

УДК 355.45:351.86(477)

DOI <https://doi.org/10.32782/2311-8040/2026-2-7>

Мовчан Анатолій Васильович,

доктор юридичних наук, професор,

професор кафедри оперативно-розшукової діяльності,

Львівський державний університет внутрішніх справ,

вулиця Городоцька, 26, Львів, 79000, Україна

ORCID: <https://orcid.org/0000-0002-6997-6517>

Scopus-Author ID: <https://www.scopus.com/authid/detail.uri?authorId=58689980100>

Researcher ID: <https://www.webofscience.com/wos/author/rid/AAJ-7771-2021>

МІЖВІДОМЧА ВЗАЄМОДІЯ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ: СУТНІСТЬ, ПРОБЛЕМИ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ

Анотація. У статті досліджено сутність та значення міжвідомчої взаємодії у діяльності сил сектору безпеки і оборони. Проаналізовано основні проблеми координації між суб'єктами безпекового середовища, визначено принципи ефективної взаємодії та окреслено сучасні інструменти її вдосконалення. Зазначається, що система суб'єктів міжвідомчої взаємодії є складною багаторівневою структурою. Її ефективність визначається рівнем координації, чіткістю розподілу повноважень та здатністю до інтеграції зусиль усіх учасників. Підкреслюється, що аналіз практики свідчить про наявність низки проблем реалізації міжвідомчої взаємодії, серед яких: відсутність єдиних механізмів координації, обмежений обмін інформацією, технічна несумісність систем, фрагментарність нормативно-правового регулювання та недостатній рівень підготовки персоналу.

Серед основних напрямів удосконалення взаємодії виділяється створення спільних ситуаційних центрів, впровадження інтегрованих інформаційних систем, проведення міжвідомчих навчань, стандартизація процедур діяльності та використання сучасних інформаційних технологій. Особливу увагу приділено міжнародному досвіду та можливостям його імплементації в Україні. Підкреслюється, що у країнах НАТО широко застосовується принцип взаємосумісності (interoperability), який передбачає здатність різних сил діяти в єдиному операційному середовищі. Її реалізація забезпечується через стандартизацію процедур, уніфікацію технічних рішень і спільну підготовку персоналу. Запропоновано практичні рекомендації щодо підвищення ефективності міжвідомчої співпраці.

Ключові слова: міжвідомча взаємодія, сектор безпеки і оборони, правоохоронні органи, координація, національна безпека, управління, інтеграція.

Movchan Anatolii. INTER-AGENCY INTERACTION OF FORCES IN THE SECURITY AND DEFENSE SECTOR: ESSENCE, PROBLEMS, AND DIRECTIONS FOR IMPROVEMENT

Abstract. The article examines the essence and significance of interagency interaction in the activities of the security and defense sector forces. The main problems of coordination between subjects of the security environment are analyzed, the principles of effective interaction are determined, and modern tools for its improvement are outlined. It is noted that the system of subjects of interagency interaction is a complex multi-level structure. Its effectiveness is determined by the level of coordination, the clarity of the distribution of powers, and the ability to integrate the efforts of all participants. It is emphasized that the analysis of practice indicates the presence of a number of problems in the implementation of interagency interaction, including: the lack of unified coordination mechanisms, limited information exchange, technical incompatibility of systems, fragmentation of regulatory and legal regulation, and insufficient level of personnel training.

Among the main areas of improving interaction, the creation of joint situational centers, the implementation of integrated information systems, conducting interdepartmental exercises, standardization of activity procedures, and the use of modern information technologies are highlighted. Particular attention is paid to international experience and the possibilities of its implementation in Ukraine. It is emphasized that the principle of interoperability, which implies the ability of different forces to operate in a single operational environment, is widely applied in NATO countries. Its implementation is ensured through the standardization of procedures, the unification of technical solutions, and joint training of personnel. Practical recommendations are proposed to improve the effectiveness of interagency cooperation.

Key words: *interagency cooperation, security and defense sector, law enforcement agencies, coordination, national security, management, integration*

Вступ. Сучасне безпекове середовище характеризується високим рівнем складності, гібридності та багатовимірності загроз. В умовах повномасштабної збройної агресії проти України особливої актуальності набуває формування якісно нового рівня організації діяльності сектору безпеки і оборони. За таких обставин визначальним чинником забезпечення національної безпеки є не лише інституційна спроможність окремих суб'єктів, а й ефективність їхньої взаємодії та координації. Саме міжвідомча взаємодія створює передумови для своєчасного реагування на загрози, раціонального використання наявних ресурсів і досягнення стратегічних цілей у сфері безпеки та оборони держави [1; 2].

Міжвідомча взаємодія являє собою сукупність організаційних, управлінських, комунікаційних та інформаційних заходів, спрямованих на узгодження діяльності суб'єктів сектору безпеки і оборони з метою досягнення спільних цілей і забезпечення належного рівня національної безпеки. Основними складовими такої взаємодії є своєчасний обмін інформацією, координація управлінських рішень, спільне планування заходів, а також чітке визначення функцій, повноважень і відповідальності кожного учасника процесу.

