

СТРАТЕГІЇ ВДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ЗАСАД ОХОРОНИ ДИПЛОМАТИЧНИХ ПРЕДСТАВНИЦТВ НАЦІОНАЛЬНОЮ ГВАРДІЄЮ УКРАЇНИ

Беринець Михайло Михайлович¹

Опубліковано	Секція	УДК
28.04.2025	Право	[342.951 : 351.82](477)

DOI: <https://doi.org/10.5281/zenodo.15353077>

Анотація. У статті розглянуто проблему охорони дипломатичних представництв в Україні в умовах воєнного стану, зокрема визначено сучасні загрози їхній безпеці та проаналізовано рівень нормативно-правового забезпечення діяльності Національної гвардії України (НГУ) у цій сфері. З'ясовано, що міжнародно-правовий фундамент охорони дипустанов закладено у Віденській конвенції про дипломатичні зносини 1961 року, яка вимагає від держави перебування вживати всіх належних заходів для їх захисту. Охарактеризовано положення чинного законодавства України, зокрема Закону «Про Національну гвардію України», яким на НГУ покладено функції щодо забезпечення охорони дипломатичних установ. Доведено, що в умовах воєнного стану окремі правові норми, які регулюють використання спеціальних засобів, є неузгодженими з оперативними потребами забезпечення безпеки, а також містять обмеження, що ускладнюють реагування у разі реальної загрози.

Запропоновано комплексну стратегію вдосконалення організаційно-правових засад охорони, яка включає: оновлення нормативної бази, формалізацію міжвідомчої взаємодії, створення мобільних підрозділів швидкого реагування, посилення кіберзахисту та інформаційної стабільності. Акцентовано увагу на необхідності впровадження стандартів інформаційної гігієни серед військовослужбовців, покращення технічного оснащення охоронних підрозділів та розгортання систем відеоспостереження з елементами штучного інтелекту. Обґрунтовано доцільність створення ситуаційних центрів при МВС або РНБО з метою оперативного реагування на загрози, а також впровадження системи регулярних навчань для підвищення готовності сил охорони до кризових сценаріїв.

Сформовано висновки про необхідність системної модернізації нормативного забезпечення охорони дипломатичних об'єктів, а також адаптації національної моделі до загрозо-орієнтованого підходу, що базується на принципах ризик-менеджменту та міжвідомчої координації. У контексті досвіду країн НАТО доведено доцільність поєднання воєнно-цивільних ресурсів для ефективного захисту дипломатичних установ, з урахуванням зростаючої ролі кібербезпеки та інформаційної протидії у забезпеченні національної безпеки України.

Ключові слова: дипломатичні представництва, охорона, Національна гвардія України, воєнний стан, міжнародне право, нормативно-правове забезпечення, міжвідомча взаємодія, кібербезпека, ризик-менеджмент, національна безпека.

¹ Слухач кафедри військового права та правоохоронної діяльності Інституту стратегічних комунікацій, <https://orcid.org/0000-0002-5898-3228>

STRATEGIES FOR IMPROVING THE ORGANIZATIONAL AND LEGAL BASIS OF PROTECTION OF DIPLOMATIC MISSIONS BY THE NATIONAL GUARD OF UKRAINE

Abstract. The article considers the problem of protecting diplomatic missions in Ukraine under martial law, in particular, identifies current threats to their security and analyzes the level of regulatory and legal support for the activities of the National Guard of Ukraine (NGU) in this area. It is found that the international legal foundation for the protection of diplomatic missions is laid in the Vienna Convention on Diplomatic Relations of 1961, which requires the host state to take all appropriate measures to protect them. The provisions of the current legislation of Ukraine, in particular the Law "On the National Guard of Ukraine", which assigns the NGU the functions of ensuring the protection of diplomatic institutions, are characterized. It is proven that in conditions of martial law, certain legal norms regulating the use of special means are inconsistent with the operational needs of ensuring security, and also contain restrictions that complicate the response in the event of a real threat.

