [6]. Для подолання цих викликів доцільним є: розроблення комплексної стратегії стратегічних комунікацій СБУ із чіткими механізмами реалізації; впровадження професійної підготовки комунікаційних спеціалістів у сфері безпеки; розширення використання сучасних аналітичних технологій OSINT для оперативного виявлення загроз; посилення міжвідомчої координації та партнерства з громадянським суспільством і медіа у рамках єдиної системи кризових комунікацій.

Отже, стратегічні комунікації виступають інформаційною опорою ефективної антитерористичної діяльності Служби безпеки України, сприяють посиленню довіри суспільства до держави та утвердженню цінностей демократичної безпеки. У перспективі вони мають стати інтегрованим компонентом державної політики безпеки, що забезпечуватиме не лише протидію тероризму, а й розвиток національної стійкості у широкому сенсі.

Список використаних джерел:

1. Служба безпеки України. Щорічна доповідь про результати діяльності у сфері протидії тероризму. Київ : СБУ, 2024. 42 с. URL : https://ssu.gov.ua/ (дата звернення: 28.10.2025).
2. Войтович Р. В. Стратегічні комунікації як інструмент державного управління. Державне управління: удосконалення та розвиток. 2020. № 5. URL: https://www.dy.nayka.com.ua/?op=1&z=1763 (дата звернення: 28.10.2025).
3. Гончаренко В. І. Теоретико-методологічні засади стратегічних комунікацій у системі національної безпеки. Інформаційне суспільство. 2021. № 1. С. 34–40. URL : https://iss.gov.ua/journal (дата звернення: 28.10.2025).

4. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України : Указ Президента України від 25.02.2017 № 47/2017. Офіційний вісник Президента України. 2017. № 5. Ст. 122. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 28.10.2025).
5. Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV. Відомості Верховної Ради України. 2003. № 25. Ст. 180. URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 28.10.2025).
6. Кошель П. М. Розвиток комунікаційних компетентностей у системі національної безпеки. Вісник Національної академії державного управління при Президентові України. 2021. № 3. С. 45–52. URL: https://visnyk-nadu.academy.gov.ua/ (дата звернення: 28.10.2025).

КОЧИН В. Д.,
курсант, Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

КАЛЄНІЧЕНКО Л. І.,
доктор юридичних наук, професор,
завідувач кафедри,
Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ
(науковий керівник)

ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ЯК ІНСТРУМЕНТ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У СЕКТОРІ БЕЗПЕКИ: ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯЦІЯМ

У сучасному світі інформація стала одним із найважливіших ресурсів, що впливають на різні сфери життя, зокрема на безпеку держави. Інформаційні операції, як складова стратегічних комунікацій, відіграють ключову роль у забезпеченні національної безпеки. В умовах зростаючої загрози дезінформації та маніпуляцій, які можуть бути використані як інструменти гібридних війн, важливо зрозуміти, як інформаційні операції можуть бути ефективно використані для протидії цим викликам.

Метою є аналіз ролі інформаційних операцій у секторі безпеки, зокрема в контексті протидії дезінформації та маніпуляціям. Буде розглянуто, як інформаційні операції можуть зміцнити інформаційну стійкість суспільства, підвищити обізнаність громадян і забезпечити ефективну комунікацію між державними структурами та населенням.

Інформаційні операції охоплюють широкий спектр дій, спрямованих на формування, поширення та управління інформацією з метою досягнення стратегічних цілей. Стратегічна комунікація охоплює цілеспрямовані програми та заходи, спрямовані на встановлення

ефективного діалогу з основними аудиторіями. Це реалізується через механізми зв'язків із громадськістю, публічну дипломатію, інформаційні кампанії та спеціальні операції, які забезпечують цілісність і ефективність комунікативних процесів [1, с. 224]. У секторі безпеки ці операції можуть включати в себе як проактивні, так і реактивні дії. Проактивні інформаційні операції спрямовані на запобігання загрозам і формування позитивного іміджу держави. Основні цілі проактивних дій включають:

- формування довіри (допомагають створити довіру між державними інститутами та населенням). Це може бути досягнуто через відкриту комунікацію, інформування громадян про діяльність сил сектору безпеки та їхні досягнення;
- підвищення обізнаності (інформаційні кампанії, спрямовані на підвищення обізнаності населення про загрози, такі як тероризм або дезінформація, є важливими проактивними заходами). Це дозволяє громадянам краще розуміти ризики та реагувати на них;
- зміцнення іміджу (проактивні дії можуть включати в себе PR-кампанії, які сприяють формуванню позитивного іміджу сил сектору безпеки). Це може бути особливо важливим у часи криз, коли довіра до державних інститутів може бути підірвана;
- співпраця з громадськістю (ініціативи з залучення громадян до співпраці з поліцією та іншими державними структурами). Це може бути реалізовано через програми громадського контролю або волонтерські проекти.

Реактивні інформаційні операції, навпаки, спрямовані на реагування на вже існуючі загрози або кризи. Основні цілі реактивних дій включають:

- швидке реагування на дезінформацію: у разі виникнення дезінформації або неправдивих новин, реактивні інформаційні операції спрямовані на оперативне спростування цих відомостей. Це може включати в себе випуск офіційних заяв, прес-релізів або використання соціальних медіа для розповсюдження правдивої інформації.
- управління кризами: реактивні дії також включають в себе управління кризовими ситуаціями, такими як терористичні акти або природні катастрофи. У таких випадках важливо швидко інформувати населення про заходи безпеки та дії, які вживаються для вирішення ситуації.
- відновлення довіри: після кризи або інциденту, реактивні інформаційні операції можуть бути спрямовані на відновлення довіри до державних інститутів. Це може включати в себе відкриті

зустрічі з громадянами, де обговорюються вжиті заходи та плани на майбутнє.

- аналіз та оцінка загроз: реактивні операції також включають в себе аналіз і оцінку загроз, які виникають у результаті дій противника. Це дозволяє адаптувати стратегії та методи роботи сил сектору безпеки.

Однією з основних загроз у сучасному інформаційному середовищі є дезінформація. Вона може мати різні форми, включаючи фальшиві новини, маніпуляції з фактами та спотворення інформації. Наприклад, фейкове повідомлення зазвичай побудоване таким чином, щоб зацікавити, привернути увагу, тому воно дуже швидко поширюється. Крім того, фейкові новини зазвичай спрямовані на емоційне сприйняття [2]. Дезінформація може використовуватися для дестабілізації суспільства, підриву довіри до державних інститутів та створення паніки серед населення. У цьому контексті інформаційні операції стають важливим інструментом для виявлення, спростування та нейтралізації дезінформації. Одним із прикладів успішної протидії дезінформації є використання соціальних медіа для швидкого реагування на неправдиву інформацію. Державні органи можуть створювати спеціалізовані команди, які моніторять інформаційний простір, виявляють дез-інформацію та оперативно реагують на неї. Такі команди можуть використовувати різноманітні канали комунікації, включаючи офіційні веб-сайти, соціальні мережі та медіа, щоб донести правдиву інформацію до громадян.

Важливим аспектом інформаційних операцій є навчання населення критичному мисленню. Громадяни повинні вміти розпізнавати дезінформацію та маніпуляції, що дозволить їм краще захищати себе від негативного впливу. Державні органи можуть організовувати тренінги, семінари та інформаційні кампанії, спрямовані на підвищення медіаграмотності населення. У Концепції впровадження медіаосвіти в Україні (2016) поняття «медіаграмотність» визначено складовою медіакультури, що стосується вмінь користуватися інформаційними технологіями, «виражати себе і спілкуватися за допомогою медіазасобів, свідомо сприймати і критично тлумачити інформацію, розуміти реальність, сконструйовану медіаджерелами, осмислювати владні стосунки, міфи і типи контролю, які вони культивують» [3]. Також важливо зазначити, що інформаційні операції не повинні обмежуватися лише протидією дезінформації. Вони повинні включати в себе активну комунікацію з громадянами, що дозволяє формувати довіру та підтримку з боку суспільства. Державні органи повинні бути відкритими до діалогу, враховувати думки громадян та реагувати на їхні запити.

Успішні інформаційні операції також потребують співпраці між різними державними структурами, приватним сектором та громадськими організаціями. Громадські організації забезпечують уряд аналітичними

даними, допомагають розробляти й вдосконалювати нормативно-правову базу, надають експертні оцінки соціальних реформ і контролюють їхнє впровадження. Співпраця з державою дозволяє оперативно реагувати на зміни у соціальній сфері, забезпечуючи ефективний розподіл ресурсів і якісне надання послуг [4, с. 390]. Спільні зусилля можуть забезпечити більш ефективну протидію дезінформації та маніпуляціям. Наприклад, співпраця з медіа може допомогти у поширенні правдивої інформації та спростуванні фальшивих новин. Журналісти можуть допомогти в перевірці фактів, що дозволяє уникнути поширення неправдивої інформації. Медіа можуть виступати як посередники, які доносять правдиву інформацію до широкої аудиторії. Медіа можуть допомогти в створенні контенту, який пояснює складні теми, запобігаючи їх спотворенню. Спільні прес-конференції та брифінги з медіа забезпечують прозорість і довіру до інформації.

Отже, інформаційні операції є важливим інструментом стратегічних комунікацій у секторі безпеки. Вони дозволяють не лише протидіяти дезінформації та маніпуляціям, але й зміцнювати довіру до державних інститутів та підвищувати обізнаність населення. У сучасному інформаційному середовищі, де дезінформація може мати серйозні наслідки, важливо використовувати всі доступні ресурси для забезпечення інформаційної безпеки. Співпраця між державними структурами, приватним сектором та громадськістю є ключем до успіху в цій сфері. Тільки спільними зусиллями можна створити стійке інформаційне середовище, яке захистить суспільство від загроз дезінформації та маніпуляцій.

Список використаних джерел:

1. Стратегічні комунікації для безпекових і державних інституцій : практичний посібник / Л. Компанцева та ін. ; за ред. О. Давліканової, Л. Компанцевої. Київ : ТОВ «ВІСТКА», 2022. 278 с.
2. Посмітна В. В. Особливості антиукраїнської маніпулятивної пропаганди в сучасних умовах. Науковий вісник Міжнародного гуманітарного університету. 2023. № 59. Том 3. С. 35–39.
3. Концепція впровадження медіаосвіти в Україні. URL: ms.detector.media/.../ kontseptsiya_vprovadzhennya_mediaosviti_v_ukraini_nova_red.
4. Ігонін Р.В. РОЛЬ ГРОМАДСЬКИХ ОРГАНІЗАЦІЙ В ІНФОРМАЦІЙНО-ПРАВОВОМУ ЗАБЕЗПЕЧЕННІ СОЦІАЛЬНОГО ЗАХИСТУ НАСЕЛЕННЯ. Науковий вісник Ужгородського Національного Університету, 2025, Серія ПРАВО. Випуск 88: частина 2. DOI: https://doi.org/10.24144/2307-3322. 2025. 88.2.53.

КУЗНЄЦОВА В. Ю.,
курсант, Навчально-науковий інститут
поліцейської діяльності
Національної академії внутрішніх справ

ПЕРКАТИЙ І. Р.,
курсант, Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

ПЕРКАТИЙ Р. М.,
кандидат педагогічних наук,
старший викладач кафедри вогневої підготовки,
Національна академія внутрішніх справ
(науковий керівник)

ЦИВІЛЬНО-ВІЙСЬКОВА ВЗАЄМОДІЯ ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

З початком повномасштабного вторгнення РФ на територію України, наша країна зазнала неабияких змін, особливо ця ситуація вплинула на суспільство. 24 лютого 2022 року багато українців мусили зробити важкий вибір у своєму житті – залишитися на території держави чи виїхати за кордон. Але важливим є не тільки те, де вони перебувають, а й те, що відчувають і як наближують нашу перемогу, оскільки й серед тих осіб, які залишились в Україні, є люди, які намагаються заробити за рахунок воєнного стану, розкрадаючи предмети гуманітарної допомоги, зброю та фінанси.

Після того, як Російська Федерація розпочала повномасштабне вторгнення в Україну, порівняно менша за чисельністю та гірше оснащена українська армія швидко перейшла до активних дій. Серед українських військових на передовій були й офіцери цивільно-військового співробітництва (далі – ЦВС), які здатні відігравати життєво важливу роль у захисті цивільного населення, взаємодіючи із провідними представниками громад, допомагаючи військовим командирам оцінювати гуманітарну обстановку з метою підвищення ефективності військових операцій та зменшення шкоди для цивільного населення внаслідок бойових дій, а також допомагаючи координувати діяльність цивільних та військових органів влади. Під час російських бомбардувань, які часом були безжалісними і невибірковими, українські офіцери ЦВС допомагали інформувати цивільне населення про правила поведінки під час комендантської години та на блокпостах, особисто евакуювали цивільне населення або допомагали координувати його евакуацію, а також надавали підтримку у відновленні об’єктів критичної інфраструктури [1, с. 1].

В умовах дії воєнного стану дуже важливим аспектом є взаємодія військових і цивільного населення, оскільки не завжди збройні сили

можуть швидко вивчити місцевість і знайти все необхідне для нормального перебування в тій чи іншій обстановці. Цивільне населення набагато краще орієнтується в місцях, де вони проводять велику частину свого життя, також соціум зобов'язаний підтримувати військових, оскільки сили оборони безпосередньо захищають нашу країну і без них ми всі могли б навіть не уявляти свого теперішнього таким, яким воно зараз є. Збройні конфлікти не стосуються лише військовослужбовців, вони залишають свій відбиток на кожному українцеві незалежно від того чи він цивільна особа, чи військовий. Доки Збройні Сили України намагаються зберегти нашу незалежність і суверенітет, дії цивільного населення активно спрямовані на відбудування всього зруйнованого в умовах воєнного стану і в післявоєнний період ця діяльність також буде зосереджена в руках звичайних людей, тому цивільне населення потребує захисту і підтримки зараз задля щасливого майбутнього потім.

З початком повномасштабного вторгнення РФ 2022 року потреба Збройних Сил України (ЗСУ) у здійсненні заходів ЦВС значно зросла. Механізми ЦВС досі продовжують адаптуватися до масштабу та темпів конфлікту, що загострило багато вже наявних проблем, серед яких обмежені можливості для підготовки офіцерів ЦВС, нестача транспортних засобів для забезпечення доступу підрозділів ЦВС до постраждалих громад, а також відсутність законодавства, яке б чітко визначало завдання та повноваження офіцерів ЦВС. Наприклад, через стрімке формування Сил територіальної оборони (ТрО) офіцери ЦВС, призначені до складу ТрО, не проходили професійний відбір або підготовку за програмою ЦВС. Багато з них до переведення на ці посади працювали в інших сферах або мали іншу спеціальність. Крім того, термінове перетворення багатьох цивільних адміністрацій на військові адміністрації (ВА) спричинило певну плутанину щодо розподілу повноважень, а також конфлікт між ВА та військовим командуванням [1, с. 1–2].

Згідно з Законом України (далі – ЗУ) «Про внесення змін до деяких законів України у сфері національної безпеки і оборони щодо надання допомоги на догоспітальному етапі та здійснення цивільно-військового співробітництва» від 20.11.2024 року було внесено зміни до деяких ЗУ, наприклад, ЗУ «Про оборону України» було доповнено поняттям ЦВС, а саме:

«цивільно-військове співробітництво – комплекс заходів Збройних Сил України та інших військових формувань, утворених відповідно до законів України, щодо координації та взаємодії з органами виконавчої влади, органами місцевого самоврядування, громадськими об'єднаннями, організаціями та громадянами з метою створення сприятливих умов для виконання Збройними Силами України покладених на них завдань та функцій, у тому числі на території держави-агресора, а також інших заходів, спрямованих на формування у цивільного населення оборонної свідомості, готовності до національного спротиву» [2].

Військова доктрина передбачає, що підрозділи ЦВС є основними суб'єктами, на які покладено завдання координувати заходи захисту цивільного населення між новоствореними ВА та військовим командуванням. Таким чином, на нинішньому етапі війни офіцери ЦВС відіграють важливу роль у сприянні евакуації цивільного населення з небезпечних районів, слугуючи «містком» між ВА та військовим командуванням з питань евакуації. Вони також допомагають планувати інші заходи захисту та поширюють серед цивільного населення критично важливу інформацію – наприклад, про будівництво та розташування укриттів [1, с. 13].

Офіцери ЦВС співпрацюють із військовими адміністраціями, допомагаючи їм досягти різноманітних цілей, у тому числі таких:

- захист життя, здоров'я, фізичного та психологічного благополуччя мешканців територій, прилеглих до районів ведення бойових дій;
- допомога у задоволенні базових потреб громадянам, які проживають на тимчасово окупованих територіях або у так званих «сірих зонах»;
- надання додаткового захисту окремим категоріям вразливих громадян, зокрема внутрішньо переміщеним особам, особам з інвалідністю, людям похилого віку, дітям тощо;
- захист та відновлення об'єктів критичної інфраструктури, які перебувають у віданні місцевих державних адміністрацій;
- організація патріотичних та просвітницьких заходів [1, с. 14].

Відповідно до вищезазначеного ми можемо стверджувати, що дії ЦВС спрямовані на підтримку цивільного населення та певної координації їх дій у разі потреби. Військові можуть оцінити ситуацію, яка найменш зашкодить людям, і в подальшому за допомогою ЦВС скоординувати дії населення для їх захисту від загрози.

Однією з найважливіших функцій ЦВС на нинішньому етапі війни є допомога в оцінюванні операційного середовища за політичною, військовою, економічною, соціальною, інформаційною та інфраструктурною складовими (ПВЕСІІ), а також розробка покрокового плану евакуації цивільного населення та запобіжних заходів для мінімізації шкоди цивільному населенню. Аналіз ПВЕСІІ проводять для того, щоб дати військовим цілісне уявлення про цивільне середовище, та як усі ці фактори можуть сприяти або перешкоджати успішному виконанню бойового завдання. Він може мати вирішальне значення для забезпечення того, що військові сприятимуть захисту цивільного населення і не завдаватимуть йому шкоди під час ведення бойових дій. CIVIC (Центр з питань захисту цивільного населення в умовах конфлікту) дізнався, що підхід ПВЕСІІ не тільки став частиною процесу підготовки офіцерів ЦВС, але і його почали застосовувати в процесі прийняття рішень військовим командуванням. Наприклад, офіцери ЦВС

оперативного командування «Північ» використовують цей підхід для оцінки цивільного середовища та активно залучені до планування військових операцій [1, с. 16].

Незважаючи на певні попередження та ознаки наближення російської агресії, повномасштабне вторгнення РФ в Україну стало для багатьох суб'єктів всередині країни несподіванкою. Багато гуманітарних організацій також виявилися не готовими до масштабу та обсягу гуманітарних потреб, спричинених вторгненням, і стикалися з труднощами у наданні допомоги через обмеження доступу та безпекові обмеження. У той час як з'явилася ціла низка національних і волонтерських організацій, які допомагали реагувати на потреби, що виникали, українські військові, в тому числі офіцери ЦВС, відіграли значну роль у наданні гуманітарної допомоги прифронтовим населеним пунктам і евакуйованому населенню, допомагаючи задовольнити нагальні потреби, зокрема, доставляючи харчові продукти, одяг і опалювальне обладнання в Донецьку область, а також фільтри для очищення води в Житомирську та Миколаївську області. Дослідження CIVIC виявило кілька прикладів того, як офіцери ЦВС сприяли співпраці між військовими та волонтерськими організаціями для надання такої життєво важливої допомоги [1, с. 16].

Мета цивільно-військового співробітництва полягає у створенні сприятливих умов у ЦС для досягнення військових цілей шляхом організації та підтримання належного рівня цивільно-військової взаємодії з об'єктами цивільного середовища в районах виконання завдань за призначенням (дислокації) частин та підрозділів ЗСУ та інших складових сил оборони [3, с. 9].

До напрямків зосередження основних зусиль ЦВС під час стратегічного розгортання ЗСУ та інших складових сил оборони належать:

- забезпечення військового командування оперативною, достовірною та повною інформацію про стан цивільного середовища в регіоні та його вплив на виконання завдань стратегічного розгортання військ (сил);
- забезпечення ефективної взаємодії між військовим командуванням та регіональними об'єктами цивільного середовища, населенням регіону в інтересах стратегічного розгортання військ (сил);
- формування у цивільного населення сприятливого ставлення до військ (сил) шляхом роз'яснення правових засад їх дій, із залученням місцевих засобів масової інформації;
- недопущення блокування військових колон на шляхах розгортання або висування військ (сил), вантажів, місць дислокації, районів дій військ (сил) або обмеження свободи їх пересування;

- недопущення перешкоджання діяльності органам, що здійснюють мобілізаційне розгортання, та об’єктам цивільного середовища, які виконують мобілізаційні завдання;
- координація розгортання підрозділів гуманітарних організацій, інших об’єктів цивільного середовища для виконання заходів в інтересах оборони держави [3, с. 18].

Підсумовуючи, ми можемо стверджувати, що цивільно-військове співробітництво в умовах воєнного стану є дуже важливим, оскільки воно спрямоване на безпосередній захист цивільного населення в зоні бойових дій та поруч з ними. А підтримка народу забезпечує сильний дух нації, який не опускає руки перед труднощами і до кінця бореться за нашу перемогу. Також важливість пояснюється тим, що співпраця цивільних і військових осіб призводить до того, що перші не чинять непотрібних дій у панічному стані, так як дія ЦВС дає чіткі завдання і порядок порятунку в тій чи іншій ситуації.

Список використаних джерел:

1. Роль цивільно-військового співробітництва у захисті цивільного населення: досвід України. URL: https://civiliansinconflict.org/wp-content/uploads/2023/10/The-Role-of-CIMIC-in-POC_UKR_Final.pdf (дата звернення: 18.10.2024).
2. Про внесення змін до деяких законів України у сфері національної безпеки і оборони щодо надання допомоги на догоспітальному етапі та здійснення цивільно-військового співробітництва : Закон України від 20.11.2024 № 4068-IX // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4068-20 (дата звернення: 19.10.2025).
3. Доктрина «Цивільно-військове співробітництво». URL: https://sprotyvg7.com.ua/wp-content/uploads/2022/03/.pdf (дата звернення: 18.10.2024).

МАРТИНЕНКО М. С.,
працівник Збройних Сил України,
науковий співробітник
науково-методичного центру,
Воєнна академія імені Євгенія Березняка

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ В КОНТЕКСТІ МІЛІТАРНИХ ЗАСАД СУЧАСНОЇ РОСІЙСЬКОЇ АВТОКРАТІЇ

У контексті гібридної війни, яку веде російська федерація, інформаційно-психологічні операції (далі ІПсО) перетворилися на стратегічний інструмент, що поєднує пропаганду, дезінформацію та кібероперації з військовими діями [1, с. 156]. Авторитарний режим путіна використовує ці операції для збереження влади всередині країни та проекції сили за її межами, розглядаючи інформаційний простір як поле бою. За даними досліджень RAND Corporation та армійських публікацій США, російська концепція «інформаційного протиборства»

включає психологічний вплив на супротивника, населення та власні сили, з метою досягнення перемоги без значних втрат [1, с. 156]. У сучасній автократії ІПсО слугують для маніпуляції суспільною свідомістю, поділу союзників та виправдання агресії, як у випадку з Україною. Доповідь структурується навколо визначення, тактик, мілітарної інтеграції, прикладів та наслідків для режиму.

Інформаційні та психологічні операції росії кореняться в радянській традиції «активних заходів» і «рефлексивного контролю» – теорії, розробленої в 1960-х роках, яка передбачає маніпуляцію рішеннями супротивника через дезінформацію [2, с. 67]. У сучасній автократії путіна ІПсО еволюціонували в самостійну форму війни, як описано в Концепції кібербезпеки рф 2016 року та Доктрині інформаційної безпеки 2016 року [3, с. 33]. Режим розглядає інформаційний простір як продовження військового, де «інформаційне протиборство» включає психологічні атаки для деморалізації ворога та консолідації суспільства. Мілітарні засади автократії посилюються через інтеграцію ІПсО з гібридною війною, де дезінформація готує ґрунт для військових дій. Наприклад, у пострадянському просторі режим використовує наративи про «захист російськомовних» для виправдання інтервенцій, як у Грузії 2008 року, де пропаганда супроводжувала кібератаки. У внутрішній політиці ІПсО слугують для придушення дисидентства через закони про «фейкові новини» (2019 рік) та «іноземних агентів», що ізолюють суспільство від зовнішнього впливу, забезпечуючи стабільність автократії. Загалом, ІПсО є інструментом для «перемоги без жертв», де психологічний тиск замінює кінетичну силу, підкріплюючи мілітарну орієнтацію режиму.

Російські ІПсО базуються на моделі «вогняного шлангу брехні» – швидкому поширенні множинних суперечливих наративів для створення інформаційного хаосу [4, с. 45]. Тактики включають дезінформацію через державні ЗМІ (Russia Today, Sputnik), троль-фабрики та кібер-інструменти для хакерських атак і ботів.

У мілітарному контексті рефлексивний контроль створює передбачення щодо реакції супротивника та нав’язування йому помилкових рішень, як у «активних заходах» для поділу альянсів. Психологічні операції спрямовані на деморалізацію ворога через шокові ефекти (як ракети для терору) та маніпуляцію морально-психологічним станом власних сил через пропаганду «захисту вітчизни». У глобальному півдні (Африка, Латинська Америка) росія використовує антизахідні наративи, звинувачуючи НАТО у створенні та використанні біолабораторій чи неоколоніалізмі, для вербування найманців і створення альянсів.

Ще однією з тактик ізоляції населення від «деструктивного впливу» Заходу через цензуру та «суверенний інтернет» (закон 2019 року) є кіберінтеграція, яка включає хакерські групи (наприклад Fancy Bear) для витоку даних та електронної війни, як у 2007 році проти

Естонії. Подібна тактика ізолює, посилюючи мілітарний контроль над інформацією.

У сучасній російській автократії ІПсО інтегровані в доктрину «гібридної війни», де інформаційний фронт є продовженням військового, як описано в доктрині Герасимова 2013 року [5, с. 15]. Мілітарні засади режиму, що орієнтовані на «нове покоління війни», роблять ІПсО незалежною формою бойових дій, де психологічні атаки готують ґрунт для кінетичних операцій. Наприклад, у Криму 2014 року дезінформація про «захист росіян» супроводжувала «зелених чоловічків» – безмаркованих військових, що дозволило анексію без значних втрат. У глобальному півдні ІПсО підтримують військові інтервенції, як у Центральноафриканській Республіці, де пропаганда через Russia Today та тролів виправдовувала найманців Вагнера, забезпечуючи доступ до ресурсів для фінансування автократії. Внутрішньо ІПсО стабілізують режим через «морально-психологічне забезпечення» армії, де пропаганда протидіє «інформаційній експансії» Заходу, як у законах про «фейкові новини». Інтеграція з кібероперaціями (хакерство, електронна війна) робить ІПсО інструментом для паралізування супротивника, як у Грузії 2008 року, де кібератаки поєднувалися з дезінформацією. Для автократії це означає посилення контролю над суспільством, де інформація стає зброєю для запобігання «кольоровим революціям».

У війні проти України з 2014 року росія застосовувала ІПсО для деморалізації населення: дезінформація про «біолабораторії НАТО» та «нацистський режим» виправдовувала агресію, а рефлексивний контроль намагався впливати на уряд через фейкові новини [6, с. 56]. У глобальному півдні, як в Африці, ІПсО через Russia Today та тролів звинувачували Захід у неоколоніалізмі, вербуючи найманців для Вагнера (наприклад, з Куби та Малі), що фінансувало автократію. У Латинській Америці наративи про «антиімперіалізм» через Sputnik підтримували антизахідні режими, як у Венесуелі, для обходу санкцій. ІПсО в Центральній Азії маніпулювали «захистом російськомовних», як у Казахстані 2017 року, для виправдання військової присутності. Ці приклади показують, як ІПсО слугують мілітарним засадам автократії для проекції сили без прямих втрат.

ІПсО посилюють автократію, забезпечуючи внутрішню стабільність через цензуру та пропаганду, як закони про «іноземних агентів» 2012–2023 років, що ізолюють суспільство від західного впливу. Мілітарно ІПсО готують суспільство до війни, як наративи про «Велику Вітчизняну» для мобілізації. Глобально ІПсО обходять санкції, створюючи альянси на півдні для ресурсів (Африка) та вербування (Латинська Америка), фінансуючи військово-промисловий комплекс. Однак ризики включають репутаційні втрати та контрзаходи Заходу, як

заборона Russia Today в ЄС. Для автократії ІПсО – інструмент «перемоги без жертв», де психологічний вплив замінює кінетичну силу, але залежність від них робить режим вразливим до інформаційних контратак.

В доповіді розглянуто застосування інформаційно-психологічних операцій, які є фундаментом мілітарних засад сучасної російської автократії, перетворюючи інформацію на зброю для внутрішнього контролю та зовнішньої агресії. Вони дозволяють досягати цілей гібридної війни з мінімальними втратами.

Для протидії в інформаційній війні рф необхідно запровадити програми з медіа грамотності в школах, вищих навчальних закладах та для дорослих. Навчати розпізнавати фейки, перевіряти джерела та уникати емоційного реагування. Розробляти AI-інстументи для автоматичного виявлення фейків, аналізу наративів та блокування пропагандистських акаунтів.

