

МІЖНАРОДНИЙ ДОСВІД УЧАСТІ ПРАВООХОРОННИХ ОРГАНІВ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ ТА МОЖЛИВОСТІ ЙОГО АДАПТАЦІЇ В УКРАЇНІ

Макарчук В. В.

ВСТУП

Останні десятиліття позначилися радикальними змінами у підходах до національної безпеки, що зумовлено глобалізацією, технологічним прогресом і новими викликами. Якщо у XX столітті пріоритетом був захист від традиційних криз (злочинність, збереження критичної інфраструктури – телекомунікацій, аеропортів, лікарень), то у XXI столітті акцент змістився на управління комплексними ризиками (тероризм, кіберзагрози, гібридна війна, міждержавні конфлікти), проактивні стратегії (прогнозування загроз замість реактивного реагування та штучний інтелект), міжсекторальну взаємодію (інтеграція зусиль правоохоронних органів, військових, економічних і соціальних інститутів). Ці зміни вимагають переосмислення адміністративно-правового статусу правоохоронних органів як ключових суб'єктів безпекової політики.

Правоохоронні органи як суб'єкти формування державної політики у сфері національної безпеки репрезентують систему загальнодержавних цілей (захист індивідуальної, громадської (публічної) та державної безпеки через нормотворчу, контрольну та оперативну діяльність) та функціональну спеціалізацію (контррозвідка, публічна безпека, захист територіальної цілісності. Проте сучасні реалії вимагають уточнення їхніх повноважень у сфері кібербезпеки та гібридних загроз.

Метою даного дослідження є аналіз міжнародного досвіду участі правоохоронних органів у забезпеченні національної безпеки та оборони, зокрема механізмів адаптації інноваційних підходів до українських реалій.

Розглядаються такі ключові аспекти:

1. Трансформація функцій правоохоронних органів – від реактивного реагування до проактивного прогнозування загроз із застосуванням штучного інтелекту, дронів та аерокосмічного моніторингу.

2. Міжнародна координація – роль Національного центрального бюро Інтерполу в Україні у боротьбі з транснаціональною злочинністю та інтеграція з Європолом.

3. Правові та технологічні виклики – баланс між безпекою та приватністю, зокрема при використанні систем відеоспостереження та кіберзасобів.

4. Організаційні реформи – пропозиції щодо створення Центру координації при РНБО для синхронізації дій усіх силових структур.

Актуальність дослідження підкреслюється введенням воєнного стану, що демонструє необхідність посилення спроможностей правоохоронних органів у сфері кібербезпеки, контррозвідки та адаптації європейських стандартів. Наприклад, досвід країн ЄС (Швеції, Латвії) у сфері «тотальної оборони» та космічної безпеки може стати орієнтиром для України.

1. Правові та технологічні виклики – баланс між безпекою та приватністю, зокрема при використанні систем відеоспостереження та кіберзасобів

Важливо зазначити, що майже всі країни світу прагнуть забезпечити стабільну та ефективну співпрацю з різними партнерами, враховуючи природу організованої злочинності, яка не знає меж. Це надає правоохоронній діяльності у сфері національної безпеки та оборони значний міжнародний аспект. Для України подібне питання також залишається актуальним. Слід уточнити, що наразі розв'язання проблем, пов'язаних зі злочинністю транснаціонального характеру або такою, що виходить за межі держави, здійснюється українськими правоохоронними органами виключно через Національне центральне бюро Інтерполу. Відповідно до Постанови Кабінету Міністрів України «Про Національне центральне бюро Інтерполу» від 25 березня 1993 року № 220¹, Національна поліція виконує функції Національного центрального бюро Інтерполу. Щороку в січні Голова Національної поліції подає Міністру внутрішніх справ звіт про діяльність Національного центрального бюро Інтерполу, який потім передається для інформування Кабінету Міністрів України.

Згідно з положеннями статті 23 Закону України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII², Національна поліція зобов'язана виконувати основні функції, що їй покладаються:

¹ Про Національне центральне бюро Інтерполу : Постанова Каб. Міністрів України від 25.03.1993 № 220 : станом на 16 груд. 2017 р. URL: <https://zakon.rada.gov.ua/laws/show/220-93-п#Text>

² Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII : станом на 16 серп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>

1) забезпечення представництва України, взаємодії та виконання міжнародних зобов'язань у рамках Міжнародної організації кримінальної поліції – Інтерполу, а також Європейського поліцейського офісу; виконання ролі Національного центрального бюро Інтерполу в Україні;

2) налагодження координації правоохоронних органів та інших державних інституцій України з Інтерполом і Європолом, а також забезпечення взаємодії з відповідними органами інших країн у питаннях, що підпадають під компетенцію цих міжнародних організацій;

3) надання можливості доступу українським правоохоронним органам до інформаційно-телекомунікаційних систем і баз даних Інтерполу та Європолу, а також внесення в ці системи інформації від правоохоронних органів України.

Згідно з довідкою про основні результати службової діяльності Національного центрального бюро Інтерполу в Україні, у 2022 році означеним суб'єктом відповідно до визначених завдань і функцій здійснювалися заходи щодо:

1) представництва та забезпечення виконання зобов'язань України в Міжнародній організації кримінальної поліції – Інтерпол;

2) формування та реалізації державної політики у сфері вдосконалення співробітництва Національної поліції України з правоохоронними органами іноземних держав, міжнародними організаціями та установами, участі у розробленні проєктів міжнародних договорів України з питань боротьби зі злочинністю та їх укладання;

3) координації, організації та забезпечення співробітництва органів та підрозділів поліції та інших органів державної влади України з компетентними органами іноземних держав у сфері боротьби зі злочинністю, яка має транснаціональний характер, з використанням можливостей Інтерполу, зокрема, за такими основними напрямками як: а) установлення місцезнаходження осіб, які розшукуються, з метою їх затримання, арешту, обмеження свободи пересування та подальшої видачі (екстрадиції); б) установлення місцезнаходження осіб чи об'єктів, що становлять інтерес для правоохоронних органів України чи інших держав-членів Інтерполу; с) надання чи отримання інформації, що стосується розслідування злочинів, кримінального минулого або злочинної діяльності осіб; д) надання чи отримання інформації з метою попередження про осіб, події, об'єкти, способи вчинення злочинів, що становлять реальну загрозу публічній безпеці та порядку й можуть завдати істотної шкоди майну чи громадянам; е) ідентифікація осіб чи невпізнаних трупів; ф) проведення криміналістичних досліджень; г) надання чи отримання інформації з питань публічної безпеки й порядку; h) ідентифікація загроз, організованих

груп та злочинних організацій, тенденцій розвитку злочинності; і) обмін досвідом з питань боротьби зі злочинністю та правоохоронної діяльності³.

Україна активно залучає механізми міжнародного співробітництва у боротьбі з транснаціональною злочинністю через Національне центральне бюро Інтерполу (НЦБ), яке функціонує у складі Національної поліції. Щорічно голова Національної поліції України подає офіційний звіт про результати роботи бюро через МВС до Кабміну.

НЦБ Інтерполу в Україні виконує комплексне завдання з координації міжнародного співробітництва:

1) представницькі функції: Взаємодія з Інтерполом та Європолом; Участь у розробці міжнародних угод; Забезпечення виконання міжнародних зобов'язань;

2) оперативно-інформаційна діяльність: Доступ до міжнародних баз даних; Обмін оперативною інформацією; Ідентифікація осіб та кримінальних угруповань;

3) координаційні механізми: Організація спільної роботи з зарубіжними колегами; Підготовка екстрадиційних запитів; Аналіз тенденцій транснаціональної злочинності.

Дослідники пропонують різні підходи до класифікації функцій НЦБ, що відображають його роль у національній та міжнародній правоохоронній системі.

Модель Є. Говійка акцентує на багаторівневій координації діяльності НЦБ:

1. Внутрішня координація (забезпечення взаємодії між українськими правоохоронними органами (СБУ, Нацполіція, ДБР) та уніфікація процедур обробки запитів щодо міжнародного розшуку).

2. Міжнародна взаємодія (участь у спільних операціях з іноземними бюро Інтерполу та реалізація міжнародних правових інструментів).