A comprehensive strategy for improving the organizational and legal foundations of security is proposed, which includes: updating the regulatory framework, formalizing interdepartmental interaction, creating mobile rapid response units, strengthening cyber defense and information stability. Attention is focused on the need to implement information hygiene standards among military personnel, improving the technical equipment of security units and deploying video surveillance systems with elements of artificial intelligence. The feasibility of creating situational centers at the Ministry of Internal Affairs or the National Security and Defense Council for the purpose of operational response to threats, as well as implementing a system of regular exercises to increase the readiness of security forces for crisis scenarios, is substantiated.

Conclusions were drawn about the need for systematic modernization of the regulatory support for the protection of diplomatic facilities, as well as adaptation of the national model to a threat-oriented approach based on the principles of risk management and interagency coordination. In the context of the experience of NATO countries, the feasibility of combining military-civilian resources for the effective protection of diplomatic institutions has been proven, taking into account the growing role of cybersecurity and information countermeasures in ensuring the national security of Ukraine.

Keywords: diplomatic missions, security, National Guard of Ukraine, martial law, international law, regulatory support, interagency interaction, cybersecurity, risk management, national security.

Вступ

Постановка проблеми дослідження. Формування дієвої системи охорони дипломатичних представництв на території України в контексті зростання зовнішніх і внутрішніх загроз становить один із пріоритетних напрямів забезпечення національної безпеки та дотримання міжнародно-правових зобов'язань держави. Відповідно до норм Віденської конвенції про дипломатичні зносини 1961 року, держава перебування зобов'язана вживати всіх необхідних заходів для захисту приміщень дипломатичних місій від посягань будь-якого характеру. В українській правовій системі виконання цього обов'язку покладено, зокрема, на Національну гвардію України як військове формування з визначеним колом правоохоронних повноважень. Правові підстави для реалізації зазначених функцій встановлено у низці нормативно-правових актів міжнародного і національного рівнів, зокрема в Конституції України, законах України «Про Національну гвардію України», «Про правовий режим воєнного стану», «Про правовий режим надзвичайного стану», а також у відповідних підзаконних нормативних актах Міністерства внутрішніх справ України.

Разом із тим, чинне правове регулювання діяльності Національної гвардії України у сфері охорони дипломатичних установ характеризується відсутністю системності, обмеженою гнучкістю в умовах функціонування особливих правових режимів і недостатнім рівнем нормативного забезпечення міжвідомчої взаємодії. Практичне виконання охоронних завдань здійснюється в умовах підвищеної динаміки безпекових викликів, що зумовлює потребу у розробленні гнучких організаційно-правових механізмів, удосконаленні алгоритмів планування і реагування, а також оптимізації кадрового та матеріально-технічного ресурсу. Окрему складність становить відсутність уніфікованих моделей тактичної організації служби охорони, а також неузгодженість правового статусу підрозділів НГУ, які залучаються до охорони дипломатичних об'єктів у періоди дії надзвичайного або воєнного стану.

З огляду на зазначене, актуалізується необхідність науково обґрунтованого визначення стратегічних підходів до вдосконалення організаційно-правових засад охорони дипломатичних представництв в Україні, що дозволить забезпечити належну реалізацію функцій Національної гвардії відповідно до міжнародних стандартів, підвищити ефективність безпекової взаємодії та забезпечити стабільність у сфері дипломатичного захисту.

Аналіз останніх досліджень та публікацій. Питання правового статусу та організаційних функцій Національної гвардії України, її місця у системі сил безпеки та оборони, а також особливостей реалізації повноважень в умовах правового режиму воєнного або надзвичайного стану, знайшли відображення у науково-практичному дискурсі. Значний внесок у теоретичне осмислення функціонування НГУ здійснили такі дослідники, як Г.С. Буга, О.В. Агапов, І.М. Волков, Д.О. Горбач, О.А. Олещенко, В.І. Перепадя та інші вітчизняні науковці.

