прикордонних структур. Це дозволяє підвищити обґрунтованість управлінських рішень, здійснювати прогнозування загроз, планувати службово-бойове застосування підрозділів і координувати дії з іншими суб'єктами забезпечення державної безпеки.

Використання засобів радіоелектронної боротьби (окопних РЕБ, антидронових рушниць) в найближчій перспективі стане обов'язковим елементом мобільних груп швидкого реагування, які в разі ускладнення обстановки мають бути готовими запобігти неправомірному застосуванню FPV дронів та дронів інших типів. Це зумовлює необхідність для гвардійців володіти знаннями у сфері радіоелектроніки, які раніше були характерні переважно для вузькопрофільних фахівців. Є перспектива розширення використання БпАК та НРК в інтересах виконання завдань під час охорони громадського порядку, припинення масових заворушень, охорони особливо важливих державних об'єктів, тощо.

Таким чином короткий аналіз впливу сучасних технологій на тактику застосування підрозділів НГУ в ході виконання службово-бойових завдань дає напрям для подальших наукових розвідок в напрямку розширення можливостей використання.

ЯРОШИК ВАСИЛЬ СЕРГІЙОВИЧ
курсант 125 навчальної групи факультету забезпечення державної безпеки Київський інститут Національної гвардії України

ЯРЕМА ВЛАДИСЛАВ ВАЛЕРІЙОВИЧ
старший викладач кафедри соціально-гуманітарних дисциплін Київський інститут Національної гвардії України

ЦИВІЛЬНО-ВІЙСЬКОВЕ СПІВРОБІТНИЦТВО В НАЦІОНАЛЬНІЙ ГВАРДІЇ УКРАЇНИ: ПРАКТИЧНИЙ ВИМІР ТА СУЧАСНІ ВИКЛИКИ

В умовах тривалої повномасштабної збройної агресії проти України межа між фронтом і тилом стала максимально розмитою, а забезпечення стійкості держави вимагає комплексного підходу. Для Національної гвардії України (НГУ), яка органічно поєднує функції військового формування та правоохоронного органу, ефективна взаємодія з цивільним населенням перестала бути виключно допоміжним елементом. Відповідно до Закону України «Про Національну гвардію України» та Закону України «Про правовий режим воєнного стану», на гвардійців покладається широкий спектр завдань із забезпечення державної безпеки. У цьому контексті цивільно-військове співробітництво (ЦВС) стає критичною запорукою успішного виконання як бойових, так і стабілізаційних завдань. Наукова новизна полягає у систематизації практичного досвіду підрозділів НГУ у сфері цивільно-військового співробітництва (ЦВС/CIMIC) під час повномасштабної війни, визначенні ключових аспектів їхньої інтеграції з громадами, а також обґрунтуванні необхідності формування специфічних лідерських компетенцій у військовослужбовців для роботи з цивільним середовищем. З огляду на це, мета доповіді – проаналізувати роль цивільно-військового співробітництва у зміцненні обороноздатності держави, забезпеченні життєдіяльності громад та окреслити перспективи розвитку системи підготовки кадрів для підрозділів CIMIC у структурі НГУ.

Сучасний досвід ведення бойових дій доводить, що успіх військових операцій залежить не лише від наявності новітнього озброєння чи тактичної переваги, а й від міцності тилу та безпосередньої підтримки місцевого населення. Згідно з чинною доктриною Збройних Сил України, цивільно-військове співробітництво розглядається як невід'ємна складова оперативного мистецтва. Особлива роль НГУ у системі ЦВС зумовлена її подвійною природою: будучи складовою Сил оборони України, вона одночасно виконує правоохоронні

функції. Це дозволяє підрозділам НГУ виступати найбільш ефективним комунікаційним та координаційним «містком» між військовим командуванням, місцевими військовими адміністраціями та територіальними громадами.

Аналіз практичної діяльності підрозділів CIMIC НГУ за останні роки дозволяє виокремити декілька ключових аспектів та напрямів роботи:

1. Гуманітарна безпека, логістика та відновлення правопорядку. На деокупованих територіях (Київщина, Харківщина, Херсонщина) військовослужбовці НГУ одними з перших забезпечували доставку гуманітарних вантажів (продовольства, питної води, медикаментів) у райони з повністю зруйнованою логістичною інфраструктурою. Це сприяло не лише фізичному виживанню населення, а й поверненню відчуття присутності державної влади, відновленню базового правопорядку та запобіганню мародерству.

2. Евакуаційні заходи в умовах екстремального ризику. Евакуація цивільного населення з районів активних бойових дій (Бахмут, Авдіївка, прикордоння Сумщини та Харківщини) часто здійснювалася із залученням бронетехніки НГУ безпосередньо під вогнем противника. Участь в організації «зелених коридорів» вимагала від гвардійців не лише тактичної майстерності, а й значної психологічної витримки для координації дій та заспокоєння громадян, зокрема осіб похилого віку, які перебували у стані глибокого шоку.

3. Формування безпечного середовища та протимінна діяльність. Залучення піротехнічних підрозділів НГУ для перевірки цивільних об’єктів, ліній електропередач та сільськогосподарських угідь є критично важливим для відновлення економіки регіонів. Крім того, проведення систематичних занять з мінної безпеки для цивільних формує високий рівень довіри місцевих мешканців. Завдяки цій співпраці громадяни оперативно повідомляють гвардійців про підозрілі предмети, що безпосередньо рятує життя.

4. Інформаційна стійкість та протидія когнітивним загрозам. Шляхом прямої комунікації з громадами офіцери CIMIC ефективно нейтралізують ворожі інформаційно-психологічні операції (ІПСО) та поширюють верифіковану інформацію. Спільні тренування з цивільним населенням щодо алгоритмів дій під час ракетно-дронових обстрілів та надання домедичної підготовки підвищують загальну резистентність суспільства до стресових факторів війни.