3. Робота з Генеральним секретаріатом Інтерполу (виконання рекомендацій та стандартів організації та участь у формуванні глобальної антикримінальної політики).

4. Аналітико-прогностична діяльність (виявлення тенденцій транснаціональної злочинності (кіберзлочинність, торгівля людьми) та розробка превентивних стратегій на основі даних)⁴.

³ Довідка про основні результати службової діяльності Національного центрального бюро Інтерполу в Україні у 2022 році. *Доступ до правди*, 2022. URL: https://dostup.pravda.com.ua/request/104660/response/372851/attach/3/01.2023.pdf?cookie_paththrough=1

⁴ Говійко Є. А. Адміністративно-правовий статус Національного центрального бюро Інтерпол : автореф. дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2011. 23 с.

Модель В. Гайчука та Т. Малиновської зосереджена на оперативно-технічних аспектах:

1. Підготовка міжнародних запитів (юридична експертиза документів для екстрадиції чи розшуку та дотримання процедурних вимог Інтерполу (наприклад, уникання політизованих запитів)).

2. Обмін оперативною інформацією (швидкий пошук та передача даних про злочинців через бази Інтерполу (наприклад, систему I-24/7) та координація з прикордонними службами для блокування переміщень злочинних угруповань).

3. Науково-технічне співробітництво (впровадження сучасних технологій (біометрія, аналіз Big Data) та участь у міжнародних дослідницьких проєктах).

4. Методичне забезпечення (створення інструкцій для українських правоохоронців щодо роботи з Інтерполом та тренінги з міжнародного кримінального права)⁵.

Обидві моделі доповнюють одна одну. Для повноцінної реформи НЦБ варто поєднати: стратегічні елементи Говійка (наприклад, аналітичний блок) та практичні інструменти Гайчука-Малиновської (робота з базами даних). Оптимальним рішенням може стати створення єдиного стандарту функціонування НЦБ, що інтегрує обидві концепції.

Отже, НЦБ Інтерполу в Україні виконує стратегічну роль у забезпеченні міжнародної правової допомоги, протидії організованим злочинності, захисті національних інтересів у кіберпросторі, розвитку міжнародного поліцейського співробітництва. Українська система міжнародного поліцейського співробітництва продовжує вдосконалюватись, адаптуючись до нових викликів глобалізованого світу.

Так, Г. Пономаренко виділяє наступні групи повноважень правоохоронних органів у сфері національної безпеки: 1) боротьба з правопорушеннями; 2) охорона публічного порядку; 3) забезпечення публічної безпеки; 4) охорона та захист власності від протиправних посягань; 5) забезпечення реалізації прав, свобод і законних інтересів фізичних осіб та прав і законних інтересів юридичних осіб⁶. Класифікація Г. Пономаренка (є базовою, але недостатньою для сучасних умов. Її недоліки:

⁵ Гайчук В. А., Малиновська Т. М. Напрямки вдосконалення міжнародного співробітництва правоохоронних органів у боротьбі зі злочинністю: нормативно-правовий аспект. *Актуальні проблеми сучасної науки в дослідженнях молодих учених* : тези доп. учасників наук.-практ. конф. Харків, 2017. С. 113–114.

⁶ Пономаренко Г. О. Адміністративно-правові засади управління у сфері забезпечення внутрішньої безпеки держави : дис. ... д-ра юрид. наук: 12.00.07. Харків, 2008. С. 59.

1. Не враховує транснаціональні загрози: наприклад, міжнародну організовану злочинність або втручання третіх країн.

2. Відсутність акценту на превенцію: сучасні стратегії вимагають профілактики радикалізації, моніторингу соціальних мереж.

3. Обмеженість у контексті оборони: правоохоронні органи часто залучені у військово-цивільній взаємодії (наприклад, під час воєнного стану).

Стосовно інтеграції цивільного та військового секторів, то такі країни, такі як Латвія та Швеція, розробили нові стратегії, що поєднують цивільну і військову складові: Закон Латвії «Про національну безпеку» 2000 року⁷ та Концепція Національної безпеки 2019 року⁸ визначають дії для підготовки нації до конфліктів, зокрема захисту суверенітету. Це потребує повної перебудови політики, а не її часткових змін. Концепція «сучасної тотальної оборони» Швеції базується на максимальному захисті у сучасних умовах⁹. Вплив війни в Україні також спонукав Швецію та Фінляндію до вступу в НАТО.

Останнім часом європейські країни переглянули свої оборонні програми. Тепер увага зосереджена на посиленні правоохоронних органів – від загальних завдань до спеціальних операцій із застосуванням технологій спостереження. Стосовно використання сучасних технологій, то воно має як переваги: моніторинг руху, екології, захист інфраструктури, боротьба зі злочинністю; так і суперечності: питання приватності, пропорційності заходів та суспільна дискусія.

Для ефективного впровадження технологій спостереження потрібно:

1. Дослідити соціально-політичні наслідки їх використання.

2. Визначити технічні, правові та соціальні аспекти застосування.

3. Розробити законодавчу базу, що балансуватиме безпеку та права громадян (розробка правової основи для використання технологій спостереження в національній безпеці є критично важливою; необхідний детальний аналіз соціальних і політичних проблем, що виникають через збільшення використання технологій спостереження; важливо прояснити різноманіття сфер застосування з технічної, правової та соціальної точок зору, щоб виявити можливості та виклики).

⁷ National Security Law. *Latvijas Vēstnesis*, 2000. URL: <https://likumi.lv/ta/en/en/id/14011-national-security-law>

⁸ National Security Concept. *Latvijas Vestnesis*, 2019. URL: <https://likumi.lv/ta/en/en/id/309647-on-approval-of-the-nationalsecurity-concept>

⁹ Lindgren, F., & Odlund, A., 2017. Total Defence at the Crossroads. URL: https://sldinfo.com/wp-content/uploads/2018/12/http___webbrapp.ptn_.foi_se_pdf_cb1cc21f-26c9-4738-a70f-9c81b92c0744.pdf

Відповідно, сучасні виклики у сфері безпеки вимагають нових підходів та рішень, які повинні враховувати як технологічні, так і соціальні аспекти, забезпечуючи баланс між безпекою та правами громадян.

Згідно з міжнародним досвідом, у соціальному середовищі моніторинг виступає ключовим елементом та інструментом регулювання суспільних відносин¹⁰. Мова йде про механізми та інститути, завдяки яким суспільство прагне підтримувати встановлені стандарти та бажану модель поведінки серед громадян. Система соціального регулювання одночасно включає два компоненти: пристосування окремих осіб до колективних правил, а також гарантії безпеки, які надає суспільство. Обмежений рівень суспільного контролю, а отже й спостереження, є необхідним для стабільного розвитку соціуму. Разом із тим, моніторинг має двозначний характер, адже може як сприяти захисту прав, так і посилювати нерівність між інститутами влади та громадянами.

Ілюстрацією цього слугують суперечки навколо застосування ШІ у правоохоронній діяльності та системах нагляду, де порушуються питання порушення свобод особистості. Як справедливо відмітили дослідниці Л. Сорока та К. Куркова у роботі, присвяченій правовим, етичним та технічним аспектам використання ШІ та космічних технологій: «Спільна робота громадських організацій і технологічних розробників має сприяти виявленню зон ризику та захисту найуразливіших верств населення. Лише консолідовані зусилля всіх сторін у галузі прав людини дозволять запобігти або зменшити зловживання при впровадженні ШІ та космічних технологій у сфері безпеки, оборони та правоохоронної діяльності»¹¹.

Усі форми спостереження умовно поділяються на дві категорії: із залученням наземних технологічних рішень та з використанням аерокосмічних систем. Серед найпоширеніших інструментів моніторингу – відеоспостереження. Для його реалізації застосовуються оптичні сенсори, здатні фіксувати зображення у видимому спектрі, а також складні, але економічно вигідні технології обробки та зберігання даних. Сфера використання відеоспостереження охоплює різноманітні сценарії – від публічного моніторингу в містах до спеціалізованих застосувань. Відкриті системи відеофіксації активно

¹⁰ Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung, 2022. URL: <https://dserver.bundestag.de/btd/20/042/2004200.pdf>

¹¹ Soroka L., Kurkova K. Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues. *Advanced Space Law*, Volume 3, 2019. P. 135. DOI: <https://doi.org/10.29202/asl/2019/3/11>

використовуються правоохоронцями для профілактики злочинності, тоді як приватні структури застосовують їх для комерційних цілей (наприклад, охорона торговельних центрів).