Питання міжвідомчої взаємодії у сфері безпеки і оборони розглядали у своїх працях О. М. Бандурка, А. В. Боровик, А. Г. Вархов, Д. О. Горбач, В. А. Денісенко, Н. З. Дерев'яно, О. В. Зайчук, В. Б. Звір, Д. П. Калаянов, Ю. Р. Кардашевський, О. Ф. Кобзар, А. Т. Комзюк, О. В. Кузьменко, І. О. Ліпко, Ю. М. Миколенко, Г. М. Сащук, Н. П. Свиридчук, В. І. Шкінчук та інші науковці.

Зокрема, у статті «Модель досягнення взаємосумісності комунікаційних та інформаційних систем: запровадження досвіду НАТО в інтересах сил оборони держави» (2023) Ліпко І. О., Звір В. Б. та Миколенко Ю. М. запропонували модель досягнення взаємосумісності комунікаційних та інформаційних систем (КІС) ЗСУ на основі стандартів НАТО [3].

У статті «Еволюція стратегічних комунікацій сектору безпеки та оборони України як інструменту протидії інформаційним загрозам» (2025) Сащук Г. М. досліджує становлення й еволюцію стратегічних комунікацій (StratCom) сектору безпеки та оборони України з 2014 р. до 2025 р. як інструменту протидії інформаційним загрозам [4].

Разом із тим, стрімка трансформація безпекового середовища, цифровізація управління та активне входження України до євроатлантичного безпекового простору вимагають системного аналізу сучасних інструментів взаємодії з урахуванням концепції взаємосумісності (interoperability).

Метою статті є визначення сутності міжвідомчої взаємодії, аналіз основних проблем її реалізації та розроблення рекомендацій щодо підвищення ефективності функціонування сектору безпеки і оборони.

Матеріали та методи. Для досягнення поставленої мети визначено такі завдання: з'ясувати сутність, структуру та значення міжвідомчої взаємодії як елемента забезпечення національної безпеки; проаналізувати основні проблеми та деструктивні чинники, що стримують ефективну координацію між суб'єктами сектору безпеки і оборони (нормативні, інформаційні, технічні, організаційно-кадрові); визначити принципи та сучасні інструменти вдосконалення міжвідомчої співпраці, зокрема у частині створення спільних ситуаційних центрів та інтегрованих інформаційних систем; дослідити міжнародний досвід (зокрема концепцію interoperability у країнах НАТО) та окреслити шляхи його адаптації та імплементації в українську практику; сформулювати прикладні рекомендації щодо нормативно-правового, технічного та організаційного забезпечення міжвідомчої координації.

Для розв'язання поставлених завдань використано комплекс наукових методів: системний та структурно-функціональний (для аналізу сектору безпеки як цілісної багаторівневої системи); формально-догматичний

(для виявлення прогалин у нормативно-правовому регулюванні); порівняльно-правовий (для вивчення стандартів НАТО та концепції взаємосумісності); метод моделювання та проблемно-цільовий підхід (для розробки інструментів міжвідомчої координації та практичних рекомендацій).

Наукова новизна одержаних результатів полягає у системному обґрунтуванні концептуальних засад вдосконалення міжвідомчої взаємодії через інтеграцію трьох ключових компонентів: нормативно-процедурного (стандартизація процедур), технологічного (міжвідомчі ситуаційні центри та єдиний інформаційний простір) та кадрово-оперативного (спільні навчання за стандартами НАТО). Набули подальшого розвитку підходи щодо адаптації принципу взаємосумісності (interoperability) до національної системи управління в умовах сучасних гібридних та збройних загроз.

Практичне значення результатів. Сформульовані висновки та рекомендації можуть бути використані у нормотворчій діяльності при доопрацюванні законодавства у сфері національної безпеки і оборони, у практичній діяльності керівного складу суб'єктів сектору безпеки під час організації взаємодії та функціонування ситуаційних центрів, а також у освітньому процесі вищих навчальних закладів зі спеціальною формою навчання.

Результати. Система міжвідомчої взаємодії в Україні охоплює широкий спектр органів державної влади, військових формувань, правоохоронних органів та інших інституцій, діяльність яких спрямована на забезпечення національної безпеки і оборони держави. Її функціонування характеризується багаторівневістю та міжсекторальним характером, що зумовлює потребу в ефективній координації, узгодженості управлінських рішень і чіткому розподілі повноважень між усіма учасниками взаємодії.

Відповідно до чинної нормативно-правової бази та наукових підходів суб'єктів міжвідомчої взаємодії доцільно класифікувати за функціональним принципом, виходячи зі специфіки покладених на них завдань і ролі в системі забезпечення національної безпеки.

Ключове місце у структурі міжвідомчої взаємодії посідає військовий компонент, до складу якого входять Збройні Сили України, інші військові формування, утворені відповідно до законодавства, а також Сили територіальної оборони. Основним призначенням цих суб'єктів є забезпечення оборони держави, стримування та відсіч збройної агресії, захист суверенітету й територіальної цілісності України. У межах міжвідомчої взаємодії вони відіграють провідну роль у плануванні та проведенні оборонних операцій, координації спільних дій із правоохоронними органами, розвідувальними структурами та іншими складовими сектору безпеки і оборони під час реагування на кризові ситуації та загрози [1; 2].