Однак у зазначених наукових дослідженнях залишено поза увагою системний аналіз трансформацій охоронної функції НГУ в контексті загроз державному суверенітету та безпеці іноземних дипломатичних місій, що ускладнює формування ефективних стратегій удосконалення правового забезпечення цієї діяльності в сучасних умовах.

Мета статті – визначити та обґрунтувати стратегії вдосконалення організаційно-правових засад охорони дипломатичних представництв Національною гвардією України.

Результати

Охорона дипломатичних представництв (посольств, консульських установ) в Україні регламентується як міжнародним, так і внутрішнім правом. На міжнародному рівні ключовим документом є Віденська конвенція про дипломатичні зносини (1961), стаття 22 якої зобов'язує країну перебування «застосовувати всі належні заходи для захисту приміщень представництв від будь-якого вторгнення чи збитків» та запобігання порушенню спокою дипустанов. Конституція України проголошує повагу до принципів дипломатичного імунітету, недоторканності дипломатичних представництв, а також орієнтацію зовнішньої політики держави на забезпечення національної безпеки шляхом міжнародного співробітництва. На законодавчому рівні питання охорони іноземних дипломатичних місій закріплені у низці нормативно-правових актів. Зокрема, згідно із Законом України «Про Національну гвардію України», до основних завдань цього військового формування віднесено охорону дипломатичних представництв, консульських установ іноземних держав і представництв міжнародних організацій, акредитованих в Україні [3].

У період дії воєнного стану зазначене законодавство передбачає розширення повноважень Національної гвардії України, зокрема в частині забезпечення охорони приміщень, будівель та іншого майна дипломатичних представництв у разі їх евакуації,

а також супроводу персоналу таких місій. Окремі організаційні аспекти залучення підрозділів НГУ до виконання зазначених функцій врегульовано Положенням «Про організацію та несення служби з охорони дипломатичних представництв, консульських установ іноземних держав і представництв міжнародних організацій в Україні», затвердженим наказом МВС. У цьому документі визначено порядок несення служби, умови мобілізаційної готовності, а також механізми взаємодії НГУ з іншими суб'єктами сектору безпеки і оборони у разі настання надзвичайних або воєнних ситуацій [2].

Важливе значення у забезпеченні належного рівня охорони об'єктів дипломатичного статусу має функціональна координація дій через Міністерство закордонних справ України. Зокрема, Департамент державного протоколу та відповідні підрозділи МЗС здійснюють загальну координацію процесів захисту дипломатичних представництв, забезпечуючи належну комунікацію з силовими структурами та сприяючи виконанню міжнародно-правових зобов'язань України в цій сфері.

Отже, чинна нормативна база містить низку положень, що визначають завдання НГУ в охороні дипмісій і підкреслюють міжнародні зобов'язання України. Зокрема, законодавство прямо покладає на НГУ захист дипустанов від зовнішніх загроз і передбачає участь у заходах при введенні воєнного стану [3]. Однак деякі аспекти нормативного забезпечення потребують уточнення та адаптації. Наприклад, слід детальніше прописати процедури застосування права сили та спецзасобів у дипломатичній сфері, зважаючи на обмеження, накладені міжнародним правом (вимога згоди глави місії) і умовами воєнного стану.