Негласний відеомоніторинг застосовують органи національної безпеки та оборони для стеження за підозрюваними особами з метою запобігати загрозам або кримінального розслідування. Цей метод принципово відрізняється від публічного відеоспостереження у відкритих зонах щодо цілей та наслідків, а також супроводжується жорсткими правовими обмеженнями.

Розвиток відеоспостереження залишається суперечливою темою. Наприклад, у США його масштаби значно зросли після теракту 11 вересня, проте на відміну від Великої Британії, де рівень моніторингу вважається одним із найвищих у світі (за деякими даними, кількість камер на одного мешканця там найбільша¹²), американська система менш інвазивна.

В Україні регулювання цієї сфери закріплено в Цивільному кодексі (п. 2 ч. 1 ст. 302)¹³ та в Законі України «Про захист персональних даних» (ч. 2 ст. 14)¹⁴. Ці нормативно-правові акти забороняють збір, зберігання чи поширення даних про особисте життя без згоди громадянина, крім винятків, пов'язаних із: національною безпекою, економічним добробутом, захистом прав людини.

Можна навести наступні приклади обмежень:

1) Відеофіксація на робочому місці вважається обробкою персональних даних і вимагає явної згоди працівника. Камери мають бути помітними, а про їх наявність – попереджено.

2) Прихований моніторинг дозволений лише правоохоронним органам за судовим рішенням. Порушення цього правила тягне кримінальну відповідальність¹⁵.

Стосовно досвіду США в правовому регулюванні прихованого відеоспостереження, так Четверта поправка до Конституції США¹⁶

¹² Video Surveillance Laws by State: Everything You Need to Know. *UpCounsel Technologies*, 2020. URL: <https://www.upcounsel.com/video-surveillance-laws-by-state>

¹³ Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 9 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

¹⁴ Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 18 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

¹⁵ Правомірність використання технічних засобів відеоспостереження на робочому місці. *Східне міжрегіональне управління Державної служби України з питань праці*, 2021. URL: <https://smu.dsp.gov.ua/news/pravomirnist-vykorystannia-tekhnichnykh-zasobiv-videosposterezhennia-na-robochomu-mistsi/>

¹⁶ What Does the Fourth Amendment Mean? *Administrative Office of the U.S.*, 2023. URL: <https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0#:~:text=The%20Constitution%2C%20through%20the%20Fourth,deemed%20unreasonable%20under%20the%20law>

встановлює ключові принципи: 1. Судовий контроль: Будь-який ордер на обшук/спостереження потребує попередньої санкції суду з аналізом «ймовірної причини». 2. Парадокс публічного розкриття: Особа втрачає конституційний захист, якщо свідомо оприлюднює дані (наприклад, соціальні медіа), але зберігає право на приватність у громадських просторах за певних умов. 3. Регіональна специфіка: Окремі штати мають право вводити додаткові обмеження. Наприклад, у штаті Флорида криміналізовано приховану зйомку в місцях з очікуванням приватності (ванні кімнати), але не на пляжах¹⁷.

Стосовно проблемних аспектів аерокосмічного моніторингу, то при застосуванні супутникових технологій виникають суперечності:

1. Технологічні можливості та права людини: Висока деталізація знімків може фіксувати особисті дані без явної згоди.

2. Правова невизначеність: Відсутність єдиних міжнародних стандартів для розмежування «громадського» та «приватного» простору у повітряному просторі.

3. Ризик зловживань: Віддалений моніторинг ускладнює фіксацію фактів незаконного збору даних.

Баланс інтересів у національній безпеці полягає в наступному:

1. Судова санкція залишається обов'язковою умовою, але критерії «надзвичайності» часто розмиті.

2. Етична дилема: Розширення технічних можливостей правоохоронців суперечить принципу мінімальної достатності втручання.

3. Транскордонний характер: Аерокосмічні технології вимагають міжнародної гармонізації законів (наприклад, використання даних іноземних супутників).

Отже, досвід США демонструє, що навіть розвинені правові системи потребують постійного оновлення норм для врахування: динаміки технологій, суспільної толерантності до моніторингу, захисту «концепції приватності» у цифрову епоху. Для України актуально запозичення механізму «подвійних гарантій» – судовий контроль та спеціальні закони.

Досвід Великобританії стосовно інтеграції науки, бізнесу та оборонного сектору полягає у фінансуванні досліджень: 1) Виділення 1,2% оборонного бюджету (приблизно £18 млрд щорічно) на інновації¹⁸. 2) Створення Центру оборонного підприємництва (CDE)

¹⁷ National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security. Presented to Parliament by the Secretary of State for Defence By Command of Her Majesty February, 2012. URL: <https://assets.publishing.service.gov.uk/media/5a75b74840f0b67f59fcf0ed/cm8278.pdf>

¹⁸ About us The Centre for Defence Enterprise (CDE) funds innovative research that could lead to a cost-effective capability advantage for UK armed forces and national security.

у складі DSTL (Лабораторія оборонних наук і технологій) для підтримки стартапів і малих підприємств¹⁹; інфраструктурній підтримці: 1. CDE фокусується на дослідженнях з підтвердженням концепції, тоді як Служба оборонних постачальників займається впровадженням готових рішень. 2. Залучення широкого кола виконавців, включаючи новачків у сфері оборони²⁰.

Відповідно до Right2INFO.org, неурядової організації, яка виступає за ефективне законодавство та практику, концепція тесту щодо можливої шкоди (Harm Test) та тесту збалансованості суспільного інтересу (Public Interest Test) виникає з вимоги, що обмеження доступу до інформації повинні бути пропорційними та дійсно потрібні. Закон Нового Південного Уельсу «Про державну інформацію (публічний доступ)» від 2009 року передбачає, що всі державні установи зобов'язані розкривати або оприлюднювати інформацію, якщо немає значних суспільних інтересів, що заперечують розголошення. Основним принципом при виконанні цього зобов'язання є презумпція на користь розкриття інформації, яка служить відправною точкою для всіх рішень щодо доступу до інформації²¹. Це стосується обов'язкового проактивного розкриття; авторизованого проактивного випуску, неофіційного випуску та задоволення запитів на доступ.

Отже, особи, відповідальні за прийняття рішення про розкриття інформації, повинні використовувати презумпцію на користь розкриття як основу для своїх оглядів суспільного інтересу. Таким чином, за відсутності переважних суспільних інтересів проти розголошення, правоохоронні органи та розвідувальні агентства мусять надавати інформацію як про деталі своїх дій, так і про стратегічні плани з метою дотримання права громадськості бути обізнаною про діяльність цих органів, забезпечуючи прозорість та доступність інформації щодо їхніх функцій. Велика Британія має одну з найбільш технологічно оснащених армій і правоохоронних систем у світі та гнучкі механізми комерціалізації оборонних технологій.

GOV.UK, 2023. URL: <https://www.gov.uk/government/organisations/centre-for-defence-enterprise/about#:~:text=The%20Centre%20for%20Defence%20Enterprise,armed%20forces%20and%20national%20security>

¹⁹ Procurement at MOD. Doing business with defence: information for those looking to become a supplier or contractor. GOV.UK, 2023. URL: <https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#contact-us-for-advice-and-guidance-about-selling-to-the-mod>

²⁰ Fact Sheet – What is the public interest test? IPC, 2022. URL: <https://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test>

²¹ Law Enforcement and Building Integrity. Geneva Centre for Security Sector Governance, 2023. URL: <https://securitysectorintegrity.com/institutions-and-organisations/law-enforcement/>

У контексті ефективного управління та адміністративного регулювання сектором безпеки, результативність правоохоронного забезпечення полягає в тому, що органи правопорядку та їх працівники здатні гарантувати безпеку держави та її громадян, дотримуючись принципів демократичного цивільного контролю, поваги до верховенства права та прав людини²². Міжнародно визнаним є принцип, згідно з яким уряди зобов'язані підтримувати право на інформацію, водночас встановлюючи розумні обмеження для захисту чутливої публічної інформації. Це необхідно для належної реалізації державних функцій у специфічних сферах, таких як національна безпека та оборона [23]. Крім того, існує загальноновизнана міжнародна згода на те, що прозорість у політиці та діяльності державних установ має бути нормою, а секретність як виняток. Винятки повинні бути обґрунтованими та вважатися легітимними лише в разі, якщо можна довести їхню необхідність для захисту істотних інтересів національної безпеки.