Правоохоронний компонент представлений Національною поліцією України, Національною гвардією України та іншими органами, на які покладено виконання правоохоронних функцій. Їхня діяльність спрямована на забезпечення громадської безпеки і правопорядку, захист прав і свобод громадян, а також протидію злочинності. У межах міжвідомчої взаємодії зазначені суб'єкти забезпечують підтримання стабільності в тилкових районах, беруть участь у проведенні контрдиверсійних заходів, охороні критичної інфраструктури та взаємодіють із військовими формуваннями в умовах правового режиму воєнного стану [5].

До спеціальних та розвідувальних органів належать Служба безпеки України, розвідувальні органи держави, а також підрозділи, що здійснюють контррозвідувальну діяльність. Основними завданнями цих суб'єктів є виявлення, попередження та нейтралізація загроз державній безпеці, зокрема терористичних проявів, диверсійної діяльності, інформаційних операцій, кібератак та інших форм гібридного впливу [6].

Важливою складовою системи є органи цивільного захисту, насамперед Державна служба України з надзвичайних ситуацій. Їхня діяльність спрямована на реагування на надзвичайні ситуації природного, техногенного та воєнного характеру, ліквідацію їх наслідків, захист населення і територій, а також координацію гуманітарних та евакуаційних заходів [5].

Особливе місце в системі міжвідомчої взаємодії посідають органи державної влади та органи місцевого самоврядування, які забезпечують реалізацію державної політики у сфері національної безпеки й оборони, координацію діяльності суб'єктів безпеки на державному та регіональному рівнях, а також організаційне, фінансове й ресурсне забезпечення відповідних заходів [2; 7].

До допоміжних і партнерських суб'єктів належать підприємства оборонно-промислового комплексу, суб'єкти приватного сектору, зокрема у сфері кібербезпеки та інформаційних технологій, громадські об'єднання, волонтерські організації та міжнародні партнери України. Їхній внесок полягає у забезпеченні сектору безпеки і оборони сучасними технологіями, матеріально-технічними ресурсами, експертно-аналітичною підтримкою, а також у реалізації спільних програм і проєктів, спрямованих на зміцнення обороноздатності та стійкості держави [8].

Таким чином, система суб'єктів міжвідомчої взаємодії являє собою складну багаторівневу структуру, до складу якої входять органи державної влади, військові формування, правоохоронні органи, спеціальні служби, органи цивільного захисту, а також інші державні та недержавні інституції. Ефективність її функціонування значною мірою залежить від рівня координації діяльності, чіткості розмежування повноважень і відповідальності, а також здатності до консолідації ресурсів та зусиль усіх учасників [1; 2].

Водночас аналіз сучасної практики функціонування сектору безпеки і оборони України свідчить про наявність низки проблем, які негативно впливають на ефективність міжвідомчої взаємодії. Серед них слід виокремити недосконалість механізмів координації, обмеженість інформаційного обміну між окремими суб'єктами, технічну несумісність інформаційно-комунікаційних систем, фрагментарність нормативно-правового регулювання, а також недостатній рівень професійної підготовки персоналу до виконання спільних завдань в умовах кризових ситуацій.

У зв'язку з цим формування ефективної системи міжвідомчої взаємодії має ґрунтуватися на сукупності базових принципів, серед яких визначальними є єдність управління, оперативність і безперервність обміну інформацією, чіткий розподіл повноважень та відповідальності, сумісність організаційних процедур і технологій, а також взаємна довіра між усіма учасниками процесу [3; 9].

Серед пріоритетних напрямів удосконалення міжвідомчої взаємодії доцільно виокремити розвиток спільних ситуаційних та координаційних центрів, впровадження інтегрованих інформаційно-аналітичних систем, проведення регулярних міжвідомчих навчань і тренувань, стандартизацію процедур планування та реагування, а також активне використання сучасних цифрових технологій і засобів захищеного обміну інформацією [3; 7].

Міжнародний досвід переконливо свідчить, що ефективна міжвідомча взаємодія є одним із визначальних чинників забезпечення національної безпеки та стійкості держави до сучасних викликів і загроз. У країнах – членах НАТО важливе значення надається принципу взаємосумісності (interoperability), який передбачає здатність різних сил, структур та органів діяти в єдиному операційному середовищі, використовуючи узгоджені процедури, стандарти та засоби комунікації [10].

Важливим інструментом розвитку міжвідомчої взаємодії в країнах НАТО є проведення багатонаціональних навчань, зокрема Steadfast Defender, Trident Juncture та Sea Breeze. Під час таких заходів відпрацьовуються механізми координації дій між військовими формуваннями, правоохоронними органами, розвідувальними структурами та органами цивільного захисту, що сприяє підвищенню рівня оперативної готовності до реагування на кризові ситуації та надзвичайні події різного характеру [11].