Список використаних джерел:

1. Твердохліб М. І. Інформаційно-психологічні операції російської федерації проти України – основні етапи та цілі. *Вісник Львівського університету*. Серія «Міжнародні відносини». 2019. № 47. С. 156–172. URL: http://publications.lnu.edu.ua/bulletins/index.php/intrel/article/view/10352. (дата звернення: 21.10.2025).
2. Сидоренко О. В. Радянська спадщина в інформаційно-психологічних операціях Росії: активні заходи та рефлексивний контроль. *Військово-науковий вісник*. 2019. № 31. С. 67–74. URL: http://vnv.asv.gov.ua/index.php/vnv/article/view/231. (дата звернення: 21.10.2025).
3. Петренко Л. І. Російські доктрини інформаційної безпеки 2016 року: аналіз стратегій ІПсО. Кібербезпека: освіта, наука, техніка. 2020. Т. 8, № 1. С. 33–42. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/156. (дата звернення: 21.10.2025).
4. Бондаренко Т. П. Модель «вогняного шлангу брехні» в російських інформаційних операціях. *Вісник Київського національного університету імені Тараса Шевченка*. Журналістика. 2021. № 53. С. 45–52. URL: http://journ-knu.ua/article/view/234567. (дата звернення: 22.10.2025).
5. Григор’єв С. А. Доктрина Герасимова як основа гібридної війни Росії. Стратегічні пріоритети. 2017. № 2. С. 15–23. URL: https://niss.gov.ua/sites/default/files/2017-02/strategic-priorities-2-2017.pdf. (дата звернення: 22.10.2025).
6. Шевчук В. М. Інформаційно-психологічні операції Росії проти України: аналіз наративів (2014–2022). *Політичні науки та методика викладання суспільних дисциплін*. 2022. № 3. С. 56–64. URL: https://dspace.onua.edu.ua/items/2681d222-71dd-485d-b8d1-24ef46cd8085. (дата звернення: 23.10.2025).

НЕНЬКО Ю. П.,
доктор педагогічних наук, професор,
професор кафедри мовної підготовки,
Національний університет
цивільного захисту України

БЄЛЯЄВ Д. Ю.,
Національний університет
цивільного захисту України

ПРОФЕСІЙНА КОМУНІКАЦІЯ В СИСТЕМІ ПІДГОТОВКИ ТА ОПЕРАТИВНОЇ ГОТОВНОСТІ ФАХІВЦІВ ЦИВІЛЬНОГО ЗАХИСТУ

Професійна діяльність рятувальників належить до тих сфер, де точність і швидкість передавання інформації безпосередньо впливають на життя людей. У кризових ситуаціях комунікація стає не лише засобом координації дій, а й інструментом забезпечення безпеки, підтримання психологічної стійкості та взаємної довіри між членами команди. Рятувальні підрозділи працюють у високостресових умовах, коли будь-яке непорозуміння або затримка в обміні даними може призвести до фатальних наслідків. Тому формування високого рівня комунікативної компетентності особового складу є ключовою умовою ефективності служби цивільного захисту.

Комунікативна підготовка охоплює широкий спектр умінь: від чіткого, лаконічного мовлення та використання професійної термінології до вміння працювати в інформаційних системах, координувати дії з іншими службами, вести діалог із постраждалими та представниками громадськості. Важливим є не лише вивчення технічних засобів зв'язку, а й усвідомлення принципів інформаційної взаємодії: хто, кому, коли і в якій формі має передавати повідомлення. У межах оперативної роботи кожен член команди виконує певну комунікативну роль – від оператора центру прийому викликів до керівника рятувальної операції, і правильна організація цих ролей визначає результат усієї місії.

Досвід міжнародних служб реагування свідчить, що більшість труднощів під час ліквідації наслідків катастроф пов'язана не з нестачею ресурсів, а саме з порушеннями в комунікації. Це можуть бути неузгодженість дій між відомствами, різниця у термінології, перевантаження каналів зв'язку або відсутність спільної інформаційної картини подій. Для подолання цих проблем важливо розвивати у персоналу здатність швидко орієнтуватися в інформаційних потоках, відокремлювати головне від другорядного, а також підтримувати зворотний зв'язок, який гарантує, що повідомлення було почуте й зрозуміле.

Особливу роль у комунікативній підготовці відіграє формування ситуаційної обізнаності – здатності сприймати події навколо, усвідомлювати їх взаємозв'язки та прогнозувати розвиток ситуації. Ця обізнаність виникає лише за умови якісного інформаційного обміну. Кожен рятувальник повинен не просто отримувати накази, а розуміти загальний контекст операції: де знаходяться інші підрозділи, які ресурси доступні, які ризики існують у конкретний момент. Такий рівень усвідомлення забезпечується через систематичне тренування комунікаційних процесів у максимально наближених до реальності умовах.

Підготовка до комунікації має здійснюватися комплексно – у поєднанні мовленнєвих, когнітивних, технічних і психологічних складових. Насамперед формуються навички чіткої передачі усних та письмових повідомлень: вміння лаконічно формулювати думку, користуватися усталеними кодами й позивними, уникати двозначності. Паралельно відпрацьовується культура слухання – уміння уважно сприймати інформацію, уточнювати деталі та фіксувати ключові дані. На цьому етапі особливу увагу слід приділяти стандартизації мовлення: кожне повідомлення повинно мати чітку структуру – адресата, зміст, місце, час, підтвердження отримання.

Другою складовою є підготовка до роботи із засобами зв'язку та інформаційними системами. Сучасний рятувальник має впевнено користуватися радіостанцією, планшетом, навігаційним обладнанням, а також цифровими платформами для обміну даними. Це вимагає не лише технічної грамотності, а й розуміння логіки інформаційних потоків: які дані передаються вертикально – від керівництва до виконавців, а які горизонтально – між службами. Моделювання таких потоків у навчальному процесі дозволяє усвідомити роль кожного елемента системи та уникнути хаотичності під час реальних викликів.

Третій напрям підготовки стосується міжвідомчої комунікації. Рятувальники часто взаємодіють із медичними службами, поліцією, місцевими адміністраціями, волонтерами. Успішність спільних дій залежить від здатності швидко узгоджувати терміни, ресурси й відповідальність. Під час навчань варто створювати міжвідомчі команди, які відпрацьовують спільні сценарії реагування, тренують взаємне розуміння та вчяться використовувати єдину інформаційну мову.

Не менш важливим елементом є психологічна готовність до комунікації. Стрес, шум, фізична втома та емоційне напруження можуть призвести до втрати концентрації та агресивного стилю спілкування. Підготовка має включати розвиток емоційної стійкості, уміння зберігати самоконтроль, використовувати нейтральний тон, підтримувати командний дух і повагу до колег навіть у критичних умовах. Рятувальники повинні навчитися не лише передавати інформацію, а й регулювати власний психологічний стан, який впливає на ефективність комунікації.

Важливу роль відіграють і цифрові технології, що підтримують комунікацію у реальному часі. Сучасні системи управління рятувальними

операціями інтегрують голосові повідомлення, геолокацію, фото- та відеопотоки, сенсорні дані. Такі платформи дозволяють створити єдину інформаційну базу, доступну для всіх учасників операції. Водночас їх ефективність залежить від рівня підготовки користувачів: персонал має знати, як вводити, оновлювати та перевіряти дані, як фільтрувати інформацію, щоб не перевантажувати систему. Тому цифрова грамотність повинна стати обов'язковим компонентом комунікативного навчання.

Ефективна комунікація у рятувальних службах – це результат системного підходу, де технічна оснащеність поєднується з людським фактором. Розроблення тренінгових програм, симуляцій, рольових ігор та модульних курсів із комунікативної взаємодії дає можливість відтворити реальні умови кризових ситуацій, формувати автоматизовані навички реагування та взаємодії. Варто впроваджувати міждисциплінарні навчальні модулі, де майбутні рятувальники спільно з психологами, фахівцями з інформаційних технологій і комунікацій відпрацьовують алгоритми командної роботи.

Підсумовуючи, комунікативна підготовка рятувальників є не допоміжним, а центральним компонентом їх професійної освіти. Вона визначає якість управлінських рішень, знижує ризики, підвищує довіру та згуртованість колективу. У сучасних умовах комунікація стає ключем до ситуаційної обізнаності, а отже – до успішного виконання завдань із порятунку людей і ліквідації наслідків надзвичайних ситуацій. Формування цієї компетентності потребує постійного удосконалення програм підготовки, розвитку інформаційної інфраструктури та інтеграції цифрових рішень у практику служби цивільного захисту.

Таким чином, ефективна комунікація – це не лише технічний процес обміну повідомленнями, а комплексна культура взаємодії, що об'єднує знання, досвід, етику та психологічну готовність діяти спільно в умовах ризику. Саме від неї залежить успіх будь-якої рятувальної операції, а отже – життя і безпека людей.

Список використаних джерел:

1. Ненько Ю. П., Шевченко О. Т., Кришталь Т. М. Особливості підготовки фахівців екстрених служб до професійної комунікації під час надзвичайної ситуації. Перспективи та інновації науки (Серія «Педагогіка», Серія «Психологія», Серія «Медицина»): журнал. 2023. № 10(28), 2023. С. 328–341. DOI: https://doi.org/10.52058/2786-4952-2023-10(28)-328-340.

7 ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ СПЕЦІАЛЬНОЇ ФІЗИЧНОЇ ПІДГОТОВКИ ВІЙСЬКОВИХ ФОРМУВАНЬ ТА ПРАВООХОРОННИХ ОРГАНІВ

БОГДАНОВ М. В.,
Національна академія Служби безпеки України

ВПРОВАДЖЕННЯ ІДЕОМОТОРНОГО ТРЕНУВАННЯ В ОСВІТНІЙ ПРОЦЕС КУРСАНТІВ (СТУДЕНТІВ) У ВІЙСЬКОВИХ ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Військові заклади віщої освіти в умовах сьогодення є також потенційними цілями для агресора, як і критична інфраструктура України. Постійні сигнали «повітряної тривоги» та обстріли міст України змушують заклади вищої освіти (далі – ЗВО) функціонувати у складному режимі з постійним браком часу для викладання та засвоєння навчального матеріалу. У цих умовах доцільно розглянути необхідність впровадження ідеомоторного тренування у підготовку курсантів (студентів) військових ЗВО у зв'язку з обмеженням часу для вивчення технічних елементів рукопашного бою, подолання смуги перешкод та базових технічних елементів спортивних ігор. Проблема необхідності впровадження в процес фізичного виховання у ЗВО ефективних методів навчання розглядалась не лише нашими науковцями, але й іноземними фахівцями.

Ідеомоторне тренування широко застосовується у фізичному вихованні і спорті для підвищення ефективності процесу навчання руховим діям та вдосконалення навичок, а також з метою скорочення затраченого часу.

Ідеомоторика – мислене виконання дій, які мають бути впроваджені в тренувальному або змагальному періоді. Спеціальними дослідженнями встановлено, що коли людина подумки виконує які-небудь дії, у відповідних центрах кори головного мозку виникають нервові збудження, викликаючи ледь помітні скорочення певних м'язових груп. Тому уявне повторення певних прийомів та дій призводить до пожвавлення утвореної системи умовно рефлекторних навичок. Ось чому детальне уявне повторення рухів сприяє якнайшвидшому оволодінню руховими навичками та дозволить зробити процес навчання більш продуктивним, закріпити набуте.

У свою чергу, ідеомоторні рухи – це рухи м'язів, які відбуваються людиною несвідомо, в силу того, що вона дуже жваво уявляє собі виконання цих рухів. Такі рухи відносяться до методів психологічної саморегуляції, що представляє собою комплекс методів й програми

навчання, що спрямовані на формування внутрішніх засобів діяльності людини з керування власним станом.

Вони орієнтовані на навчання людини спеціальним прийомам довільної зміни власного стану, які надалі можуть використовуватися самостійно. У число таких методів включають: техніку нервово-м'язової релаксації, аутогенне та ідеомоторне тренування, прийоми сенсорного репродукування образів, езотеричні методи зміни стану свідомості та самогіпноз.

Психологічна підготовка спортсмена є важливим компонентом підготовки. З психології спорту написана велика кількість літератури, але в ній практично відсутня інформація відносно психологічної підготовки курсанта (студента) та використання ідеомоторного тренування під час їх навчання з дисципліни «Фізичне виховання, фізична підготовка». Такий розділ як практична психологія, а разом з нею й ідеомоторне тренування, проникає в спорт та фізичне виховання дуже важко, не говорячи вже про корисність використання ідеомоторного тренування впродовж навчання.

Ймовірно одна із причин того, що сучасні системи практичної психології не знайшли ще широкого застосування у фізичному вихованні курсантів (студентів), полягає у певних поглядах щодо їх фізичної підготовки й фізичного розвитку.

Зростаюче значення систематичних занять фізичними вправами у теперішній час, пов'язане зі специфікою діяльності у вищому навчальному закладі, а також стосуються способу життя студентської молоді. В свою чергу, специфіка діяльності військових закладів освіти потребує від відповідних установ розробки таких заходів, що здатні активізувати процес навчання, забезпечити високу ефективність використання засобів фізичної культури і спорту для зміцнення здоров'я й підвищення працездатності курсантів (студентів).

Будь-який процес навчання повинен підпорядковуватися таким групам педагогічних принципів:

– загальні принципи формування фізичної культури людини;

– методичні принципи фізичного виховання;

– принципи побудови занять у процесі фізичного виховання.

Фізичне виховання у вищому навчальному закладі – це вид виховання, специфічним змістом якого є навчання рухам, вдосконалення фізичних якостей, оволодіння спеціальними знаннями у галузі фізичної культури й формування потреби у заняттях фізичною культурою і спортом.

Навчання курсантів (студентів) з дисципліни «Фізичне виховання, фізична підготовка» у вищому військовому навчальному закладі доволі складний процес і потребує від викладача не тільки педагогічної майстерності, але й специфічних знань, завдяки яким курсанти (студенти) швидше опанують програмний матеріал. В природних умовах тренувального процесу дослідження про вплив попередньої дії в розумі

на ступне виконання рухів почали проводитися давно. Було встановлено, що уява викликає реальні зміни в частоті пульсу, подиху. Крім того, особливий інтерес полягає в тому, що зміни за своїм характером відповідають зрушенням при реальному виконанні рухів

Для розвитку м'язово-рухової уяви, що викликає попередні, мінімальні за інтенсивністю рухові імпульси рекомендується як можна ширше використовувати, наприклад, перегляд виконання технічних дій, зафіксованих за допомогою засобів запису відеозображення. Це дозволяє активніше формувати уяву про елемент, яка допомагає швидше «відчути», тобто запам'ятати інформацію в повному обсязі

«Негативного» впливу, який з'являється під час навчання технічних елементів, можна уникнути шляхом використання ідеомоторних вправ. У психології спорту ідеомоторна підготовка – це використання думки про рух, що викликає сам рух, сутність її полягає у розвитку здатності спортсмена викликати й аналізувати м'язове відчуття рухів, вносити в них корективи й опановувати керуванням рухів. До методів словесного, наочного й сенсорно-корекційного впливу можна від нести ідеомоторні, аутогенні й подібні їм методи. Ця специфічна група методів включає спеціальні способи спрямованого використання спортсменом образно го мислення, м'язово-рухових та почуттєвих уявлень для впливу на свій психічний і загальний стан, його регулювання й формування оперативної готовності до виконання певних вправ під час тренування або змагання. Зокрема, ідеомоторна вправа, являє собою уявне відтворення певної рухової дії з концентрацією уваги на вирішальних фазах його виконання. Також, відбувається вдосконалення психічного стану курсанта (студента) через підвищення впевненості, концентрації, спокою й урівноваженості. Під психологічною стійкістю розуміється цілісна характеристика особистості, що забезпечує її невразливість до стресогенного впливу складних ситуацій.

Однією з важливих складових умінь викладача з певного розділу фізичного виховання або виду спорту є уміння демонстрації ним рухових дій, тобто виконання технічних елементів. Результати досліджень показали, що використання ідеомоторного тренування позитивно сприяє вивченню, розвитку й удосконаленню технічних елементів. Виконання технічного елементу, яке планомірно і свідомо повторюється за допомогою уяви може застосовуватися на всіх етапах підготовки й на всіх курсах навчання курсантів (студентів). Активна уява виконання певних технічних дій сприяє більш швидкому оволодінню ними, зміцненню та коректуванню виконання, а також прискоренню процесу вдосконалення рухових умінь і навичок.

Механізм впливу ідеомоторного тренування виявляється в тому, що за рахунок використання м'язового потенціалу відбувається неусвідомлена й невидима іннервація м'язів, імпульсна структура якої відповідає рухам, що відчуваються, представляються або уявляються. Під час перегляду відеоматеріалу, де в уповільненому темпі показано

основні технічні елементи вправ курсант (студент) може чітко уявити себе в ролі виконавця, вносячи при цьому, уявні виправлення, саме в свої дії, знаходячись в пасивному стані. Таке уявне тренування може покращити техніку виконання прийому або дії, особливо якщо вона чергується з реальними фізичним вправами.

Під час освоєння й закріплення правильної техніки виконання кожного елементу, застосування імітаційних вправ й ідеомоторного тренування, дозволить швидше засвоїти техніку окремих елементів і краще підготуватися до виконання вправи (ідеомоторне тренування дозволяє скоротити час швидкості засвоєння технічних елементів). Це пояснюється тим, що у підсвідомість відкладаються образи виконання технічного елементу при спостереженні за виконанням дій викладачем або учасником відео зйомки та м'язові імпульси, що виникають при власній імітації цих рухів

Із формування рухової уяви починається процес безпосередньої роботи, що спрямований на засвоєння техніки. Перший етап розпочинається з відео демонстрації техніки виконання рухових дій. На другому і третьому етапах навчальний фільм періодично використовують для усунення значних та поширених помилок, що спотворюють техніку виконання рухової дії, і як наслідок – швидшого та якіснішого оволодіння нею.

Вивчення психологічної саморегуляції організму взагалі та ідеомоторного тренування зокрема, як структурної одиниці комплексної фізичної підготовки курсанта (студента), дозволило визначити, що саме із впровадженням у навчання прийомів ідеомоторного тренування можна розраховувати на підвищення технічної майстерності й психологічної надійності, підведення кінцевого результату до стану найвищої результативності під час контрольного виконання вправ.

Підсумовуючи можна зазначити, що впровадження даного способу навчання технічним діям в основний освітній процес курсантів (студентів) суттєво покращує формування у них правильної уяви про техніку рухової дії, скорочує час оволодіння нею, покращує результативність при виконанні вправи в цілому.

Список використаних джерел:

1. Круцевич Т. Ю. Теорія і методика фізичноговиховання : підр. для студ. вищ. навч. закл. фіз. виховання і спорту: у 2 т. Київ : Національний університет фізичного і спорту України, вид-во «Олімп. література»; 2017. Т. 2. 448 с.
2. Платонов В. М. Сучасна система спортивного тренування. Київ : Перша друкарня; 2020. 704 с.
3. Уейнберг Р. С. Основи психології спорту та фізичної культури / Р.С. Уейнберг, Д. Гоулд. Київ : Олимпийская литература,1998. С. 71–72.

БОНДАРОВИЧ О. П.,
Національна академія Служби безпеки України

ВПЛИВ СПОРТИВНИХ ТРЕНУВАНЬ НА ВОЛЮ ТА ПСИХОЛОГІЧНУ СТІЙКІСТЬ ВІЙСЬКОВОСЛУЖБОВЦІВ СБ УКРАЇНИ ПІД ЧАС ВИКОНАННЯ ОПЕРАТИВНО-БОЙОВИХ ЗАВДАНЬ

В умовах воєнного стану в Україні, забезпечення безпеки держави та готовності сектору безпеки і оборони до відбиття збройної агресії з боку Російської федерації визнано основним стратегічним напрямом реалізації державної політики у сфері національної безпеки і оборони.

До завдань Служби безпеки України в умовах воєнного стану входить попередження, виявлення, припинення розвідувально-підривної діяльності Російських спецслужб, розкриття злочинів проти миру і безпеки людства, тероризму, корупції, організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Всі ці завдання виконуються військовослужбовцями Служби безпеки України під час виконання оперативно-службових завдань в умовах збройного конфлікту. Тобто під впливом значних психічних та фізичних навантажень.

Досвід бойових дій показав зниження ефективності виконання оперативно-бойових завдань у зв’язку з недостатнім розвитком фізичних, вольових якостей а також недостатньої психологічної стійкості в екстремальних ситуаціях, які знаходяться в прямій залежності від фізичної підготовленості військовослужбовців. Питання розвитку зазначених якостей є ключовим питанням у сучасній спортивній психології. Ці якості формують основу успішної діяльності в умовах високої фізичної та емоційної напруги.

Розвиток вольових якостей та психологічної стійкості спортсменів є фундаментальним завданням сучасної спортивної підготовки. Вольові якості, такі як наполегливість, рішучість, самоконтроль і здатність до подолання труднощів, формують основу успішної спортивної діяльності. У свою чергу, стійкість – це здатність спортсмена зберігати емоційну рівновагу, витримувати фізичні та психологічні навантаження, а також адаптуватися до умов змагань.

Фізична підготовка забезпечує витривалість і силу, що слугують базою для виконання спортивних завдань. Проте психологічний компонент тренувань не менш важливий, оскільки саме він визначає здатність спортсмена ефективно діяти в умовах психологічного тиску та невизначеності [1].

Сучасні дослідження демонструють, що найбільший ефект у формуванні волі досягається завдяки інтеграції фізичних і когнітивних

технік. Наприклад, використання візуалізації успіху, самонавіювання та вправ на розвиток концентрації позитивно впливає на здатність спортсменів долати психологічні бар'єри. Такі підходи дозволяють посилити впевненість у собі, знижують рівень тривожності та підвищують готовність до виконання складних завдань. Саме тому одним із ключових аспектів тренувального процесу є поєднання фізичної підготовки та психологічного загартування.

Роль тренера у тренувальному процесі є надзвичайно важливою. Тренер виконує функцію наставника, мотиватора та психологічної підтримки. Стиль керівництва тренера має значний вплив на формування вольових якостей. Демократичний стиль, який базується на довірі, підтримці та заохоченні, сприяє зростанню самостійності та рішучості у спортсменів. Водночас авторитарний підхід може бути ефективним у короткостроковій перспективі, але часто призводить до емоційного вигорання.

Окрім індивідуальних тренувань, командна динаміка відіграє важливу роль у формуванні стійкості спортсменів. Дослідження свідчать, що позитивний психологічний клімат у команді сприяє підвищенню здатності долати труднощі та підтримувати високу мотивацію. Командні тренування, що включають елементи взаємодопомоги, координації та групової підтримки, підсилюють вольові якості, як-от колективна рішучість і взаємна відповідальність [5].

Особливу увагу слід приділити тренуванням зі спортивних єдиноборств. Саме такі види спорту найбільшою мірою наближені до складних ситуацій службово-бойової діяльності співробітників Служби безпеки України. Значне психологічне навантаження військовослужбовці СБ України отримують під час затримання а в разі крайньої необхідності і ліквідацію правопорушників, злочинців, терористів, та інших кримінальних елементів оскільки воно може супроводжуватись чиненням опору, іноді озброєного. Тому затримання є одним із найбільш небезпечних дій для здоров'я та життя співробітників СБ України. Так саме заняття спортивними єдиноборствами (рукопашним боєм, боротьбою, боксом, тощо) формують такі якості як сміливість, рішучість, самовладання та витримку, здатності до подолання внутрішніх і зовнішніх перешкод на шляху до виконання завдання, вміння діяти холоднокровно та ефективно в екстремальних умовах. Тому психологічна підготовка в спортивних єдиноборствах, зокрема використання когнітивних технік, таких як візуалізація, самонавіювання та дихальні вправи, позитивно впливає на здатність спортсменів долати стресові ситуації та адаптуватися до умов змагань. Такі підходи не лише зміцнюють впевненість у собі, але й підвищують загальну мотивацію та емоційну стійкість.

Ключовим етапом тренувального процесу є робота зі стресом. Високий рівень напруги під час змагань часто стає причиною зниження результатів. Техніки подолання стресу, такі як дихальні вправи,

медитація, контроль уваги, допомагають спортсменам швидше адаптуватися до екстремальних умов. Психологічна підготовка також включає розвиток мотивації, яка визначає здатність спортсмена ставити перед собою довгострокові цілі та наполегливо їх досягати [3].

На основі аналізу зазначеного можна зробити висновок, що інтеграція фізичних, психологічних та соціальних компонентів спортивних тренувань в службову діяльність військовослужбовців Служби безпеки України забезпечує найбільшу ефективність успішного виконання оперативно-бойових завдань.

Список використаних джерел:

1. Гатфілд К. Психологічна підготовка у спорті: тренування стійкості та впевненості. Київ : Науковий світ; 2020. 2-ге вид. 245 с.
2. Флетчер К. Вплив командної динаміки на емоційну стійкість спортсменів. Львів : Спорт і психологія; 2019. С. 123–154.
3. Харді Е. Гендерні аспекти розвитку стійкості у спортсменів: психологічний підхід. Дніпро : Видавництво ДДУ; 2020. 1-ше вид. С. 30–68.
4. Вайнберг Р. Психологія спорту: основи мотивації та вольових якостей. Харків : Основа; 2018. 3-тє вид. С. 45–87.

ВОЛКОВ М. С.,
Національна академія Служби безпеки України

ФОРМУВАННЯ ПСИХОЛОГІЧНОЇ ГОТОВНОСТІ ВІЙСЬКОВОСЛУЖБОВЦІВ ДО ДІЙ В ЕКСТРЕМАЛЬНИХ УМОВАХ ЗАСОБАМИ ФІЗИЧНОЇ ПІДГОТОВКИ

Довготриваюча російсько-українська війна довела, що сучасний бій – це надзвичайно важке випробування фізичних та духовних сил військовослужбовців, здатність діяти в у складних, небезпечних активно діяти у складних, небезпечних і стресових ситуаціях бойової обстановки, зберігаючи працездатність, самоконтроль та рішучість. Бій є жорстокою боротьбою між метою, мотивами, переконаннями, настроями, волею і думками з обох протидіючих сторін [3]. Високий рівень функціональної і фізичної підготовленості військовослужбовців є одним із основних аспектів, який сприяє їхній професійній майстерності та відповідальному виконанню службових обов’язків.

Фізичні тренування відіграють важливу роль у формуванні психологічної готовності військовослужбовців до дій в екстремальних умовах. Психологічна готовність є основою психологічної стійкості і дає змогу ефективно залучати військовослужбовців до службової діяльності та обирати оптимальну стратегію виконання завдань. Психологічна готовність до виконання бойових завдань може бути описана як комбінація специфічних психологічних властивостей та станів

особистості, що об’єднує особистісну та функціональну готовність [4].

Під час формування психологічної готовності особового складу надзвичайно важливим є врахування теоретичних і практичних аспектів їхньої професійної підготовки, оскільки ці аспекти сприяють особистісному зростанню фахівців, розвитку їхньої психологічної стійкості до тривалого нервово-психічного і фізичного навантаження, а також здатності адаптуватися до екстремальних умов та приймати рішення з мінімальним емоційним впливом та іншими важливими навичками. Головною метою психологічної підготовки є формування психічної стійкості та готовності особового складу до бойових дій (виконання завдань за призначенням) [1].

У провідних країнах НАТО накопичений дуже значний та цінний досвід у формуванні психологічної стійкості та бойової активності у військовослужбовців. Західні фахівці підходять до цієї проблеми комплексно. Вони розглядають існуючі наукові підходи до розуміння психологічної стійкості військовослужбовців як частину цілісних особистісних характеристик, окремих особистісних якостей, комбінацій різних особистісних чинників, стилю поведінки та іншого. Головним засобом фізичної підготовки військ Збройних Сил країн НАТО є спорт. Регулярні змагання на рівні Альянсу проводяться з дотриманням однакових правил, що сприяє уніфікації змісту та організації фізичної підготовки. Підвищення рівня бойової готовності фізичної підготовки досягається шляхом збільшення кількості військово-прикладних вправ у програмах і створення з них спеціальних комплексів. Зазвичай, ці комплекси розглядаються як самостійні розділи бойової підготовки, на які виділяється окремий час [5].

Фізична підготовка має великий потенціал для підвищення морально-психологічної готовності військовослужбовців, зокрема її психологічного аспекту. У наукових дослідженнях було доведено, що за допомогою фізичних тренувань можна збільшити стійкість організму до впливу психогенних факторів бойової діяльності на 30–40 % [2]. Фізична підготовка розглядається як єдиний процес, спрямований на поліпшення фізичної природи їхньої психологічної стійкості до тривалого нервово-психічного і фізичного навантаження, а також здатності адаптуватися до екстремальних умов та приймати рішення з мінімальним емоційним впливом та іншими важливими навичками. Головною метою психологічної підготовки є формування психічної стійкості та готовності особового складу до бойових дій (виконання завдань за призначенням) [1].

Фізична підготовка має великий потенціал для підвищення морально-психологічної готовності військовослужбовців, зокрема її психологічного аспекту. У наукових дослідженнях було доведено, що за допомогою фізичних тренувань можна збільшити стійкість організму до впливу психогенних факторів бойової діяльності на 30–40 % [5].

Враховуючи особливості психологічної підготовки військовослужбовців, варто зазначити наступне: заняття з фізичної підготовки

повинні включати такі елементи, як марш-кидки та багатоборство, долання вогневих смуг з вибуховими ефектами, пересування в умовах сильно пересіченої місцевості, а також включення завдань гірської підготовки, боксу і рукопашного бою; для спеціальної фізичної підготовки важливою є імітація реальних умов, навчання на незнайомій місцевості з умовною втратою зв'язку, збір особового складу у різний час доби, виконання завдань скороченим складом зі збільшенням психічного навантаження, метання бойових гранат, долання водних перешкод зі зброєю у складі підрозділу [5]. Фізичні тренування, які включатимуть зазначені елементи будуть ефективними для формування психологічної готовності військовослужбовців та сприятимуть розвитку морально-психологічних якостей, необхідних для успішного виконання бойових завдань в екстремальних умовах. Правильно організована фізична підготовка може стати важливим інструментом для формування психологічної готовності військових до дій в екстремальних умовах. Особисте знання військовослужбовцем своїх психологічних особливостей дозволяє контролювати свою психіку і діяти ефективно навіть у складних ситуаціях. Фізичні тренування будуть ефективними в контексті формування психологічної готовності у випадку правильної їхньої організації та врахуванні всіх важливих аспектів. Правильна організація фізичної підготовки може сприяти покращенню психологічного стану військовослужбовців і допомогти їм успішно подолати виклики, з якими вони зіштовхуються у сучасних умовах. В ході дослідження було також визначено, що особливий вплив на розвиток психіки мають техніки рукопашного бою, що дозволяють удосконалити прийоми та дії в умовах великого напруження та невизначеності. Залучення військовослужбовців до виконання рукопашних технік у складних умовах допомагає виховати в них такі психологічні якості, як мобільність і оперативність розуму, а також винахідливість і кмітливість. Ефективним у підготовці військовослужбовців є також кросфіт – високоінтенсивна фізична програма, яка поєднує елементи силової підготовки, кардіотренування та гімнастики і сприяє розвитку широкого спектра фізичних якостей та ментальної стійкості. Перспективами подальших досліджень може бути порівняння ефективності різних типів фізичних тренувань на формування психологічної готовності військовослужбовців, що допоможе з'ясувати, який підхід до фізичної підготовки є найбільш ефективним.