2. Трансформація функцій правоохоронних органів – від реактивного реагування до проактивного прогнозування загроз із застосуванням штучного інтелекту, дронів та аерокосмічного моніторингу

Обговорюючи використання аерокосмічних технологій правоохоронними органами для забезпечення національної безпеки та оборони, варто звернути увагу на низку важливих питань. Глобальна доступність таких технологій у поєднанні зі швидкими темпами їх розвитку ставлять перед уповноваженими суб'єктами нові виклики, адже вони повинні протистояти дедалі більш складним і різноманітним загрозам. Це включає не лише складні військові системи, але й креативне використання цивільних технологій. Супротивники легше можуть придбати високотехнологічні продукти на відкритому ринку, що потенційно знижує переваги в операційній діяльності. Щоб залишатися конкурентоспроможними та захищати себе від загроз, країни прагнуть розвивати власні технічні можливості, підтримувати інфраструктуру та науково-дослідні установи, а також бути обізнаними у сучасних технологіях, що стимулює інвестиції в науку і технології.

Доцільно проаналізувати ключові аспекти Європейської космічної стратегії безпеки та оборони. Так, у 2022 році керівництво

²² Кардона Ф. Балансування відкритості та конфіденційності в оборонному секторі: уроки успішної міжнародної практики. *Центр з розбудови доброчесності в оборонному секторі*, 2018. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/BB-GGG-6-ukr.pdf

Європейського Союзу включило космічний простір до переліку пріоритетних сфер у Стратегічному компасі, підкресливши необхідність формування спеціальної програми з питань безпеки та оборони. Відповідно до цього рішення, Європейська комісія разом із Високим представником із зовнішньої політики підготували першу в історії ЄС Космічну стратегію безпеки та оборони.

Жозеп Боррель, високий представник із закордонних справ та віцепрезидент Європейської Комісії, зазначив: «Космос перетворився на критичний елемент не лише для функціонування європейських суспільств і економік, а й для забезпечення стабільності та захисту. Безпека в космосі – це передумова його подальшого освоєння. Відповідно до положень Стратегічного компаса, ми вперше запропонували комплексний підхід, що об'єднує всі інструменти для захисту космічної інфраструктури ЄС та гарантує доступність космічних технологій для всіх»²³.

Основні положення даної Стратегії:

1. Розширення механізмів захисту: Діюча система моніторингу загроз, розроблена для супутникової навігаційної системи Galileo, буде поширена на всі космічні активи ЄС.

2. Оперативне реагування: Запровадження механізмів швидкого застосування інструментів ЄС у разі виникнення космічних ризиків.

3. Моніторинг орбітальної активності: Надання доступу до даних спостереження через національні космічні команди для виявлення аномалій та захисту інфраструктури.

4. Навчання та тестування: Проведення спеціальних тренувань для оцінки готовності до космічних загроз та вдосконалення механізмів солідарності.

5. Подвійне використання технологій: Інтеграція оборонних потреб у нові космічні програми, зокрема розвиток сервісів, що поєднують цивільні та військові функції.

Стратегія передбачає запуск двох експериментальних ініціатив:

1. Інформаційний сервіс з моніторингу космосу – на основі наявних можливостей держав-членів.

2. Урядова служба спостереження Землі – у межах програми Copernicus, що доповнить існуючі ресурси.

Для підвищення ефективності заплановано:

1. Посилення зв'язку між космічною галуззю, обороною та безпекою на рівні ЄС.

²³ EU Space Strategy for Security and Defence for a stronger and more resilient European Union. *European Commission*, 2022. URL: https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence_en

2. Спільні дослідження та розробки, зокрема підтримку стартапів, що працюють на стику космічних і оборонних технологій.

3. Підготовку кваліфікованих фахівців для забезпечення конкурентоспроможності Європи в космічній сфері.

Ключові завдання європейської космічної стратегії:

1. Захист космічної інфраструктури – забезпечення стабільності роботи супутникових систем та підтримка національних виробників.

2. Розширення оперативних можливостей – розвиток технологій для ефективних дій у космічному просторі.

3. Підвищення рівня безпеки – інтеграція космічних рішень у системи оборони та розвідки.

Хоча є складності у реалізації космічної політики. Так, координація з іншими організаціями – взаємодія з Європейським космічним агентством (ESA) та окремими країнами-членами потребує чіткого розподілу повноважень. Також існують юридичні обмеження – різні правові режими для цивільного та військового космосу ускладнюють прийняття єдиних рішень²⁴.

Отже, Європейська космічна стратегія безпеки та оборони спрямована на: захист критичної інфраструктури від зовнішніх загроз; максимальне використання космічних технологій для зміцнення безпеки; створення єдиного механізму координації між країнами-членами ЄС. Космічна політика ЄС спрямована на створення незалежних механізмів захисту та розвиток інновацій. Безпілотні технології стають ключовим інструментом у реагуванні на сучасні загрози. Подолання адміністративних та технічних викликів дозволить ЄС посилити свою роль у космічній галузі. Ці підходи дозволяють Європі не лише протистояти викликам, а й закріпити свої позиції як одного з ключових гравців у космічній галузі.

Проаналізувавши сучасні стратегії забезпечення технологічної безпеки та оборони інших країн в умовах глобальних викликів слід виділити:

1. Глобалізацію та доступність передових технологій створюють нові загрози для національної безпеки:

1) Демократизація високотехнологічних рішень: супротивники можуть використовувати комерційні технології (дрони, штучний інтелект, кіберзасоби) для асиметричних дій.

2) Скорочення операційних переваг: традиційні системи оборони стають менш ефективними через швидке поширення інновацій.

²⁴ Cellerino Chiara. EU Space Policy and Strategic Autonomy: Tackling Legal Complexities in the Enhancement of the Security and Defence Dimension of the Union in Space. *European Papers – A Journal on Law and Integration*, 2023. URL: <https://www.europeanpapers.eu/es/europeanforum/eu-space-policy-and-strategic-autonomy>

3) Необхідність адаптації: держави мають інвестувати не лише у власні розробки, а й у підтримку науково-дослідних інституцій.

2. Для ефективного протидіяння сучасним загрозам необхідно:

1) Підтримка науково-технічного потенціалу (збільшення інвестицій у дослідження та створення спеціалізованих фондів для стартапів).

2) Створення екосистеми інновацій (сприяння співпраці між університетами, приватним сектором і силовими структурами та пільгові умови для малих і середніх підприємств, що розробляють технології безпеки).

3) Нормативне регулювання (чіткі правила використання новітніх технологій з урахуванням прав людини та міжнародна координація для запобігання зловживанням технологіями).

Отже, технологічна незалежність стає ключовим чинником національної безпеки. Державно-приватне партнерство (як у Великій Британії) дозволяє швидко адаптуватися до нових викликів. Інвестиції в інновації мають бути системними, а не реактивними. Для України актуально запозичення кращих практик (з урахуванням місцевих реалій) та розвиток власної інноваційної інфраструктури у сфері оборони та безпеки.

За останніми даними, понад 5 000 установ громадської безпеки у Сполучених Штатах активно застосовують безпілотні літальні апарати (БПЛА), причому близько 67% із них – це правоохоронні органи. Міністерство оборони США прогнозує, що БПЛА зможуть виконувати функції, які раніше покладалися на пілотовані літаки, зокрема: дозаправка у повітрі, повітряні бої, стратегічне бомбардування, управління бойовими діями, боротьба з ППО противника, електронна війна²⁵.