У державах Європейського Союзу сформовано розвинену систему інтегрованого управління кризами (Integrated Crisis Response), яка забезпечує комплексний підхід до реагування на надзвичайні ситуації та загрози безпеці. Одним із ключових елементів цієї системи є

механізм Integrated Political Crisis Response (IPCR), що забезпечує координацію дій між інституціями ЄС та державами-членами під час кризових ситуацій. Його функціонування сприяє оперативному обміну інформацією, узгодженню політичних рішень і мобілізації необхідних ресурсів для подолання кризових явищ [12].

Показовим прикладом ефективної міжвідомчої співпраці є діяльність агентства Frontex, яке координує взаємодію прикордонних служб держав-членів ЄС. У межах його функціонування впроваджено єдині інформаційні системи, спільні операції та стандартизовані процедури реагування на транскордонні загрози, що забезпечує високий рівень узгодженості дій усіх учасників процесу [13].

У Сполучених Штатах Америки ефективна міжвідомча взаємодія реалізується через систему National Incident Management System (NIMS) та діяльність Department of Homeland Security (DHS). Зазначена система забезпечує координацію між федеральними, штатними та місцевими органами влади, а також суб'єктами приватного сектору під час реагування на надзвичайні ситуації та кризові події [14].

Особливу увагу в американській практиці приділено діяльності так званих fusion centers – міжвідомчих аналітичних центрів, які забезпечують інтеграцію та аналіз інформації, отриманої від правоохоронних органів, розвідувальних служб, кібербезпекових структур та інших суб'єктів безпеки [15].

Узагальнення міжнародного досвіду дає підстави стверджувати, що ключовими передумовами ефективної міжвідомчої взаємодії є наявність єдиної системи координації, стандартизованих процедур діяльності, сучасних інформаційних технологій, високого рівня професійної підготовки персоналу та розвинутої культури міжвідомчого співробітництва. Використання зазначених підходів є важливим для подальшого вдосконалення системи безпеки і оборони України та підвищення її стійкості в умовах сучасних загроз.

Досвід Ізраїлю також заслуговує на увагу. У цій країні ефективна взаємодія забезпечується через тісну координацію між армією,

розвідувальними службами та поліцією. Значна увага приділяється оперативному обміну інформацією та швидкому прийняттю рішень у режимі реального часу [16].

З урахуванням результатів проведеного аналізу та сучасних викликів у сфері національної безпеки доцільно запропонувати комплекс практичних заходів, спрямованих на підвищення ефективності міжвідомчої взаємодії суб'єктів сектору безпеки і оборони України.

1. Формування єдиної міжвідомчої інформаційної системи. Одним із пріоритетних напрямів удосконалення міжвідомчої взаємодії є створення інтегрованої цифрової платформи, яка забезпечуватиме оперативний обмін інформацією між усіма суб'єктами сектору безпеки і оборони в режимі реального часу. Така система має передбачати використання уніфікованих форматів даних, захищених каналів зв'язку, механізмів диференційованого доступу до інформаційних ресурсів, а також інструментів аналітичної обробки та узагальнення даних.

Важливим кроком у цьому напрямі стало затвердження Кабінетом Міністрів України постановою від 13 листопада 2025 р. № 1471 Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки та кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними та розвідувальними органами, а також суб'єктами оперативно-розшукової діяльності [17].

2. Удосконалення нормативно-правового забезпечення. Необхідною умовою підвищення ефективності міжвідомчої взаємодії є системне вдосконалення нормативно-правової бази, що регулює діяльність суб'єктів сектору безпеки і оборони. Це передбачає чітке розмежування їхніх повноважень, нормативне закріплення механізмів координації, визначення процедур обміну інформацією та усунення наявних правових колізій і дублювання функцій.

Важливим інструментом реалізації зазначених завдань є Дорожня карта взаємосумісності, схвалена Комітетом сектору безпеки і оборони Ради Україна–НАТО 17 червня 2024 року та представлена під час Вашингтонського са-

міту НАТО у липні 2024 року [6]. Документ визначає основні напрями досягнення взаємосумісності між українськими структурами безпеки та оборони і відповідними інституціями держав – членів НАТО.

3. *Забезпечення технічної та процедурної сумісності.* Ефективна міжвідомча взаємодія неможлива без належного рівня технічної та процедурної сумісності. У зв'язку з цим актуальним є впровадження єдиних стандартів зв'язку та обміну даними, модернізація існуючих інформаційно-комунікаційних систем, інтеграція відомчих ІТ-рішень у спільний інформаційний простір, а також стандартизація алгоритмів дій і процедур реагування в кризових ситуаціях [18].

4. *Розвиток системи підготовки та підвищення кваліфікації кадрів.* Людський фактор залишається одним із ключових чинників забезпечення ефективної міжвідомчої взаємодії. У зв'язку з цим особливої актуальності набуває створення системи безперервної професійної підготовки та підвищення кваліфікації персоналу суб'єктів сектору безпеки і оборони. Доцільним є впровадження міжвідомчих освітніх програм, проведення регулярних спільних тренувань і навчань, розвиток навичок командної роботи, а також формування лідерських компетентностей у сфері кризового менеджменту та стратегічного управління [19].