Список використаних джерел:

1. Жембровський С., Сич Р. Спеціальна фізична підготовка майбутніх офіцерів-прикордонників як складова формування їх готовності до професійної діяльності.
2. Вісник Національної академії Державної прикордонної служби України. 2019. № 3. URL: https://periodica.nadpsu.edu.ua/index.php/pedvisnyk/article/view/5 (дата звернення: 20.10.2025).
3. Капосльоз Г. Психологічна готовність військовослужбовців до бойової діяльності: системний підхід щодо діагностування, формування та підтримання

станів. Вісник Національного університету оборони України. 2023. № 72(2). С. 47–57. DOI: https://doi.org/10.33099/2617-6858-2023-72-2-47-57 (дата звернення: 20.10.2025).
4. Клочков В. Сучасні погляди на проблему формування психологічної стійкості військовослужбовців в умовах бойових дій. Вісник Національного університету оборони України. 2022. № 67(3). С. 71–79. DOI: https://doi.org/10.33099/2617-6858-2022-67-3-71-79 (дата звернення: 20.10.2025).
5. Лініченко Ю. А., Вознюк К. Г. Фізична підготовка у Збройних Силах провідних держав НАТО як засіб готовності до дій військовослужбовців в умовах воєнного стану. Modern problems of science, education and society : proceedings of the 4th International scientific and practical conference (Kyiv, June 19-21, 2023). Kyiv, Ukraine, 2023. С. 1148–1150. URL: https://er.chdtu.edu.ua/bitstream/ChSTU/4460/1/MODERN-PROBLEMS-OF-IENCEEDUCATION-AND-SOCIETY-19-21.06.23.pdf#page=1148 (дата звернення: 06.07.2025).
6. Українець В. М. Психологічна стійкість військовослужбовців: сутність поняття. Наукова дискусія: питання педагогіки та психології: матеріали міжнародної науково-практичної конференції (м. Київ, Україна, 3–4 грудня 2021 р.). Київ, 2021. С. 168–169. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/16684/1/2021.pdf#page=168 (дата звернення: 20.10.2025).

ВОРОНЦОВ О. С.,
кандидат педагогічних наук,
Національна академія Служби безпеки України

ВПЛИВ ЗАСОБІВ ВІЙСЬКОВО-СПОРТИВНИХ БАГАТОБОРСТВ НА ФІЗИЧНУ ПІДГОТОВЛЕНІСТЬ КУРСАНТІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Навченість військовослужбовців і їх командирів умілим діям в умовах сучасного бою, тобто тактиці, є одним із найважливіших показників рівня бойового навчання і запорукою успіху у вирішенні покладених на них завдань.

У сучасному загальновійськовому бою військовослужбовцям доводиться переходити до оборони в умовах безпосереднього зіткнення з противником – під час наступу чи після невдалого зустрічного бою. Вони змушені в ході бою захопити вигідний для оборони рубіж і під вогнем противника проводити всі роботи, пов’язані з організацією оборони. Складність такого переходу до оборони полягає в тому, що слід продовжувати бій і водночас вибирати позицію, обладнувати її в інженерному відношенні, організовувати систему вогню. Крім того, підрозділи спочатку будуть змушені оборонятися, маючи у своєму розпорядженні сили й засоби, з якими вели наступ.

Тому особливої ваги при підготовці вказаних підрозділів набуло:

– формування у командирів вміння: приймати сміливі, ініціативні, нестандартні рішення; обирати найбільш доцільний варіант побудови бойового порядку; організовувати самостійні дії у відриві від головних сил;

стійко та безперервно здійснювати управління підрозділом у складних умовах;

– навчання військовослужбовців різноманітним способам і прийомам пересування на полі бою із безперервним веденням розвідки противника (як у пішому порядку, так і на бойовій техніці), подолання інженерних загороджень та природних перешкод, умілого ведення вогню, прикриттю один одного під час виконання бойового завдання, дій у складі дрібних бойових груп – «двійок» та «трійок»;

– формування у підлеглого особового складу фізичної витривалості та психологічної готовності до виконання завдань в екстремальних умовах.

Водночас, стрімке зростання використання новітніх типів озброєння, специфіка виконання завдань з їх застосуванням під час бойових дій та кардинальна зміна тактики ведення бойових операцій вимагають перегляду підходів до підготовки військовослужбовців сектору безпеки та оборони.

Військова агресія Росії проти України обумовлює особливу потребу в підвищеному рівні підготовки, що стало пріоритетом у наукових дослідженнях, спрямованих на трансформацію професійного навчання майбутніх фахівців сектору безпеки та оборони у закладах вищої освіти зі специфічними умовами навчання.

Фізична підготовка військовослужбовців сектору безпеки та оборони України є невід'ємною частиною їхньої загальної підготовки. Вона спрямована на забезпечення військовослужбовців необхідними фізичними якостями для виконання вимог сучасних бойових завдань. Специфіка служби у підрозділах сектору безпеки та оборони вимагає здатності одночасно зосереджувати увагу на різноманітних об'єктах і діях. Запорукою високої бойової готовності та боєздатності особового складу сектору безпеки і оборони є необхідний рівень професійних знань, достатня мотивація, відмінний фізичний розвиток та високий функціональний стан основних систем організму військовослужбовців.

В умовах бойових дій останніх років виникла гостра потреба у радикальних змінах освітніх програм закладів вищої освіти, які здійснюють підготовку фахівців для сектору безпеки і оборони України. Реальна практика ведення бойових дій постійно змінюється, озброєння та військова техніка швидко вдосконалюються. Зміна воєнно-політичної ситуації у світі, поява нових зразків озброєння, сучасні способи ведення бойових дій вимагають постійного оновлення підходів та вдосконалення підготовки військових професіоналів. Це також підвищує вимоги до їхньої фізичної та психічної готовності до виконання завдань за призначенням.

Проведення низки реформ у підготовці військових фахівців сектору безпеки і оборони вимагає аналізу та радикальної зміни програм навчання бойової підготовки з урахуванням новітніх підходів, форм та способів застосування військ.

Перший науково обґрунтований підхід до структури та змісту програми спеціальної фізичної підготовки курсантів сектору безпеки і

оборони передбачає використання засобів військово-спортивних багатоборств.

Засоби військово-спортивних багатоборств включають в себе фізичні вправи для розвитку сили, витривалості, швидкості та спритності, а також специфічне обладнання, таке як пневматичні гвинтівки (пістолети) для стрільби, імітаційні гранати для метання та спортивний інвентар для подолання смуги перешкод.

Специфічні засоби та вправи:

– плавання: 50 метрів на час;

– стрільба: з пневматичної гвинтівки (пістолета);

– біг: на 100 метрів та на 3000 метрів;

– силові вправи: підтягування на перекладині;

– подолання смуги перешкод: включає елементи, що імітують подолання природніх та штучних перешкод;

– метання імітаційних гранат.

До цієї програми вперше включено виконання вправ зі стрільби з пневматичної зброї та виконання прикладних дій зі зброєю. Вона надає можливість розвитку лідерських якостей курсантів під час навчальних занять з дисципліни «Спеціальна фізична підготовка».

Ця програма спрямована на підвищення рівня спеціальної фізичної підготовленості курсантів сектору безпеки і оборони за допомогою використання засобів військово-спортивних багатоборств у навчальних заняттях. У розділах програми, таких як «Лижна підготовка», «Плавання», «Рукопашна підготовка», розширено кількість вправ військово-прикладного характеру, які наближені до реальних ситуацій бойових дій.

Науковцями виявлено, що сучасні методики і системи проведення змагань з багатоборств максимально адаптовані до реальних умов бою, тому не тільки підвищують рівень фізичної підготовленості курсантів сектору безпеки і оборони України, а й сприяють покращенню їх морально-психологічного стану на полі бою.

За допомогою засобів військово-спортивних багатоборств формується вольова та емоційна стійкість військовослужбовців. Зокрема, виховання сміливості та рішучості здійснюється під час виконання завдань, які є новими для виконання, зокрема ходьба по колодах, пеньках; подолання висотних перешкод; перестрибування траншей, парканів; влізання на високі перешкоди; стрибки у воду, подолання водних перешкод. Розвиток ініціативності, кмітливості та винахідливості відбувається у процесі розв’язання задач, які потребують прийняття самостійних рішень: подолання ділянок замкнутого простору; пірнання у довжину в обмундируванні; рукопашний бій. Вправи, які передбачають значних та тривалих фізичних навантажень та психологічного напруження, по типу марш-кидку, що поєднано із подоланням перешкод, транспортування пораненого, перенесення ящиків, перетягування мішків; переповзання по-пластунськи в складних погодних умовах, виховують у військовослужбовців наполегливість і завзяття. Виконання вправ, які

потребують точності руху, незважаючи на фізичні навантаження та психічне напруження, та відбуваються у швидкій динаміці змін (плавання в спорядженні та зі зброєю; відпрацювання дій у воді під час подолання водних перешкоду; затримка дихання під водою; перебування тривалий час у холодній воді; подолання елементів психологічної смуги перешкод) сприяють розвитку витримки і володіння собою.

З'ясовано, що правильний вплив на фізіологічний розвиток формує загальну морально-психологічну готовність захисника України. Найбільш ефективним засобом фізичної підготовки є впровадження в освітній процес майбутніх офіцерів військово-прикладних видів спорту, серед яких провідне місце займають військово-спортивні багатоборства, що мають комплексний вплив на розвиток курсантів, оскільки передбачають високий загальний рівень фізичної підготовленості у поєднанні із формуванням військово-прикладних навичок та вмінь.

ЄВТУШЕНКО В. В.,
Національна академія Служби безпеки України

РУКОПАШНИЙ БІЙ ЯК ІНСТРУМЕНТ ВИЖИВАННЯ В УМОВАХ БОЙОВИХ ДІЙ

Досвід бойових дій в Україні підтвердив, що діяльність військовослужбовців та співробітників Сил безпеки і оборони України, відбувається в критичних умовах, супроводжується значним фізичним і моральним напруженням, постійною втомою та іншими несприятливими факторами.

Діяльність відомств і структур сектору безпеки і оборони України має комплексний характер і здійснюється в специфічних, непередбачуваних умовах, іноді в стані підвищеного ризику. Це вимагає від співробітників високого рівня професійної підготовки, психологічної стійкості до екстремальних ситуацій, а також загальної та спеціальної фізичної витривалості. Володіння вогнепальною зброєю, спеціальними засобами та прийомами рукопашного бою є необхідними навичками. Безпосереднє оволодіння практичними навичками застосування фізичного впливу сприяє формуванню об'єктивної готовності фахівця Сил безпеки і оборони України до ефективних і своєчасних дій у протидії злочинцям з мінімальним ризиком для власного здоров'я та життя.

В умовах воєнного стану, коли загроза для життя та безпеки є надзвичайно високою, військовослужбовці Сил безпеки і оборони України зіштовхуються з численними викликами. Одним з ключових навичок, які допомагають забезпечити виживання та ефективне виконання службових обов'язків, є рукопашний бій. Це вміння має вирішальне значення у ближньому бою, коли можливості застосування вогнепальної зброї обмежені або неможливі. Розглянемо роль

рукопашного бою у військовій тактиці та способи його ефективного використання. Рукопашний бій є однією з найдавніших форм фізичного протистояння, яка пройшла еволюційний шлях від примітивних сутичок до цілісної бойової системи, важливої як у військових, так і в цивільних умовах. У період воєнного стану, коли загроза для життя та безпеки різко зростає, рукопашний бій набуває особливої актуальності як оптимальна система самозахисту та боротьби.

Різноманітні методи захисту та нападу відомі з моменту виникнення людського суспільства. Первісні люди, об'єднуючись у племена, використовували прості знаряддя праці для здобуття їжі, полювання та захисту від великих тварин. Подальший розвиток суспільства призвів до розпаду племінних структур, виникнення соціальних нерівностей і появи військових конфліктів. Методи ведення бойових дій еволюціонували та вдосконалювалися разом із розвитком озброєння, проте рукопашний бій залишався основним видом протистояння.

За часів Київської Русі, яка понад дві третини часу свого існування провела у війнах проти візантійців, половців, татар та інших народів, рукопашний бій набув значного поширення як система військового самозахисту та нападу. Постійна боротьба нашого народу проти ворогів виховала у воїнів такі якості, як мужність, завзятість, міцність духу, а також дозволила накопичити великий досвід бойового мистецтва. Набуті навички воїнів разом із талантами їхніх полководців сприяли здобуттю численних історичних перемог, завойованих безпосередньо в рукопашному бою.

Військовослужбовці Сил безпеки та оборони України можуть опинитися в ситуаціях, коли вони не можуть використовувати вогнепальну зброю або не можуть зробити це через загрози для цивільного населення. У таких ситуаціях навички рукопашного бою можуть забезпечити ефективний захист та контроль над ворогом. Це особливо важливо для правоохоронців, які працюють у зонах бойових дій.

Ключовим елементом рукопашного бою є здатність контролювати супротивника, не завдаючи йому зайвої шкоди. Військовослужбовці часто діють у обмеженому просторі, де кожен рух має бути ретельно продуманим. Контроль ситуації дозволяє приборкати супротивника, використовуючи його слабкі місця для подальшої нейтралізації загрози. Такі методи, як захоплення його за руки, опускання на землю та підтримка контролю, мінімізують ризик для військовослужбовця та інших. У критичних ситуаціях, коли контроль над супротивником неможливий, військовослужбовці можуть бути змушені застосовувати ударні прийоми для швидкої нейтралізації загрози. Ефективне нанесення ударів руками або ногами може вирішити конфлікт за лічені секунди, завдавши шкоди супротивнику та не давши йому продовжувати свої агресивні дії. Здатність правильно наносити удари та визначати

оптимальний момент для їх застосування є важливим елементом підготовки військовослужбовців Сил безпеки та оборони України.

Сучасні конфлікти, особливо під час війни, часто включають не лише традиційні бойові операції, а й партизанську війну, операції сил спеціального призначення та захист цивільного населення. За цих обставин майстерність рукопашного бою є невід'ємною частиною підготовки військовослужбовців, правоохоронців та спецпідрозділів. Тісний контакт з ворогом, раптові атаки або необхідність нелетальної оборони роблять рукопашний бій вирішальним елементом сучасної тактики підрозділів.

Самозахист у рукопашному бою під час воєнного стану охоплює не лише практичні фізичні навички, а й психологічну підготовку, яка сприяє збереженню контролю над ситуацією, швидкому ухваленню рішень та мінімізації ризиків. Військовослужбовці сил безпеки та оборони України мають бути готовими діяти у небезпечних умовах, де важливо не тільки нейтралізувати загрозу, але й запобігти подальшій ескалації насильства. Ефективна система самозахисту будується на зрозумілих і дієвих прийомах, які дозволяють миттєво реагувати на небезпеку навіть у стресових ситуаціях чи за обмежений час для дій.

Основними техніками вважаються:

– застосування захватів і блокувань, що сприяють контролю над рухами противника та унеможливлюють його подальші дії;

– порушення рівноваги, метод, який дозволяє ефективно використати силу опонента проти нього самого;

– точні та швидкі удари, спрямовані на слабкі місця тіла противника з метою усунення загрози.

Окрім традиційних технік рукопашного бою, ефективна система самозахисту також передбачає використання підручних засобів, таких як палиці чи ножі, які можуть виявитися дієвими у ближньому бою. У період воєнного стану ці засоби дозволяють військовослужбовцям діяти результативно тоді, коли стандартні методи захисту або нападу стають недоступними. Водночас фізична підготовка залишається основою для опанування навичок рукопашного бою.

Це включає розвиток сили, витривалості, координації рухів та швидкості реакції. У таких умовах військові та правоохоронці особливу увагу приділяють поєднанню фізичних тренувань із відпрацюванням практичних бойових навичок, аби досягти максимальної готовності до будь-яких сценаріїв. Крім фізичних якостей, значну роль відіграє й психологічна підготовка. Особовий склад має бути налаштований діяти у надзвичайних ситуаціях, де необхідно зберігати спокій і контролювати емоції. Тренування в умовах підвищеного стресу сприяють виробленню стійкості до впливу адреналіну та забезпечують здатність адекватно реагувати на небезпеку.

Рукопашний бій є невід'ємним елементом системи самозахисту та ведення бойових дій в умовах воєнного стану. Ефективна методика

охоплює як фізичну, так і психологічну підготовку, використання сучасних бойових прийомів і здатність швидко адаптуватися до динамічних умов конфліктів. Опанування навичок рукопашного бою має величезне значення, адже саме вони можуть стати ключем до збереження життя та забезпечення безпеки тоді, коли інші способи захисту виявляються недоступними або малоефективними.

Список використаних джерел:

1. Євтушенко В. В., Бондарович О. П., Денисюк О. В., Івахно О. В. Спеціальна фізична та психологічна підготовка співробітників СБ України до оперативно-службової діяльності в умовах підвищеного ризику : навч. посібник. Київ : НА СБУ, 2016. 300 с.
2. Пожидаєв М. Ю. Фізична підготовка курсантів ЗВО зі специфічними умовами навчання під час воєнного стану в Україні. Scientific Collection «InterConf». 2024. С. 290–296.
3. Чумак І. О., Олійник Н. А. Рукопашний бій : повний курс рукопашної підготовки підручник для вищих навчальних закладів. Вінниця : ВНАУ, 2018. 258 с.

ІВАХНО О. В.,
Національна академія Служби безпеки України

ФІЗИЧНА ПІДГОТОВКА У ЗБРОЙНИХ СИЛАХ ПРОВІДНИХ ДЕРЖАВ НАТО ЯК ЗАСІБ ПСИХОЛОГІЧНОЇ ГОТОВНОСТІ ВІЙСЬКОВОСЛУЖБОВЦІВ ДО ДІЙ В ЕКСТРЕМАЛЬНИХ УМОВАХ (ВОЄННИХ ДІЯХ)

Участь військовослужбовців сектору безпеки і оборони України у миротворчих операціях вимагає від особового складу високого рівня бойової готовності. Даний факт пов’язаний з тим, що у сучасних умовах успішне використання бойової техніки та озброєння, якими б сучасними вони не були, залежить від людей, які ними керують, від їх професійної, морально-психологічної та фізичної підготовленості [3, 4].

У поліпшенні боєздатності Збройних Сил України велика роль належить і фізичній підготовці (далі – ФП), значення якої у зв’язку з революцією у військовій справі не зменшилася, а навпаки, продовжує рости, оскільки сучасний бій збільшує вимоги до здатності військово-службовців переносити значні фізичні і психічні напруження [5].

Значні, граничні фізичні і нервово-психічна навантаження, які доводиться переносити особовому складу в процесі сучасних воєнних дій, призводить до істотного зниження боєздатності військово-службовців. Найвиразніше це виявляється в погіршенні показників ведення вогню і здійснення маневру на полі бою, в зниженні прудкості і точності дій при використанні бойової техніки і зброї. Ступінь зниження боєздатності військовослужбовців в ході виконання бойових завдань

визначається величиною і характером навантажень, які переносяться, спеціальною виучкою, рівнем фізичної підготовленості, фізичного розвитку, станом здоров'я і іншими чинниками [1, 6].

У збройних силах провідних держав НАТО розробляються концепції фізичної готовності, спрямовані на завчасний розвиток у особового складу фізичних та психологічних якостей та військово-прикладних навичок, які забезпечують виконання бойових задач у різноманітних, у тому числі й екстремальних умовах [5].

На даний час у збройних силах провідних країн НАТО прийняті три різні концепції ФП військ:

концепція «придатності» – у Німеччині:

концепція «готовності» – у США та Великої Британії;

концепція «мобілізації» – у Франції.

Для організації кожної із цих концепції існує характерне визначене поєднання засобів, методів та організаційних форм, які у сукупності створюють направленість ФП військ.

Так, у *збройних силах Німеччини* для здійснення концепції фізичної «придатності» використовуються такі традиційні засоби, як гімнастика, легка атлетика, плавання та рухливі ігри у формі навчально-тренувальних занять. Зв'язок фізичної та бойової підготовки згідно з цією концепцією, здійснюється способом перенесення якостей та навичок, які сформовані та розвинуті у процесі ФП, у військово-професійну діяльність [6, 9].

Метою ФП вважається «виховуюча дія на цілісну людську особистість способом навчання рухам, укріплення здоров'я та раціонального використання вільного часу».

Високий рівень фізичного розвитку розглядається як необхідна умова успішного оволодіння військово-професійною діяльністю. У той же час підкреслюється, що військово-прикладні вправи не відносяться до фізичної підготовки і не повинні використовуватись у відведений для неї час.

Перенесення якостей та навичок, які отримані у результаті занять спортом, на військово-професійну діяльність, на погляд німецьких спеціалістів, забезпечуються усією системою навчання та виховання військовослужбовців.

Концепція фізичної готовності, яка прийнята у *збройних силах США* та Англії, направлена на забезпечення готовності військ функціонувати у будь-який час та в будь-яких умовах під дією фізичного та психологічного стресу. Для її здійснення передбачається використання військово-прикладних засобів та методів. Традиційні засоби ФП виконують при цьому підготовчу та допоміжну функції. Для ФП військ характерним є прагнення реально змоделювати бойові навантаження [6, 8].

Принцип моделювання навантажень передбачає також періодичне створення екстремальних ситуацій, які вимагають від особового складу

граничного фізичного та психологічного напруження. З цією метою у арміях США та Великої Британії практикуються тривалі переходи за дуже пересіченою місцевістю, у пустелі чи болотах, у негоду і з викладкою, яка значно перевищує нормальну. Доведення солдат до повного знесилення вважається прекрасним засобом не тільки фізичного, але і психологічного загартування.

Із спеціалізованих курсів підготовки, що використовуються у *ЗС США*, можна виділити наступні:

«курс пригод», що являє собою скрите пересування у важко прохідній місцевості;

«курс мобільної підготовки», що включає в себе греблю на човні, плавання в обмундируванні та подолання спеціальних перешкод;

«курс повітряно-штурмової підготовки», що включає в себе посадку на вертоліт з трапу на висоті 15–20 метрів, безпосадкове десантування з канату із висоти 30–40 метрів та марш-кидок на 10 миль з повною викладкою у пересіченій місцевості.

Існують ще й спеціальні курси підготовки до дій у горах, у пустелі, у джунглях та арктичних районах. Сутність цих курсів становить тренування і перевірка стійкості, професійних навичок та ефективність бойової стрільби на фоні великих фізичних чи психологічних напружень.

Програми фізичної підготовки *збройних сил Великої Британії* включають в себе такі дисципліни: загальнорозвиваючу гімнастику, легку атлетику, плавання, футбол, баскетбол, бокс, дзюдо. Крім того, у частинах, що призначені для безпосередньої участі у бойових діях, програми фізичної підготовки доповнюються подоланням перешкод, рукопашним боєм та «курсом пригод», що являє собою комплекс прийомів та дій, пов’язаних з пересуванням у важкопрохідній місцевості, подолання природних та штучних перешкод на фоні виконання тактичних задач [6, 7].

У збройних силах Великої Британії є частини, бойове призначення яких визначає особливі вимоги до їх фізичної готовності. Це відноситься перш за все до парашутистів, морських піхотинців, розвідників та диверсантів. У зміст ФП включені стрибки з парашутом, скелелазіння, орієнтування, способи скритного та швидкого пересування у важкопрохідній місцевості, плавання з аквалангом, курс виживання в екстремальних умовах тощо.

Іншу позицію у цьому відношенні займають спеціалісти та командування *збройних сил Франції*. Вони вважають, що прогнозування та моделювання реальних бойових навантажень на заняттях з фізичної підготовки є ненадійним і недоцільним, тому що непомірне навантаження може нанести шкоду здоров’ю військовослужбовців та викликати у них стійке негативне відношення до занять ФП.

Головним компонентом фізичної готовності французи вважають здатність до повної мобілізації духовних та фізичних сил для

розв’язання конкретних завдань. Основними засобами виховання такої здатність, за їх, поглядами, є спортивне тренування та систематична участь у змаганнях. Регулярні заняття обраним видом спорту створюють стимул для досягнення найвищих результатів, чого неможливо домогтися звичайними методами ФП.

Характерною особливістю фізичної та психологічної підготовки французької армії є курс «Командо», що являє: собою комплекс прийомів та дій, які виконуються в умовах підвищеної небезпеки та ризику і пов’язані із значними фізичними та психічними навантаженнями [6].

У зміст курсу входять:

– «смуга ризику», окремі ділянки якої долаються під справжнім вогнем;

– скелелазіння;

– переправи через водні перешкоди;

– «втеча з полону»;

– «біг із танками»;

– «виживання у складних умовах» і ряд інших дій.

На відміну від бундесверу, де в основі фізичної підготовки також лежить спорт, французька система широко використовує військово-прикладні вправи та види спорту.

Спортивна направленість ФП збройних сил Франції відповідає системі їх комплектування переважно призовниками, для яких заняття спортом є стимулом для підвищення рівня своєї підготовки і одночасно мотивацією до військової служби, в той час як у США та Великої Британії найманих солдатів стимулює грошове утримання, розмір якого заложить безпосередньо від рівня їх військово-професійної, у тому числі і фізичної підготовки.

Командування НАТО за останні 10–12 років неодноразово вживало заходи для підвищення рівня фізичної готовності своїх військ. Інтенсифікація ФП військ провідних країн НАТО досягається по різному:

збільшенням службового часу, що відводиться на ФП (у Німеччині – до 4,5 годин на тиждень, у армій Франції та ВМС США – до 8 годин на тиждень);

використанням позаслужбового часу для різних оздоровчих та спортивних програм (програма «Біг заради життя», «Програма президентських нагород»);

стимулюванням досягнення високих результатів через матеріальну зацікавленість (США, Англія) або через масовий спорт (Німеччина, Франція);

вдосконаленням системи планування: в армії США при збереженні ліміту часу на ФП (3 години на тиждень) заняття проводяться щоденно від 15 до 45 хвилин;

виділенням військово-прикладних вправ у самостійні предмети бойової підготовки: рукопашний бій, курс «Командо» у Франції, курс амфібійної підготовки у США та інші;

застосуванням сучасних методів тренування: кругового, інтервального та інших;

вдосконаленням матеріальної бази;

підвищенням вимог та контрольних нормативів, а також ускладненням умов їх виконання. Нормативи підвищуються, головним чином, у вправах на загальну та силову витривалість за рахунок збільшення дистанції та кількості повторень (США). В усіх провідних арміях НАТО відпрацьовані таблиці оцінок, які стимулюють підвищення результатів фізичної підготовки.

Уніфікація ФП військ здійснюється як у середині збройних сил окремих країн, так і на рівні всього блоку НАТО в цілому. Основним засобом уніфікації ФП служить спорт. Багаточисленні спортивні змагання, які проводяться за єдиними правилами, сприяють формуванню єдиних вимог до змісту та організації ФП, особливо у тих країнах, де вона основана на спорті (Німеччина, Франція).

Велику роль в уніфікації ФП відіграють спортивні заходи, які проводяться у рамках регіональних командувань НАТО, такі як чемпіонати союзного командування мобільних сил у Європі чи змагання на приз Південно-Європейського командування НАТО.

Тенденція до уніфікації проявляється також у змісті контрольних нормативів по фізичній підготовці.

Наприклад, в армії США замість семи різних тестів, які використовувались раніше, випрацюваний єдиний армійський тест, до якого за змістом наближаються тести ВПС та ВМС. У той же час спостерігається і протилежний процес – спеціалізація програм та контрольних тестів з ФП [5].

Підвищення військової прикладності ФП військ країн НАТО здійснюється за рахунок збільшення у програмах кількості військово-прикладних вправ та створення спеціалізованих комплексів військово-прикладних вправ, прийомів та дій, таких як курс рукопашного бою, курс повітряно-штурмової та аеромобільної підготовки, курс диверсійно-розвідувальної підготовки.

Як правило, ці комплекси розглядаються як самостійні розділи бойової підготовки, і заняття з неї проводяться у спеціально відведений час.

Для підвищення військової прикладності ФП особлива увага звертається на розвиток найбільш важливих у військовій справі фізичні та психічні якості: витривалість, стійкість, самовладання, сміливість, агресивність, згуртованість та інших. З цією метою застосовуються комплекси вправ, які пов’язані з небезпекою та ризиком, командні та індивідуальні види спорту, такі як військові багатоборства, орієнтування, парашутним спорт, альпінізм та інші.

Для ФП військ НАТО у теперішній час характерним є підсилення психологічної направленості. У керівних документах підкреслюються тісний зв'язок і взаємозалежність фізичної та психологічної готовності військ.

Фізична підготовка розглядається як один із найважливіших компонентів повної бойової готовності, як базовий фактор для реалізації технічної та психічної готовності військ.

Найбільш важливим компонентами фізичної готовності вважаються: сила, силова та загальна витривалість, військово-прикладні рухові навички, а також психічні якості.

Вдосконалюється система перевірки та оцінки ФП з метою підвищення її об'єктивності, оперативності та адекватності задачам бойової підготовки: введення стандартного єдиного перевірочного комплексу (тесту) для усіх видів Збройних Сил; введення комплексних військово-прикладних тестів з фізичної підготовки для видів Збройних Сил; введення комплексних спеціалізованих тестів для родів військ та сил флоту, що поєднують фізичні вправи з високим навантаженням, професійні прийоми та бойову стрільбу.