Сьогодні державні та приватні структури все частіше об'єднуються для протидії новим загрозам. Уряд Бангладешу залучив компанію BAE Systems до розслідування масштабної кібератаки на банк, в результаті якої було викрадено понад 90 млн доларів. Ця компанія виявила причетність злочинної групи Lazarus. BAE Systems також спеціалізується на підтримці країн у боротьбі з кіберзлочинністю, допомагаючи розробляти стратегії протидії шахрайству та захисту громадян. Наприклад, уряд Австралії активно співпрацює з недержавними експертами, зокрема: Центром передового досвіду з поліцейської діяльності (CEPS), Університетом Чарльза Стерта, Коледжем

²⁵ Unmanned Aircraft Systems and How they Improve Security at Home & Abroad. MAG Aerospace, 2023. URL: <https://www.magaero.com/unmanned-aircraft-systems-and-how-they-improve-security-at-home-abroad/>

національної безпеки. Так, Австралійська дослідницька рада фінансує проекти, спрямовані на підвищення рівня безпеки²⁶.

Сучасна концепція безпеки передбачає залучення різних учасників:

1. Державні інституції: правоохоронні органи (поліція, спецслужби), військові структури та екстрені служби (пожежники, медики, цивільний захист).

2. Приватний сектор: оператори критичної інфраструктури, кібербезпека та аналітичні центри, логістичні та технологічні компанії.

3. Громадськість: волонтерські організації та громадяни (наприклад, у реагуванні на катастрофи).

Проведений аналіз актуалізує дискусійне питання щодо доцільності концентрації міжнародних координаційних функцій у Національній поліції України. Хоча однозначного рішення не існує, світова практика демонструє переважну модель, коли саме поліцейські структури виконують цю роль. Яскравим прикладом служить досвід Австралії, де Федеральна поліція (AFP) реалізує три ключові функції: 1) обробка міжнародних запитів; 2) координація транскордонного співробітництва; 3) виконання міжнародних угод.

Австралійська модель передбачає:

1. Створення мережі офіцерів зв'язку в стратегічних регіонах.

2. Активну взаємодію з Інтерполом, Європолом та УНП ООН.

3. Участь у багатосторонніх антикримінальних ініціативах. Цей підхід перетворив правоохоронну діяльність на інструмент зовнішньої політики, що поєднує дипломатичну присутність, обмін оперативною інформацією, спільні оперативні процедури.

Австралійський Закон GIPA встановлює чіткий алгоритм:

1. Презумпція розкриття інформації.

2. Поетапна оцінка суспільного інтересу.

3. Диференційовані механізми оприлюднення²⁷.

Сучасні виклики, пов'язані з кіберзлочинністю, маніпуляціями інформацією та транснаціональними загрозами, вимагають перегляду чинної нормативної бази України. Ключовими проблемами є недосконалість процедур оцінки ризиків, відсутність стандартизованих механізмів для проведення Harm Test (оцінка можливої шкоди) та Public Interest Test (баланс суспільних інтересів).

В Україні існує встановлений порядок оприлюднення публічної інформації державними органами, що має значний суспільний інтерес. Проте, Закон України «Про доступ до публічної інформації» не

²⁶ National Security and Law Enforcement. BAE Systems, 2023. URL: <https://www.baesystems.com/en/digital/markets/national-security-and-law-enforcement>

²⁷ Our global work. Australian Federal Police, 2023. URL: <https://www.afp.gov.au/about-us/our-global-work>

передбачає механізмів для проведення тестування на визначення можливої шкоди від розголошення інформації, а також тесту збалансованості суспільного інтересу, які б могли сприяти правоохоронним органам у прийнятті обґрунтованих рішень щодо розкриття інформації. Як наслідок, існує нагальна потреба в суттєвій модернізації інформаційного законодавства України. Важливо розробити концепцію розвитку цієї галузі права, що інтегруватиме різні правові інститути. Зокрема, розвиток інформаційного законодавства повинен здійснюватися через реалізацію двох основних завдань: ухвалення нової редакції базового закону «Про інформацію» та спеціалізованих законів у сфері інформаційного права; систематизацію цього законодавства шляхом кодифікації, зокрема прийняття Інформаційного кодексу, який би інтегрував окремі правові інститути цієї галузі.

Інформаційний кодекс же має містити:

- 1) чіткі критерії конфіденційності та доступу до інформації;
- 2) процедури швидкого реагування на кіберзагрози;
- 3) спеціальні закони для регулювання міжнародного обміну даними та захисту цифрової інфраструктури.

Впровадження Інформаційного кодексу в Україні є стратегічним кроком для формування сучасного цифрового середовища, яке поєднує правові, технологічні, соціальні та економічні інновації. Цей процес має враховувати як міжнародні стандарти, так і національні особливості, зокрема в умовах війни та кіберзагроз.

Для ефективної реалізації Кодексу необхідно забезпечити гармонізацію з європейським законодавством, зокрема з GDPR та Digital Services Act. Це передбачає посилення захисту персональних даних, особливо в умовах активних кібератак, а також встановлення чітких правил відповідальності для цифрових платформ. Останнє включає механізми боротьби з дезінформацією, модерацію шкідливого контенту та забезпечення прозорості алгоритмів.

Успіх Кодексу залежатиме від розвитку цифрової інфраструктури, зокрема державних сервісів на кшталт «Дії», та посилення кібербезпеки. Важливим напрямком є регулювання штучного інтелекту – від обмеження його використання для маніпуляцій до заохочення інновацій у сфері публічних послуг.

Соціальна адаптація до нових норм вимагатиме підвищення цифрової грамотності, особливо серед вразливих груп населення. Ключовим завданням залишається боротьба з дезінформацією, а також залучення ЗМІ до поширення перевіреної інформації.

Для стимулювання бізнесу до дотримання Кодексу необхідні податкові пільги та підтримка ІТ-сектору. Прозорість цифрового

середовища також сприятиме залученню іноземних інвестицій та інтеграції України в єдиний цифровий ринок ЄС.

Військовий стан обумовлює необхідність балансу між свободою слова та безпековими обмеженнями, що ускладнює впровадження європейських стандартів. Іншим ризиком є корупція, яка може вплинути на розподіл ресурсів, призначених для цифрової трансформації. Успішне впровадження Інформаційного кодексу залежатиме від системного підходу, адаптації міжнародного досвіду до українських реалій та консолідації зусиль держави, бізнесу та громадянського суспільства. В умовах війни це також питання національної безпеки та стійкості цифрового простору. Реалізація запропонованих заходів дозволить підвищити ефективність боротьби з транснаціональною злочинністю, зміцнити довіру громадян до державних інститутів через прозорість і відкритість та забезпечити відповідність європейським стандартам.

Сучасні технології відеоспостереження стали неодмінним елементом забезпечення публічної безпеки. В Україні, де кількість камер перевищує 50 тис., але їх функціонування залишається фрагментованим, запровадження єдиної системи є актуальним завданням. Однак це потребує комплексного аналізу правових, соціально-політичних та технічних аспектів.

1. Правові аспекти

1) конфлікт між безпекою та приватністю: Закон має балансувати між доступом правоохоронних органів до даних та обмеженнями стосовно недоторканності приватного життя. Вирішальним буде механізм судового чи екстреного доступу до архівів;

2) відповідальність за зловживання: Відсутність чітких санкцій за незаконне використання даних може призвести до порушень з боку правоохоронців або хакерських атак на систему.

2. Соціально-політичні аспекти

1) довіра громадян: Досвід країн ЄС (наприклад, Німеччини) показує, що прозорість збору даних (публічні звіти про використання камер) зменшує опір суспільства;

2) дискримінаційний потенціал: Ризик упередженого аналізу даних ШІ (наприклад, автоматична ідентифікація осіб за етнічною ознакою) вимагає заборони використання алгоритмів з неперифікованою точністю.