5. *Розвиток інституційних механізмів координації.* Важливим напрямом удосконалення міжвідомчої взаємодії є розвиток інституційних механізмів координації діяльності суб'єктів сектору безпеки і оборони. З цією метою доцільно створювати або вдосконалювати діяльність постійно діючих координаційних структур, зокрема міжвідомчих ситуаційних центрів, спільних оперативних штабів та аналітичних центрів типу *fusion centers* [20].

6. *Впровадження сучасних інформаційних технологій.* Цифрова трансформація сектору безпеки і оборони є одним із визначальних чинників підвищення ефективності міжвідомчої взаємодії. Перспективними напрямами розвитку є використання систем штучного інтелекту для аналізу та прогнозування загроз,

впровадження технологій Big Data для обробки великих масивів інформації, застосування геоінформаційних систем (GIS) для підтримки управлінських рішень, а також посилення кіберзахисту інформаційних ресурсів та критичної інформаційної інфраструктури [21].

7. *Формування культури міжвідомчої співпраці.* Не менш важливою умовою ефективної взаємодії є розвиток організаційної культури, заснованої на принципах партнерства, довіри та спільної відповідальності за досягнення стратегічних цілей. Це передбачає подолання відомчої ізольованості, стимулювання обміну досвідом і кращими практиками, розвиток горизонтальних комунікацій, а також утвердження принципів відкритості, взаємної підтримки та професійної солідарності [22].

8. *Розширення міжнародного співробітництва.* Важливим чинником удосконалення міжвідомчої взаємодії є активізація міжнародного співробітництва у сфері безпеки та оборони. Поглиблення співпраці з міжнародними партнерами створює можливості для запозичення передового досвіду, участі у спільних навчаннях і тренуваннях, отримання технічної, експертної та консультативної допомоги, а також забезпечення поступової інтеграції України до європейських та євроатлантичних безпекових структур [23].

Висновки. На основі проведеного дослідження сутності, проблем та перспектив розвитку міжвідомчої взаємодії сил сектору безпеки і оборони України сформульовано такі висновки та прикладні рекомендації:

– з'ясовано, що міжвідомча взаємодія у сфері національної безпеки є складною багаторівневою функціонально-організаційною системою, ефективність якої визначається рівнем координації, чіткістю розподілу повноважень та здатністю суб'єктів безпекового середовища до інтеграції зусиль у єдиному операційному середовищі;

– аналіз практики довів, що основними бар'єрами на шляху до ефективної координації є: *нормативна фрагментарність* – відсутність єдиного уніфікованого нормативно-правового акта, який би чітко регламентував порядок та алгоритми міжвідомчої співпраці

в умовах критичних ситуацій; *інформаційні та технічні бар'єри* – відомча замкненість, відсутність захищених каналів автоматизованого обміну даними у режимі реального часу та технічна несумісність спеціальних засобів зв'язку; *кадрові та процедурні відмінності* – брак спільних тренувань за єдиними стандартами та різноманітність внутрішньовідомчих регламентів прийняття рішень;

обґрунтовано, що базовим орієнтиром для вдосконалення вітчизняної системи координації має слугувати євроатлантичний принцип взаємосумісності (interoperability), який передбачає досягнення триєдиної сумісності: *оперативної* (спільні процедури й алгоритми дій), *технічної* (єдині стандарти зв'язку та передачі даних) та *доктринально-організаційної* (спільне розуміння завдань та єдина культура управління).

З метою розв'язання виявлених проблем та підвищення стійкості сектору безпеки і оборони пропонується комплекс заходів за трьома основними напрямками:

1) *нормативно-правове та процедурне забезпечення*: ініціювати розробку та затвердження на рівні Кабінету Міністрів України уніфікованого Порядку міжвідомчої взаємодії суб'єктів сектору безпеки і оборони під час реагування на критичні загрози; запровадити розробку та постійне оновлення Спільних стандартних операційних процедур (Joint SOPs) для типових кризових сценаріїв (кібератаки, диверсійно-розвідувальні загрози, надзвичайні ситуації техногенного чи військового характеру);

2) *технологічна та інформаційна інтеграція*: прискорити розбудову та інтеграцію Головного ситуаційного центру України із ситуаційними центрами органів військового управління, СБУ, Національної поліції, ДПСУ та ДСНС на основі хмарних технологій та захищеного протоколу передачі даних; запровадити міжвідомчі аналітичні осередки (fusion centers) для акумуляції, аналізу та поширення розвідувальної й оперативної інформації між суб'єктами реагування у режимі 24/7; забезпечити перехід на єдині стандарти шифрування, цифрового захищеного зв'язку та обміну даними, сумісні з протоколами НАТО (STANAG);

3) *кадрове та оперативне забезпечення*: включити до навчальних програм закладів вищої освіти зі специфічними умовами навчання обов'язкові спільні командно-штабні навчання та практичні тренінги з опрацювання міжвідомчих зв'язків; запровадити практику короткострокового стажування офіцерів зв'язку та аналітиків у ситуаційних центрах суміжних відомств для подолання відомчих бар'єрів та підвищення рівня взаємної довіри.