Список використаних джерел:

1. Анохін Євген Дмитрович. Фізична підготовка в арміях провідних держав НАТО: навчальний методичний посібник. Львів : ЛВІ, 2005. 115 с.
2. Романчук С. В., Романчук В. В. Фізична підготовка в сухопутних військах збройних сил провідних держав НАТО. ЗБІРНИК НАУКОВИХ ПРАЦЬ. Вип. 14. Львів : 2010. Т. 2. 302 с.
3. Романчук С. В., Романчук В. В. Фізична підготовка в сухопутних військах збройних сил провідних держав НАТО. ЗБІРНИК НАУКОВИХ ПРАЦЬ. Вип. 14. Львів : 2010. Т. 1. С. 296–302.
4. Петрачков О. В. Особливості системи оцінювання фізичної підготовленості військовослужбовців провідних країн світу. Збірник наукових праць Педагогічна освіта: теорія і практика КПНУ імені Івана Огієнка. 2013. Вип. 15. С. 82–89.
5. Про рішення Ради Національної безпеки і оборони України від 14.09.2020 Індивідуальна фізична підготовка військовослужбовців за стандартами НАТО, як засіб психологічної готовності військовослужбовців до дій в екстремальних умовах (воєнних діях): військова навчально-методична публікація / Центр оперативних стандартів і методики підготовки ЗС України. Житомир. 2022. 94 с.
6. Пангелова Н. Є. Організація фізичної підготовки в арміях провідних країн світу. ВІСНИК КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКОГО НУ ІМЕНІ ІВАНА ОГІЄНКА. Кам'янець-Подільський, 2015. Випуск 8. С. 268–274.
7. Особливості організації та змісту систем фізичної підготовки у збройних силах держав-членів НАТО та України. Одеров А. М. та інші. УКРАЇНСЬКИЙ ЖУРНАЛ МЕДИЦИНИ, БІОЛОГІЇ ТА СПОРТУ. Київ, 2020. Том 5. № 2 (24). С. 271–282.
8. Одеров А. М., Шлямар І. Л., Балдецький А. В. Система перевірки та оцінювання фізичної підготовленості військовослужбовців збройних сил іноземних держав. МОЛОДА СПОРТИВНА НАУКА УКРАЇНИ. Львів : ЛДУФК, 2013. Т. 2. Вип.17. С. 109–113.
9. Фізична підготовка іноземних армій В. А. Щеголев, Г. Г. Дмитриєв, В. П. Сущенко та інші. Київ : НУФКС. 2007. 272 с.

КОВАЛЬЧУК Р. О.,
заступник начальника
кафедри фізичного виховання і спорту,
Національна академія
Державної прикордонної служби України
імені Б. Хмельницького

ГРИЦІВ М. С.,
курсант факультету безпеки державного кордону,
Національна академія
Державної прикордонної служби України
імені Б. Хмельницького

ФІЗИЧНА КУЛЬТУРА І ПСИХОЛОГІЧНА СТІЙКІСТЬ ПЕРСОНАЛУ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

У сучасних умовах тривалого воєнного стану та високого психологічного навантаження особливого значення набуває питання збереження ментального здоров'я військовослужбовців та всього населення України. Психологічна стійкість стає однією з ключових складових професійної готовності, особливо для персоналу Державної прикордонної служби України, який щодня виконує завдання підвищеної складності та ризику.

У межах Всеукраїнської програми з підтримки ментального здоров'я «Ти як?», започаткованої першою леді України Оленою Зеленською, соціологічна компанія Gradus Research провела другу хвилю дослідження, присвячену психологічному стану українців. Результати показали, що понад 70 % опитаних громадян регулярно відчувають стрес або сильну емоційну напругу, проте лише 2 % звертаються за допомогою до психологів.

Основними способами подолання стресу більшість респондентів називали перебування в інтернеті (39 %) та перегляд телепрограм (33 %), тоді як заняття спортом (11 %) і прогулянки на природі (16 %) опинилися серед найменш популярних способів розслаблення. Ця тенденція свідчить про низький рівень фізичної активності, що негативно впливає не лише на фізичний стан, а й на емоційне благополуччя людини.

Відповідно до даних Всесвітньої організації охорони здоров'я (ВООЗ), близько 25 % дорослого населення та понад 80 % підлітків не виконують мінімальних рекомендацій щодо фізичної активності. Організація наголошує, що для підтримання здоров'я необхідно щонайменше 150 хвилин швидкої ходьби або 75 хвилин бігу на тиждень.

Регулярні фізичні вправи сприяють не лише зміцненню тіла, але й розвитку психологічної стійкості, підвищенню стресостійкості, самоконтролю та емоційної врівноваженості. Для військовослужбовців ДПСУ фізична культура має особливе значення, адже допомагає зберігати

високу працездатність, оперативно реагувати на стресові ситуації, а також підтримувати моральний дух у складних умовах служби.

Регулярна фізична активність суттєво знижує рівень кортизолу – основного гормону стресу, який утворюється під час нервового напруження. Надлишок кортизолу негативно позначається на роботі організму, особливо на діяльності головного мозку, погіршуючи концентрацію, пам'ять і загальний психічний стан.

Під час рухової активності в організмі активізується вироблення ендорфінів та серотоніну – так званих «гормонів радості». Ці біологічно активні речовини допомагають покращити настрій, зменшити біль, знизити рівень тривожності й сприяють загальному психологічному комфорту. Науково доведено, що регулярні тренування покращують кровообіг у мозку, стимулюють утворення нових нервових клітин і позитивно впливають на його структуру.

Недостатня рухова активність, навпаки, підвищує ризик розвитку серцево-судинних захворювань, інсульту та цукрового діабету другого типу, які вважаються чинниками ризику когнітивного зниження та деменції.

Результати досліджень показують, що навіть 30 хвилин помірних фізичних вправ здатні значно зменшити прояви тривоги, а короткі прогулянки тривалістю 15–30 хвилин перед сном сприяють покращенню сну, когнітивних функцій і емоційної рівноваги. Посилення когнітивних можливостей, у свою чергу, підвищує увагу, пам'ять, мотивацію та сприяє швидшому навчанню. Включення фізичних вправ у щоденний режим сприяє формуванню стабільного позитивного настрою та підвищенню життєвого тонусу.

Під час виконання фізичних навантажень необхідно контролювати частоту серцевих скорочень (ЧСС), щоб уникнути перевантаження. Оптимальний показник максимальної частоти серцевих скорочень (МЧСС) обчислюється за формулою: 220 – вік (для чоловіків) або 226 – вік (для жінок). Під час тренувань не рекомендується перевищувати верхню межу МЧСС, адже це може негативно вплинути на серцево-судинну систему.

Які біохімічні процеси лежать в основі гарного настрою після занять спортом?

З точки зору фізіології та біохімії, позитивний вплив фізичних навантажень на емоційний стан людини пояснюється роботою гіпоталамо-гіпофізарно-надниркової системи. Саме вона відповідає за реакцію організму на стресові чинники. Регулярна рухова активність сприяє нормалізації її функціонування, що, у свою чергу, зменшує чутливість організму до стресу та підтримує внутрішню рівновагу.

Під час фізичних вправ у людини знижується рівень стресогенних гормонів – кортизолу, адреналіну, катехоламінів та адренокортикотропіну. Одночасно підвищується концентрація норадреналіну, серотоніну та ендорфінів, які відомі як «гормони задоволення». Вони активують центри винагороди в мозку, покращують настрій, підсилюють почуття задоволеності, формують мотивацію до дії, сприяють кращій самооцінці та підвищують впевненість у власних силах. Також ці процеси сприяють нормалізації сну й зниженню ризику тривожних і депресивних розладів.

Для військовослужбовців Державної прикордонної служби України, які щоденно працюють у стресових умовах, ці біохімічні механізми мають особливе значення. Фізична підготовка виступає не лише засобом зміцнення тіла, а й потужним інструментом психологічної стабілізації. Регулярні тренування допомагають підтримувати оптимальний рівень гормонів стресу, завдяки чому прикордонники легше адаптуються до емоційних навантажень, швидше відновлюються після кризових ситуацій і демонструють вищу стійкість до психічного виснаження.

Кортизол, який вважається основним маркером стресу, відіграє двояку роль. Його короткочасне підвищення під час фізичних навантажень сприяє мобілізації енергетичних ресурсів організму, проте після тренування його концентрація у крові знижується нижче початкового рівня. Дослідження показують, що після інтенсивних занять спортом рівень кортизолу може залишатися зниженим протягом 24–48 годин, що позитивно впливає на загальне самопочуття та психоемоційний стан.

Подібну динаміку демонструє і адреналін – гормон, який виробляється надниркovими залозами у відповідь на стрес і викликає збудження, прискорене серцебиття, дихання та реакцію «бийся або тікай». Після закінчення фізичних навантажень його рівень поступово знижується, сприяючи розслабленню, стабілізації серцево-судинної діяльності та відновленню емоційного балансу.

Таким чином, фізична активність виступає природним механізмом захисту організму від надмірного впливу стресу, запобігаючи розвитку тривожних і депресивних станів. Для персоналу ДПСУ систематичні заняття фізичною підготовкою є не лише елементом службової дисципліни, а й важливим чинником зміцнення ментального здоров’я, підвищення бойової готовності та формування психологічної стійкості в умовах сучасних викликів.

Список використаних джерел:

1. Всесвітня організація охорони здоров'я. Рівень фізичної активності для підтримання здоров'я: глобальні рекомендації. Женева : ВООЗ, 2020.
2. Gradus Research. Дослідження психологічного стану українців у межах програми «Ти як?» за ініціативи Олени Зеленської. Київ, 2023. URL: https://gradus.app.
3. Міністерство охорони здоров'я України. Фізична активність і психічне здоров'я: аналітичний звіт. Київ : МОЗ, 2023.
4. Зеленська О. Національна програма з ментального здоров'я «Ти як?». Офіс Першої леді України, 2023.
5. Круцевич Т. Ю., Воробйов М. І. Теорія і методика фізичного виховання. Київ : Олімпійська література, 2021. 368 с.
6. Савченко В. І., Шевченко О. А. Фізична підготовка військовослужбовців: методичний посібник. Харків : ХНУПС, 2022. 212 с.
7. Литвиненко В. В. Психологічна стійкість військовослужбовців в умовах бойової діяльності. Київ : НАДУ, 2020. 185 с.
8. American Psychological Association. Exercise and Stress: Get Moving to Manage Stress. APA, 2022. URL: https://www.apa.org.
9. Ratey, J. & Hagerman, E. Spark: The Revolutionary New Science of Exercise and the Brain. New York: Little, Brown and Company, 2019.
10. Сайт Державної прикордонної служби України. Фізична підготовка прикордонників як складова бойової готовності. URL: https://dpsu.gov.ua.

МАНЯК С. В.,
аспірант, Навчально-науковий інститут
«Придніпровська державна академія
фізичної культури і спорту»

ОТКИДАЧ В. С.,
доктор філософії,
старший викладач кафедри фітнесу
та адаптивного спорту,
Український державний університет
імені М. Драгоманова

ФІЗИЧНА ПІДГОТОВЛЕНІСТЬ КУРСАНТІВ СИЛ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

В умовах глобальної трансформації ведення бойових дій, постійного удосконалення тактики ведення бою, використання новітньої техніки стає нагальною проблема підготовки особового складу до продуктивної дії в цих умовах за максимально короткий термін.

Фізична підготовка військовослужбовців сектору безпеки та оборони є критично важливою для їх успішної діяльності в будь-яких умовах. Основні аспекти фізичної підготовки включають в себе збереження та підвищення фізичної сили, витривалості, швидкості, гнучкості та координації.

Програми фізичної підготовки для військовослужбовців зазвичай розробляються з урахуванням специфічних потреб сил сектору безпеки та оборони. Вони можуть включати в себе такі елементи, як:

1. **Силові тренування:** це включає у себе роботу з вагами, вправи з власною вагою тіла, а також використання спеціального обладнання для зміцнення м'язів;

2. **Кардіотренування:** збільшення витривалості серцево-судинної системи через біг, плавання, велосипед або інші види аеробної активності;

3. **Тактична фізична підготовка:** включає в себе тренування, спрямовані на розвиток навичок, які безпосередньо стосуються військової діяльності, таких як рухи в бойовій обстановці, навчання ефективному маневруванню, робота зі зброєю тощо;

4. **Гнучкість і координація:** вправи для поліпшення гнучкості та координації можуть допомогти у запобіганні травм та покращенні загального фізичного функціонування;

5. **Здоровий спосіб життя:** важливим елементом фізичної підготовки є також правильне харчування, відпочинок і здоровий сон.

Ці елементи допомагають забезпечити, що військовослужбовці будуть готові до фізичних випробувань і викликів, з якими вони можуть зіткнутися у сфері безпеки і оборони.

Фізична підготовленість – це фізичний стан військовослужбовця, який характеризується наявним рівнем розвитку фізичних, спеціальних якостей, ступенем сформованості військово-прикладних рухових навичок і вмінь [1].

Фізична підготовленість військовослужбовців є важливою складовою їхньої професійної підготовки і включає в себе кілька основних аспектів: 1) силова підготовка: розвиток м'язової сили, яка необхідна для виконання різних фізичних завдань, таких як перенесення вантажів, стрільба з важкої зброї тощо; 2) витривалість: здатність виконувати тривалі фізичні навантаження без суттєвого зниження ефективності. Вона включає як кардіореспіраторну витривалість (здатність серцево-судинної системи підтримувати тривалу роботу), так і м'язову витривалість; 3) швидкість і спритність: здатність швидко реагувати на зміну обстановки, швидко переміщатися та здійснювати необхідні дії в бойових умовах; 4) гнучкість: здатність виконувати рухи з повною амплітудою в суглобах, що важливо для уникнення травм та виконання різних завдань; 5) морально-психологічна стійкість: хоча це не є фізичним аспектом, моральна витривалість і психологічна готовність до стресових ситуацій безпосередньо впливають на загальну фізичну підготовленість.

Фізична підготовленість військовослужбовців залежить від декількох факторів: 1) Загальний стан здоров'я: важливу роль відіграє фізичний стан організму, включаючи відсутність хронічних захворювань та травм; 2) Вік: молодші військовослужбовці, як правило, мають вищий

рівень фізичної підготовленості, проте з досвідом старші можуть мати перевагу в витривалості та психологічній стійкості; 3) Рівень тренованості: регулярні тренування та виконання спеціальних фізичних вправ значно покращують підготовленість; 4) Раціон харчування: адекватне і збалансоване харчування сприяє підтримці належного рівня енергії і відновленню після фізичних навантажень; 5) Мотивація та моральний дух: висока мотивація і позитивний моральний дух підвищують ефективність тренувань і здатність справлятися з фізичними труднощами.

Фізична підготовленість є ключовим фактором успіху в бойових діях та забезпечує ефективність виконання службових обов'язків військовослужбовцями.

До основних принципів фізичної підготовленості військовослужбовців можна віднести: 1) **Комплексність**: (включає в себе всі аспекти фізичної підготовки: силу, витривалість, швидкість, гнучкість та координацію; забезпечує всебічний розвиток фізичних якостей, необхідних для виконання військових завдань). 2) **Цілеспрямованість**: (програми тренувань повинні бути орієнтовані на конкретні завдання та вимоги військової служби; включає спеціальні вправи для розвитку фізичних якостей, необхідних для виконання конкретних бойових або службових завдань. 3) **Систематичність**: (регулярне проведення тренувань є критично важливим для досягнення та підтримання високого рівня фізичної підготовленості; включає планування і контроль за процесом тренування). 4) **Індивідуальний підхід**: (урахування фізичних можливостей та стану здоров'я кожного військовослужбовця; адаптація тренувальних програм відповідно до потреб і можливостей індивідуума). 5) **Поєднання фізичних та психічних навантажень**: (балансування фізичних навантажень з психологічними тренуваннями для забезпечення загальної стійкості та витривалості).

Ці принципи допомагають в формуванні фізичної підготовленості військовослужбовців і забезпечують їх ефективність у виконанні службових обов'язків.

В основних доктринальних документах армії США, стосовно готовності, а саме фізичної готовності, фізична підготовленість трактується, як здатність відповідати фізичним вимогам будь-якої службової або бойової позиції, смертельно небезпечно пересуватися на полі бою, виконувати завдання і продовжувати воювати, перемагати і повертатися додому здоровими [9].

Згідно доктрини H2F (США), головна мета фізичної підготовки – це досягнення летальності руху, що передбачає здатність фізично вступати в бій і знищувати ворога. Летальність руху полягає у здатності застосовувати та підтримувати необхідний рівень сили, витривалості та швидкості для виконання тренувальних та бойових завдань. Ця фізична мета тісно пов'язана з оптимальною психічною функцією, адже мета та функція нерозривно пов'язані. Здатність витримувати фізичний тиск

залежить від душевної стійкості, яка формується шляхом тренувань ключових компонентів фізичної готовності та завдань, що їх підтримують. Компоненти фітнесу, енергетичних систем, професійних і фізичних навичок, необхідних для досягнення летальності руху, мають бути ретельно узгоджені з часом і структурними можливостями військовослужбовця. Структурні можливості – це внутрішні резерви, що дозволяють солдату ефективно виконувати фізичні завдання. Летальність руху має бути опанована через ретельне відтворення тих рухів, які потрібні для виконання професійних завдань і ведення бою. Вправність у цих рухах повинна навмисно і цілеспрямовано вдосконалюватися, доки не стане природною частиною дій військовослужбовця як на тренуваннях, так і в зіткненнях з противником [9].

Інтеграція в євроатлантичний безпековий простір та отримання членства в НАТО є важливими аспектами стратегії України, що передбачають узгодження підходів до підготовки військовослужбовців сил сектору безпеки і оборони України у сферах фізичної готовності і спортивної майстерності.

Фізична підготовка і спорт виконують різноманітні функції. Загальні серед них включають світоглядну, виховну, освітню, розвиваючу, видовищну, рекламну, комунікативну, комерційну, стимулюючу, оздоровчо-гігієнічну, загально-культурну та методологічну. Специфічні функції охоплюють змагальну, гедоністичну, нормативну, престижну, прикладну функції, а також функцію «відволікання».

Розглядаючи проблему підвищення рівня фізичної підготовленості науковці застосовують різні підходи для вирішення даного питання.

А саме, підвищення рівня фізичної підготовленості засобами різних видів спорту займались Вербицький С. О. зі співавторами [5], Казначеєв В. М., Павлов Р. В. [3], Назимок В. В. [6], Откидач В. С. [2], Пронтенко К. В. [8], Рядова Л. О. зі співавторами [4], Чуйко О. зі співавторами [7].

Однак, попри значний обсяг наукових досліджень, залишається актуальним питання вивчення впливу систематичних занять різними видами спорту на здоров’я та фізичну підготовленість студентів.

Фізична підготовленість є важливим компонентом у розвитку професійної компетентності, особливо в таких сферах, як військова справа, спорт, служба безпеки, рятувальні служби та інші професії, що вимагають високої фізичної активності. Вона сприяє не лише підвищенню фізичних можливостей, але й розвитку витривалості, стресостійкості, здатності швидко приймати рішення в екстремальних ситуаціях.

Список використаних джерел:

1. Наказ Міністра оборони України від 05.08.2021 року № 225 «Про затвердження Інструкції з фізичної підготовки в системі Міністерства оборони України».

2. Откидач В. С., Корчагін М. В., Золочевський В. В., Хліманцов Т. В. Вплив занять військово-спортивним багатоборством на рівень фізичної підготовленості курсантів вищих військових навчальних закладів. Вісник Запорізького національного університету. Фізичне виховання та спорт. № 2 (2020). С. 75–81.
3. В. М. Казначеєв, Р. В. Павлов Значення ігрових видів спорту при підготовці поліцейських у закладах вищої освіти. *Підготовка поліцейських в умовах реформування системи МВС України. Харків, 2019.* С. 243–246.
4. Рядова Л. О., Рожков В. О., Подмарьова І. А., Тихонова А. О. Вплив спортивних ігор на стан здоров'я та рівень фізичної підготовленості у здобувачів закладів вищої освіти. *Науковий часопис НПУ імені М. П. Драгоманова. Випуск 12 (172) 2023.* С. 162–168.
5. Вербицький С. О., Путров С. Ю., Путров О. Ю., Луценко С. Г. Аналіз показників загальної та спеціальної фізичної підготовленості студентів, які займаються каратете кіокушин. *Науковий часопис НПУ імені М. П. Драгоманова. Випуск 12 (172) 2023.* С. 48–52.
6. Назимок В. В. Фізична та спеціальна фізична підготовленість студентів, що займаються боксом у процесі фізичного виховання. *Реабілітаційні та фізкультурно-рекреаційні аспекти розвитку людини, № 9, 2021.* С. 174–181.
7. Чуйко О., Власюк О., Пікінер О., Чернявська О., Токмакова С. Особливості фізичної підготовленості студентів з різними рівнями здоров'я під впливом секційних занять тайським боксом. Науково-практичний журнал Спортивний вісник Придніпров'я. № 1. 2021. С. 192–200.
9. Пронтенко, К. В. Удосконалення фізичної підготовленості курсантів ВВНЗ операторського профілю на етапі первинного навчання засобами гирьового спорту. *Педагогіка, психологія та медико-біологічні проблеми фізичного виховання і спорту: наук. моногр./за ред. С. Єрмакова* 2008, 7. С. 94–97.
10. Department of the Army. FM 7-22 Holistic Health and Fitness. 2020. Available online: URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN30714-FM_7-22-000-WEB-1.pdf.

ОТКИДАЧ В. С.,
доктор філософії,
старший викладач кафедри фітнесу
і адаптивного спорту,
Український державний університет
імені М. Драгоманова

КЛЮЧНИК В. В.,
викладач кафедри фізичного виховання
спеціальної фізичної підготовки і спорту,
Військовий інститут танкових військ
Національного технічного університету
«Харківський політехнічний інститут»

НОЖОВИЙ БІЙ В СИСТЕМІ СПЕЦІАЛЬНОЇ ФІЗИЧНОЇ ПІДГОТОВКИ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Попри стрімкий розвиток технологій озброєння, тактики ведення бою, ніж зберігає свою актуальність як простий, надійний і

багатофункціональний засіб ураження. У руках підготовленого фахівця він може виконувати широкий спектр задач, від нелетального порізу м'яких тканин до тяжких ушкоджень внутрішніх органів, проте його ефективність визначається не технічною складністю, а рівнем підготовки та тактичним застосуванням.

На відміну від вогнепальної зброї, ніж не потребує боєприпасів і не підлягає технічним відмовам у вигляді осічок, що робить його складовою екіпіровки багатьох підрозділів спеціального призначення сектору сил та оборони. Через відносно менші вимоги до фізичної сили все більше фахівців у сфері рукопашного бою включають ножову техніку в навчальні програми, водночас підкреслюючи необхідність етичних, правових і медичних обмежень у підготовці та застосуванні [1].

Ножовий бій вимагає системного навчання. Він має свою методику, яка дає змогу навчити володіти ножем в якості зброї для нападу або і при виконанні бойових завдань (штурмі окопу, щілини, виконання бойових завдань в будівлі). Саме тому тренінг з ножем вимагає серйозного і системного підходу. Власник зброї зобов'язаний мати кілька варіантів дій, і мати здатність вибрати потрібний, виходячи з конкретної ситуації.

Співробітники спеціальних служб та правоохоронних органів сил сектору безпеки та оборони повинні бути готові реагувати на такі загрози, однак підготовка має відповідати в цілому правовим і медичним стандартам.

Дослідження в галузі тактичної підготовки свідчать про ефективність модульних програм, що поєднують теорію (право, психологія конфлікту), симуляцію та медичну підготовку [2,5]. Водночас етичні та правові дослідження підкреслюють ризики неправильної інтерпретації тактичних навичок та необхідність навчання в рамках норм застосування сили [4]. Сучасні підходи рекомендують використовувати реалістичні, але безпечні симулятори (foam/soft rubber props), системи відеоаналізу та стандартизовані сценарії для мінімізації ризику травм і правопорушень [3].

Мета дослідження: імплементація ножового бою в систему спеціальної фізичної підготовки співробітників СБУ.

Основні задачі: навчитися психологічному впливу на супротивника, а також ефективному протистоянню цьому впливу; отримати знання про психологію ножового бою; відпрацювати отримані навички на практиці; закріпити отримані навички у ситуаційних задачах і рольових тренінгах.

Робота з ножем вимагає серйозного і системного підходу. Власник зброї зобов'язаний мати кілька варіантів дій, і мати здатність вибрати потрібний, виходячи з конкретної ситуації.

Існуюча система спеціальної фізичної підготовки не задовольняє в повній мірі вимоги сьогодення, підходи та засоби ведення війни, проведення спеціальних операцій з застосуванням новітніх технологій та

тактик змінюються шаленими темпами. Майбутній фахівець сектору безпеки та оборони повинен відповідати нинішнім підходам до підготовки співробітників спеціальних підрозділів, що зумовлює нас постійно удосконалювати напрями підготовки. Спеціальна фізична підготовка відіграє важливу роль у підготовці майбутнього фахівця і потребує постійного удосконалення і інтеграції різних направлень та засобів фізичного виховання в підготовку майбутніх фахівців.

Список використаних джерел:

1. Воробєй О. Спортивний ножовий бій. Основи. Історичний клуб «Холодний Яр». 2018. 96 с.
2. Butler F. K., Holcomb J. B., Giebner S. M. Tactical Combat Casualty Care //*Journal of Trauma and Acute Care Surgery*. 2016. Vol. 80, No. 6. P. 1–5.
3. Fletcher D., Hanton S., Wagstaff C. R. D. *Performance under pressure: a model of psychological and physiological adaptation*// *Sport, Exercise, and Performance Psychology*. 2020. Vol. 9, No. 4. P. 595–610. DOI: 10.1037/spy0000206.
4. Kraska P. B. *Militarization and policing – an international perspective*// *Policing & Society*. 2017. Vol. 27, No. 1. P. 1–3. DOI: 10.1080/10439463.2016.1234463.
5. Seamon M. J., Haut E. R., Van Arendonk K. J., Barbosa R. R., Chiu W. C., Dente C. J. *Stop the Bleed: Hemorrhage Control Education and Effect on Mortality* // *Prehospital and Disaster Medicine*. 2016. Vol. 31, No. 1. P. 79–87. DOI: 10.1017/S1049023X15005573.
6. World Health Organization. *Prehospital trauma care systems*. Geneva : World Health Organization, 2018. 112 p. URL: https://www.who.int/publications/i/item/9789241512601.

ПАЛЕВИЧ С. В.,
доктор філософії, доцент,
Національна академія Служби безпеки України

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ЗАСАДИ ВИКОРИСТАННЯ МОДЕЛІ TPSR У СПОРТИВНИХ ІГРАХ ДЛЯ РОЗВИТКУ ЖИТТЄВИХ КОМПЕТЕНТНОСТЕЙ

Спортивні ігри виступають ефективним засобом розвитку ключових життєвих компетенцій, зокрема відповідальності, лідерських якостей, уміння співпрацювати, самоконтролю та емоційної стійкості. Вони створюють природне середовище для формування не лише фізичних умінь і навичок, але й соціально-емоційних якостей особистості, сприяючи її всебічному та гармонійному розвитку (Тітаренко & Бабачук, 2024; Цимбалюк та ін., 2024; Чернявська, 2024).

Заняття з фізичного виховання та організована спортивна діяльність поза межами навчальних занять забезпечують інтеграцію цих компетенцій у повсякденну поведінку здобувачів освіти. Проте традиційні програми фізичного виховання переважно зосереджуються на розвитку фізичних якостей, недостатньо використовуючи потенціал

спортивних ігор як інструменту формування життєвих і соціально-поведінкових навичок (Круцевич & Кашуба, 2003; Kashuba, 2014).

Спортивні ігри давно привертають увагу дослідників як ефективний інструмент формування життєвих компетенцій у молоді. Зокрема, Hellison D. R. (2011) у своїй моделі TPSR (Teaching Personal and Social Responsibility) показав, що через активну участь у спортивних іграх здобувачі вищої освіти розвивають повагу до інших, самоконтроль, здатність працювати в команді та відповідальність. Ця модель була підтверджена у численних дослідженнях, зокрема Petitpas A. J. із співавторами (2005), які акцентували увагу на перенесенні набутих навичок у позааудиторній сфері діяльності здобувачів освіти.

Wright P. M. та Richards K. A (2020, 2021) продемонстрували, що спортивні ігри ефективно формують у здобувачів освіти навички лідерства, співпраці та вирішення конфліктів. Автори відзначили, що ігрові ситуації створюють природні умови для взаємодії, в яких здобувачів освіти вчяться приймати рішення, адаптуватися до змін і брати на себе відповідальність за результат.

Спеціалісти на чолі з Bailey R. (2009) підкреслили важливість спортивних ігор як засобу формування «м'яких навичок» (soft skills), таких як комунікація, емпатія, критичне мислення та здатність працювати в команді. Водночас, автори зауважили, що впровадження таких підходів у навчальні програми вимагає підготовки педагогів та зміни акцентів у викладанні фізичної культури.

Goudas M. та Giannoudis G. (2008) дослідили вплив ігрових видів спорту на емоційний розвиток школярів, показавши, що участь у спортивних іграх знижує рівень тривожності та сприяє розвитку емоційної стійкості. Hemphill M. A. із співавторами (2019) доповнюють цю тезу, вказуючи на важливість групових видів спорту для формування у здобувачів освіти почуття приналежності та командної єдності.

Opstoel K. разом з іншими дослідниками (2020) показали, що участь у спортивних іграх може бути ключовим чинником для розвитку життєвих компетенцій, необхідних для соціальної адаптації. Автори зазначають, що взаємодія у спортивній грі сприяє розвитку таких навичок, як співпраця, прийняття рішень, розв'язання конфліктів і емпатія, що важливо для соціалізації молоді.

Згідно з дослідженнями Liao C. C. із співавторам (2023), використання спортивних ігор як педагогічного інструменту дозволяє створити мотиваційний клімат, що підтримує розвиток автономії та соціальної компетентності здобувачів освіти. Крім того, дослідження Cronin L. D. та Allen J. (2017) наголошують на важливості ігрових ситуацій для розвитку адаптивності здобувачів освіти, що є необхідною навичкою в умовах сучасного світу.

Вітчизняні дослідники також акцентують увагу на значущості спортивних ігор для формування життєвих компетенцій. Так, роботи Круцевича Т. В. і Кашуби В. О. (2003) вказують на необхідність

розробки сучасних програм фізичного виховання, які б враховували соціально-емоційні аспекти освіти. Водночас Пангелова Н.Є. (2014) наголошує на важливості використання спортивних ігор для профілактики асоціальної поведінки серед здобувачів освіти.