3. Технічні аспекти

1) сумісність інфраструктур: Інтеграція камер різних поколінь (від аналогових до IP-систем) вимагатиме значних інвестицій. Досвід Естонії свідчить, що модульний підхід (поетапне підключення) ефективніший⁴

2) кібербезпека: Єдині стандарти шифрування даних та регулярні аудити є обов'язковими для запобігання витоку інформації. Країни ЄС (наприклад, Німеччина, Франція) обмежують збір біометричних даних через камери судовим дозволом. Відкрите відеоспостереження у громадських місцях супроводжується інформаційними табличками, а архіви зберігаються не довше 30 діб.

Масове використання розпізнавання обличчя в КНР (наприклад, система «Соціальний кредит») демонструє, як технології можуть перетворитися на інструмент політичного контролю. Федеральні закони США (на кшталт Biometric Information Privacy Act) забороняють використання AI-аналізу відеоданих без згоди громадян, але окремі штати (наприклад, Каліфорнія) вводять додаткові обмеження.

Відповідно до ст. 17 Конституції України, право на недоторканність приватного життя²⁸ обмежує масштабне використання відеомоніторингу. Подібні норми вимагають явної згоди на обробку біометричних даних, що суперечить автоматизованому збору інформації через камери.

Ключові нормативні акти в сфері відеоспостереження:

1. Цивільний кодекс України (ст. 302)²⁹: Забороняє збір та поширення інформації про особисте життя без згоди, за винятком випадків, пов'язаних із національною безпекою або захистом прав людини.

2. Закон України «Про захист персональних даних» (ст. 14)³⁰: Встановлює обмеження на обробку персональних даних, включаючи відеозйомку, без явної згоди суб'єкта.

3. Кримінальний кодекс України: Передбачає відповідальність за незаконне використання прихованих засобів спостереження (ст. 359)³¹.

Практика застосування показує, що відкрите спостереження у громадських місцях або на робочих місцях мають бути помітними, а працівники – попереджені про їхню наявність. Стосовно прихованого спостереження, то дозволяється лише для правоохоронних органів за рішенням суду, що узгоджується з міжнародними стандартами (наприклад, Європейською конвенцією з прав людини).

²⁸ Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text>

²⁹ Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 9 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

³⁰ Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 18 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

³¹ Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 1 лют. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

У сучасному контексті акценти в галузі національної безпеки та оборони змістилися у бік посилення спроможностей правоохоронних органів виконувати свої загальні та специфічні завдання, зокрема через активне впровадження технологій спостереження. Такі технології, завдяки своїм численним можливостям, значно розширюють здатність до оцінки ризиків і визначення потенційних загроз. Це свідчить про те, що всі напрями національної безпеки можуть отримати вигоду від їх впровадження, включаючи моніторинг дорожнього руху, контроль навколишнього середовища, боротьбу з природними катастрофами, захист критичної інфраструктури, а також підтримку правопорядку і кримінальне переслідування. Проте, використання технологій спостереження нерідко викликає дискусії у суспільстві, наукових колах та політичній сфері, породжуючи питання щодо реальних переваг безпеки, ефектів та наслідків, а також пропорційності самих технологічних заходів. З огляду на вищевикладене, виникає необхідність створення достовірної інформаційної бази для формування політичних рішень щодо прийняття відповідного правового підґрунтя для використання технологій спостереження у секторі національної безпеки та оборони. Для цього важливо ретельно проаналізувати питання соціального та політичного характеру, які стають актуальними зі зростаючим використанням таких технологій. Критично важливо вивчити різноманіття можливих сфер застосування з погляду їх технічної, юридичної та соціальної складності, щоб всебічно визначити як потенційні можливості, так і виклики.

Досвід Німеччини доводить, що прозорість (публічні звіти про використання камер) зменшує суспільний спротив. Історичний досвід (китайська система «Соціальний кредит») показує, що технології можуть перетворитися на інструмент контролю. Відповідно технології повинні служити інтересам суспільства, а не ставати інструментом тотального контролю.

Запровадження єдиної системи відеомоніторингу має потенціал підвищити безпеку, але вимагає:

1. Гармонізації з європейськими стандартами (наприклад, Директивою ЄС про ШП).
2. Механізмів захисту від зловживань та дискримінації.
3. Активної участі громадянського суспільства у формуванні політики.

Отже, світовий досвід показує, що без чітких правових рамок відеоспостереження перетворюється на інструмент репресій. Україна має унікальний шанс інтегрувати європейські стандарти, уникаючи шляху тотального контролю. Як зазначають експерти, «технології повинні служити людині, а не навпаки».

Поняття «інтереси держави» та «безпека громадян» є надзвичайно широкими та складними для точного визначення. Так, інтереси держави – це сукупність стратегічних цілей та пріоритетів, що визначають розвиток і стабільність країни. До них належать:

1. Суверенітет і територіальна цілісність – захист незалежності, кордонів і конституційного ладу.
2. Економічна стабільність – забезпечення економічного зростання, контролю над ключовими галузями.
3. Міжнародний вплив – збереження авторитету на міжнародній арені, дипломатія.
4. Соціальна гармонія – запобігання конфліктам у суспільстві, підтримка громадської згоди.

Безпека громадян передбачає захист життя, здоров'я, прав і свобод особи, що охоплює:

1. Фізичну безпеку – запобігання злочинності, тероризму, надзвичайним ситуаціям.
2. Соціальні гарантії – доступ до медицини, освіти, соціальних послуг.
3. Екологічна безпека – контроль за довкіллям і якістю життя.
4. Кібербезпека – захист персональних даних і цифрового простору.

Держава забезпечує безпеку громадян як частину своїх інтересів, оскільки стабільне суспільство є основою для реалізації стратегічних цілей. Наприклад, ефективна правоохоронна система одночасно зміцнює довіру до влади (інтерес держави) і захищає людей (безпека громадян). Проте в окремих випадках може виникати конфлікт між цими поняттями (наприклад, обмеження свобод під час воєнного стану), що вимагає балансування.

Відтак, на нашу думку, замість використання термінів «інтереси держави» та «безпека громадян» у розглянутій постанові доцільно вдаватися до більш узагальненого поняття «публічні інтереси». Це поняття слід розуміти як суттєві потреби значної кількості як фізичних, так і юридичних осіб, які забезпечуються органами публічної адміністрації згідно з їхньою законодавчо визначеною компетенцією. Таке тлумачення «публічних інтересів» було надано Великою Палатою Верховного Суду у постанові від 13 лютого 2019 р. по справі №233/4308/17³².

³² Велика Палата ВС визначила, що таке «публічний інтерес». *Судово-юридична газета*, 2019. URL: <https://sud.ua/ru/news/publication/137267-velika-palata-vs-viznachila-scho-take-publichniy-interes>

Функціональність системи може бути забезпечена лише за умови чіткого розподілу ролей кожного з її складових елементів з відповідним закріпленням сфер відповідальності. Проте, така система повинна бути структурована таким чином, щоб існував необхідний рівень взаємозв'язків між елементами, що дозволяє їй ефективно виконувати покладені на неї завдання.

Мілітаризація поліції як процес надання правоохоронним органам військових характеристик, таких як спеціальне озброєння, техніка, тактика дій та організаційна структура. Це явище має як прихильників, так і критиків у світовому контексті.

Так, після 11 вересня 2001 року поліція США отримала значну кількість військової техніки (наприклад, бронемашини MRAP). Це призвело до агресивніших поліцейських тактик, особливо під час протестів (наприклад, у Фергюсоні, 2014), хоча SWAT-підрозділи ефективні в операціях проти терористів або злочинних угруповань.

У Мексиці та Бразилії поліція часто використовує армійські методи для боротьби з організованою злочинністю, іноді це призводить до порушень прав людини (наприклад, жорстокість у фавелах Ріо-де-Жанейро).

У Франції після терактів 2015 року поліція отримала більше повноважень, але під суворим законодавчим контролем, а у Німеччині спецпідрозділи (GSG-9) діють лише в екстремальних випадках, щоб уникнути надмірної мілітаризації.

У таких країнах, як Південна Корея чи Ізраїль, поліція тісно взаємодіє з армією, особливо в зонах конфліктів (наприклад, ізраїльська поліція на Західному березі), хоча є ризик: стирання меж між правоохоронними та військовими функціями³³.