В існуючій системі охорони дипустанов виникають правові колізії і суттєві прогалини. Однією з таких проблем є обмеження застосування спецзасобів та сили на території дипмісій. Так, українське законодавство забороняє військовослужбовцям НГУ застосовувати фізичний вплив чи спецзасоби у приміщеннях і на земельних ділянках диппредставництв без попередньої письмової згоди голови відповідної місії [3]. Унаслідок наявних законодавчих обмежень, у ситуаціях реальної загрози (зокрема у разі виявлення озброєних диверсійно-розвідувальних груп на території дипломатичного представництва) військовослужбовці Національної гвардії України не мають повноважень на оперативне застосування силових заходів без попереднього погодження з уповноваженими органами. Така вимога створює ризики затримки реагування, що суперечить самому призначенню охоронної функції, а також потенційно унеможлиблює своєчасну нейтралізацію загрози. В умовах правового режиму воєнного стану подібна правова колізія породжує ситуацію, за якої для забезпечення безпеки дипломатів або припинення терористичної дії необхідне залучення інших суб'єктів безпекового сектору (зокрема підрозділів Національної поліції або Служби безпеки України), що ускладнює реагування та може мати критичні наслідки в умовах високої динаміки загроз.

Також існує неузгодженість повноважень і координації між силовими відомствами. Завдання охорони дипустанов у воєнний час формально закріплено за НГУ, проте МВС, СБУ, Прикордонна служба та місцева поліція залучаються за ситуацією без чіткої нормативної єдності, що спричиняє дублювання зусиль або, навпаки, «прогалини» – наприклад, у віддалених регіонах дипломатичні місії можуть бути на сторожі місцевої поліції, а НГУ практично не залучався. Відсутність загальнонаціональної стратегії охорони дипмісій під час війни посилює ці розбіжності. Крім того, багато підзаконних актів (наказів, інструкцій) давно не оновлювались з огляду на реалії сучасного конфлікту, а нерегульованість питань розподілу відповідальності між цивільними службами та військовими породжує операційні збої.

До практичних труднощів належать також кадрово-технічні проблеми. Так наявні підрозділи НГУ (наприклад, 22-га окрема бригада) чисельно та ресурсно обмежені. Вони змушені одночасно охороняти десятки об'єктів, що перевантажує особовий склад.

Нестача спеціалізованої техніки (бронетранспортерів, БПЛА, систем ППО малої дальності), застаріла зв'язкова мережа і недостатня кіберзахищеність комунікацій дипломатичних об'єктів створюють додаткові вразливості. Наприклад, останніми роками російські хакерські угруповання АРТ29 здійснили масштабні кібератаки по посольствах у багатьох країнах Європи [6], що вимагає від України підсилити ІТ-безпеку своїх дипустанов. Інформаційна агресія, що є складовою гібридної війни проти України, охоплює й дипломатичну сферу. Зокрема, фіксується активне поширення дезінформації та провокаційних повідомлень, зокрема фейків про нібито наявні загрози для співробітників іноземних дипломатичних місій, закликів до насильницьких дій або штурму посольств, що належать державам-партнерам України. Недостатній рівень уваги до інформаційного захисту об'єктів дипломатичного призначення становить серйозну практичну проблему, оскільки розповсюдження неперевіреної або навмисно викривленої інформації здатне спричинити масову паніку, дестабілізацію громадського порядку та створення умов для організованих провокацій поблизу дипломатичних установ.

У контексті повномасштабної війни спектр загроз для дипломатичних представництв істотно розширився. Ракетні та авіаудари по містах України стали реальністю. Так, у грудні 2024 року внаслідок російського ракетного обстрілу Києва були пошкоджені посольства шести держав (Албанія, Аргентина, Палестина, Північна Македонія, Португалія, Чорногорія) [4], що продемонструвало прямий ризик руйнувань об'єктів дипломатичного призначення і травмування персоналу. У таких умовах охорона дипмісій вимагає потужної протиракетної та протиповітряної оборони на місцях, а також ефективної системи швидкого оповіщення.

Війна загострила небезпеку терактів і диверсій. Вітчизняна розвідка фіксує спроби підготовки диверсій проти стратегічних об'єктів, і дипломатичні установи не є виключенням. Як зазначав командир 22-ї бригади, під час воєнного стану головним завданням було запобігти проникненню диверсантів на територію закордонних дипустанов – завдяки цьому жодне посольство Києва не зазнало руйнувань чи нападів [5]. Проте ризик залишається, особливо у вигляді замаскованих СВП чи снайперського вогню по посольській охороні. НГУ має постійно проводити розвідку загроз та навчання з протидії терористам, перевіряти підозрілих осіб та транспортні засоби поблизу дипмісій.