Попри наявні напрацювання, дослідники наголошують, що системна інтеграція спортивних ігор у навчальні програми залишається напрямом, який потребує подальшого наукового опрацювання. Зокрема, актуальним є питання адаптації ігрових методик до різних вікових категорій і рівнів фізичної підготовленості здобувачів освіти**,** а також аналіз довготривалих результатів упровадження таких програм у контексті формування життєвих компетентностей.

Водночас методика TPSR (Teaching Personal and Social Responsibility) у структурі програм спортивних ігор для здобувачів освіти в умовах української системи вищої освіти залишається недостатньо дослідженою**.** Потребують уточнення педагогічні механізми адаптації спортивних ігор до індивідуальних можливостей здобувачів освіти**,** а також оцінка їх впливу на розвиток автономії, лідерських якостей і відповідальності під час освітнього процесу.

Список використаних джерел:

1. Круцевич, Т.В., & Кашуба, В.О. (2003). Формування здорового способу життя учнівської молоді засобами фізичного виховання. *Теорія і методика фізичного виховання і спорту, 2*(1), с. 5–9.
2. Пангелова, Н.Є. (2014) *Теоретико-методичні засади формування гармонійно розвиненої особистості дитини дошкільного віку в процесі фізичного виховання* : автореферат дис. ... доктора наук з фіз. виховання і спорту (24.00.02). Національний університет фізичного виховання і спорту України.
3. Тітаренко, С., & Бабачук, Ю. (2024). Формування фізичної готовності до школи у дітей старшого дошкільного віку засобом спортивних ігор. *Спортивні ігри*, 4(34), с. 79–88. URL: https://doi. org/10.15391/si.2024-4.10.
4. Цимбалюк , Ж. О., Мусієнко, А. В., Спузяк, В. Б., Солодовник, В. М., & Руденко, А. В. (2024). Розвиток життєвих компетенцій через фізичну активність: огляд літератури та аналіз підходів. *Педагогічна Академія: наукові записки*, (11). URL: https://doi. org/10.5281/zenodo.14249200.
5. Чернявська, Т. (2024). Емоційне благополуччя та успішність у командних видах спорту. Спортивні ігри, 1(31), с. 75–85. URL: https:// doi.org/10.15391/si.2024-1.07.
6. Armour, K. M. (2011). Sport pedagogy: An introduction for teaching and coaching. *Sport, Education and Society, 16*(2), p. 243–251. URL: https://doi.org/ 10.4324/9781315847108.
7. Bailey, R., Armour, K., Kirk, D., Jess, M., Pickup, I., Sandford, R., & the BERA Physical Education and Sport Pedagogy Special Interest Group (2009). The educational benefits claimed for physical education and school sport: An academic review. *Research Papers in Education,* 24(1), p. 1–27. URL: https://doi.org/10.1080/ 02671520701809817.

ПОДРУШНЯК В. М.,
Національна академія Служби безпеки України

ЩОДО ПІДСТАВ ЗАСТОСУВАННЯ ЗАХОДІВ ФІЗИЧНОГО ВПЛИВУ ВІЙСЬКОВОСЛУЖБОВЦЯМИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Застосування зброї, спеціальних засобів та фізичної сили регламентується законами про відповідні органи та військові формування сил безпеки та сил оборони України.

Служба безпеки України є державним органом спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України, а змістом статті 26 регламентовано підстави і порядок застосування виключно зброї, спеціальних засобів та бойової техніки військовослужбовцями Служби безпеки України на підставах і в порядку, передбачених Законом України «Про Національну поліцію», військовими статутами Збройних Сил України та іншими актами законодавства [3, с. 18].

Поліція уповноважена у ході своєї діяльності застосовувати такі заходи примусу як фізичний вплив (сила) [2, с. 34–36], військовослужбовці під час виконання службових обов'язків мають право застосовувати заходи фізичного впливу [4, с. 8, 9; 5, с. 38, 39, 113].

Функції органів, підрозділів та співробітників Служби безпеки України, що здійснюють контррозвідувальну діяльність, визначаються Законом України «Про Службу безпеки України» [1, с. 4], в ході контррозвідувальної діяльності органи, підрозділи та співробітники Служби безпеки України мають право зберігати, носити, застосовувати, використовувати зброю, спеціальні засоби, вживати заходів фізичного впливу відповідно до законів України та інших актів законодавства України [1, с. 6].

А оскільки згідно статті 19 Конституції України, правовий порядок у державі базується на принципах, що гарантують: жодна особа не може бути змушена до виконання дій, яких не передбачено законодавством. Державні органи та їхні посадові особи повинні діяти виключно на основі повноважень, у межах своєї компетенції та у спосіб, визначений Конституцією й законами України [6, с. 6], то питання щодо застосування військовослужбовцями Служби безпеки України заходів фізичного впливу потребує врегулювання, так як відповідним законом передбачено лише застосування виключно зброї спеціальних засобів та бойової техніки [1, с. 6].

З метою врегулювання зазначеного питання вважаємо за доцільне:

1. назву статті 26 Закону України «Про Службу безпеки України» викласти у такій редакції: «Підстави і порядок застосування зброї, спеціальних засобів, заходів фізичного впливу та бойової техніки»;

2. абзац перший тексту статті 26 Закону України «Про Службу безпеки України» викласти у такій редакції: «Військовослужбовці Служби безпеки України мають право зберігати, носити, використовувати і застосовувати зброю, спеціальні засоби, застосовувати заходи фізичного впливу на підставах і в порядку, передбачених Законом України “Про Національну поліцію”, військовими статутами Збройних Сил України та іншими актами законодавства».

Список використаних джерел:

1. Закон України «Про контррозвідувальну діяльність» від 26.12.2002 № 374-IV / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text (дата звернення: 20.10.2025).
2. Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 20.10.2025).
3. Закон України «Про Службу безпеки України» від 25.03.1992 № 2229-XII / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 20.10.2025).
4. Закон України «Про Статут внутрішньої служби Збройних Сил України» від 24.03.1999 № 548-XIV / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/548-14#Text (дата звернення: 20.10.2025).
5. Закон України «Про Статут гарнізонної та вартової служб Збройних Сил України» від 24.03.1999 № 550-XIV / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/550-14#Text (дата звернення: 20.10.2025).
6. Конституція України від 28.06.1996 № 254к/96-ВР / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 20.10.2025).

САДОВСЬКИЙ П. Л.,
Національна академія Служби безпеки України

РАЦІОНАЛЬНІ МЕТОДИ ПІДВИЩЕННЯ РІВНЯ ФІЗИЧНОЇ ПІДГОТОВЛЕНОСТІ ВІЙСЬКОВОСЛУЖБОВЦІВ У ПОЛЬОВИХ УМОВАХ

З початком збройної агресії проти України значно зросли вимоги до фізичної підготовки військовослужбовців. Умови сучасного бою вимагають від них максимальної фізичної та психоемоційної витривалості, готовності виконувати завдання в екстремальних умовах, таких як складний клімат та перепади температур, обмежена можливість відпочинку та харчування тощо. Окрім того, необхідно враховувати специфіку бойової діяльності, яка передбачає тривалі піші переходи, перенесення важкого спорядження та виконання завдань у повному спорядженні.

Фізична підготовка у польових умовах є важливим компонентом

загальної бойової готовності. Її основна мета – забезпечення високого рівня фізичної та морально-психологічної готовності особового складу до виконання завдань. Науковці, такі як О. В. Петрачков, С. В. Гоманюк, В. О. Мельник, підкреслюють важливість адаптації фізичного тренування до специфічних умов, у яких діють військовослужбовці. Важливими факторами, які впливають на ефективність фізичної підготовки, є не лише рівень загальної витривалості, а й спеціальні прикладні навички, необхідні для бойових дій.

Ефективним напрямом розвитку загальних і спеціальних фізичних якостей та прикладних навичок є комбінована інтеграція елементів системи CrossFit із використанням підручних засобів. У польових умовах часто бракує необхідного спортивного обладнання, тому військовослужбовці застосовують альтернативні методи тренувань. Наприклад, використовують саморобні перекладини, гирі з пластикових пляшок, наповнених піском, або автомобільні шини. Такий підхід дозволяє ефективно підтримувати фізичну форму навіть у віддалених районах.

Система CrossFit набула популярності серед військових завдяки її універсальності та ефективності. Ця методика тренувань спрямована на розвиток силової витривалості, швидкісно-силових якостей та загальної функціональної підготовки. Особливо важливим є те, що CrossFit дозволяє змінювати інтенсивність вправ залежно від рівня підготовки військовослужбовців. Дослідження, проведені вітчизняними та зарубіжними вченими, підтверджують, що регулярні заняття за цією системою сприяють підвищенню фізичної готовності військовослужбовців до виконання завдань у бойових умовах.

Окрему увагу слід приділити стандартам фізичної підготовки, які адаптовані до сучасних потреб Сектору безпеки і оборони. Вони включають спеціальні вправи, спрямовані на розвиток прикладних рухових навичок, таких як подолання перешкод, метання гранат, швидка посадка і висадка з техніки, тривале перебування у бойових машинах. Виконання цих стандартів є обов’язковим елементом тренувального процесу, що дозволяє військовослужбовцям досягати високого рівня боєздатності.

У польових умовах фізичне тренування має поєднувати загальну та спеціальну підготовку. Наприклад, вправи з обтяженнями, марш-кидки, виконання завдань у повному спорядженні дозволяють адаптувати організм до реальних бойових навантажень. Також важливим є формування командної згуртованості підрозділів через колективне виконання вправ. Це не лише покращує фізичну готовність, а й сприяє підвищенню морально-психологічної стійкості військовослужбовців.

Досвід бойових дій також показує необхідність впровадження фізичних вправ відновлювально-рекреаційного характеру. Військово-

службовці, які перебувають у польових умовах протягом тривалого часу, стикаються зі значним нервово-психологічним напруженням і фізичним виснаженням. Для відновлення їхньої працездатності рекомендується проводити оздоровчий біг, спортивні ігри, вправи на розтяжку та дихальну гімнастику. Такі заходи сприяють зняттю емоційного напруження та відновленню фізичного стану.

Не менш важливим аспектом є підвищення рівня підготовленості командирів підрозділів, які відповідають за організацію фізичних тренувань. Від їхніх знань і навичок залежить якість тренувального процесу, мотивація особового складу та ефективність виконання завдань. Таким чином, необхідно розробляти програми підготовки для командирів, які враховують специфіку польових умов та особливості бойової діяльності.

Підсумовуючи, слід зазначити, що фізична підготовка у польових умовах є ключовим елементом забезпечення боєздатності військово-службовців. Ефективними підходами можна вважати такі, як використання підручних засобів із впровадженням системи CrossFit та адаптація стандартів фізичної підготовки до реальних умов бойових дій, що дозволяють підвищити ефективність тренувального процесу. Поєднання загальної та спеціальної підготовки, а також впровадження відновлювальних заходів сприяє підтриманню фізичного стану та морально-психологічної стійкості особового складу.

Список використаних джерел:

1. Романчук В. М. Фізична підготовка у Збройних Силах України : навч. посіб. / В. М. Романчук, С. В. Романчук. Житомир : ЖВІРЕ, 2004. 144 с.
2. Корольчук М. С. Психофізіологія діяльності / М. С. Корольчук. Київ : Ельга Ніка-Центр, 2003. 400 с.
3. Петрачков О. В., Гоманюк С. В., Мельник В. О. Фізична підготовка військовослужбовців в умовах сучасного конфлікту. Фізкультура і спорт. 2023;12(3). С. 45.
4. Шлямар І. Л., Романчук С. В, Воронцов О. С. Настанова з фізичної підготовки у Сухопутнихвійськах Збройних Сил України : навч.-метод. посіб. / Київ. 2021. С. 73–80.
5. Белей А. Організація варіантів фізичної підготовки і вирішення деяких задач психологічної підготовки з курсантським складом ВНЗ / А. Белей // Матеріали відкритої наук.-метод. конф. «Фізична підготовка військовослужбовців», 29–30 квітня 2003 р. Київ, 2003. С. 68–69.

СУХОРАДА Г. І.,
кандидат наук з фізичного виховання та спорту, доцент,
професор кафедри
фізкультурно-спортивної реабілітації,
Навчально-науковий інститут фізичної культури
та спортивно-оздоровчих технологій
Національного університету оборони України

ОСНОВНІ ПОЛОЖЕННЯ НОРМАТИВНО-ПРАВОВИХ АКТІВ У СФЕРІ ФІЗИЧНОЇ КУЛЬТУРИ І СПОРТУ МІНОБОРОНИ ЩОДО ЗАБЕЗПЕЧЕНЯ ФОРМУВАННЯ ПСИХОЛОГІЧНОЇ ГОТОВОСТІ ОСОБОВОГО СКЛАДУ ДО ВИКОНАННЯ ВІЙСЬКОВО-ПРОФЕСІЙНИХ ЗАВДАНЬ

У Міністерстві оборони України (далі – Міноборони) проводиться певна робота з формування психологічної готовості військово-службовців, зокрема засобами фізичної підготовки і спорту, до виконання військово-професійних завдань за призначенням.

Першим етапом провадження вимог законодавства з даного важливого напряму є закріплення цих вимог у нормативно-правових актах та інших керівних документах сфери фізичної культури і спорту військовослужбовців системи Міноборони.

У Концепції розвитку фізичної підготовки і спорту в системі Міністерства оборони України (далі – Концепція) [1] визначено, що серед проблем, на вирішення яких вона спрямована, є і така, як недостатній рівень розвитку військово-прикладного спорту серед особового складу як важливого фактору підвищення їхньої фізичної і психологічної готовності.

Серед причин виникнення вищезазначеної проблеми є і така, як недостатній рівень знань щодо потенціалу військово-прикладного спорту та використання його можливостей як важливого засобу підвищення рівня фізичної і психологічної готовності особового складу, військово-професійної діяльності, військово-патріотичного виховання, формування професійно-важливих навичок та вмінь для виконання службово-бойових завдань за призначенням.

Фахівці сфери фізичної культури і спорту дотримуються думки, що метою Концепції є сприяння у забезпеченні подальшого розвитку та вдосконалення фізичної підготовки і спорту серед особового складу, відведення їй однієї з провідних ролей у системі Міноборони, зокрема у формуванні готовності до перенесення екстремальних фізичних і психологічних навантажень у період підготовки та ведення бойових дій, виховання морально-вольових якостей.

Вбачається, що це є важливим аспектом щодо забезпечення

фізичної і психологічної готовності військовослужбовців до виконання завдань за призначенням. Тому, виділене проблемне питання входять до змісту пріоритетних напрямів розвитку фізичної підготовки і спорту військовослужбовців.

Згідно з вимогами Програми розвитку фізичної підготовки і спорту в системі Міністерства оборони України (далі – Програма) [2], командири (начальники) усіх ланок управління щопівріччо звітують про виконання запланованих заходів з фізичної підготовки і спорту з особовим складом підрозділів, військових частин, закладів, установ, організацій, органів військового управління видів, окремих родів військ (сил) Збройних Сил України, Державної спеціальної служби транспорту, інших військових організаційних структур.

Відповідно до Інструкції з фізичної підготовки в системі Міністерства оборони України (далі – Інструкція) [3], серед обов'язків командирів підрозділів – керівників форм фізичної підготовки і спорту військовиків, – є забезпечення фізичної готовності особового складу до виконання військово-професійних завдань за призначенням. Водночас, ця вимога, у першу чергу стосується також і самих командирів-керівників, які здійснюють підготовку підлеглого особового складу. Тому, підготовка підрозділів, забезпечення їх психологічної готовності до виконання завдань за призначенням є важливим елементом системи повсякденної діяльності військ.

З метою вирішення завдань фізичної підготовки і спорту та досягнення її мети щодо забезпечення фізичної і психологічної готовності військовослужбовців до виконання завдань за призначенням, в Інструкції передбачається таке:

обумовленість спеціальних завдань фізичної підготовки військовослужбовців видів та окремих родів військ (сил) Збройних Сил України особливостями їх професійної діяльності та бойового застосування;

поділ військовослужбовців чоловічої та жіночої статі на вікові групи та категорії відповідно до вимог службової діяльності до рівня їх фізичної готовності;

визначення відповідальності керівників усіх ланок управління щодо керівництва фізичною підготовкою і спортом підпорядкованими військовими частинами, підрозділами та підлеглим особовим складом;

забезпечення належної фізичної готовності підлеглих військовослужбовців, стану фізичної підготовки і спорту у військових частинах;

наявність спортивного активу військових частин і підрозділів для керівництва спортивно-масовою роботою;

врахування особливостей навчальних і бойових завдань у мирний час та особливий період для забезпечення виконання програм з фізичної

підготовки, а також визначення потрібної кількості часу на усі її форми під час здійснення планування;

забезпечення підготовки кадрів, керівників і виконавців, а також здійснення заходів контролю та обліку фізичної підготовки і спорту, реалізацію заходів всебічного забезпечення системи фізичної культури і спорту військовослужбовців;

проведення форм фізичної підготовки відповідними керівниками та командирами підрозділів згідно з визначним їхнім змістом та методикою.

Потрібно зазначити, що окремо в Інструкції також визначено комплекс заходів щодо формування та вдосконалення психологічної готовості особового складу до виконання завдань за призначенням.

Саме тому, керівники, командири (начальники) усіх ланок управління зобов'язані проводити виховання військовослужбовців у процесі фізичної підготовки і спорту, яке спрямоване на формування переконання щодо важливості занять фізичними вправами, потреби у систематичному їх виконанні, вдосконалення морально-психологічних якостей для підвищення боєздатності військ, яке забезпечується застосуванням методів переконання, прикладу, змагання, заохочення, примусу та впливу колективу; об'єктивною оцінкою зрушень у якостях, що виховуються; підбором вправ, в яких психічні якості особистості проявляються в найбільшій мірі; застосуванням раціональних методів і методичних прийомів їх виконання.

При цьому потрібно дотримуватися таких рекомендацій:

психічна та емоційна стійкості забезпечуються виконанням фізичних вправ в умовах нервово-психічного напруження (за наявності небезпеки), а саме: під час подолання водних перешкод; стрибках у воду; пірнання в довжину та глибину; виконання вправ з елементами ризику; прийомів рукопашного бою та подолання перешкод в ускладнених умовах;

сміливість і рішучість розвиваються вправами, що містять елементи новизни, ризику та небезпеки у разі зміни й ускладнення умов їхнього виконання: пересування на значній висоті по вузькій опорі; стрибки в глибину; стрибки через широкі та глибокі перешкоди; зіскоки з гімнастичних снарядів; опорні стрибки; стрибки у воду; акробатичні вправи; спуски з крутих схилів і стрибки на лижах; вправи на спеціальних снарядах; навчальні двобої в рукопашному бою;

ініціатива та винахідливість розвиваються вправами, що вимагають прийняття самостійних рішень: спортивні та рухливі ігри; прийоми рукопашного бою; прийоми та дії за раптово поданими командами чи сигналами; біг з орієнтуванням на місцевості;

наполегливість і завзятість розвиваються вправами, пов'язаними із

значними та тривалими фізичними та нервово-психічними навантаженнями, особливо в умовах змагань: біг на середні та довгі дистанції; вправи з гирями та інші силові вправи, що виконуються на максимальну кількість разів;

витримка та самовладання розвиваються вправами, пов'язаними з необхідністю діяти точно та впевнено в умовах фізичних і нервово-психічних навантажень: подолання складних перешкод; плавання в обмундируванні зі зброєю; пірнання; дії на воді та під водою; метання гранат на точність;

стійкість уваги, здатність її до широкого розподілу та переключення формуються за допомогою спеціальних вправ і додаткових завдань, в обстановці, що швидко змінюється: спортивні та рухливі ігри, єдиноборства;

впевненість у своїх силах і цілеспрямованість розвиваються шляхом комплексного виконання всіх перелічених вправ.

Отже, дотримання вимог Інструкції командирами з точки зору забезпечення навчання та виховання підлеглих, їхньої підтримки та розвитку допомагає зміцнити лідерські якості, сприяє гендерній рівності та покращує взаємопідтримку між членами військових колективів у сфері фізичної культури і спорту військовослужбовців.

Вищевказані нормативно-правові акти Міноборони у сфері фізичної культури і спорту військовослужбовців доповнюються іншими керівними документами, які створюються на основі вимог Концепції та Інструкції. Зокрема, такими є видові настанови з фізичної підготовки – нормативно-методичні документи із забезпечення функціонування фізичної підготовки у видах, окремих родах військ (сил) Збройних Сил України, Державній спеціальній службі транспорту, інших військових організаційних структурах.

Список використаних джерел:

1. Концепція розвитку фізичної підготовки і спорту в системі Міністерства оборони України. Затверджена наказом Міністерства оборони України від 28.12.2022 № 452. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/v0452322-22.
2. Програма розвитку фізичної підготовки і спорту в системі Міністерства оборони України, затверджена наказом Міністерства оборони України від 28 липня 2023 року № 441. / URL: https://www.mil.gov.ua/ministry/normativno-pravova-baza/nakazi-ministra-oboroni-ukraini/nakazi-ministerstva-oboroni-ukraini-za-2023-rik.html.
3. Інструкція з фізичної підготовки в системі Міністерства оборони України. Затверджена наказом Міністерства оборони України від 05.08.2021 № 225, зареєстрована у Міністерстві юстиції України 01.10.2021 за № 1289/36911 (із змінами). / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/z1289-21.

ШЛЯМАР І. Л.,
кандидат наук з фізичного виховання та спорту,
заслужений працівник фізичної культури
та спорту України,
Національна академія Служби безпеки України

ОРГАНІЗАЦІЯ ФІЗИЧНОЇ ПІДГОТОВКИ У ЗБРОЙНИХ СИЛАХ ПРОВІДНИХ КРАЇН СВІТУ

Сили сектору безпеки й оборони України тривалий час ведуть активні бойові дії із захисту держави від повномасштабної агресії з боку російської федерації. На початку вторгнення всі сподівались що війна закінчиться в короткостроковій перспективі, то сьогоднішні реалії свідчать, що війна іде на виснаження, в тому числі людських ресурсів.

Досвід бойових дій свідчить, що діяльність військовослужбовців сил сектору безпеки й оборони України, в тому числі Служби безпеки України, проходить у критичних умовах, при значних фізичних навантаженнях, постійній втомі та інших несприятливих чинниках бойової діяльності. Успішне виконання бойових завдань щодо захисту держави залежить від рівня не тільки професійної, а й фізичної готовності військовослужбовців, яка відіграє ключову роль у підготовці військовослужбовця, особливо в разі надмірних фізичних навантажень та нервово-психологічних напружень під час бойових дій та екстремальних ситуацій. Особливості оперативно-службової діяльності військово-службовців Служби безпеки України визначаються потребою проведення диверсійних дій у тилу ворога, контррозвідувальних заходів у зоні бойових дій, корегування ведення вогню артилерією, посилення оборони на найбільш небезпечних ділянках фронту, знешкодження диверсійно-розвідувальних груп противника та інших заходів, що передбачають високий рівень фізичної підготовленості військово-службовців.

З метою імплементація в освітній процес досвіду підготовки персоналу для країн-членів Північноатлантичного Альянсу з метою посилення взаємосумісності та спроможностей вітчизняної спецслужби в умовах євроатлантичної інтеграції проведено аналіз організації фізичної підготовки в арміях інших держав [6, 8]:

метою фізичної підготовки у Збройних силах Сполучених Штатів Америки, Великої Британії та Франції є вплив на фізичну здатність військовослужбовців виконувати професійні обов’язки, і лише в Німеччині мета фізичної підготовки полягає у впливі на цілісну особистість людини через тренування руху, зміцнення здоров’я, заняття спортом та раціональне використання вільного часу;

загальними завданнями фізичної підготовки армій провідних країн є розвиток основних фізичних якостей (розвитку загальної витривалості та м’язової сили надають перевагу в армії США; формування військових,

військово-прикладних навичок (за винятком Німеччини). При цьому відзначається значне підвищення працездатності та зміцнення здоров'я військовослужбовців;

принципи фізичної підготовки Збройних сил, що комплектуються за контрактом (США, Велика Британія), різняться направленістю підготовки військовослужбовців до бойових дій у будь-якому місці та в будь-який час на фоні максимальної подібності обстановки і психологізації підготовки, у порівнянні з більш спокійним характером принципів фізичної підготовки армій, що комплектуються змішано;

з поміж засобів фізичної підготовки, які використовуються у військах, імітації реального бойового навантаження, створенню екстремальних ситуацій, що вимагають від особового складу високого фізичного та психічного напруження, надають перевагу в Збройних силах, що комплектуються за контрактом. Звичайні засоби фізичної підготовки тут виконують підготовчу та допоміжну функції. В Збройних силах зі змішаним характером комплектування, переважає використання прикладних вправ та різних видів спорту [1, 2].

Інтенсифікація фізичної підготовки здійснюється завдяки [7, 8]:

збільшенню службового часу, що відводиться на заняття фізичною підготовкою (Німеччина – до 4,5 годин на тиждень, Франція і ВМС США – до 8 годин на тиждень);

використанню позаслужбового часу для оздоровчих та спортивних програм;

стимулюванню досягнення високих результатів у фізичній підготовці шляхом матеріальної зацікавленості або залучення військовослужбовців до масового спорту;

вдосконаленню системи планування фізичної підготовки (проведення щоденних занять фізичними вправами тривалістю 15–45 хвилин при 3 годинах занять на тиждень);

виділенню найбільш прикладних розділів (рукопашний бій, долання перешкод, курси «Командо», курс амфібійної підготовки й т.ін.) у самостійні предмети бойової підготовки;

удосконаленню навчально-матеріальної бази для занять фізичною підготовкою;

застосуванню сучасних методів тренування;

підвищенню вимог та ускладненню контрольних нормативів і умов їх виконання [1,2].

Основним засобом фізичної підготовки військ Збройних сил країн НАТО є спорт. Систематичні змагання на першість Альянсу проводяться за однаковими правилами, що сприяє формуванню єдиних вимог до змісту та організації фізичної підготовки [3, 4, 5].

Підвищення боєздатності фізичної підготовки здійснюється шляхом збільшення в програмах практичної кількості військово-прикладних вправ та створення з них спеціальних комплексів, розглядаються як самостійні розділи підготовки, на які виділяється окремий час.

Із метою підвищення військової придатності фізичної підготовки розвиваються найважливіші фізичні та психічні якості для виконання військово-професійних дій: витривалість, стійкість, самовладання, сміливість, згуртованість та інше. Для розвитку цих якостей використовуються вправи та види діяльності, командні й індивідуальні види спорту, показники яких пов'язані з ризиком та небезпекою (багатоборство, орієнтування, парашутний спорт, альпінізм та інше).

Слід зазначити, що в усіх провідних країнах світу значна увага приділяється контролю за рівнем дотримання військовослужбовцями вимог фізичної підготовки та професійної діяльності, їх загальній та спеціальній фізичній підготовленості, а також чіткій диференціації нормативів відповідно до особливостей військової служби. Така багаторівнева система перевірки та оцінювання зовнішньої готовності заснована на бальній системі, яка дає чітке уявлення про рівень фізичної підготовленості військовослужбовців.

Результативність забезпечується шляхом систематичного залучення військовослужбовців до занять фізичною підготовкою, участі у змаганнях. Виконання бойових завдань під час відбиття збройної агресії з боку російської федерації вимагає від військовослужбовців Служби безпеки України не тільки високого рівня професійних знань і навичок, але й значних фізичних та вольових зусиль.

Список використаних джерел:

1. URL: http://www.army.mil (дата звернення: 03.10.2025).
2. URL: http://www.army.com / content / new-fitness-and-combat-read-iness-tests (дата звернення: 06.10.2025).
4. Романчук С. В. Теоретико-методичні засади фізичної підготовки курсантів ВВНЗ Сухопутних військ ЗСУ: автореферат дисертації доктора наук з ФВіС, Львів, 2013. 42 с.
5. Bundesministerium der Verteidigung. Bonn, 1996, p. 296.
6. URL: http://www.sportschule.bundewehr.de (дата звернення: 06.10.2025).
7. Анохін Є. Д. Фізична підготовка в арміях провідних держав НАТО: навч. метод. посіб. Львів : ЛВІ, 2005. 115 с.
8. Одеров А. М., Добровольський В. Б., Корчагін М. В. Особливості організації та змістовне наповнення систем фізичної підготовки у збройних силах держав-членів НАТО та України: наукова стаття. Український журнал медицини, біології та спорту. Київ 2020. Том 5, № 2 (24). 271–282 с.
9. Шлямар І. Л., Івахно О. В. Аналіз організації фізичної підготовки в Збройних Силах провідних країн світу : наукова стаття. Науковий часопис НПУ ім. М.П. Драгоманова, категорія Б, № 4 (163), 2023. С. 208–215.

8 ЗАСТОСУВАННЯ РОБОТИЗОВАНИХ СИСТЕМ ПРИ ВИКОНАННІ ОПЕРАТИВНО-БОЙОВИХ ЗАВДАНЬ

АНДЕРСОН Г. Г.,
Національна академія Служби безпеки України

ПІДГОТОВКА ПЕРСОНАЛУ ДО ЗАСТОСУВАННЯ РОБОТИЗОВАНИХ СИСТЕМ У СЕКТОРІ БЕЗПЕКИ ТА ОБОРОНИ

Підготовка фахівців до застосування роботизованих систем (роботизованих платформ, безпілотних наземних апаратів, автономних мобільних модулів, дистанційно керованих бойових та інженерних комплексів) є критичним компонентом реформування оборонного сектору. Масове впровадження робототехніки в сучасних конфліктах та спеціальних операціях змінює вимоги до підготовки операторів, інженерів та командирів підрозділів, формує нові стандарти тактики, логістики й технічної експлуатації.