Конфлікт інтересів: Мовчан А. є членом редакційної колегії журналу. Для забезпечення незалежності редакційного процесу рукопис розглядався редактором, який не мав конфлікту інтересів з автором. Автор не брав участі у відборі рецензентів, процесі рецензування та прийнятті рішення щодо публікації статті. Рукопис пройшов стандартну процедуру подвійного сліпого рецензування.

Список використаних джерел:

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
2. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. *Урядовий кур'єр*. 2020. 16 вер. (№ 179).
3. Ліпко І., Звір В., Миколенко Ю. Модель досягнення взаємосумісності комунікаційних та інформаційних систем: запровадження досвіду НАТО в інтересах сил оборони держави. *Збірник наукових праць Центру воєнно-стратегічних досліджень НВУОУ*. 2023. № 2. С. 108–120. DOI: <https://doi.org/10.33099/2304-2745/2023-2-78/108-120>.
4. Сашук Г. М. Еволюція стратегічних комунікацій сектору безпеки та оборони України як інструменту протидії інформаційним загрозам. *Політичне життя*. 2025. № 3. С. 103–108. DOI: <https://doi.org/10.31558/2519-2949.2025.3.13>.
5. Дорожня карта взаємосумісності з НАТО. *Офіційний сайт Міністерства внутрішніх справ України*. URL: <https://mvs.gov.ua/jevroatlanticna-integraciia/doroznia-karta-vzajemsumisnosti-z-nato>

6. Денісенко В. А. Взаємодія Служби безпеки України з іншими суб'єктами сектору безпеки і оборони: адміністративно-правові проблеми координації. *Правові новели*. 2025. № 27. С. 218–226. DOI: <https://doi.org/10.32782/ln.2025.27.26>.
7. Боровик А. В., Вархов А. Г., Дерев'янка Н. З. Адміністративно-правовий механізм взаємодії суб'єктів сектору безпеки й оборони щодо забезпечення національної безпеки: питання теорії та практики : монографія. Одеса : Юридика, 2024. 186 с.
8. Комзюк А. Т., Шкіндюк В. І. Поняття взаємодії та координації у сфері правоохоронної діяльності як об'єкту адміністративно-правового регулювання. *Вісник кримінологічної асоціації України*. 2025. № 1 (34). С. 863–872. DOI: <https://doi.org/10.32631/vca.2025.1.72>.
9. NATO-Ukraine Action Plan // North Atlantic Treaty Organization : official website. 2002. Nov. 22. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/22/nato-ukraine-action-plan?selectedLocale=uk>
10. NATO Interoperability Standards: Enabling Seamless Coalition Operations Through Cross-Enterprise Orchestration. URL: <https://r4.ai/nato-interoperability-standards-coalition-operations/>
11. NATO Begins Exercise STEADFAST DETERRENCE 2026: Securing the High North, Reinforcing Transatlantic Collaboration on Collective Defence. Joint Warfare Centre : official website. 2026. URL: <https://www.jwc.nato.int/article/steadfast-deterrence-2026-begins/>
12. EU integrated political crisis response (IPCR) arrangements. EUR-Lex : Access to European Union law. URL: <https://eur-lex.europa.eu/EN/legal-content/summary/eu-integrated-political-crisis-response-ipcr-arrangements.html>
13. Frontex: Irregular border crossings into the EU down 40% in the first four months of 2026. Frontex : official website. 2026. URL: <https://www.frontex.europa.eu/media-centre/news/news-release/frontex-irregular-border-crossings-into-the-eu-down-40-in-the-first-four-months-of-2026-MwZAin>
14. National Incident Management System and Incident Command System. Division of Homeland Security and Emergency Services : official website of New York State. URL: <https://www.dhses.ny.gov/national-incident-management-system-and-incident-command-system>
15. Свиридчук Н. П., Кардашевський Ю. Р. Ф'южн-центри як важливий компонент моделі Intelligence-led Policing (ILP). *Аналітично-порівняльне правознавство*. 2023. № 6. С. 504–509. DOI: <https://doi.org/10.24144/2788-6018.2023.06.87>.
16. Матвієнко Ю. Приклад для України: Як в Ізраїлі реформують розвідувальні та спеціальні служби. *Defence Express*. URL: https://defence-ua.com/weapon_and_tech/jak_v_izrajili_reformujut_rozviduvalni_ta_spetsialni_sluzhbi-5668.html
17. Уряд затвердив Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти та правоохоронних органів. *Голос України*. 2025. 17 листоп. URL: <https://www.golos.com.ua/article/388473>
18. Закон про електронні комунікації: парламент закріпив нові стандарти якості мобільного зв'язку. Український центр аналітики та досліджень UCAI. URL: <https://ucaai.com.ua/solutions/3225-zakon-pro-elektronn-komunkac-parlament-zakrpiv-nov-standarti-yakost-moblnogo-zvyazku>
19. Спінко С. Людський фактор: як зробити персонал запорукою успіху компанії. *Delo.ua*. URL: <https://delo.ua/business/lyudskii-faktor-yak-zrobiti-personal-faktorom-uspixu-kompaniyi-436071/>
20. Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» : Указ Президента України від 18.06.2021 № 260/2021. Рада національної безпеки і оборони України : офіційний вебсайт. URL: <https://www.rnbo.gov.ua/ua/Ukazy/4916.html>
21. Структура цифрової трансформації у Силах оборони: як це працює та як долучитися. Офіційний сайт Міністерства оборони України. URL: <https://mod.gov.ua/explanation/it-vertikal-u-silah-oboroni-yak-cze-praczuue-ta-yak-doluchitisa>
22. Шимановська-Діанич Л. М. Розвиток організаційної культури як важливий фактор забезпечення основної конкурентної переваги компанії. *Актуальні проблеми інноваційної економіки та права*. 2023. № 1–2. С. 71–76. DOI: <https://doi.org/10.36887/2524-0455-2023-1-12>.
23. Співпраця з міжнародними організаціями: можливості та перспективи. Народний комітет України. URL: <https://nku.com.ua/spivpracya-z-mizhnarodnymy-organizacziyamy-mozhlyvosti-ta-perspektyvy/>