Хоча в Україні рідко спостерігаються акції протесту біля іноземних посольств (як це сталося наприклад у Західній Європі), теоретично можливі провокації, коли агресор намагатиметься використати демонстрації для нападів на дипустанови. Особливо це стосується країн, які відкрито підтримують Україну чи запровадили санкції проти РФ. В умовах мобільних соціальних мереж та «клікових» загроз існує небезпека, що хакнути масову акцію, спровокувати хаотичні заворушення у центрі Києва, створити загрозу для дипломатів і співробітників консульств. Організувати безпеку у таких ситуаціях складно, адже треба одночасно контролювати цивільні протести та охороняти охоронювані об'єкти, уникнувши ескалації конфлікту з місцевим населенням.

Інформаційна війна супроводжує бойові дії, агресор системно розповсюджує вигадки про «небезпечні дії» дипломатичних представництв, втручання закордонних спецслужб, «загрози життю російськомовного населення» поблизу посольств. Такі кампанії можуть спровокувати напругу та недовіру місцевих жителів або стати виправданням для покарання персоналу місій. Окрім того, атаки на репутацію українських дипломатичних установ (наприклад, фейки про їхню корупційну діяльність) можуть знизити ефективність зовнішньої політики. Важливим викликом є створення власної стійкої системи інформаційного захисту, тобто своєчасне спростування фейків, роз'яснення мети роботи дипломатів і розкриття реальних фактів.

Останнім часом дедалі більше виявляється, що дипломатичні установи стають об'єктами потужних кібератак. У листопаді 2023 року Рада нацбезпеки повідомила, що російське угруповання АРТ 29 здійснило широкомасштабні атаки на посольства в усьому світі (Італія, Греція, Румунія, Азербайджан тощо) [6]. Основна мета – зібрати розвідувальну інформацію для прийняття рішень у сфері зовнішньої політики і оборони. Для України це означає необхідність посилення кіберзахисту дипломатичних каналів зв'язку, авіа- та телекомунікаційних систем. В умовах воєнного стану і тотальної присутності кіберзагроз навіть «цифрова» атака (злам електронної пошти, систем відеоспостереження, пожежної сигналізації дипмісії) може створити хаос і небезпеку. Тому своєчасне впровадження сучасних засобів інформаційно-технічного захисту стало критично важливим завданням.

Отже, на основі проведеного аналізу пропонуємо впровадити наступні кроки:

1. Уточнення повноважень НГУ та співробітництва. Потрібно оновити законодавчі акти для чіткішої фіксації ролі НГУ у захисті дипломатичних об'єктів під час воєнного стану. Наприклад, розглянути скасування чи пом'якшення обмежень на застосування спецзасобів у випадках реальної загрози для посольства – як це передбачено статтею 17 Закону України «Про Національну гвардію України [3]. Також доцільно закріпити механізми координації роботи НГУ з МВС, СБУ та Службою зовнішньої розвідки в окремому підзаконному нормативі (наказ МВС чи РНБО), встановивши єдиний «командний пункт» для прийняття рішень.

2. Запропонувати введення спеціального нормативного акту (наказ МВС або рішення РНБОУ) для воєнного стану, що знімає частину дипломатичного «протоколу» в інтересах безпеки. Наприклад, чітко прописати порядок взаємодії із дипломатами при евакуації, режим конфіденційності інформації, що унеможливить інтерпретацію закону «як завгодно» в критичній ситуації та усуне прогалини, коли норма права не відповідає потребам захисту.