Сучасні роботизовані комплекси виконують широкий спектр завдань: розвідка, спостереження, доставка боєприпасів і вантажів, евакуація поранених, інженерне розмінування, вогнева підтримка, боротьба з БпЛА, коригування артилерії. Це вимагає інтегрованої системи навчання, що поєднує технічну, тактичну, логістичну та правову складові. Традиційна військово-технічна підготовка не забезпечує достатнього рівня взаємодії з автономними та напівавтономними системами, тому створюються спеціалізовані навчальні програми.

Ключовим елементом підготовки є формування компетентностей оператора: знання принципів керування, навігації, каналів зв’язку, протидії РЕБ, основ штучного інтелекту, сенсорних систем, технічного обслуговування та ремонту. Оператор повинен уміти діяти автономно в умовах деградованої навігації, втрати супутникового зв’язку або наявності ворожих перешкод. Водночас командири повинні розуміти особливості застосування робототехніки в загальновійськових операціях, планувати маршрути, інтегрувати роботизовані платформи в бойові порядки та оцінювати ризики.

Важливим принципом є модульність і стандартизація підготовки. Роботизовані системи різних виробників часто відрізняються інтерфейсами, типами підсистем, протоколами передачі даних. Уніфікований підхід дозволяє готувати операторів на універсальних тренажерах, а техніків – на робочих зразках (силова установка, БпАК/UGV-зв’язок, оптоелектронні сенсори, платформи на гусеничному чи колісному шасі тощо). Це скорочує час навчання і підвищує ефективність підрозділу.

Окремим напрямом є розвиток навчально-тренувальної інфраструктури. До неї належать полігони для випробувань, симуляційні центри, віртуальні середовища та змішані тренажери (VR/AR), які дозволяють моделювати бойові умови без ризику втрати техніки. Симуляційні платформи надають можливість аналізувати помилки, будувати сценарії застосування, тренувати екіпажі одночасно, інтегруватися з навчанням артилерії, саперів, розвідки, підрозділів логістики.

Ефективна підготовка включає:

– базову технічну підготовку (конструкція, енергоживлення, сенсори, системи керування);

– тактичну підготовку (маршрути, приховане переміщення, взаємодія з підрозділом, безпека);

– експлуатаційно-ремонтну підготовку (заміна модулів, діагностика, профілактика);

– інформаційну та кібербезпеку (захист каналів, шифрування, протидія перехопленню);

– протидію РЕБ та відновлення керування в умовах перешкод;

– правові рамки застосування штучного інтелекту і автономних систем.

Підготовка також має охоплювати питання етики, відповідальності за бойове застосування, врахування міжнародного гуманітарного права та правил застосування сили. Оскільки роботизовані платформи можуть нести летальне озброєння, необхідно формувати культуру безпеки, алгоритми перевірки цілей, взаємодії з системами розпізнавання «свій-чужий», запобігання помилкам оператора.

У перспективі роль роботизованих систем у секторі оборони зростатиме – як у повністю автономних рішеннях, так і у форматі «людина-машина» [1]. Це означає необхідність постійного оновлення навчальних програм, створення доктринальних документів, інтеграції міжнародного досвіду та розвитку національної виробничої бази. Країни-партнери НАТО вже впроваджують стандарти навчання операторів, механіків та штабних офіцерів [2], що дозволяє уніфікувати принципи використання та зробити роботизовані системи частиною мережево-центричних операцій.

Підготовка фахівців у цій сфері не обмежується військовими задачами. Роботизовані платформи активно застосовуються у гуманітарному розмінуванні, рятувально-пошукових операціях, охороні критичної інфраструктури, патрулюванні кордону. Тому навчання має бути комплексним і мультидисциплінарним – із залученням військових, інженерів, програмістів, аналітиків та фахівців із кібербезпеки. Такий підхід формує кадровий резерв і сприяє розвитку національних спроможностей.

Отже, якісна підготовка персоналу є ключовим чинником ефективного застосування роботизованих систем. Від рівня підготовки оператора

та командування залежить живучість техніки, точність виконання завдань і здатність швидко адаптуватись до змін. Система навчання повинна бути динамічною, орієнтованою на практику, стандартизованою, інтегрованою з науковими дослідженнями та виробниками. Такий підхід забезпечує реальну бойову ефективність і мінімізує ризики втрат.

Список використаних джерел:

1. Укрінформ. Бойові дії в Україні довели вирішальне значення дронів та штучного інтелекту в сучасній війні. URL: https://www.ukrinform.ua/rubric-world/3915836-bojovi-dii-v-ukraini-doveli-virisalne-znacenna-droniv-ta-stucnogo-intelektu-v-sucasnij-vijni-borrel.html.
2. STANAG 4586 – Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability. URL: https://publications.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SCI-271/EN-SCI-271-03.pdf.

ГНАТУШ А. Р.,
кандидат біологічних наук,
Національна академія Служби безпеки України

СТЕПАНЕЦЬ В. В.,
директор з продукту STETMAN LLC

ТЕПЛОВИЙ СЛІД ТЕРМІНАЛІВ СУПУТНИКОВОГО ЗВ'ЯЗКУ – ДОСВІД СУЧАСНОЇ ВІЙНИ

З початком широкомасштабного вторгнення Російської Федерації у 2022 році в Україні відбулося масове застосування терміналів супутникового зв'язку типу Starlink та аналогічних систем інших виробників. За попередніми оцінками, їхня кількість перевищує 200 тисяч одиниць. Це є першим випадком у світовій практиці, коли цивільна технологія настільки масштабно залучається у збройний конфлікт.

Одним із ключових аспектів експлуатації терміналів супутникового зв'язку у бойових умовах є теплове демаскування, що істотно впливає на безпеку їх використання. Сучасні тепловізійні засоби спостереження стали доступними широкому колу користувачів і активно застосовуються у розвідувальних безпілотних літальних апаратах, FPV-дронах та стаціонарних системах спостереження. Це створює високі ризики виявлення будь-яких джерел тепла, у тому числі електронного обладнання.

Супутниковий термінал являє собою складну електронну систему, у якій значна частка споживаної енергії перетворюється на тепло. Приблизно 70–80 % енергоспоживання припадає на теплові втрати, які формуються у таких компонентах, як радіовипромінювачі, підсилювачі сигналу, обчислювальні модулі (процесори, контролери) та блоки

живлення. Із підвищенням інтенсивності передачі даних зростає й обсяг тепловиділення, що вимагає ефективного відведення тепла.

Технологічна основа сучасних терміналів супутникового зв'язку з плоскими антенами полягає у використанні активних фазованих антенних решіток (АФАР). Для правильного формування променю випромінювання необхідна висока точність орієнтації антени, що потребує значних обчислювальних ресурсів. Високе електронне навантаження зумовлює підвищене тепловиділення, яке, у разі недостатнього охолодження, може призвести до збоїв чи повної відмови пристрою. Саме тому питання відведення тепла є критично важливим для стабільної роботи терміналів.

Однією з характерних експлуатаційних проблем АФАР-систем є накопичення вологи, снігу або криги на поверхні антени, що погіршує пропускання радіохвиль. Для запобігання цьому явищу у конструкціях часто передбачають автоматичні системи підігріву або розігріву корпусу. У ранніх версіях терміналів Starlink застосовувалися окремі нагрівальні елементи, які вмикалися автоматично. У новіших моделях ця функція реалізована шляхом зміни режимів роботи випромінювачів, без використання додаткових нагрівальних елементів.

Разом з тим, алгоритм автоматичного нагріву у терміналах Starlink має недоліки. Будь-яке погіршення якості сигналу інтерпретується системою як необхідність увімкнення підігріву, що збільшує тепловий слід пристрою. Вимкнути цей режим можливо лише через налаштування авторизованого користувача, що в польових умовах часто неможливо. Отже, засоби теплового маскування можуть парадоксально спричинити зворотний ефект – активацію нагріву і посилення демаскування.

У терміналах Starlink тепло відводиться через корпус за рахунок природної конвекції. Ефективність цього процесу залежить від стану зовнішньої поверхні: забруднення, пил, фарбування або нанесення плівки погіршують теплопровідність і знижують тепловіддачу. Використання герметичних чохлів або ізолюючих покриттів призводить до ефекту «термоса», через що корпус перегрівається, а внутрішні компоненти можуть виходити з ладу.

Інші виробники супутникових терміналів (Kymeta, Satcube, Intellian, Hughes) часто застосовують активне охолодження з використанням вентиляторів або повітряних каналів. Такий підхід забезпечує швидше відведення тепла, однак має недоліки: накопичення пилу та вологи у вентиляційних каналах, можливість появи шуму, що створює демаскувальні фактори, а також необхідність регулярного технічного обслуговування.

Перегрів є однією з найпоширеніших причин збоїв у роботі терміналів. У системах Starlink передбачено кілька рівнів термозахисту:

- при температурі 107–113 °C – зниження продуктивності;
- при 115–125 °C – перехід у режим очікування;

- при 118–128 °C – аварійне вимкнення.

Якщо охолодження є неефективним, система переходить у ці режими постійно, що призводить до втрати стабільності зв'язку. Аналогічні термозахисні механізми реалізовані і в терміналах інших виробників, хоча порогові значення можуть різнитися. Незважаючи на це, перегрів залишається типовою проблемою експлуатації супутникових систем зв'язку у бойових умовах і потребує подальших інженерних удосконалень.

Таким чином, досвід використання терміналів супутникового зв'язку у сучасних бойових умовах показав, що теплове демаскування є суттєвим чинником, який впливає на їхню безпеку та ефективність застосування. Особливості конструкції та режимів роботи таких систем зумовлюють підвищене тепловиділення, що потребує оптимізації способів охолодження. Застосування захисних чохлів, як правило, призводить до перегріву супутникових терміналів. Тому для забезпечення стійкої роботи та зниження ризиків виявлення необхідне поєднання ефективних методів теплового маскування і відведення тепла. Подальші дослідження доцільно спрямувати на вдосконалення конструктивних рішень, спрямованих на мінімізацію теплового сліду терміналів супутникового зв'язку.

ГРЕБНЬОВ В. О.,
здобувач вищої освіти,
Національний університет
цивільного захисту України

КАЛЬЧЕНКО Я. Ю.,
доктор філософії,
доцент кафедри,
Навчально-науковий інститут
пожежної і техногенної безпеки
Національного університету
цивільного захисту України

АНАЛІЗ МЕТОДІВ ЗАСТОСУВАННЯ БПЛА ТА РОБОТИЗОВАНОЇ ТЕХНІКИ ПРИ ГАСІННІ ПОЖЕЖ ТА ЛІКВІДАЦІЇ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Актуальність застосування БПЛА у пожежогасінні виникає в потребі підвищення ефективності, оперативності та безпеки проведення пожежно-рятувальних робіт. Традиційні методи іноді не дозволяють швидко визначити осередки загорянь особливо на промислових об'єктах або в зонах бойових дій. Використання БПЛА дозволяє проводити розвідку, моніторинг і навіть локалізацію пожежі на відстані, знижуючи ризики для рятувальників та підвищуючи керованість процесу гасіння.

В умовах воєнного стану в Україні підвищується ризик виникнення надзвичайних ситуацій від наслідків ворожих обстрілів, робота пожежних підрозділів стає більш небезпечною через насиченість різними пожежовибухонебезпечними речовинами, широкого використання токсичних, біотехнологічних мікроорганізмів, вірусів, радіоактивних речовин, ускладненням технологічних процесів на виробничих підприємствах та від можливого повторного ракетного удару в місця виникнення надзвичайних ситуацій. В умовах сьогодення для успішного виконання поставлених завдань підрозділами ДСНС України під час надзвичайних ситуацій в умовах воєнного стану потрібно використання принципово новаторської пожежної техніки, що дозволить зменшити ризик втрат особового складу пожежного підрозділу, зменшити час локалізації та розвідки на пожежі, зосередити подачу вогнегасних речовин безпосередньо в зону горіння, підвищити оперативні дії особового складу та створити необхідні умови для забезпечення їхньої працездатності в екстремальних умовах.

Застосування безпілотних літальних апаратів при гасінні пожеж та ліквідації надзвичайних ситуацій ґрунтується на виконані наступних задач:

1. Моніторинг і розвідка місця події, що дозволяє швидко оцінити масштаби і ступінь небезпеки.
2. Пошук і виявлення постраждалих або людей, що опинилися в зоні ризику, навіть у важкодоступних районах, з подальшою передачею координат рятувальникам.
3. Збір і передача відео- та фотоданих у реальному часі для координації дій аварійно-рятувальних груп і прийняття оперативних тактичних рішень.
4. Оцінка ситуації щодо рівня токсичного, хімічного чи радіаційного забруднення повітряного простору, що допомагає обрати безпечні шляхи підходу і методи ліквідації наслідків.
5. Патрулювання великих територій для запобігання ризикам, виявлення джерел загорянь або аварій, що розвиваються.
6. Підтримка зв’язку між різними підрозділами рятувальників, забезпечення візуальної інформації, яка допомагає уникнути диверсій, неправильної оцінки ситуації та сприяє ефективному управлінню ресурсами.
7. Використання в ролі першої лінії реагування для швидкого реагування на виклики, що значно прискорює процеси порятунку і ліквідації наслідків НС.

Вже сьогодні існують зразки безпілотних апаратів літакового типу, що здатні скидати вогнегасні речовини на осередок пожежі, але вони непридатні до використання в умовах мегаполісів або промислових об’єктів. До того ж, якщо осередок пожежі розташований в приміщенні, такі апарати просто неможливо застосувати. Тому для створення пожежно-рятувальних безпілотних систем потрібні безпілотні апарати

вертолітного типу або мультикоптери. Мультикоптери широко використовуються для фото- та відеозйомки з повітря. Але, як правило, це моделі з низькою вантажопідйомністю, що не відповідає пожежно-рятувальним завданням.

Підрозділи ДСНС України при вирішенні оперативно-тактичних задач використовують роботизовану техніку, що дозволяє ефективно виконувати задачі без залучення особового складу безпосередньо у осередку надзвичайної ситуації.

Тактичні роботи пожежогасіння можуть виконувати наступні завдання:

1. Розвідка (отримання розвідувальної інформації в режимі, наближеному до реального час).
2. Виконання гасіння пожеж у разі ракетного обстрілу та розуміння керівником гасіння пожежі ситуації (забезпечення усіх рівнів інформацією про події , що відбуваються на надзвичайній ситуації).
3. Безпека (надання додаткового часу і більшого простору для реагування на загрози і здійснення передислокації на пожежі для сил і засобів та розширення зони безпечного виконання поставлених завдань).
4. Гасіння пожеж (локалізація та ліквідація осередку пожежі шляхом подачі води або піни).
5. Транспортування вантажів (пересування та транспортування вантажів та частин конструкцій, буксирування пошкоджених транспортних засобів).
6. Забезпечення відеоспостереження за станом надзвичайної ситуації (ретрансляція відеозв’язку і отримання додаткових інформаційних даних).
7. Підтримка виявлення небезпечних речовин (виявлення вибухонебезпечних предметів, мін, саморобних вибухових пристрої в, бактеріологічних, хімічних та радіаційних речовин та матеріалів).
8. Пошук і рятування постраждалих (використання для підвищення ефективності евакуації потерпілих та здійснення пошуково-рятувальних місій).

В умовах воєнного стану підрозділами ДСНС України Одеської, Рівненської, Житомирської, Львівської, Тернопільської, Хмельницької та Волинської областей неодноразово використовувались роботи пожежогасіння Magirus Wolf R1 та Alpha Wolf R1 при ліквідації наслідків надзвичайних ситуацій та під час обстрілів.

Їх впровадження значно підвищило оперативність та ефективність дій оперативно-рятувальних служб цивільного захисту, особливо в умовах обмеженого простору та складних умовах на пожежі. Вони ефективно показали себе, як на виробничих підприємствах, де доступ до осередку пожежі може бути обмеженим через специфічні умови, так і у місцях зі складною топографією, наприклад, у тунелях чи на вузьких вулицях. Крім того, вони надзвичайно корисні на військових об’єктах та в енергетичних комплексах, де пожежна безпека є ключовим питанням.

Однак у процесі планування оперативного використання тактичного робота пожежогасіння враховуються наступні обмеження, що приведені в таблиці 1 та таблиці 2 [1].

Табл.1. Рельєфні обмеження
під час застосування роботизованої техніки

Рельєфні умови	**Показник обмеження**	**Вплив на робота**
Нахил	до 30°	Вивід з ладу вузлів та оснащення, вплив на стабільність і погіршення продуктивності тактичного робота пожежогасіння
Спуск	до 30°	
Бічнии нахил	до 35°	
Глибина броду	до 16 см	

Для виконання завдань пожежно-рятувального призначення безпілотні системи повинні задовольняти досить специфічним вимогам. Це й припустиме корисне навантаження, і точність маневрування, і наявність систем швидкозмінних кріплень для установки пожежно-рятувального обладнання. Та й саме пожежно-рятувальне обладнання для використання разом із такими безпілотними системах повинне відповідати специфіці нових технологій гасіння.

Можна виділити два ключових напрямки. Перше – це використання створення пожежно-рятувальних безпілотних систем на основі автономних літальних апаратів з швидкозмінними модулями пожежогасіння. Такий пожежний дрон міг би подавати вогнегасні речовини в осередок пожежі через виносний телескопічний ствол. При цьому залежно від площі загоряння може бути задіяно кілька апаратів, для кожного з яких може бути організована оперативна зміна використаного модуля на новий, з повним запасом вогнегасної речовини.

Табл.2. Метеорологічні обмеження
під час застосування роботизованої техніки

Погодні умови	**Обмеження**	**Вплив на робота**	**Зв'язок**
Обмерзання	Може створювати небезпечні умови під час руху робота	Низька якість відеоспостереження, зниження швидкості руху, зменшення ефективності опцій	Може погіршуватися прийом
Сильний вітер	Може створювати небезпечні умови під час руху, що можуть призвести до виводу з ладу	Зниження швидкості руху, зменшення ефективності опцій	Може погіршуватися прийом

Сильний дощ	Може знижувати ефективність використання функцій робота та створювати небезпечні умови під час керування	Низька якість відеоспостереження, зниження швидкості руху, зменшення ефективності опцій	Не впливає
Туман	Робот в більшості випадків може виконувати відповідні роботи	Низька якість відеоспостереження	Не впливає
Підвищена температура осередку пожежі	Може призвести до втрати зв’язку та виводу з ладу вузлів та оснащення робота	Зменшення дальності подачі струменя води або піни, вивід з ладу вузлів та оснащення, обмеження щодо маневреності	Може перерватися прийом
Понижена температура (нижче -15:С) оточуючого середовища	Може викликати вивід з ладу вузлів та оснащення робота	Вивід з ладу вузлів та оснащення	Може перерватися прийом

Друге – це створення пожежно-рятувальних безпілотних систем, що працюють у технологічному зв’язку з наземною пожежною технікою. У такому варіанті з наземної техніки на літальний апарат можуть подаватися як вогнегасні речовини, так і живлення самого дрону. Цілком можливо, що обидві ці тактики знайдуть своє застосування на практиці й дозволять значно розширити можливості пожежно-рятувальних підрозділів у гасінні пожеж і, як наслідок, мінімізувати соціальні й матеріальні втрати.

Список використаних джерел:

1. Інструкція з експлуатації. Тактичний робот для місій Magirus Wolf R1. MAGIRUS WOLF R1, нім. REV. 02 Оригінальна інструкція з експлуатації квітень 2022.
2. Fire Fighting Drones. URL: https://www.dslrpros.com/ firefighting-drones.html (дата звернення: 26.10.2025).

ГУЛЕНКО К. І.,
здобувач вищої освіти,
Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

ТІМОШИН А. С.,
кандидат фізико-математичних наук,
доцент кафедри
інформаційних систем та технологій,
Харківський національний університет
внутрішніх справ
(науковий керівник)

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ КАНАЛІВ УПРАВЛІННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Актуальність дослідження. У сучасних бойових умовах активно впроваджуються роботизовані системи (дрони, безпілотні наземні комплекси, автономні платформи), і роль безпілотних літальних апаратів (UAV) зростає. Вони застосовуються для розвідки, цілевказання, ударів по ворогу, розмінування, логістики та охорони об'єктів [1, с. 205]. Дрони та автономні платформи зменшують ризики для військових, підвищують точність ударів і забезпечують оперативну перевагу на полі бою.

Постановка проблеми. Управління такими системами здійснюється через радіоканали або захищені мережі, що в свою чергу – робить їх вразливими до кібератак. Ці системи залежать від обміну критичною інформацією, тому безпечна й надійна організація зв'язку в мережах безпілотних літальних апаратів є «ключовим викликом» для військових і науковців. У разі перехоплення чи підміни сигналів керування противник може отримати контроль над технікою або змусити її працювати на нього. Так, у реальних конфліктах атаки на зв'язок (наприклад, GPS-спуфінг та глушіння каналів) вже призводили до виведення з ладу безпілотників та втрати тактичних переваг. Отже, сьогодні тема про захист каналів управління є ключовим аспектом інформаційної безпеки сучасних бойових роботизованих систем [1, с. 206].

Мета дослідження. Головним завданням цього дослідження є аналіз можливих кібератак на безпілотні літальні апарати, їх класифікації та методи протидії.

Основна частина. Система зв'язку є важливим компонентом системи безпілотних літальних апаратів. Його основне завдання – встановити двосторонній канал передачі даних між повітрям і землею. Цей канал використовується для дистанційного керування, телеметрії та передачі інформації про завдання від наземної станції управління до безпілотника. Дистанційне керування дозволяє керувати безпілотником і

його обладнанням на великій відстані, а телеметрія контролює стан БПЛА (Безпілотний літальний апарат). Передача інформації про завдання надсилає дані відео та зображень, зібрані бортовими датчиками місії, на станцію керування через бездротовий канал низхідної лінії зв'язку. Якість цієї передачі безпосередньо впливає на можливість ідентифікації та виявлення цілей [2]. Згідно викладеного вище тексту ми можемо виділити декілька потенційних загроз для БПЛА:

- Перехоплення та підміна сигналів (spoofing): якщо канал управління не зашифровано й не автентифіковано, противник може прослуховувати телеметрію та передачі команд або активно вставляти фальшиві пакети. Наприклад, на канали GPS або управління можна подавати «фальшиві» координати (GPS-spoofing), щоб ввести БПЛА в оману. За відсутності цифрових підписів і захисту на рівні каналу зловмисник може віддалено перехоплювати командні повідомлення або підміняти їх іншими, змінюючи маршрут чи поведінку робота [3]. В Україні з початку 2024 року діє система «Покрова», здатна відхиляти курс безпілотників, таких, як «Шахед-131/136», що діє методом GPS-spoofing проти безпілотників.
- Глушіння каналів (jamming): означає навмисне порушення частот або створення перешкод сигналам GNSS. Тобто jamming створює перевантаження справжніх частот шумом або перебоями, що ускладнює прийом оригінального сигналу та часто призводить до втрати з'єднань або неточних даних. У конфлікті в Україні виявлено, що російські засоби радіоелектронної боротьби генерували інтенсивний шум, що змушувало українські дрони падати або зазнавати перешкод під час польоту.
- Несанкціонований доступ до систем управління: якщо мережа керування не захищена належним чином (немає сегментації, слабкі паролі, уразливі протоколи), противник може пробитися в систему управління. Через вразливості в ПЗ або слабкі механізми авторизації зловмисник здатен отримати доступ до командних серверів чи контролерів, змінивши права доступу або перенаправивши управління технікою. Особливо небезпечними є атаки «людина-посередині» (MITM) та використання вкрадених облікових даних для входу в систему.

Перед описом конкретних методів слід зазначити: забезпечення кіберзахисту каналів управління бойовими роботизованими системами передбачає не просто додавання одного засобу, а формування багаторівневої системи заходів, яка враховує технічні, організаційні та процедурні аспекти. У межах цієї системи мають комбінуватися засоби, що забезпечують конфіденційність, цілісність і доступність зв'язку, а також швидке виявлення та реагування на порушення. Нижче наведено ключові групи методів, які демонструють такий підхід.

- Криптографічний захист: запровадження сильних шифрувальних алгоритмів для каналу управління гарантує конфіденційність і

цілісність команд. Використовують симетричні шифри (наприклад, AES) та асиметричні (RSA, ECC) для шифрування команд і телеметрії [4]. Цифрові підписи дозволяють перевіряти достовірність кожного повідомлення і виключати підміни. Крім того, застосовуються стандартні безпечні канали (TLS, IPsec, DTLS, VPN) для створення захищених тунелів зв'язку між пультом і безпілотником. Дослідження показують, що впровадження таких протоколів значно знижує можливість перехоплення та модифікації управлінських команд.

- Аутентифікація та авторизація: кілька рівнів перевірки операторів і системних компонентів ускладнюють несанкціонований доступ. Застосовуються багатофакторна аутентифікація (пароль + OTP-токен чи біометричний фактор) при вході до системи керування. Реалізовуються суворі політики контролю доступу (access control) та журнали подій, щоб можна було оперативно виявити незвичні спроби входу.
- Маскування сигналів (HopSync): щоб приховати сигнали управління, використовуються технології маскування. Наприклад, команди можна передавати «вбудованими» у фоновий канал даних або надлишкові пакети, які виглядають як звичайний трафік. Інновація HopSync полягає у використанні криптографічних, часових обчислень для визначення кожного частотного стрибка, без будь-якого центрального годинника чи рукостискання. Усі вузли починають із спільного використання секретного криптографічного ключа (або «насіннєвого коду») заздалегідь – його можна безпечно розповсюдити перед розгортанням (навіть за допомогою офлайн-методу, такого як сканування QR-коду або асиметричний груповий обмін ключами). Після розгортання кожен вузол незалежно обчислює наступний частотний канал на основі поточного часу та спільного секрету, використовуючи односторонню криптографічну функцію. Зв'язок залишається захищеним від перехоплення та jamming [5].
- Виявлення вторгнень (IDS/IPS): системи моніторингу мережевого трафіку та поведінки допомагають оперативно реагувати на атаки. Використовують спеціальні рішення типу IDS/IPS, які аналізують аномальні шаблони трафіку, фальшиві пакети або нехарактерну активність. Виявивши відхилення (наприклад, різке збільшення потоку або підозрілі командні послідовності), система може автоматично сповістити оператора чи заблокувати зв'язок. Застосування штучного інтелекту і машинного навчання в таких системах дозволяє навчати моделі розпізнавання нових типів атак. Згідно з дослідженнями, поєднання IDS і методів машинного навчання забезпечує раннє виявлення кіберзагроз і зниження ризику їх успіху.
- Резервування та відновлення: для забезпечення безперервності керування використовують резервні канали зв'язку. Це можуть бути

супутникові зв'язки (наприклад, Starlink), додаткові радіочастоти, лазерні або оптичні канали на випадок заглушення основного зв'язку. Системи мають автоматично переключатися на запасний канал у разі перебоїв. Також запроваджують механізми «останніх повідомлень» – наприклад, якщо зв'язок втрачено, автономна платформа може повернутися на безпечну точку (get-you-home) або перейти в захищений режим. Таким чином забезпечується швидке відновлення управління та зменшується залежність від єдиного каналу зв'язку.

Отримані результати узгоджуються з теоретичними моделями кібер-фізичних систем (CPS) у робототехніці: база – це інформаційна безпека (конфіденційність, цілісність, доступність) та безпека керування (control security). Як зазначено у літературі, сучасні роботизовані системи слід проектувати за принципами secure-by-design, modular decomposition, data/information channel protection [7]. Крім того, дослідження показують, що простого шифрування недостатньо – треба резервування каналів, стрибкоподібна частота, збалансована архітектура – що також підтверджує потребу в багаторівневому підході.

Комбіноване застосування цих методів випливає з природи загроз: оскільки атака може бути як пасивною (прослуховування, перехоплення), так і активною (глушіння, підміна, DDoS), то потрібен і захист каналів (шифрування, маскування), і перевірка достовірності (аутентифікація), а також можливість виявлення порушень (IDS/IPS), а також резервні механізми для збереження функціональності системи. Теоретичні роботи з кібербезпеки роботизованих систем підтверджують, що лише багаторівневий, комбінований підхід дозволяє досягти високого рівня стійкості. Так, український досвід бойових дій свідчить про активне використання високозахищених каналів управління з декількома рівнями захисту. Зокрема, для оперативного зв'язку й керування БПЛА широко застосовується супутникова система Starlink. Її термінали встановлюють на дронах і станціях управління – це дає змогу передавати реальний відеопотік, координати цілей та інші дані навіть за відсутності наземної інфраструктури.

Висновок. Аналізуючи, можемо зробити висновок, що кіберзахист каналів управління роботизованими бойовими системами вимагає комплексного підходу. Необхідно одночасно впроваджувати різні технології захисту – від сучасних криптографічних протоколів до адаптивних частотних схем та систем моніторингу. Аналітика мережевого трафіку з використанням штучного інтелекту і багатошарові моделі безпеки допомагають виявляти нетипові загрози й оперативно реагувати на них. В ході дослідження були виділені найзначущі методи захисту каналів управління роботизованими бойовими системами: криптографічний захист (шифрування, підписи), багаторівнева аутентифікація/авторизація, стеганографія та фонове маскування каналів. Ці

методи охоплюють як запобіжні заходи (prevention), так і засоби виявлення (detection) та реагування (response) на кіберзагрози. Перспективним напрямом є розробка автономних систем управління, які самостійно виявляють спроби кібервтручання та реагують на них, забезпечуючи безпечне функціонування безпілотної техніки.

Рекомендації. На мою думку, для покращення захищеності роботизованих бойових систем потрібно використовувати машинне навчання для аналізу нормальної поведінки каналів і виявлення відхилень у режимі реального часу. Це дасть змогу ідентифікувати нові або нестандартні атаки, поки вони ще не наробили шкоди. У сучасних роботизованих системах цей підхід стане одним з кращих способів раннього попередження атак. Звісно, системи керування, мікропрограми, прошивки пристроїв треба регулярно оновлювати, закривати відомі вразливості та впроваджувати он-лайн або безпечні over-the-air оновлення. Це дозволить мінімізувати ризик використання відомих дір. Також, потрібно організувати багаторівневе навчання персоналу та регулярні тренування. Наприклад, проведення «red team / blue team» вправ допомагає виявити слабкі місця системи до реальної атаки. Симуляції атак на такі системи, допоможе бути готовим до можливої атаки в майбутньому.