References:

1. Verkhovna Rada of Ukraine. (2018). *Pro natsionalnu bezpeku Ukrainy* [On the national security of Ukraine] (Law of Ukraine No. 2469-VIII). *Vidomosti Verkhovnoi Rady*, (31), Art. 241. [in Ukrainian].

2. President of Ukraine. (2020, September 14). *Stratehiia natsionalnoi bezpeky Ukrainy* [National security strategy of Ukraine] (Decree No. 392/2020). *Uryadovyy Kuryer*, (179). [in Ukrainian].
3. Lipko, I., Zvir, V., & Mykolenko, Yu. (2023). Model dosiahnennia vzaiemosumisnosti komunikatsiinykh ta informatsiinykh system: zaprovadzhennia dosvidu NATO v interesakh syl oborony derzhavy [Model for achieving interoperability of communication and information systems: Implementation of NATO experience in the interests of the state defense forces]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU*, (2), 108–120. <https://doi.org/10.33099/2304-2745/2023-2-78/108-120> [in Ukrainian].
4. Sashchuk, H. M. (2025). Evoliutsiia stratehichnykh komunikatsii sektoru bezpeky ta oborony Ukrainy yak instrumentu protydyi informatsiynym zahrozam [Evolution of strategic communications of the security and defense sector of Ukraine as a tool for countering information threats]. *Politychne Zhyttia*, (3), 103–108. <https://doi.org/10.31558/2519-2949.2025.3.13> [in Ukrainian].
5. Ministry of Internal Affairs of Ukraine. (n.d.). *Dorozhnia karta vzaiemosumisnosti z NATO* [Roadmap for interoperability with NATO]. <https://mvs.gov.ua/jevroatlantica-integraciia/dorozhnia-karta-vzaiemosumisnosti-z-nato> [in Ukrainian].
6. Denysenko, V. A. (2025). Vzaiemodii Sluzhby bezpeky Ukrainy z inshymy subiektamy sektoru bezpeky i oborony: administratyvno-pravovi mekhanizmy koordynatsii [Interaction of the Security Service of Ukraine with other actors of the security and defense sector: Administrative and legal problems of coordination]. *Pravovi Novely*, (27), 218–226. <https://doi.org/10.32782/ln.2025.27.26> [in Ukrainian].
7. Borovyk, A. V., Varkhov, A. H., & Derevianko, N. Z. (2024). *Administratyvno-pravovyi mekhanizm vzaiemodii subiektiv sektoru bezpeky i oborony shchodo zabezpechennia natsionalnoi bezpeky: pytannia teorii ta praktyky* [Administrative and legal mechanism of interaction between actors of the security and defense sector in ensuring national security: Theory and practice] (Monograph). Yurydyka. [in Ukrainian].
8. Komziuk, A. T., & Shkindiuk, V. I. (2025). Poniattia vzaiemodii ta koordynatsii u sferi pravookhoronnoi diialnosti yak obiekta administratyvno-pravovoho rehuliuвання [Concept of interaction and coordination in law enforcement as an object of administrative legal regulation]. *Visnyk Kryminolohichnoi Asotsiatsii Ukrainy*, (1), 863–872. <https://doi.org/10.32631/vca.2025.1.72> [in Ukrainian].
9. North Atlantic Treaty Organization. (2002, November 22). *NATO-Ukraine action plan*. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/22/nato-ukraine-action-plan?selectedLocale=uk> [in English].
10. R4 AI. (n.d.). *NATO interoperability standards: Enabling seamless coalition operations through cross-enterprise orchestration*. <https://r4.ai/nato-interoperability-standards-coalition-operations/> [in English].
11. Joint Warfare Centre. (2026). *NATO begins exercise STEADFAST DETERRENCE 2026: Securing the High North, reinforcing transatlantic collaboration on collective defence*. North Atlantic Treaty Organization. <https://www.jwc.nato.int/article/steadfast-deterrence-2026-begins/> [in English].
12. EUR-Lex. (n.d.). *EU integrated political crisis response (IPCR) arrangements*. Access to European Union Law. <https://eur-lex.europa.eu/EN/legal-content/summary/eu-integrated-political-crisis-response-ipcr-arrangements.html> [in English].
13. Frontex. (2026). *Frontex: Irregular border crossings into the EU down 40% in the first four months of 2026*. European Border and Coast Guard Agency. <https://www.frontex.europa.eu/media-centre/news/news-release/frontex-irregular-border-crossings-into-the-eu-down-40-in-the-first-four-months-of-2026-MwZAin> [in English].
14. New York State Division of Homeland Security and Emergency Services. (n.d.). *National incident management system and incident command system*. <https://www.dhses.ny.gov/national-incident-management-system-and-incident-command-system> [in English].
15. Svyrydiuk, N. P., & Kardashevskiy, Yu. R. (2023). Fiuzhn-tsentry yak vazhlyvyi komponent modeli Intelligence-Led Policing (ILP) [Fusion centers as an important component of the Intelligence-led Policing (ILP) model]. *Analitychno-Porivnialne Pravo Navstvo*, (6), 504–509. <https://doi.org/10.24144/2788-6018.2023.06.87> [in Ukrainian].
16. Matviyenko, Yu. (n.d.). *Pryklad dlia Ukrainy: Yak v Izraili reformuiut rozviduvalni ta spetsialni sluzhby* [An example for Ukraine: How intelligence and special services are reformed in Israel]. Defence Express. https://defence-ua.com/weapon_and_tech/jak_v_izrajili_reformujut_rozviduvalni_ta_spetsialni_sluzhbi-5668.html [in Ukrainian].
17. Uryad zatverdyv Poryadok vzayemodii subiektiv natsionalnoyi systemy reahuvannya na kiberintsydynty ta pravookhoronnykh organiv [The Government approved the Procedure for interaction between subjects of the national cyber incident response system and law enforcement agencies]. (2025, November 17). *Holos Ukrainy*. <https://www.golos.com.ua/article/388473> [in Ukrainian].