3. Розширити 22-гу бригаду охорони дипломатичних представництв і створити подібні підрозділи у регіонах. Окрім батальйонів стаціонарної охорони, необхідно сформувати спеціальні мобільні загони швидкого реагування – аналог до естонської «Бригади охорони посольств». Вони мають бути укомплектовані бронеавтомобілями та медичною технікою для негайного реагування на інциденти біля дипустанов. Досвід Естонії показує ефективність «програмної» охорони – поліція і прикордонники утворюють Службу охорони дипмісій за оцінкою загроз [7]. Україна може впровадити подібну мультиагенційну систему, де НГУ виконує роль «оператора охорони», а інші служби – додаткову підтримку.

4. Створити міжвідомчий штаб (на рівні оперативного командування НГУ, ГШ ЗСУ, МВС і МЗС) для оперативного моніторингу безпеки дипустанов. Цей штаб повинен мати доступ до розвідувальних даних, повітряного спостереження та прогнозів СБУ, аби координувати дії у разі загрози. Регулярні командно-штабні навчання з відпрацювання атак на посольства (реальні сценарії з брейнштурмом) підвищать готовність сил реагування.

5. Організувати контр-розвідувальні та превентивні заходи – перевірка підозрілих співробітників дипустанов, контроль переміщень автотранспорту, спецпідрозділи НГУ для виявлення вибухівки. Встановлення «сірих зон» доступу (периметр посольства + прилеглі квартали) під наглядом гвардії. Запровадити регулярні опитування персоналу посольств про наявні ризики та аутсорс ризиків (наприклад, консультації з Держспецзв'язку щодо кібер- і техзахисту).

6. Військовослужбовці, які призначаються на охорону дипустанов, мають пройти додаткове навчання з питань дипломатичного протоколу, англійської (і інших мов), психологічної стійкості та тактичної медицини. Елітні спостережні групи НГУ потрібно

забезпечити практичною підготовкою з охорони представництв (натурні заняття в посольствах, тренажери кризових ситуацій).

7. Запровадити системні курси з вивчення іноземних мов та культурних особливостей держав, представникам яких надається охорона, є доцільним заходом, що сприятиме підвищенню ефективності міжособистісної та міжвідомчої взаємодії з іноземними дипломатами, зниженню ризику комунікативних непорозумінь у кризових ситуаціях, а також покращенню здатності своєчасно ідентифікувати інформаційно-психологічні впливи та потенційні провокації в інформаційному середовищі відповідних країн.

8. Ввести спеціальні контрактні посади в НГУ з привабливими умовами служби (вищі зарплати, доплати за службу біля дипломатичних об'єктів) для залучення професійних воїнів. Розглянути можливість залучення резервістів та ветеранів війни на контрактній основі, які мають бойовий досвід та дисципліну. Це дозволить збільшити людський ресурс охоронних підрозділів без надмірного розростання постійної армії.

Крім того, на наш погляд, для посилення безпеки потрібно масово впровадити відеоспостереження з автоматичним аналізом поведінки, датчики руху і диму, охоронну сигналізацію з безпечним каналом зв'язку. Створити централізований ситуаційний центр, куди стікатимуть тривожні сповіщення з усіх дипмісій. Варто використовувати безпілотні літальні апарати для патрулювання периметра уночі. Естонський досвід програми «Guard Service of Embassies» показує ефективність комплексного підходу. Так, у посольства підключають і стаціонарні системи (IP-відеоспостереження), і мобільні групи (прийом і реагування на тривоги).

А також, значно посилити інформаційну і кібероборону, тобто забезпечити дипмісії захищеними VPN-каналами, системами шифрування та антивірусного захисту, найняти спеціалістів з кібербезпеки під об'єкти дипломатичної служби. Ввести обов'язкове багатофакторне автентифікування на всіх офіційних ресурсах посольств. Регулярно проводити аудит IT-інфраструктури дипмісій і симуляції кібератак, що допоможе запобігати витоку конфіденційної інформації та нейтралізувати хакерські загрози, які дедалі частіше використовуються проти дипломатів.