Список використаних джерел:

1. UAV Exploitation: A New Domain for Cyber Power. URL: https://ccdcoe.org/uploads/2018/10/Art-14-Assessing-the-Impact-of-Aviation-Security-on-Cyber-Power.pdf#:~:text=The%20lack%20of%20security%20protecting,to%20the%20full%20range%20o (дата звернення: 17.10.2025).
2. Як дрони спілкуються? Посібник із частоти та перешкод. URL: https://www.airmobi.com/uk/how-do-drones-communicate-a-guide-to-frequency-and-interference (дата звернення: 17.10.2025).
3. Onthe Requirements for Successful GPS Spoofing Attacks. URL: Wayback Machine (дата звернення: 17.10.2025).
4. Encryption Standarts: AES, RSA, ECC, SHA and Other Protocols. URL: https://dev.to/hardy_mervana/encryption-standards-aes-rsa-ecc-sha-and-other-protocols-460c (дата звернення: 17.10.2025).
5. How HopSync Works: Cryptographic Time-Driven Hopping. URL: https://beechat.network/2025/07/29/hopsync-a-stateless-frequency-hopping-revolution-in-military-mesh-communications/ (дата звернення: 17.10.2025).
6. INTRUSION DETECTION SYSTEMS. URL: https://elartu.tntu.edu.ua/bitstream/lib/44254/2/IMSTT_2023_Chernyk_O_A-Intrusion_detection_systems_126.pdf (дата звернення: 17.10.2025).
7. Cybersecurity of Robotic Systems: Leading Challenges and Robotic System Design Methodology. URL: https://www.mdpi.com/2079-9292/10/22/2850 (дата звернення: 17.10.2025).

КІБІТКІН С. О.,
кандидат технічних наук,
Національна академія Служби безпеки України

ДОСВІД БОЙОВОГО ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ НАЗЕМНИХ СИСТЕМ ІЗ ОПТОВОЛОКОННИМ КАНАЛОМ ЗВ'ЯЗКУ

Практика застосування безпілотних наземних систем (БнНС) у сучасних конфліктах свідчить про їх перехід від експериментального озброєння до постійного елемента бойових дій [1]. Один із найбільш перспективних напрямів – використання оптоволоконного каналу зв'язку, який забезпечує одночасно високу пропускну здатність, захищеність від радіоелектронного впливу та низьку ймовірність перехоплення керуючих сигналів. Це суттєво розширює спектр завдань, які можуть виконувати БнНС під вогневим та радіоелектронним впливом противника.

Досвід бойового застосування свідчить, що платформи з оптоволоконним каналом зв'язку доцільно залучати для інженерної розвідки, локального розмінування, підтягування боєприпасів або медевакуації на коротких дистанціях, ведення прихованої спостережної діяльності, а також коригування вогню з укритих позицій. Оптична лінія дає можливість передавати необроблене відео, телеметрію та сигнали керування зі значно меншою затримкою, ніж у більшості радіоканалів, що особливо важливо в умовах вогневого контакту та коротких «вікон» часу для ухвалення рішень.

У районах активної роботи засобів радіоелектронної боротьби (РЕБ) бездротовий канал нерідко стає непридатним: сигнал глушиться, а платформа – втрачає керування. На відміну від радіочастотного зв'язку, оптоволоконна передача даних не випромінює хвиль і не формує радіопортрет, що суттєво знижує імовірність виявлення [2]. Такий спосіб зв'язку також дає змогу організувати передачу даних з БнНС у закритих приміщеннях, тунелях, підземних комунікаціях чи міських руїнах, де радіосигнал екранується конструкціями.

Разом із тим, бойовий досвід демонструє ряд обмежень. Найуразливіше місце – оптичний кабель. Його легко пошкодити уламками, колісною технікою або умисними діями противника. Крім того, протягування кабелю обмежує маневр та максимальну відстань виходу БнНС, вимагає спеціальних котушок, систем натягу, інженерного планування маршруту та навченого персоналу. Якщо траса прокладена відкрито, супротивник отримує можливість визначити місце її початку або орієнтовний напрямок роботи платформи.

Систематизація бойового досвіду дозволяє сформулювати кілька практичних рекомендацій. По-перше, оптимальним підходом є гібридні архітектури: оптика – як основний канал, радіоканал або супутниковий – як резерв. Автоматичне перемикання запобігає втраті керування у разі розриву кабелю. По-друге, доцільними є модульні котушки з сенсорами натягу, що зменшують імовірність обриву та полегшують швидке згортання системи. По-третє, маскування кабельних трас (траншеї, трубопроводи, підповерхневі укриття, захисні короби) істотно підвищує живучість системи. По-четверте, ефективність БнНС залежить від підготовки персоналу не лише до керування, а й до ремонту в польових умовах – швидкої зварки оптоволокна, монтажу тимчасових муфт та відновлення каналу під обстрілом.

Практика також засвідчує, що оптоволоконні БнНС найбільш ефективні у завданнях короткої та середньої дальності, де критична передача високоякісного відео і низька затримка керування, а ризик радіозаглушення – максимальний. У довготривалих і динамічних наступальних діях їхня мобільність поступається радіокерованим системам, але у штурмових, оборонних, міських та інженерних операціях вони демонструють суттєві переваги.

Отже, оптоволоконний канал зв’язку істотно підсилює можливості безпілотних наземних систем у зонах активної роботи РЕБ, підвищує якість збору розвідданих та безпеку особового складу. Ефективність застосування визначається не лише технічними параметрами платформи [3], а й грамотним плануванням маршруту, організацією маскування та професійною підготовкою операторів. Подальші перспективи розвитку пов’язані зі створенням автоматичних систем прокладання та збору кабелю, захищених оптоволоконних боксів, а також уніфікації «гібридних» каналів зв’язку з автоматичним перемиканням.

Список використаних джерел:

1. ОП 3-0(46) Доктрина «Застосування безпілотних систем у силах оборони України». Київ, Центральне управління безпілотних систем Генерального штабу Збройних Сил України, 2024. 64 с.
2. Kagan Yalcın, Fiber-Optic Drone Technologies: A Multidisciplinary Review from Communication Fundamentals to Military Applications. MSc Mechanical Engineering. Izmir University of Economics. pp. 1-10, June 2025. DOI: https://doi.org/10.5281/zenodo.15620221.
3. Технічні вимоги до безпілотних наземних комплексів (систем). Затверджених Міністром оборони України від 09.01.2025 № 764. 48 с.

КРИВОНОС В. М.,
кандидат технічних наук,
начальник кафедри експлуатації
та застосування безпілотних авіаційних систем
та комплексів повітряної розвідки,
Харківський національний університет
Повітряних Сил ім. Івана Кожедуба

ТУПИЦЯ І. М.,
доктор філософії,
старший викладач кафедри експлуатації
та застосування безпілотних авіаційних систем
та комплексів повітряної розвідки,
Харківський національний університет
Повітряних Сил ім. Івана Кожедуба

ДОСЛІДЖЕННЯ СПОСОБІВ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ОБРОБКИ ДАНИХ ПОВІТРЯНОЇ РОЗВІДКИ В УМОВАХ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ

Висока динаміка бойових дій на території України призвела до суттєвого зростання вимог до розвідувальної інформації, що формується бортовими оптико-електронними системами повітряної розвідки. Слід зазначити, що до основних вимог відносяться наступні [1, 2]: оперативність обробки розвідувальної інформації, що формуються сенсорами різних спектрів (видимого, інфрачервоного); достовірність розвідувальної інформації. З метою виконання першої пропонується використання інструментів автоматизації окремих етапів дешифрування розвідувальної інформації. На сьогоднішній день з цією метою активно застосовуються технології комп'ютерного зору та глибокого машинного навчання, що дозволяють автоматизувати такі процеси, як [3]:

1. Виявлення та класифікація об'єктів інтересу на цифрових зображеннях.

2. Локалізація об'єктів інтересу на цифрових зображеннях. Сучасні алгоритми комп'ютерного зору з цією метою використовують обмежувальні рамки для об'єктів інтересу, що виявляються.

3. Відстежування об'єктів інтересу в масштабі часу, наближеного до реального.

При цьому слід зазначити, що використання зазначеного напрямку для обробки розвідувальної інформації дозволяє створити умови для забезпечення необхідного рівня достовірності. З цією метою для оцінки адекватності моделей комп'ютерного зору використовуються відповідні метрики (кількісні показники) – Precision, Recall, mAP.

Проте, одним з основних проблемних аспектів використання зазначених технологій в інтересах повітряної розвідки є зростання вимог до

професійних здібностей персоналу збору та обробки розвідувальної інформації в напрямку використання сучасних інформаційних технологій [4].

Тому актуальним постає питання пошуку шляхів автоматизації окремих етапів дешифрування даних повітряної розвідки з метою підвищення оперативності обробки розвідувальної інформації в умовах зниження вимог до професійних здібностей персоналу збору та обробки розвідувальної інформації.

З метою вирішення вищезазначеної наукової задачі пропонується використання ресурсів відкритих веб-платформ (Roboflow, Ultralytics) та платформ візуального програмування (Orange Data Mining). Використання перших дозволяє підвищити оперативність формування моделей комп'ютерного зору в інтересах повітряної розвідки за рахунок використання графічних процесорів хмарних сервісів [5]. Так, використання функціональних можливостей платформи Ultralytics дозволяє змоделювати результати обробки великих масивів даних без необхідності використання локальних ресурсів (станцій керування та контролю безпілотних літальних апаратів). Проте, проблемним аспектом використання зазначеної платформи є необхідність доступу до глобальної мережі Інтернет, що не допускається в умовах обробки службових даних. В свою чергу, основною перевагою використання платформ візуального програмування типу Orange Data Mining є можливість локального використання в умовах зниження вимог до персоналу збору та обробки розвідувальної інформації з використання сучасних інформаційних технологій. Останнє пов'язано з тим фактом, що практична реалізація робочих процесів на досліджуваній платформі відбувається шляхом використання відповідних віджетів (модулів) з можливістю візуальної та кількісної оцінки результатів, що формуються.

Тому подальші наукові дослідження будуть спрямовані на інтеграцію синтезу зазначених платформ в процес обробки розвідувальної інформації з метою підвищення оперативності дешифрування даних повітряної розвідки.

Список використаних джерел:

1. Тупиця І. М., Кривонос В. М., Кібіткін С. О., Іващук Л. А., Бєлівцов А. О. Концептуальна модель автоматизації процесу дешифрування даних повітряної розвідки з використанням технологій системи штучного інтелекту. Системи озброєння і військова техніка. 2023. № 1 (73). С. 75–81. DOI: https://doi.org/10.30748/soivt.2023.73.09.
2. Тупиця І. М., Дейнеженко І. О., Крижанівський Є. С., Пархоменко М. В., Волков Ю. П., Ейдельштейн Г. Б. Метод автоматизації процесу виявлення об'єктів для підвищення ефективності дешифрування даних повітряної розвідки. Системи обробки інформації. 2023. № 2 (173). С. 63–73. DOI: https://doi.org/10.30748/soi.2023.173.08 .
3. Тупиця І. М., Кривонос В. М., Василенко Р.В., Галепа О. Г., Штанько В. А. Концепція інтеграції сучасних прогресивних технологій в систему формування та обробки даних повітряної розвідки. *Системи обробки інформації*. 2025. № 1(180). С. 81–88. DOI: https://doi.org/10.30748/soi.2025.180.09.

4. Tupitsya I., Kryvonos V., Kibitkin S., Ivashchuk B., Drol O., Shtanko V. Model of automated processing of air reconnaissance data in the conditions of application of unmanned aviation systems. *Scientific Works of Kharkiv National Air Force University*. 2025. № 2 (84). С. 141–149. DOI: https://doi.org/10.30748/zhups.2025.84.16.
5. Тупиця І. М., Іващук Б. М., Волков Ю. П., Пархоменко М. В., Галепа О. Г. Алгоритм формування моделі комп'ютерного зору в інтересах системи повітряної розвідки. *Вісник Вінницького політехнічного інституту*. 2025. № 3. С. 140–146. DOI: https://doi.org/10.31649/1997-9266-2025-180-3-140-146.

ЛЕНСЬКИЙ М. М.,
Національна академія Служби безпеки України

БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ В СИСТЕМІ УПРАВЛІННЯ СУЧАСНИМИ БОЙОВИМИ ОПЕРАЦІЯМИ

У сьогоденні безпілотні літальні апарати (далі – БпЛА) стали невід'ємною складовою системи управління сучасними бойовими операціями. Їх стрімкий розвиток і широке впровадження докорінно змінили уявлення про структуру командування, планування та ведення бою. Якщо у минулому процес управління військами базувався на обмеженому обміні інформацією між розвідкою та штабами, то сьогодні БпЛА забезпечують безперервний збір, передачу й аналіз даних у реальному часі, стаючи ключовим інструментом реалізації концепції «мережецентричних» операцій.

Система управління бойовими діями залежить від швидкості прийняття рішень, точності інформації та узгодженості дій між різними рівнями командування. У цьому контексті безпілотні платформи відіграють роль універсального інструменту, який поєднує функції спостереження, розвідки, наведення, ретрансляції зв'язку та навіть нанесення ударів. Завдяки розвитку сенсорних систем, тепловізійних і мультиспектральних камер, засобів супутникової навігації та передачі даних БпЛА стали «очима» та «вухами» командирів усіх ланок – від тактичної до стратегічної. Їх використання дозволяє створювати актуальну ситуаційну картину, оперативно реагувати на зміни обстановки та забезпечувати зворотний зв'язок між усіма учасниками операції.

Розвідувальні можливості БпЛА мають вирішальне значення для скорочення інформаційного розриву між підрозділами, що діють у полі бою, і командними пунктами. Дані, отримані від дронів, інтегруються у системи ситуаційної обізнаності, де вони обробляються аналітичними алгоритмами або штучним інтелектом, після чого командири отримують готові рекомендації для прийняття рішень. Це дозволяє суттєво

скоротити часовий цикл від виявлення цілі до її ураження. На практиці цей процес часто зводиться до кількох хвилин, що є критично важливим у сучасній війні, де швидкість реакції визначає успіх або поразку операції.

Однією з головних переваг використання БпЛА є підвищення рівня ситуаційної обізнаності командування. Безпілотники забезпечують суцільне спостереження території у різних діапазонах – видимому, інфрачервоному, радіо та тепловому. Отримані дані допомагають своєчасно виявляти противника, прогнозувати його наміри та виявляти зміни у структурі оборони. Особливо ефективним є застосування БпЛА у розвідці позицій артилерії, знищенні техніки противника, коригуванні вогню та оцінці результатів ураження. Такі можливості забезпечують неперервний замкнутий цикл «виявлення → аналіз → дія → контроль», який є основою сучасного управління військами.

Крім розвідувальних функцій, БпЛА активно використовуються як елемент вогневої системи. Озброєні дрони здатні завдавати точкових ударів по цілях, що зменшує потребу у залученні пілотованої авіації та дозволяє уникнути втрат особового складу. У поєднанні з наземними або морськими роботизованими системами БпЛА формують єдине бойове середовище, де рішення про вогневе ураження можуть прийматися напівавтономно. Такі підходи значно підвищують ефективність малих мобільних груп, що діють у відриві від основних сил, і дають змогу виконувати складні завдання навіть в умовах ізоляції або обмеженого зв’язку.

Особливе значення має взаємодія людини з безпілотною системою. Хоча рівень автономності сучасних дронів зростає, остаточне рішення про застосування сили залишається за людиною. Тому важливо забезпечити чітке розмежування між автоматизованими процесами збору інформації й людським контролем за застосуванням озброєння. Зловживання автономними функціями може призвести до помилкових рішень або втрати контролю над діями платформи, тому питання безпеки, відповідальності й правового регулювання залишаються ключовими у сфері розвитку військових безпілотників.

До переваг широкого застосування БпЛА належить також можливість значного скорочення людських втрат. Дрони виконують найризикованіші завдання – розвідку переднього краю, проліт над позиціями противника, наведення артилерії, пошук мінних заго-роджень – без необхідності відправляти туди особовий склад. Крім того, застосування безпілотників сприяє оптимізації логістичних операцій: вони можуть доставляти медикаменти, боєприпаси чи спорядження в райони, куди неможливо дістатися наземним транспортом. Така гнучкість робить їх незамінними в умовах динамічної обстановки,

особливо під час ведення бойових дій у міській місцевості або на важкодоступних територіях.

Водночас існують серйозні виклики. Найвразливішим місцем залишається система зв'язку. При втраті каналу управління дрон може стати некерованим. Радіоелектронна боротьба, глушіння сигналів GPS, спуфінг чи кібератаки здатні вивести безпілотну платформу з ладу. Саме тому питання захищеності каналів передачі даних, шифрування, автентифікації та створення резервних систем управління мають першочергове значення.

Не менш важливою є підготовка персоналу. Оператори БпЛА повинні володіти не лише технічними навичками керування, а й розумінням тактичного контексту, логіки прийняття рішень, особливостей взаємодії із штабами та іншими системами. Це вимагає нових навчальних програм, симуляційних тренажерів і комплексного підходу до формування «цифрової культури» військового управління. Сучасна армія, яка використовує безпілотники, повинна мислити не окремими платформами, а мережевими рішеннями, де кожен дрон – це елемент загальної системи збору, обробки та застосування інформації.

Слід зазначити, що ефективність застосування БпЛА напряму залежить від стійкості системи управління. Навіть найсучасніші дрони не принесуть користі без швидкого та точного аналізу даних, інтеграції розвідки з вогневими засобами і гнучкого планування. Тому ключовим напрямом розвитку є створення інтегрованих командно-інформаційних систем, які поєднують БпЛА з іншими роботизованими платформами, супутниковими системами та засобами кіберзахисту. У таких умовах командир отримує можливість не лише бачити ситуацію в реальному часі, а й передбачати розвиток подій.

Таким чином, безпілотні літальні апарати стають центральним елементом сучасної військової архітектури управління. Вони змінюють саму філософію ведення війни, де ключовим ресурсом стає інформація, а головним завданням – швидке перетворення даних на рішення. Поєднання автономності, швидкодії та безпеки робить БпЛА інструментом, який не лише підсилює вогневу міць, а й забезпечує стратегічну перевагу у сфері командування і контролю. Проте реалізація їхнього потенціалу можлива лише за умови технологічної сумісності, високого рівня кіберзахисту, професійної підготовки операторів і чіткого правового регулювання. В умовах сучасних збройних конфліктів дрони стали не просто засобом підтримки, а одним із ключових чинників, що визначають успіх бойових операцій і загальне військове управління Силами безпеки й оборони.

МЕЛЕНТІ Є. О.,
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

КУДРЯВЦЕВА А. П.,
військовослужбовець ЗСУ

КЛАСИФІКАЦІЯ ЗАГРОЗ, ЯКІ МОЖУТЬ БУТИ РЕАЛІЗОВАНІ ЗА ДОПОМОГОЮ БЕЗПІЛОТНИХ СИСТЕМ

Положення Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» [1] регламентують визначення «організована злочинність» – це сукупність кримінальних правопорушень, що вчиняються у зв'язку з створенням та діяльністю організованих злочинних угруповань. Основні напрями розвитку системи боротьби з організованою злочинністю та механізми реалізації державної політики визначені Стратегією боротьби з організованою [2].

В умовах широкомасштабної військової агресії рф проти України значно підвищуються ризики щодо використання спецслужбами іноземних держав організованих груп та злочинних організацій, терористів, терористичних груп для ескалації насилля й жорстокості. Наслідки таких злочинних дій є прямою загрозою національній безпеці держави й можуть призвести до підриву авторитету органів державної влади, правоохоронних органів, дестабілізації суспільно-політичної обстановки, порушення нормального функціонування об'єктів критичної інфраструктури, формування сепаратистських рухів, повалення конституційного ладу. Окремо актуалізується питання про інструментарій, який може бути застосований зловмисниками для реалізації своїх протиправних дій.

З початком широкомасштабної збройної агресії рф проти України значно збільшився незаконний обіг вогнепальної зброї, боєприпасів, саморобних вибухових пристроїв [3]. У криміналітету з'явились нові можливості з отримання зброї, боєприпасів, вибухонебезпечних речовин, а також безпілотних систем.

Досвід застосування складових сектору безпеки і оборони під час відсічі збройної агресії рф продемонстрував масштабне зростання ролі безпілотних систем та інших безекіпажних технологій. Ці засоби поступово перетворилися на критичний компонент спроможностей сектору безпеки й оборони, забезпечуючи розвідку, цілевказання, вогневе ураження, логістичну підтримку та підвищення ситуаційної обізнаності на полі бою. Масштабне впровадження дронів і роботизованих платформ суттєво вплинуло на тактику, оперативне планування й характер сучасних бойових дій, посилюючи ефективність підрозділів і зменшуючи ризики для особового складу.

Поряд зі збільшенням кількості традиційних засобів озброєння та військової техніки в Україні значно зросла кількість безпілотних систем (повітряні, наземні, морські платформи). Зокрема, більшість безпілотних систем та їх складових виготовлялись за кордоном, проте, починаючи з початку 2022 року має місце активний розвиток вітчизняного виробництва дронів і роботизованих систем. Спостерігається надшвидка трансформація вітчизняного оборонно-промислового комплексу і розвиток вітчизняної інфраструктури для проєктування, розробки і виготовлення новітніх зразків озброєння, таких як: безпілотні авіаційні комплекси, дрони-перехоплювачі, наземні й надводні, підводні роботизовані платформи, а також боєприпаси до них. На сьогодні вже з'явилася можливість самостійно придбати (надрукувати на 3D-принтері за кліше) складові частини, плати керування, мікроконтролери, завантажити з мережі Інтернет прошивку й зібрати дрон в домашніх умовах.

Збільшується кількість фахівців, які володіють сучасними компетентностями з питань застосування безпілотних систем, а громадські організації активного долучені до здійснення навчання (підготовки) персоналу, як цивільних, так і військових фахівців.

Водночас ринок безпілотних систем став не тільки перспективним напрямком військово-промислового комплексу, новими складовими економічної діяльності, сільського господарства, але й джерелом загроз для об'єктів критичної інфраструктури, цивільного населення та приватності життя людини загалом. Такі динамічні зміни в ландшафті ризиків є серйозним викликом в загальнодержавній системі боротьби з тероризмом.

Безпілотні системи щодня доводять свою ефективність на полі бою, вони стали об'єктом зацікавленості не тільки представників силових структур, органів державної влади, але й терористичних організацій, розвідувально-диверсійних груп і організованої злочинності. Для прикладу, рф залучає до проведення терористичних атак ударні повітряні безпілотники типу камікадзе для знищення об'єктів цивільної критичної інфраструктури України [4]. Ліванська терористична організація «Хезболла» все частіше використовує дрони для атак на Ізраїль [5], а єменські хусити через свої постійні атаки на об'єкти цивільного судноплавства взагалі порушили морські торгівельні шляхи в Аденській затоці та Червоному морі [6].

Сучасні високотехнологічні безпілотні системи здатні виконувати широкий спектр завдань, а технічні характеристики таких засобів дозволяють їх застосовувати і в злочинних цілях. Саме тому безпілотники стають все привабливішим інструментом для протиправної діяльності в усьому світі.

Керуючись основними положеннями Закону України «Про національну безпеку України» [7, 8], незаконне застосування безпілотних систем слід віднести до реальних та потенційних загроз національній безпеці України. Наразі в науковій літературі класифікація загроз, які

можуть бути реалізовані за допомогою роботизованих систем, відсутня. От приміром, в [9] наведено окремі протиправні дії, що можуть бути здійсненні за допомогою дронів. З урахуванням зазначеного вище, виникає потреба у систематизації загроз, що можуть бути реалізовані організованою злочинністю, терористичним організаціями, диверсійно-розвідувальними групами за допомогою безпілотних систем.

Використання безпілотних систем зумовлює появу ряду критичних небезпек, зокрема:

розвідка та ураження об'єктів критичної інфраструктури, об'єктів терористичної зацікавленості;

вбивство вищого військово-політичного керівництва держави, громадських діячів, конкурентів у бізнесі, інших осіб;

розповсюдження зброї масового знищення, матеріалів, пов'язаних з нею (джерел іонізуючого випромінювання, сильно діючих отруйних речовин, носіїв бактерій та вірусів);

грабіж та крадіжки;

контрабанда товарів через державний кордон;

доставка зброї, наркотичних засобів до місць позбавлення волі;

викрадення персональних даних з екранів телефонів, банкоматів;

збір компрометуючих фото-відеофайлів про особу;

злом інформаційно-комунікаційних систем через мережу WiFi;

здійснення технічної розвідки;

несанкціонований політ та порушення закритого повітряного простору над аеропортами, об'єктами критичної інфраструктури;

створення завад для повітряного руху;

вандалізм, псування майна;

порушення роботи каналів зв'язку та GSM мереж;

проведення спеціальних інформаційних операцій (скид листівок, застосування акустичних систем).

Попри наведений перелік, спектр можливих ризиків не є остаточним і постійно збільшується у зв'язку зі стрімким розвитком безпілотних систем, штучного інтелекту і новітніх технологій. Цей процес закономірно супроводжується їх активним освоєнням злочинними угрупованнями, терористичними структурами та іншими суб'єктами, зацікавленими у протиправній діяльності. За таких умов розробка інтелектуальних моделей застосування безпілотних систем в загальнодержавній системі боротьби з тероризмом є актуальним науковим завданням.

Список використаних джерел:

1. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30.06.1993 р. № 3341-XII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text (дата звернення: 10.09.2025).

3. Про схвалення Стратегії боротьби з організованою злочинністю : Розпорядж. Каб. Міністрів України від 16.09.2020 р. № 1126-р. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-р#Text (дата звернення: 10.09.2025).
4. Незаконний обіг зброї як загроза національній безпеці. Цілі державної політики в сфері контролю за обігом зброї, повноваження державних органів в цій сфері - Центр безпекових досліджень «СЕНСС». *Центр безпекових досліджень «СЕНСС»*. URL: https://censs.org/nezakonnyy-obih-zbroyi-yak-zahroza-natsionalniy-bezpetsi/ (дата звернення: 10.09.2025).
5. Засоби ураження російської агресії : Довідник / Є. О. Меленті та ін. Київ : НА СБУ, 2023. 140 с.
6. Ukrinform. З Лівану випустили ракети й дрони по Ізраїлю, поранені 14 військових. *Укрінформ – актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-world/3853685-z-livanu-vipustili-raketi-j-droni-po-izrailu-poraneni-14-vijskovih.html (дата звернення: 10.09.2025).
6. Лисогор І. Британія і США відбили масовану атаку хуситів ракетами і БпЛА на судна в Червоному морі. *LB.ua*. URL: https://lb.ua/world/2024/01/10/593018_britaniya_i_ssha_vidbili_masovanu_ataku.html (дата звернення: 10.09.2025).
7. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 10.09.2025).
8. Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV : станом на 9 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 05.09.2025).
9. Dronov.NET.ua – Системы защиты от дронов. *Dronov.NET.ua – Системы защиты от дронов*. URL: https://dronov.net.ua/ (дата звернення: 10.08.2025).

СІЧКО І. Г.,
курсант, Навчально-науковий інститут № 4
Харківського національного університету
внутрішніх справ

МАЛЬЦЕВ В. В.,
викладач кафедри протидії кіберзлочинності
(науковий керівник)

РОБОТИЗОВАНІ СИСТЕМИ ДЛЯ РОЗМІНУВАННЯ ТА НЕЙТРАЛІЗАЦІЇ ВИБУХОВИХ ЗАГРОЗ У ЗОНІ БОЙОВИХ ДІЙ

За оцінками експертів, Україна сьогодні є найбільш забрудненою вибухонебезпечними предметами територією в Європі та однією з найбільш постраждалих у світі. Близько 30 % території України потребує обстеження на наявність вибухонебезпечних предметів, що становить понад 174 тис. км². Ця ситуація має катастрофічні наслідки для сільського господарства країни, оскільки значні площі орних земель стали непридатними для використання. Для ефективного протидії цим викликам необхідно застосовувати сучасні технології, включаючи дистанційне зондування, машинне навчання для аналізу ризиків та

роботизовані системи для знешкодження вибухонебезпечних предметів [1, с. 45].

Україна перетворилася на випробувальний полігон для новітніх технологій гуманітарного розмінування. Ключовою ланкою цього процесу є інтегроване використання безпілотних літальних апаратів (БПЛА) та наземних роботизованих комплексів. На етапі розвідки БПЛА з мультиспектральними камерами проводять дистанційне зондування місцевості, створюючи високотонні ортофотоплани. Отримані геопросторові дані підлягають аналізу за допомогою алгоритмів машинного навчання, навчених розпізнавати характерні ознаки вибухонебезпечних об'єктів. Цей підхід дозволяє створити «цифровий відбиток» мінного забруднення та істотно зменшити площі, що потребують безпосередньої участі саперів. Для фізичної ліквідації виявлених загроз застосовуються спеціалізовані роботизовані платформи, здатні здійснювати дистанційний підрив або транспортування вибухонебезпечних предметів [2, с. 33–34].

Сучасні наземні роботизовані комплекси для розмінування характеризуються модульною архітектурою, що дозволяє їх швидку адаптацію до різних типів завдань – від розвідки з використанням маніпуляторів до знешкодження вибухонебезпечних предметів за допомогою спеціалізованого обладнання. Застосування таких систем дозволяє значно знизити ризики для життя саперів та проводити роботи в умовах складної місцевості. Міжнародна технічна допомога у вигляді поставок спеціалізованих роботизованих комплексів суттєво посилює можливості України у сфері гуманітарного розмінування [3, с. 88].

Безпілотні літальні апарати (БПЛА) відіграють вирішальну роль у сучасному гуманітарному розмінуванні, забезпечуючи оперативну розвідку великих територій та виявлення дрібних аномалій. Сучасні платформи, оснащені багатоспектральними камерами, тепловізорами та високоточними оптичними сенсорами, значно підвищують ймовірність виявлення мін та боєприпасів. Отримані дані корелюються з магнітометричними вимірами та історичною інформацією про бойові дії в регіоні. Алгоритми машинного зору дозволяють автоматично маркувати потенційно небезпечні об'єкти для подальшої верифікації саперами, що значно знижує час обстеження та ризики для людського життя. Ці технології є особливо ефективними в сільській місцевості, де залишкові вибухонебезпечні предмети становлять серйозну загрозу для цивільного населення [4, с. 112].