Через воєнний стан Національна гвардія України змушена використовувати військові підходи, але зберігає орієнтацію на європейські стандарти. Важливо уникати надмірного застосування сили в мирний час.

Отже, мілітаризація поліції може бути виправдана в умовах війни або високого рівня злочинності, але потребує чіткого правового регулювання, щоб запобігти зловживанням. Досвід країн свідчить, що ключовим є баланс між ефективністю та захистом прав громадян.

На нашу думку, хоча правоохоронні органи виправдано відповідають за свою ділянку правоохоронної функції, відсутність центрального координаційного органу для їх діяльності у сфері національної безпеки і оборони України є критичною помилкою. Це, зокрема, зумовлює ряд нерозв'язаних питань щодо ефективності їх

³³ Blake C. Militarization of the police: A global perspective. 2020. 304 p.

діяльності загалом. До таких питань належать, наприклад, неефективний розподіл ресурсів, включаючи відсутність належного фінансування безпекових ініціатив, а також недостатнє врахування соціальних аспектів при прийнятті рішень. Правоохоронні органи володіють глибоким розумінням соціальної динаміки завдяки постійній взаємодії з громадою.

Досвід, накопичений правоохоронними органами в процесі щоденної діяльності, є унікальним і значно інформативнішим у порівнянні з формальними показниками та статистичними даними. Їхня експертна думка, сформована під час розслідування правопорушень, збору розвідувальної інформації, а також у результаті співпраці з громадою та іншими державними структурами, має виняткову цінність для аналізу та стратегічного планування державної політики у сфері національної безпеки і оборони.

Таким чином, обґрунтовується важливість створення інституційного утворення, покликаного представляти інститут правоохоронної діяльності в Україні як централізовану систему різномірних суб'єктів, що виконують правоохоронні функції у межах своїх сфер компетенції. Попри їхню спеціалізацію, ці суб'єкти разом утворюють керівну ланку правоохоронної системи, спрямовану на забезпечення взаємодії та координації в процесі охорони національної безпеки України. Таке утворення сприятиме запобіганню системним помилкам під час вирішення проблем у галузі національної безпеки і оборони та надасть цим суб'єктам повноцінне право брати участь у процесі прийняття державних рішень.

Зважаючи на те, що правоохоронні органи в досліджуваній сфері переважно поділяються на самостійні інститути, такі як Служба безпеки України та Національне антикорупційне бюро України, або структурні одиниці всередині представницьких органів – Міністерства внутрішніх справ України (включаючи Національну поліцію України, Державну службу України з надзвичайних ситуацій, Державну прикордонну службу України тощо), висловлюємо думку, що формування окремого самостійного органу влади у пропонуваному контексті є недоцільним. Так само недоцільно наділяти такими повноваженнями вже існуючі суб'єкти.

Оптимальним рішенням є створення робочого органу при Раді національної безпеки і оборони України, якій будуть делеговані відповідні функції. Щодо реалізації зазначеного, слід уточнити, що для вирішення міжгалузевих питань та забезпечення науково-аналітичного і прогностичного супроводу діяльності Ради національної безпеки і оборони України можуть створюватися міжвідомчі комісії, а також робочі та консультативні органи. Тому для розвитку правоохоронної

діяльності у сфері національної безпеки та надання правоохоронним органам політичної суб'єктності доцільним є встановлення Центру координації та взаємодії правоохоронної діяльності як її робочого органу. Цей центр повинен відповідати за демократично керовану, підвітну, компетентну, дієву та результативну систему правоохоронних органів у секторі безпеки і оборони України.

У своїй діяльності Центр має керуватися Конституцією та законами України, актами Президента України, актами Кабінету Міністрів України, розпорядженнями Секретаря Ради національної безпеки і оборони України, іншими актами законодавства України, а також спеціалізованим Положенням, що визначатиме правові та організаційні основи його функціонування.

На нашу думку, основними завданнями Центру мають бути:

1) забезпечення аналітичного та прогностичного супроводження діяльності Ради національної безпеки і оборони України щодо здійснення взаємодії та координації діяльності правоохоронних органів з питань національної безпеки;

2) вивчення, аналіз, комплексна оцінка і прогнозування результативності діяльності правоохоронних органів у всіх секторах безпеки, видання відповідних інформаційно-аналітичних документів, експертних висновків та рекомендацій;

3) підготовка для розгляду Радою національної безпеки і оборони України пропозицій стосовно:

- комплексного стратегічного плану діяльності правоохоронних органів у сфері національної безпеки і оборони;

- комплексного стратегічного плану реформування діяльності правоохоронних органів у сфері національної безпеки і оборони;

- інформаційного супроводження діяльності правоохоронних органів з питань національної безпеки;

4) розгляд проєктів рішень (планів) правоохоронних органів щодо стратегічного планування їхньої діяльності у сфері національної безпеки і оборони;

5) моніторинг стану виконання визначених Президентом України та Радою національної безпеки і оборони України завдань з питань національної безпеки правоохоронними органами.

Центр для виконання покладених на нього завдань повинен мати право в установленому порядку:

- одержувати від правоохоронних органів, підприємств, установ та організацій необхідну інформацію;

- залучати для розгляду питань, що належать до компетенції Центру, зацікавлених суб'єктів, у тому числі – представників

державних засобів масової інформації, незалежних експертів, науковців тощо;

- утворювати в разі потреби постійні або тимчасові експертні та робочі групи;

- організовувати проведення круглих столів, семінарів, нарад з питань, що належать до компетенції Центру.

Центр має утворюватись у складі керівника, секретаря та інших членів Центру, які працюють на громадських засадах. На нашу думку, до його складу мають входити в установленому порядку по одному із представників Міністра внутрішніх справ України, Міністра оборони України, Служби безпеки України, Національної гвардії України, Національної поліції України, Державної служби України з надзвичайних ситуацій, Державної прикордонної служби України, Державної міграційної служби України, Генеральної прокуратури, Національного антикорупційного бюро України, Державного бюро розслідувань, Бюро економічної безпеки України, Військової служби правопорядку в Збройних силах України, Управління державної охорони України, органів охорони державного кордону, Національного інституту стратегічних досліджень, освітньої діяльності, які готують спеціалістів у сфері забезпечення національної безпеки і оборони, суб'єктів господарювання, що здійснюють технічне в технологічне забезпечення національної безпеки і оборони, інших зацікавлених суб'єктів. Персональний склад Центру має затверджуватись секретарем Ради національної безпеки і оборони України за поданням керівника Центру³⁴.

ВИСНОВКИ

Отже, сучасний світ ставить перед Україною складні виклики у сфері національної безпеки, що потребують переосмислення традиційних підходів та інтеграції інноваційних рішень. Зміна акцентів з класичних загроз (злочинність, охорона інфраструктури) на комплексні ризики – кібератаки, гібридну війну, тероризм – вимагає проактивних заходів. Ключовими інструментами вирішення є: використання штучного інтелекту для прогнозування ризиків, міжсекторальна координація та розвиток превентивних механізмів.

Правоохоронні органи мають адаптуватися до нових реалій через: технологізацію (застосування дронів, AI-аналітики, кіберпатрулювання), міжнародну взаємодію (активізацію роботи через Інтерпол та Європол, обмін даними для боротьби з транснаціональною

³⁴ Макарчук В. В. Правоохоронні органи як суб'єкти формування та реалізації державної політики у сфері національної безпеки і оборони: адміністративно-правовий аспект : дис. ... д-ра юрид. наук : 12.00.07. Київ, 2023. С. 342–346.

злочинністю) та захист прав громадян: баланс між безпекою та приватністю, особливо при використанні систем відеоспостереження.

Європейські країни (наприклад, Швеція, Латвія) демонструють ефективність інтеграції цивільного та військового секторів. Для України актуально впровадження європейських стандартів кібербезпеки та участь у космічних програмах для захисту критичної інфраструктури.

Також доцільно створення Центру координації при РНБО для синхронізації дій усіх сил безпеки і оборони та прийняття Інформаційного кодексу для регулювання кіберпростору та захисту даних.