18. Ukrainian Center for Analytics and Research (UCAI). (n.d.). *Zakon pro elektronni komunikatsii: parlament zakrypyv novi standarty yakosti mobilnoho zviazku* [Law on electronic communications: Parliament consolidated new standards for mobile service quality]. <https://ucaai.com.ua/solutions/3225-zakon-pro-elektronn-komunkac-parlament-zakrpiv-nov-standarti-yakost-moblno-go-zvyazku> [in Ukrainian].
19. Spinko, S. (n.d.). *Liudskyi faktor: yak zrobyty personal Zaporukoiu uspikhu kompanii* [The human factor: How to make staff the key to company success]. Delo.ua. <https://delo.ua/business/lyudskii-faktor-yak-zrobiti-personal-faktorom-uspixu-kompaniyi-436071/> [in Ukrainian].
20. President of Ukraine. (2021, June 18). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 chervnia 2021 roku «Shchodo udoskonalennia merezhi situatsiinykh tsentriv ta tsyfrovoy transformatsii sfery natsionalnoi bezpeky i oborony»* [On the decision of the National Security and Defense Council of Ukraine dated June 4, 2021 «On improving the network of situation centers and digital transformation of the national security and defense sphere»] (Decree No. 260/2021). National Security and Defense Council of Ukraine. <https://www.rnbo.gov.ua/ua/Ukazy/4916.html> [in Ukrainian].
21. Ministry of Defence of Ukraine. (n.d.). *Struktura tsyfrovoy transformatsii u Sylakh oborony: yak tse pratsiue ta yak doluchytysia* [Structure of digital transformation in the Defense Forces: How it works and how to join]. <https://mod.gov.ua/explanation/it-vertikal-u-silah-oboroni-yak-cze-praczyuye-ta-yak-doluchitysia> [in Ukrainian].
22. Shymanovska-Dianych, L. M. (2023). Rozvytok mekhanizmu organizatsinoi kultury yak vazhlyvyi faktor zabezpechennia osnovnoi konkurentnoi perevahy kompanii [Development of organizational culture as an important factor in ensuring the main competitive advantage of the company]. *Aktualni Problemy Innovatsijnoi Ekonomiky Ta Prava*, (1–2), 71–76. <https://doi.org/10.36887/2524-0455-2023-1-12> [in Ukrainian].
23. People's Committee of Ukraine (NKU). (n.d.). *Spivpratsia z mizhnarodnymy mekhanizmy: mozhlyvosti ta perspektyvy* [Cooperation with international organizations: Opportunities and prospects]. <https://nku.com.ua/spivpracza-z-mizhnarodnymy-organizaciyamy-mozhlyvosti-ta-perspektyvy/> [in Ukrainian].

Creative Commons Attribution 4.0
International (CC BY 4.0)



Дата першого надходження статті до видання: 24.07.2026
Дата прийняття статті до друку після рецензування: 03.09.2026
Дата публікації (оприлюднення) статті: 00.00.2026