Інтеграція штучного інтелекту (ШІ) у процеси гуманітарного розмінування охоплює дві ключові функції: прискорення аналізу великих масивів даних та підтримку прийняття рішень оператором. Сучасні алгоритми комп'ютерного зору дозволяють істотно знизити кількість помилкових спрацьовувань шляхом аналізу текстур ґрунту, рослинності та морфологічних ознак вибухонебезпечних предметів. Прогностичні моделі, що базуються на історичних даних про перебіг бойових дій, дозволяють будувати ймовірнісні карти забруднення території. Між-

народні стандарти та рекомендації підкреслюють необхідність збереження людини в контурі прийняття рішень, водночас визнаючи потенціал ШІ для оптимізації розподілу ресурсів та скорочення часу пошуку загроз. Паралельно тривають дослідження щодо розробки етико-правових рамок застосування автономних систем у гуманітарному розмінуванні [5, с. 67–68].

Сучасні оперативні методи нейтралізації вибухонебезпечних предметів поєднують традиційні саперні методики з інноваційними роботизованими рішеннями. Серед них – дистанційне підривання виведених боєприпасів у спеціально підготовлених кар'єрах під відеоспостереженням, застосування локалізованих зарядів для мінімізації ураження уламками, а також установка інженерних бар'єрів для контролю за розльотом фрагментів. Для очищення великих площ ефективно використовуються важкі фрезерні машини, інтегровані з магнітними та радарними датчиками. Водночас, обмежені ресурси вимагають чіткого пріоритету: першочерговими завданнями є відновлення транспортної інфраструктури, сільськогосподарських угідь та об'єктів життєзабезпечення. Реалізація такого підходу неможлива без тісної координації між державними органами, міжнародними партнерами та місцевими громадами [6, с. 45].

Українські підрозділи, залучені до гуманітарного розмінування, стикаються з низкою практичних викликів: нестабільний зв'язок у зоні проведення робіт, що ускладнює дистанційне керування технікою; складність технічного обслуговування та логістичного забезпечення роботизованих комплексів у польових умовах; дефіцит кваліфікованих операторів; та висока собівартість обладнання. Додатковим фактором ризику є тактика противника щодо несистемного розміщення вибухонебезпечних пристроїв, що вимагає постійної адаптації процедур та нестандартних інженерних рішень. Для подолання цих обмежень необхідні цілеспрямовані інвестиції в підготовку операторів, створення мобільних сервісних центрів та розвиток стійких систем зв'язку [7, с. 23].

Відновлення територій після бойових дій вимагає ефективного очищення сільськогосподарських угідь та інфраструктури. Роботизовані системи забезпечують безпечне та швидке виконання цих завдань, сприяючи відновленню життєдіяльності громад. Ключовим чинником успіху є прозоре планування, координація з місцевими органами влади та залучення міжнародних донорів. Сучасні ініціативи українських та міжнародних організацій зосереджені на постачанні мобільних комплексів, підготовці місцевих фахівців та створенні власних сервісних центрів, що дозволяє зменшити залежність від зовнішньої допомоги [8, с. 91–92].

Стратегія гуманітарного розмінування в Україні має ґрунтуватися на трьох взаємопов'язаних компонентах: технологічному розвитку (модульні робототехнічні комплекси, штучний інтелект для аналізу даних, вдосконалені сенсорні системи), інституційній підтримці

(розробка національних програм, стандартизація процедур, сертифікація операторів) та міжнародній кооперації (фінансування, обмін технологіями, гармонізація стандартів безпеки). Паралельно необхідно розвивати систему інформування цивільного населення, створювати публічні карти ризиків та впроваджувати навчальні програми з мінної безпеки. Комплексна реалізація цих заходів дозволить мінімізувати гуманітарні втрати, прискорити економічне відновлення та забезпечити повернення безпечного доступу до територій [9, с. 215].

Військова агресія Росії проти України стала каталізатором розвитку та впровадження інноваційних технологій гуманітарного розмінування. Сучасний підхід поєднує дистанційну розвідку з використанням БПЛА, автоматизовану обробку аерофотознімків за допомогою штучного інтелекту та застосування наземних роботизованих комплексів для фізичного знешкодження вибухонебезпечних предметів. Однак технологічні рішення є лише частиною успіху. Для стійкого відновлення безпеки необхідні системні інституційні зміни, інвестиції в підготовку фахівців та розробка чітких стандартів використання автономних систем. Комплексна реалізація цих заходів забезпечить не лише подолання безпосередніх загроз, але й довгострокову життєздатність постраждалих громад [10, с. 248].

Список використаних джерел:

1. Коваленко В. В. *Гуманітарне розмінування в Україні: сучасні виклики та технологічні рішення*. Київ : Наука і освіта, 2024. 278 с.
2. Мельник Я. О., Захарченко В. М. Інтегровані робототехнічні комплекси для гуманітарного розмінування: сучасний стан та перспективи застосування в Україні // *Системи озброєння і військова техніка*. 2024. № 3(71). С. 30–38.
3. Шевчук В. М. *Роботизовані системи для гуманітарного розмінування: теорія та практика*. Львів : Апріорі, 2024. 245 с.
4. Ковальчук О. В., Петренко С. М. *Дистанційні методи виявлення вибухонебезпечних предметів: застосування БПЛА та штучного інтелекту*. Київ : Видавництво НТУУ «КПІ», 2024. 280 с.
5. Мороз В. П., Савченко Л. М. *Штучний інтелект у системах гуманітарного розмінування: технології, етика, перспективи*. Харків : Вид-во Харківського університету, 2024. 204 с.
6. *Інженерне забезпечення гуманітарного розмінування: теорія та практика* / за ред. І. В. Коваленка. Київ : Видавничий дім «Академперіодика», 2024. 312 с.
7. Бондар О. І., Шевчук Р. М. *Організаційно-технічні аспекти застосування роботизованих комплексів у гуманітарному розмінуванні*. Львів : Видавництво Львівської політехніки, 2024. 168 с.
8. *Гуманітарне розмінування та відновлення інфраструктури: управління, технології, практика* / за ред. В. П. Коваля. Київ : Видавництво «Логос», 2024. 245 с.
9. *Стратегічні пріоритети гуманітарного розмінування в Україні: технології, управління, безпека* / за ред. О. М. Сідорчука. Київ : Видавництво «Освіта України», 2024. 280 с.

10. *Інноваційні технології в гуманітарному розмінуванні: досвід України та світові тенденції* / за ред. В. І. Мельника, О. В. Ковальчук. Київ : Видавничий дім «Освіта України», 2024. 320 с.

СОЛОНЕНКО В. В.,
старший викладач кафедри вогневої підготовки,
Навчально-науковий інститут логістики
Національної академії Національної гвардії України

ЗАСТОСУВАННЯ РОБОТИЗОВАНИХ СИСТЕМ ПРИ ВИКОНАННІ ОПЕРАТИВНО-БОЙОВИХ ЗАВДАНЬ: ПЕРЕВАГИ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Зараз, коли бойові дії тривають щодня, а інтенсивність їх не знижується, питання використання новітніх технологій стоїть особливо гостро. Тема організації оборони та наступу має не теоретичне, а цілком практичне значення. Сучасне поле бою змінюється, і, як показує практика, ключову роль у цих змінах відіграє роботизація. Ми бачимо, як безпілотні авіаційні комплекси (БПЛА), наземні роботизовані комплекси (БПНЛА) та підводні апарати перетворюються з допоміжного засобу на основний елемент виконання оперативно-бойових завдань. З мого досвіду, ці системи вже довели, що можуть впливати на кінцевий результат операції. Мета моєї доповіді – показати реальні переваги, з якими ми стикаємося на фронті, а також окреслити виклики, які нам доведеться «відпрацьовувати» у найближчому майбутньому.

1. Підвищення рівня безпеки та ефективності особового складу

На практиці ми завжди починаємо з того, щоб максимально уберегти наших людей. Саме тому ключова перевага впровадження роботів – це критичне зниження ризику для бійців. Роботизовані системи буквально «виводять» людину з-під удару, виконуючи найбільш небезпечні завдання.

З власного досвіду, я бачу, що роботи відпрацьовують там, де піхота не може або де ризик надто високий [1]. Це:

Розмінування. Спеціалізовані комплекси заходять у забруднені зони для знешкодження мін та вибухівки. Це дозволяє зберегти саперів та прискорити просування.

Розвідка та коригування. БПЛА, особливо малого радіусу, висять над ціллю, забезпечуючи чітке спостереження вночі чи в складних умовах. Вони знімають всю інформацію і передають її в реальному часі. В результаті, ми отримуємо повну картину без втрат.

Вогнева підтримка. Ми вже використовуємо платформи, які можуть подати вогневу підтримку прямо у вогневий контакт. Це дає можливість зберегти бойовий потенціал підрозділу і підвищує нашу оперативну ефективність [3].

Таким чином, коли роботи беруть на себе цільові та найбільш ризиковані завдання, особовий склад може сфокусуватися на стратегічних рішеннях, а не на прямому виживанні.

2. Технологічні виклики та необхідність інтеграції у єдиний інформаційний простір

Однак, в реальності, не все так гладко. Просто купити багато дронів недостатньо. Щоб роботи працювали, як єдиний «кулак», ми повинні подолати серйозні технічні «головні болі».

2.1. Стійкість та автономність систем

Зараз противник активно застосовує РЕБ. Тому головна проблема – як пробити цей електронний «щит» і забезпечити стійкий зв'язок [4]. Нам потрібна максимальна автономність. Тобто, якщо зв'язок «ліг», робот має вміти самостійно вийти із зони ураження і повернутися на базу. Через це ми активно працюємо над новими алгоритмами навігації та енергозабезпеченням.

2.2. Стандартизація та інтеграція

Я стикався з тим, що у підрозділі може бути десяток різних моделей дронів, які не можуть «поділитися» інформацією між собою. Тому необхідно стандартизувати інтерфейси – щоб дрон від однієї компанії, танк від іншої, а наземний робот від третьої говорили однією мовою. Наша мета – створити єдиний бойовий «мозок», де всі дані з роботів зливаються для швидкого прийняття рішень [2].

2.3. Кібербезпека

Чим більше систем у нас на полі бою, тим більше «дірок» для ворожих кібератак. Захист наших систем управління, аби ворог не міг «підрізати» зв'язок чи перехопити контроль над роботом, є життєво важливим.

3. Етично-правові аспекти та підготовка операторів нового покоління

Впровадження роботів тягне за собою і певні «незручні» питання, які ми як армія повинні вирішити, і кардинально змінює підхід до підготовки кадрів.

3.1. Етичні та правові виклики автономності

Зокрема, коли ми говоримо про високоавтономні бойові системи (ВБС), які самі приймають рішення про ураження цілі, постає питання: хто відповідає за помилку? [5] Через це міжнародне право ще не встигло «догнати» технології. Ми вважаємо, що повинні мати чіткі інструкції, аби дії роботів відповідали законам ведення війни.

3.2. Трансформація системи підготовки

Роль військового змінилася. Зараз ти не просто стрілець, ти оператор-аналітик. З мого досвіду, майбутнє – це про підготовку не стільки до рукопашного бою, скільки до «війни в джойстику». Ми повинні переорієнтувати підготовку на:

Глибокі технічні знання (експлуатація, ремонт).

Розуміння кібербезпеки та алгоритмів ШІ.

Здатність швидко обробити масиви інформації, які «скидає» робот, і визначити пріоритети [3].

Висновки

Підсумовуючи, можна сказати, що роботизовані системи – це реальний фактор перемоги. Вони зберігають життя наших бійців і підвищують ефективність дій. Для того, щоб це реально працювало у бойових умовах, нам потрібно:

Забезпечити максимальну стійкість систем до РЕБ.

Досягти повної інтеграції різних платформ у єдиний інформаційний простір.

Нарешті, перевести систему підготовки кадрів на «технічні рейки» і визначити етичні рамки застосування автономних систем.

Ці дії дозволять нам успішно відпрацьовувати будь-які оперативно-бойові завдання у майбутньому.

Список використаних джерел:

1. Погребняк В. М., Коренев А. Г. Проблемні питання застосування бойових роботизованих систем у військових конфліктах. *Збірник наукових праць Національної академії сухопутних військ імені гетьмана Петра Сагайдачного*. 2019. № 2(54). С. 136–144.
2. Павленко В. О., Гальченко В. О. Перспективи застосування безпілотних авіаційних комплексів у бойових діях. *Наука і техніка Повітряних Сил Збройних Сил України*. 2021. № 1(42). С. 104–109.
3. Клочко О. Г. Роботизовані системи у сучасній війні: питання ефективності та безпеки. *Вісник Національного університету оборони України*. 2020. № 1(53). С. 132–138.
4. СБУ, НАУ, МОУ. *Сучасні роботизовані комплекси та системи*. Київ : Видавництво НАУ, 2022. 312 с.
5. Рябчун А. М. Етичні та правові аспекти використання автономних бойових систем. *Правове регулювання у сфері безпеки*. 2021. № 3. С. 45–51.

ЧАЛЕНКО П. В.,
курсантка, Інститут Служби безпеки України
Національного юридичного університету
імені Ярослава Мудрого

ІНТЕГРАЦІЯ БЕЗПІЛОТНИХ СИСТЕМ У КОНТРРОЗВІДУВАЛЬНІ ОПЕРАЦІЇ: ВИЯВЛЕННЯ АГЕНТУРНИХ МЕРЕЖ ТА ДОКУМЕНТУВАННЯ ПРОТИПРАВНОЇ ДІЯЛЬНОСТІ

Складна ситуація з нацбезпекою змушує по-новому оцінювати інструментарій контррозвідувальної роботи. Війна продемонструвала: звичайні оперативні прийоми вже не справляються без технологічної підтримки. Бойові безпілотні авіаційні системи (БпАС) виправдали себе

на фронті й довели корисність для спецзавдань силовиків [2]. Статистика Міноборони за 2024-й: дозволено експлуатувати 40+ різновидів дронів плюс 20+ наземних роботів, галузь розвивається блискавично, попит на нові рішення зростає [3].

Служба безпеки України, реалізуючи власний мандат із захисту держбезпеки, постійно шукає свіжі підходи до боротьби з підривними діями чужих розвідок. Гібридна війна створює умови, коли супротивник масово задіює агентуру – збирає дані, координує диверсії, розхитує внутрішню стабільність. Старі контррозвідувальні схеми тут мало-ефективні. БпАС розкривають абсолютно нові перспективи: фіксація правопорушень, формування доказової бази, розкриття агентурних структур.

Якісна зміна загроз вимагає адекватної реакції спецслужб. Якщо раніше увага концентрувалася на офіційних іноземних представниках, зараз у фокусі – розгалужені мережі впливових агентів, диверсантів, терористичних координаторів. Розкриття таких структур потребує комплексності, де технічні спостережні засоби грають провідну партію.

Практика показує: безпілотні апарати результативно вирішують декілька пріоритетних контррозвідувальних завдань:

Передусім – латентне спостереження за «цікавими» об’єктами. На відміну від наземних груп, що вимагають чимало людей і легко демаскуються досвідченими ворожими агентами, дрони забезпечують цілодобовий контроль із безпечної дистанції [11]. Критично важливо під час розробки шпигунів чи членів диверсійно-розвідувальних груп (ДРГ). Сучасні апарати баражують на сотнях метрів висоти, залишаючись непоміченими, але гарантуючи якісний відеозапис потужними камерами зі збільшенням.

Надзвичайно цінна можливість – відстеження маршрутів підозрілих фігур. Класичне наземне стеження потребує багатьох екіпажів, що змінюють одне одного проти демаскування. Завжди є ризик загубити ціль у міському трафіку чи малонаселених локаціях. БпАС позбавлені цього мінусу – один апарат безупинно супроводжує авто фігуранта годину і довше, фіксуючи зупинки, контакти, відвідувані точки. БпАС дають змогу документувати взаємодію між оперативно цікавими особами. Нинішні безпілотники мають камери високої чіткості, що фіксують деталі з кількасотметрової висоти [14]. Така фото-відеофіксація стає вагомим доказом у кримінальній справі за умови процесуальної коректності отримання. Наприклад, зустріч підозрюваного у співробітництві з чужою розвідкою та офіційного представника країни-агресора може бути зафіксована з багатьох кутів – це дасть змогу ідентифікувати учасників, записати час-місце контакту, можливу передачу речей чи документації.

Особливо важливе застосування БпАС для пошуку «конспіративних квартир» – приміщень для зустрічей агентів із кураторами. Регулярне спостереження за такими локаціями дозволяє встановлювати

всіх відвідувачів, знаходити закономірності візитів, збирати докази для кримінального переслідування.

Використання дронів виявляє закономірності та маршрути пересування, що можуть вказувати на розвідувальну активність. Систематичний контроль виявляє періодичні зустрічі в певних локаціях, відвідування критичної інфраструктури чи інші підозрілі дії [18]. Аналіз накопиченої інформації реконструює структуру агентурної мережі, встановлює зв'язки між членами, визначає ключові фігури для нейтралізації.

БпАС застосовуються для моніторингу критичних об'єктів з метою виявлення спроб несанкціонованого проникнення, фотофіксації чи іншої розвідувальної активності. Особливо актуально для енергетики, оборонпрому, транспортних вузлів. Систематичне патрулювання периметру безпілотниками швидко виявляє підозрілу активність і дозволяє превентивні дії. Безпілотні системи ефективні для фіксації слідів диверсій. При вибухах, пожежах чи інших інцидентах на критично важливих об'єктах БпАС оперативно прибувають на місце й фіксують обстановку з різних ракурсів – важливо для розслідування. Аерофото дає загальну картину місця події, виявляє шляхи підходу диверсантів, фіксує сліди, що можуть зникнути до прибуття слідчої групи.

Варто згадати можливість застосування БпАС для пошуку несанкціонованих передавачів. Окремі сучасні безпілотники мають спеціальні сенсори для виявлення радіовипромінювання. Корисно для пошуку прихованих камер, прослуховуючих пристроїв чи передавачів, встановлених іноземними агентами на оперативно цікавих об'єктах.

Важлива особливість застосування БпАС – використання в умовах підвищеної небезпеки. Скажімо, під час затримання озброєних диверсантів чи терористів дрони спостерігають за об'єктом, надаючи оперативній групі актуальні дані про локацію злочинців, їхні переміщення, можливі шляхи відступу. Це суттєво підвищує безпеку співробітників та ефективність операції.

Щодо сучасних безпілотних систем – вони мають характеристики, придатні для контррозвідувальних завдань. Зокрема, тривалість польоту окремих моделей досягає кількох годин, що дозволяє тривале спостереження без заміни апарату [9]. Деякі БпАС обладнані тепловізорами – це робить можливим спостереження вночі та за несприятливої погоди. Тепловізійні камери виявляють людей навіть у повній темряві, тумані чи за густої рослинності – критично важливо для виявлення ДРГ у приміських зонах чи лісових масивах.

Важливий технологічний момент – автоматичне відслідковування об'єктів. Сучасні системи комп'ютерного зору дозволяють БпАС автоматично супроводжувати рухомі об'єкти – авто чи пішоходів – без постійного втручання оператора. Це знижує навантаження на персонал і дозволяє паралельно контролювати кілька об'єктів.

Перспективне використання роїв безпілотників, коли кілька дронів координують дії для спільного завдання. Скажімо, один БпАС веде загальне спостереження за районом, інші зосереджуються на конкретних об'єктах інтересу. Така координація забезпечує безперервне спостереження навіть коли один дрон потребує заміни батареї чи повернення на базу.

Також важлива робота в умовах активної радіоелектронної боротьби. Сучасні системи глушіння порушують GPS-навігацію чи блокують канали управління дроном. Для протидії розробляються системи автономної навігації, що використовують інерціальні датчики, комп'ютерний зір та штучний інтелект для орієнтування без супутникових сигналів.

Проблема – тривалість польоту. Більшість електричних дронів перебувають у повітрі від 30 хвилин до 2 годин, часто недостатньо для тривалих операцій спостереження. Для вирішення можуть використовуватися системи автоматичної заміни батарей чи гібридні силові установки на бензині та електриці.

На практиці виникає питання: чи можна вважати достатньою підставою для застосування БпАС інформацію з агентурних джерел, якщо вона не підтверджена іншими доказами? Чи потрібен судовий дозвіл на застосування дронів для спостереження в кожному випадку, чи достатньо рішення керівника оперативного підрозділу? Ці питання відкриті й потребують законодавчого врегулювання.

Щоб матеріали відеоспостереження використовувалися як докази в суді, необхідне дотримання процедури їх отримання та фіксації. КПК України встановлює вимоги до належності, допустимості та достовірності доказів [5]. Практика показує: суди нерідко ставлять під сумнів докази, отримані з порушенням порядку чи за відсутності належного процесуального оформлення. Зокрема, виникають питання щодо ідентифікації технічних засобів фіксації. Чи достатньо вказати модель дрона, чи необхідно надавати детальну технічну документацію про характеристики? Як засвідчити автентичність відеозапису й довести відсутність монтажу чи втручання? Хто має право виступати оператором БпАС під час контррозвідувальних операцій – чи повинен це бути атестований співробітник СБУ, чи можна залучати цивільних спеціалістів?

Доцільно прийняти спеціальне Положення про порядок застосування безпілотних авіаційних систем у діяльності СБУ, яке б детально врегулювало всі аспекти використання цих технічних засобів. Таке Положення могло б визначити: перелік завдань, для вирішення яких допускається застосування БпАС; підстави для прийняття рішення про застосування; порядок отримання судового дозволу, якщо необхідно; вимоги до кваліфікації операторів; порядок зберігання та використання отриманих матеріалів; механізми захисту прав випадково зафіксованих осіб.

Також важливе створення спеціалізованих підрозділів у складі СБУ, які б займалися виключно застосуванням БпАС у контррозвідувальній роботі. Такі підрозділи могли б накопичувати досвід, розробляти методики, проводити навчання інших співробітників. Централізація експертизи дозволила б забезпечити однаковий рівень якості операцій з використанням безпілотників у всіх регіонах країни.

Необхідно розробити систему контролю за застосуванням БпАС для запобігання можливим зловживанням. Такий контроль може здійснюватися як внутрішніми службами безпеки СБУ, так і зовнішніми органами – прокуратурою, судами, парламентськими комітетами. Важливо забезпечити прозорість у застосуванні цих технологій, наскільки можливо без шкоди для оперативної роботи.

Європейські країни також розробляють нормативну базу для регулювання застосування БпАС у правоохоронній діяльності, намагаючись знайти баланс між потребами безпеки та захистом приватності. Німеччина прийняла детальні правила використання дронів поліцією, які вимагають судового дозволу для спостереження за конкретними особами понад певний час. Франція активно використовує БпАС для забезпечення безпеки під час масових заходів та для боротьби з тероризмом, але запровадила жорсткі обмеження щодо обробки персональних даних, зафіксованих під час таких операцій.

Ізраїль, традиційний лідер у розробці та застосуванні безпілотних технологій, активно використовує БпАС у контртерористичних операціях. Ізраїльський досвід цікавий тим, що там вдалося інтегрувати безпілотні системи в загальну систему забезпечення національної безпеки, забезпечивши ефективну координацію між різними відомствами.

Український досвід використання безпілотників у бойових умовах визнається унікальним і вивчається фахівцями з усього світу [14]. Україна фактично стала полігоном для відпрацювання нових тактик застосування БпАС, включаючи координацію дій кількох дронів, використання штучного інтелекту для аналізу отриманої інформації, протидію системам радіоелектронної боротьби. Однак це переважно стосується військового застосування. Для повноцінного впровадження БпАС у контррозвідувальну роботу необхідно адаптувати наявні технології до специфіки оперативних завдань та створити відповідну правову базу.

Цікавий досвід країн Балтії, які, маючи спільну загрозу з боку російських спецслужб, активно впроваджують сучасні технології в контррозвідувальну роботу. Естонія розробила цифрову систему управління оперативною інформацією, що дозволяє ефективно інтегрувати дані з різних джерел, включаючи БпАС, для виявлення агентурних мереж.

На мою думку, необхідно розробити та затвердити нормативні документи, які б детально регламентували порядок застосування БпАС. Доцільно створити спеціалізовані підрозділи БпАС у складі регіональних

управлінь СБУ. Налагодити систему постійної підготовки та перепідготовки операторів БпАС, а також взаємодію з науковими установами та приватними компаніями, які розробляють безпілотні технології. Україна має потужний ІТ-сектор і виробників дронів, які можуть створювати спеціалізовані рішення для потреб СБУ. І наостанок, необхідно створити систему моніторингу та оцінки ефективності застосування БпАС.

Також активно розробляються системи автономних дронів, здатних виконувати завдання без постійного контролю оператора. Такі системи зможуть самостійно патрулювати визначені території, виявляти підозрілу активність та сигналізувати про неї. Це дозволить значно розширити масштаби моніторингу без відповідного збільшення персоналу.

Перспективний напрям – розробка мікродронів, які завдяки малим розмірам практично непомітні та можуть використовуватися для спостереження в умовах міської забудови. Такі пристрої могли б проникати всередину будівель через вікна або вентиляційні отвори, забезпечуючи унікальні можливості для документування діяльності агентурних мереж.

Розробляються також спеціалізовані системи протидії ворожим БпАС. Оскільки іноземні спецслужби також можуть використовувати дрони для розвідки об’єктів СБУ або спостереження за оперативними співробітниками, необхідні ефективні засоби виявлення та нейтралізації таких загроз. Це може включати радари для виявлення малих повітряних об’єктів, системи глушіння каналів управління, навіть спеціальні дрони-перехоплювачі.

Аналізуючи вищевикладене, можливо дійти висновку, що інтеграція безпілотних систем у контррозвідувальну діяльність СБУ є об’єктивною необхідністю, зумовленою сучасними загрозами національній безпеці України. БпАС відкривають принципово нові можливості для виявлення агентурних мереж, документування протиправної діяльності та збору доказової бази. Досвід бойового застосування безпілотників в Україні показує їхню високу ефективність, і цей потенціал може бути успішно адаптований для потреб контррозвідки. Необхідно прийняття спеціальних нормативних актів, які б чітко визначали підстави та порядок застосування БпАС, вимоги до технічних характеристик обладнання, процедуру оформлення отриманих матеріалів, механізми контролю за дотриманням законності. Важливою є також розробка системи підготовки спеціалістів, яка б охоплювала технічні, правові та етичні аспекти використання безпілотних систем.

Список використаних джерел:

1. Аналіз досвіду застосування безпілотних літальних апаратів та визначення напрямку їх подальшого розвитку при веденні мережецентричних операцій. ResearchGate. 2018. URL: https://www.researchgate.net (дата звернення: 19.10.2025).
2. Доктрина Головнокомандувача ЗСУ «Застосування безпілотних систем у силах оборони України» від 01 січ. 2024 р. № 49/НВГШ. Київ : ГШ ЗСУ, 2024. 55 с.

3. З початку 2024 року Міноборони допустило до експлуатації вже понад 40 зразків безпілотників та понад 20 наземних роботів. Кабінет Міністрів України. 2024. URL: https://www.kmu.gov.ua (дата звернення: 19.10.2025).
4. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
5. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI (у редакції від 01 серп. 2025 р.). Відомості Верховної Ради України. 2013. № 9–10, № 11–12, № 13. Ст. 88.
6. Наземні роботизовані комплекси: основи та майбутнє. Молодий вчений. 2021. № 5. С. 112–118.
7. Нові зразки БпЛА в Україні – 2 суттєвих досягнення щодо безпілотників за 2024 рік. 24 Канал. 2024. URL: https://24tv.ua (дата звернення: 19.10.2025).
8. Нові тенденції використання безпілотників у 2025 році. Аналіз американського експерта. Голос Америки. 2025. URL: https://www.holosameryky.com (дата звернення: 19.10.2025).
9. Ожеван М. А. Автоматизовані робототехнічні системи озброєнь. Київ : Національний інститут стратегічних досліджень, 2017. 48 с.
10. Повноваження органів і підрозділів, які здійснюють контррозвідувальну діяльність. WikiLegalAid. URL: https://wiki.legalaid.gov.ua (дата звернення: 19.10.2025).
11. Повноваження органів і підрозділів, які здійснюють оперативно-розшукову діяльність. WikiLegalAid. URL: https://wiki.legalaid.gov.ua (дата звернення: 19.10.2025).
12. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93.
13. Про контррозвідувальну діяльність : Закон України від 26 груд. 2002 р. № 374-IV (у редакції від 31 берез. 2023 р.). Відомості Верховної Ради України. 2003. № 12. Ст. 89.
14. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.
15. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII (у редакції від 09 серп. 2024 р.). Відомості Верховної Ради України. 1992. № 22. Ст. 303.
16. Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229-XII (у редакції від 31 лип. 2025 р., із змінами, внесеними згідно із Законом № 4542-IX від 16 лип. 2025 р.). Відомості Верховної Ради України. 1992. № 27. Ст. 382.
17. Роль і місце роботизованих систем у сучасних війнах і збройних конфліктах: теоретичний аспект. ResearchGate. 2023. URL: https://www.researchgate.net (дата звернення: 19.10.2025).
18. Руснак В., Хоменко Є., Лисий О. Інноваційний підхід щодо науково-технічного супроводу експериментальних досліджень роботизованих комплексів (систем) в бойових умовах, проблеми та шляхи вирішення. Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2024. № 20(2). С. 72–77.

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В УМОВАХ ВОЄННОГО СТАНУ

Матеріали Всеукраїнської науково-практичної конференції

ВИПУСК 2

Друкується в авторській редакції

Комп'ютерне макетування *С. С. Костиря*
Художнє опрацювання *А. В. Зеленько*

Формат 60х84/16. Ум. друк. арк. 15,11.
Обл.-вид. арк. 15,84. Тираж 9 прим. Заявка № _____

Видавець і виготовлювач
Національна академія Служби безпеки України,
03066, м. Київ, вул. Михайла Максимовича, буд. 22.
Свідоцтво суб'єкта видавничої справи ДК № 6844 від 17.07.2019