Запропоновані заходи спрямовані на побудову гнучкої та технологічно оснащеної системи безпеки, здатну протистояти сучасним викликам. Ключові умови успіху – поєднання інновацій, міжнародної підтримки та дотримання демократичних стандартів. Україні необхідно діяти системно, інтегруючи власний досвід із найкращими світовими практиками.

АНОТАЦІЯ

Дослідження аналізує міжнародний досвід участі правоохоронних органів у забезпеченні національної безпеки та оборони, зокрема адаптацію інноваційних підходів до українських реалій. Основна проблематика полягає у необхідності переосмислення традиційних функцій правоохоронних структур у контексті сучасних загроз: кіберзлочинності, гібридної війни, транснаціонального тероризму. Автор акцентує на важливості технологізації (використання ШІ, дронів, аерокосмічного моніторингу), міжсекторальної координації та гармонізації законодавства з європейськими стандартами.

Дослідження доводить, що ефективна адаптація міжнародного досвіду вимагає системного підходу, поєднання технологій із демократичним контролем та врахування соціально-політичних аспектів. Для України ключовим є запозичення моделей ЄС (наприклад, єдиних стандартів відеоспостереження) із одночасною охороною прав людини.

Результати дослідження підкреслюють: стратегічні пріоритети (необхідність проактивних заходів замість реактивного реагування), важливість міжнародної інтеграції (посилення ролі Національного центрального бюро Інтерполу в Україні та співпраця з Європолем), правові ініціативи (запровадження Інформаційного кодексу для балансу між безпекою та правами громадян) та організаційні зміни (пропозиція створити Центр координації при РНБО для синхронізації дій усіх сил національної безпеки і оборони).

Доведено, що сучасна парадигма національної безпеки вимагає гнучкості правових рамок (швидке оновлення законодавства для відповіді новим загрозам), технологізації (використання AI для аналізу даних, штучного інтелекту (ШІ), дронів для спостереження), міждисциплінарності (інтеграція знань із соціології, політології, економіки, IT).

ЛІТЕРАТУРА

1. Про Національне центральне бюро Інтерполу : Постанова Каб. Міністрів України від 25.03.1993 № 220 : станом на 16 груд. 2017 р. URL: <https://zakon.rada.gov.ua/laws/show/220-93-п#Text>
2. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII : станом на 16 серп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>
3. Довідка про основні результати службової діяльності Національного центрального бюро Інтерполу в Україні у 2022 році. *Доступ до правди*, 2022. URL: https://dostup.pravda.com.ua/request/104660/response/372851/attach/3/01.2023.pdf?cookie_passthrough=1
4. Говійко Є. А. Адміністративно-правовий статус Національного центрального бюро Інтерпол : автореф. дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2011. 23 с.
5. Гайчук В. А., Малиновська Т. М. Напрямки вдосконалення міжнародного співробітництва правоохоронних органів у боротьбі зі злочинністю: нормативно-правовий аспект. *Актуальні проблеми сучасної науки в дослідженнях молодих учених*: тези доп. учасників наук.-практ. конф. Харків, 2017. С. 112–114.
6. Пономаренко Г. О. Адміністративно-правові засади управління у сфері забезпечення внутрішньої безпеки держави : дис. ... д-ра юрид. наук: 12.00.07. Харків, 2008. 442 с.
7. National Security Law. *Latvijas Vēstnesis*, 2000. URL: <https://likumi.lv/ta/en/en/id/14011-national-security-law>
8. National Security Concept. *Latvijas Vestnesis*, 2019. URL: <https://likumi.lv/ta/en/en/id/309647-on-approval-of-the-nationalsecurity-concept>
9. Lindgren, F., & Odlund, A., 2017. Total Defence the Crossroads. URL: https://sldinfo.com/wp-content/uploads/2018/12/http__webbrapp.ptn_foi_se_pdf_cb1cc21f-26c9-4738-a70f-9c81b92c0744.pdf
10. Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung, 2022. URL: <https://dserver.bundestag.de/btd/20/042/2004200.pdf>

11. Soroka L., Kurkova K. Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues. *Advanced Space Law*, Volume 3, 2019. P. 131–139. DOI: <https://doi.org/10.29202/asl/2019/3/11>

12. Video Surveillance Laws by State: Everything You Need to Know. *UpCounsel Technologies*, 2020. URL: <https://www.upcounsel.com/video-surveillance-laws-by-state>

13. Цивільний кодекс України: Кодекс України від 16.01.2003 № 435-IV : станом на 9 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

14. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 18 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

15. Правомірність використання технічних засобів відеоспостереження на робочому місці. *Східне міжрегіональне управління Державної служби України з питань праці*, 2021. URL: <https://smu.dsp.gov.ua/news/pravomirnist-vykorystannia-tekhnichnykh-zasobiv-videosposterezhennia-na-robochomu-misti/>

16. What Does the Fourth Amendment Mean? *Administrative Office of the U.S.*, 2023. URL: <https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0#:~:text=The%20Constitution%2C%20through%20the%20Fourth,deemed%20unreasonable%20under%20the%20law.>

17. National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security. *Presented to Parliament by the Secretary of State for Defence By Command of Her Majesty February*, 2012. URL: <https://assets.publishing.service.gov.uk/media/5a75b74840f0b67f59fcf0ed/cm8278.pdf>

18. About us The Centre for Defence Enterprise (CDE) funds innovative research that could lead to a cost-effective capability advantage for UK armed forces and national security. *GOV.UK*, 2023. URL: <https://www.gov.uk/government/organisations/centre-for-defence-enterprise/about#:~:text=The%20Centre%20for%20Defence%20Enterprise,armed%20forces%20and%20national%20security>

19. Procurement at MOD. Doing business with defence: information for those looking to become a supplier or contractor. *GOV.UK*, 2023. URL: <https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#contact-us-for-advice-and-guidance-about-selling-to-the-mod>

20. Fact Sheet – What is the public interest test? *IPC*, 2022. URL: <https://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test>

21. Law Enforcement and Building Integrity. *Geneva Centre for Security Sector Governance*, 2023. URL: <https://securitysectorintegrity.com/institutions-and-organisations/law-enforcement/>

22. Кардона Ф. Балансування відкритості та конфіденційності в оборонному секторі: уроки успішної міжнародної практики. *Центр з розбудови доброчесності в оборонному секторі*, 2018. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/BB-GGG-6-ukr.pdf

23. EU Space Strategy for Security and Defence for a stronger and more resilient European Union. *European Commission*, 2022. URL: https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence_en

24. Cellerino Chiara. EU Space Policy and Strategic Autonomy: Tackling Legal Complexities in the Enhancement of the Security and Defence Dimension of the Union in Space. *European Papers – A Journal on Law and Integration*, 2023. URL: <https://www.europeanpapers.eu/es/europeanforum/eu-space-policy-and-strategic-autonomy>

25. Unmanned Aircraft Systems and How they Improve Security at Home & Abroad. *MAG Aerospace*, 2023. URL: <https://www.magaero.com/unmanned-aircraft-systems-and-how-they-improve-security-at-home-abroad/>

26. National Security and Law Enforcement. *BAE Systems*, 2023. URL: <https://www.baesystems.com/en/digital/markets/national-security-and-law-enforcement>

27. Our global work. *Australian Federal Police*, 2023. URL: <https://www.afp.gov.au/about-us/our-global-work>

28. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>

29. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 1 лют. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

30. Велика Палата ВС визначила, що таке «публічний інтерес». *Судово-юридична газета*, 2019. URL: <https://sud.ua/ru/news/publication/137267-velika-palata-vs-viznachila-scho-take-publichniy-interes>

31. Blake C. Militarization of the police: A global perspective. 2020. 304 p.

32. Макаrchuk В. В. Правоохоронні органи як суб'єкти формування та реалізації державної політики у сфері національної безпеки і оборони: адміністративно-правовий аспект : дис. ... д-ра юрид. наук : 12.00.07. Київ, 2023. 426 с.

Information about the author:

Makarchuk Vitaliy Volodymyrovych,

Doctor of Legal Sciences, Docent,

Associate Professor of the Department of Constitutional Law and

Theoretical and Legal Disciplines

Bila Tserkva National Agrarian University

8/1, Soborna, Bila Tserkva, 09100, Ukraine