Особливого увагу в сучасних умовах необхідно приділити створенню в МЗС/НГУ постійного підрозділу для моніторингу інформаційного поля навколо дипмісій, що спільно з медіа-експертами та представниками посольств формуватиме єдину лінію комунікації, тобто оперативно спростовуватиме фейки та провокації в соцмережах і ЗМІ. Доцільним напрямом удосконалення організаційно-правових засад охорони дипломатичних представництв є підвищення рівня інформаційної обізнаності особового складу Національної гвардії України. Зокрема, необхідним є впровадження елементів підготовки з інформаційної гігієни, що передбачає формування навичок виявлення деструктивного інформаційного впливу, розпізнавання провокаційних або фейкових повідомлень, а також забезпечення належного порядку оперативного інформування командування про зафіксовані інформаційні інциденти.

Започаткувати публічні інформаційні кампанії про роль і функції дипмісій у безпеці України, що створить суспільне розуміння важливості їхньої недоторканості і зменшить ризик підтримки популістичних ініціатив проти них. Наприклад, публікації в медіа й соцмережах, пресбрифінги МЗС спільно з керівниками бригади НГУ, тематичні відео про будні охоронців посольств допоможуть формувати довіру громадян.

Як відомо, у країнах НАТО охорона дипломатичних представництв здійснюється за іншою моделлю, що може бути корисною для запозичення. В США функція захисту посольств належить Державному департаменту (Bureau of Diplomatic Security), який використовує спеціальний персонал (Diplomatic Security Service) і підрозділ Marine Security Guards – морської піхоти США, що постійно дислокується у закордонних місцях. Ці підрозділи високо професійні та озброєні, при цьому не залежать від місцевих силових

структур. У Польщі охорону іноземних дипмісій традиційно здійснюють польські прикордонники або державна охоронна служба (раніше BOR, нині SOP) спільно з поліцією та частково приватними охоронними агентствами. Естонія формалізувала загрозо-орієнтовану схему, всі інциденти порушень на дипломатичних об'єктах негайно доповідаються Поліції та Пограничній службі [1, с. 285]. При цьому, посольства у Естонії охороняє спеціальна Embassy Guard Service – структура з поліції та прикордонників. Захист формується на основі оцінки рівня ризику, так, у містах проводиться цілодобове спостереження, а за потреби мобілізуються патрулі і резервні групи реагування [7]. Подібно, у Німеччині захисту дипломатів забезпечує Федеральна поліція (Bundespolizei) та служба держохорони при МВС, при цьому активно використовуються кримінальна розвідка і державні спецслужби (ВКА) для прогнозування загроз.

Характерними ознаками підходу НАТО до забезпечення охорони дипломатичних установ є чітке функціональне розмежування між цивільними спеціальними службами та військовими структурами, орієнтація на принципи ризик-менеджменту, а також активне впровадження сучасних технологій у сфері безпеки. Практика Сполучених Штатів Америки та Естонії демонструє, що інтеграція державних сил охорони з приватними охоронними структурами здатна суттєво підвищити загальну ефективність захисних заходів. Водночас слід відзначити, що у США та країнах Західної Європи охорона дипломатичних представництв здійснюється відповідно до завчасно розроблених і стандартизованих процедур із залученням значних матеріальних та технічних ресурсів, тоді як в Україні подібна система лише перебуває на етапі становлення та інституціоналізації.

Таким чином, удосконалення захисту дипломатичних представництв НГУ в умовах воєнного стану потребує комплексного підходу. По-перше, необхідне оновлення нормативної бази, щоб усунути конфлікти законодавства і чітко визначити порядок дій у кризових ситуаціях (наприклад, зміни до Закону про НГУ щодо спецзасобів). По-друге, необхідно організаційно розбудувати систему охорони, перш за все створити мобільні загони швидкого реагування, покращити міжвідомчу координацію і навчання за сценаріями нападів на посольства. По-третє, інвестиції у персонал і техніку мають бути пріоритетними, тобто проводити підвищення кваліфікації охоронців дипломатичних місій, забезпечення їх сучасними засобами спостереження, бронетехнікою, засобами зв'язку. Крім того, інформаційний захист – не менш важливий, оскільки формування офіційних каналів комунікації і підвищення медіаграмотності особового складу та дипломатів допоможуть протистояти дезінформації.