5. Імплементація міжнародних стандартів. НГУ активно інтегрує стандарти НАТО (зокрема, керівництво AJP-3.19), що передбачає системний підхід до розуміння цивільного середовища. Це забезпечує прозору та дієву взаємодію з міжнародними гуманітарними інституціями (структури ООН, Міжнародний комітет Червоного Хреста) та гарантує цільовий розподіл допомоги у прифронтових зонах.

6. Військове лідерство та підготовка кадрів. Ефективність системи CIMIC критично залежить від рівня підготовки особового складу. Виконання завдань цивільно-військового співробітництва вимагає від майбутніх офіцерів НГУ не лише фахових військових знань, а й розвитку специфічних лідерських якостей. Здатність брати на себе відповідальність за життя цивільних у кризових ситуаціях, високий рівень емоційного інтелекту, емпатія та навички крос-культурної комунікації стають обов'язковими компетенціями. Саме тому впровадження сучасних методик виховання військового лідерства ще на етапі навчання курсантів у закладах вищої освіти зі специфічними умовами навчання є нагальною потребою сьогодення.

Незважаючи на значні досягнення, система ЦВС у НГУ стикається з низкою викликів. Серед них варто виокремити нестачу спеціалізованих транспортних та технічних засобів у деяких підрозділах, надзвичайно високе психоемоційне навантаження на особовий склад, а також потребу у швидкій адаптації до динамічної безпекової ситуації.

Підсумовуючи, цивільно-військове співробітництво в Національній гвардії України довело свою абсолютну ефективність як ключовий інструмент військової та соціальної стабілізації. Подальший розвиток цього напряму вимагає посилення інституційної підтримки держави, цифровізації комунікаційних каналів з територіальними громадами та якісного розширення штату кваліфікованих офіцерів CIMIC. Додаючи до базових принципів НГУ «Честь. Мужність. Закон» аспект людяності та військового лідерства, гвардійці доводять, що саме в консолідації зусиль армії та народу закладена головна стратегічна перевага України над ворогом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національну гвардію України : Закон України від 13.03.2014 № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18.
2. Про оборону України : Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12
3. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VII. URL: https://zakon.rada.gov.ua/laws/show/389-19
4. Доктрина «Цивільно-військове співробітництво» (СП 9-00(01).01) : затверджена Головнокомандувачем Збройних Сил України від 01.07.2020. URL: https://sprotyvg7.com.ua
5. Цивільно-військове співробітництво: алгоритм ефективної взаємодії громадських організацій та вищих військових навчальних закладів. *Проблеми інженерно-педагогічної освіти*. 2022. № 74. С. 25–31.

ЯХІН РОСТИСЛАВ РУШАНЬОВИЧ
курсант 2 навчального курсу 3 групи

ГОНТАР АНАСТАСІЯ ВАДИМІВНА
курсантка 2 навчального курсу 2 групи Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ МАСОВИХ КІБЕРАТАК З БОКУ АГРЕСОРА

Повномасштабне вторгнення росії на територію України, що триває з 24 лютого 2022 року, перетворило кіберпростір на середовище збройного протистояння. Кібератаки та інформаційно-психологічні операції агресора стали невід'ємними складовими гібридної війни, яка поєднує традиційні військові методи з економічними, інформаційними та кібернетичними засобами впливу. Саме тому інформаційна безпека держави в умовах інтенсивних кібератак є одним із пріоритетних завдань у системі національної безпеки України, що безпосередньо пов'язане з боєздатністю збройних сил та ефективністю системи державного управління.

Гібридна агресія росії проти України характеризується поєднанням кінетичних та некінетичних засобів: збройні удари супроводжуються кібератаками, дезінформаційними кампаніями та інформаційно-психологічними операціями. Тривале інформаційне протиборство є основою насильницького впровадження інтересів агресора, а силовому ресурсу відводиться лише підсилююча роль на окремих етапах збройного конфлікту. Посилення агресії проти суверенних держав передбачає удари по системах державного управління, економіці через ракетні обстріли інфраструктури, кібератаки та пропаганду [1].

Масові кібератаки на українські державні установи та бізнес розпочалися задовго до відкритого військового вторгнення. З початком бойових дій 24 лютого 2022 року їх кількість подвоїлася – з приблизно 200 на місяць до понад 400 [2]. Служба безпеки України у 2020 році зафіксувала 800 кібератак, у 2021 році – близько 2 000, а після початку повномасштабного вторгнення – понад 4 500. Станом на лютий 2023 року СБУ відбила понад 550 атак, при цьому в середньому на добу фіксується понад десять кібератак різних типів [3]. Найбільш поширеними стали DDoS-атаки, злом великих компаній з подальшою крадіжкою інформації та дефейс популярних ресурсів. Під прикриттям масових атак продовжують діяти кіберзлочинці, націлені на державний сектор, банківську сферу, паливно-енергетичний комплекс, наукові установи.

Федеральні спецслужби росії систематично застосовують шкідливе програмне забезпечення – віруси, трояни, програми-вимагачі, хробаки – для ураження державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Типовою методологією кібератак є збір інформації засобами OSINT, використання шкідливого програмного коду, несанкціоноване втручання в державну цифрову інформаційну інфраструктуру. Окремою загрозою залишаються фішингові атаки: лише у 2022 році Національний банк України виявив понад 4 500 фішингових ресурсів, а в першому кварталі 2023 року – вже понад 11 000 шахрайських доменів, переважна більшість яких має російське походження [4].