Зважаючи на досвід країн НАТО, Україні варто переходити до гнучкішої, ризик-орієнтованої моделі охорони, тобто активно використовувати оцінку загроз і залучати кращі практики міжнародного співробітництва. У підсумку, поєднання оновлених нормативних механізмів, вдосконаленої структури НГУ та сучасних технологій дозволить забезпечити охорону дипломатичних установ на рівні, адекватному викликам воєнного часу.

Висновки

Проведений аналіз виявив критичні прогалини у чинному законодавстві, зокрема щодо регламенту застосування спецзасобів на території дипломатичних об'єктів, а також відсутність чітких процедур взаємодії між Національною гвардією України, МВС, СБУ та іншими структурами сектору безпеки в умовах воєнного стану. Окрім нормативних колізій, спостерігається значний дефіцит кадрових і технічних ресурсів, а також недостатня кібер- та інформаційна захищеність дипломатичних об'єктів. Реальні інциденти, такі як обстріли посольств у Києві в грудні 2024 року, лише підтверджують необхідність термінової модернізації системи захисту. З урахуванням міжнародного досвіду, зокрема практики США, Естонії та країн НАТО, доцільним є перехід до

інтегрованої, загрозо-орієнтованої моделі охорони, яка передбачає оновлення нормативно-правової бази, створення мобільних підрозділів реагування, інвестування в сучасні технології та підвищення кваліфікації особового складу. У поєднанні з посиленням кіберзахисту, формуванням міжвідомчих штабів координації та інформаційною стабілізацією це дозволить адаптувати систему охорони дипломатичних представництв до умов гібридної війни та забезпечити виконання міжнародних зобов'язань України в умовах сучасних загроз.

Список літератури

1. Коломієць Ю.М., Трояновський В.С. Взаємодія Національної поліції з Національною гвардією України під час виконання службово-бойових завдань в умовах воєнного стану: постановка проблеми. *Південноукраїнський правничий часопис*. 2023. № 3. С. 283–289.

2. Про затвердження Положення про організацію та несення служби з охорони дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних організацій в Україні військовими частинами і підрозділами Національної гвардії України: Наказ МВС України від 02.02.2016 № 74. *Відомості Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/z0320-16#Text>(дата звернення: 25.04.2025)

3. Про Національну гвардію України: Закон України від 13.03.2014 № 876-VII (редакція від 27.06.2024). *Відомості Верховної Ради України*. URL: <https://zakon.rada.gov.ua/go/876-18>

4 Унаслідок російської атаки пошкоджені посольства шести країн у Києві. 2024. УКРІНФОРМ. <https://www.ukrinform.ua/rubric-regions/3940253-unaslidok-rosijskoi-ataki-postrazdali-posolstva-sesti-krain-u-kiievi.html#>:

5. У Нацгвардії розповіли, як охороняють посольства під час воєнного стану. 03.05.2022. УКРІНФОРМ. URL: <https://www.ukrinform.ua/rubric-society/3473952-u-nacgardii-rozprovili-ak-ohoronaut-posolstva-pid-cas-voennogo-stanu.html#>:

6. У Хакери з росії атакували посольства по всій Європі – звіт НКЦК. <https://www.rnbo.gov.ua/ua/Diialnist/6708.html#>:

7. Diplomatic Immunities and Privileges in Estonia. June 2022 Ministry of Foreign Affairs of the Republic of Estonia State Protocol Department. URL: file:///Users/liliia/Downloads/kasiraamat_2022_1.pdf