ПРАТ «ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

Кваліфікаційна наукова
праця на правах рукопису

МАРТИНЮК Сергій Олександрович

УДК 342.951+355.404

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ OSINT У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Спеціальність 081 «Право»

Галузь знань 08 «Право»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ С. О. Мартинюк

Науковий керівник –
Ануфрієв Микола Іванович
доктор юридичних наук, професор,
заслужений юрист України

Київ – 2025

АНОТАЦІЯ

Мартинюк С. О. Адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 Право. – ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом». – Київ, 2025.

Дисертація є одним із перших комплексних досліджень адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. У результаті дослідження запропоновано наукові положення та висновки, які містять наукову новизну, зокрема: обґрунтовано, що розвідка з відкритих джерел (OSINT) у сфері національної безпеки – це цілеспрямований процес збору, обробки й передачі інформації, що здійснюється суб'єктами OSINT з метою виявлення, попередження й нейтралізації потенційних і актуальних загроз національній безпеці з подальшим переданням інформації уповноваженим органам для ухвалення управлінських рішень, спрямованих на захист національних інтересів, забезпечення стабільності та безпеки суспільства й держави; сформульовано поняття механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, висвітлено його мету та надано характеристику шляхом виокремлення і дослідження складових елементів, властивостей, принципів та функціонування; аргументовано прийняття спеціального законодавчого акту, що має врегульовувати діяльність відповідних розвідувальних та правоохоронних органів зі здійснення розвідки з відкритих джерел; створення незалежного наглядового органу за здійсненням розвідки з відкритих джерел; впровадження єдиної інформаційної платформи для обміну інформацією між суб'єктами OSINT; пошук альтернативних джерел фінансування та інвестування у технології збору та аналізу даних; розширення міжнародної

співпраці у сфері OSINT; підвищення кваліфікації та підготовки спеціалістів зі здійснення розвідки з відкритих джерел.

У дисертації національну безпеку розглянуто в широкому і вузькому розумінні, сформульовано авторське визначення поняття «національна безпека», запропоновано функції та напрями держави у забезпеченні національної безпеки та аргументовано, що адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки має виходити з розуміння чинників, характеру, ступеню, походження небезпек, що можуть виникнути та впливати на ті важливі для нормального існування та функціонування інтереси людини, суспільства та держави, тобто про джерела, які становлять загрозу національній безпеці. Це є принциповим для сприйняття сутності адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Останнє передбачає створення правових, організаційних, економічних, технічних та інших засобів та умов, які забезпечать відповідним суб'єктам ефективну діяльність зі здійснення розвідки з відкритих джерел з метою вчасного виявлення з подальшим усуненням загроз і викликів національній безпеці.

З'ясовано, що адміністративно-правове регулювання передбачає: регулювання правовідносин між суб'єктами OSIN, визначаючи їх завдання, функції та повноваження, механізми взаємодії; забезпечення діяльності суб'єктами OSINT на різних рівнях; установлення механізму реалізації повноважень суб'єктами OSINT (форми, методи діяльності, використання інформаційних ресурсів, засоби та інструменти забезпечення національної безпеки). Обґрунтовано, що нормативно-правове забезпечення функціонування OSINT у сфері національної безпеки має багаторівневу структуру, яка охоплює конституційні, законодавчі, інституційні та міжнародно-правові акти.

У дисертації досліджено сутність поняття «адміністративно-правові засоби механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки», під яким запропоновано розуміти

сукупність правових інструментів (способів, методів тощо), закріплених нормами адміністративного права, які використовуються для реалізації завдань, що спрямовані на забезпечення національної безпеки, шляхом здійснення розвідки з відкритих джерел і дозволяють ефективно виявляти та протидіяти загрозам національній безпеці завдяки функціонуванню OSINT. З'ясовано їх види та виокремлено властивості.

Установлено, що адміністративно-правові засоби характеризують такі властивості: нормативна визначеність, комплексність, цілеспрямованість, функціональність, оперативність і адаптивність, правовий вплив. Запропоновано класифікацію адміністративно-правових засобів за такими критеріями: залежно від завдань правового регулювання у сфері OSINT (загальні та спеціальні); залежно від ступеню складності завдань OSINT (первинні (елементарні) та комплексні (складні); за призначенням для здійснення OSINT (регулятивні, охоронні і процедурні); за предметом правового регулювання у сфері OSINT; за характером (матеріальні та процедурні); за наслідками (звичайні та виняткові); за часом здійснення (постійні, тимчасові). Підкреслено, що ключову роль у здійсненні OSINT відіграють спеціальні адміністративно-правові інструменти, які забезпечують ефективність цього процесу, та наведено їхню детальну характеристику.

Охарактеризовано суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Установлено, що суб'єкти механізму адміністративно-правового функціонування OSINT у сфері національної безпеки – це сукупність державних та інші уповноважених органів (розвідувальних, правоохоронних, контррозвідувальних), що виконують комплекс завдань з виявлення, збору, аналізу та обробки інформації з відкритих джерел з метою забезпечення національної безпеки держави.

Запропоновано групування суб'єктів адміністративно-правового функціонування OSINT у сфері національної безпеки на такі організаційно-

функціональні рівні 1) суб'єкти загальної компетенції (Верховна Рада України, Президент України та Кабінет Міністрів України); 2) суб'єкти загального керівництва (Рада національної безпеки і оборони, Міністерство інформаційної політики України, Міністерство оборони України); 3) суб'єкти спеціального керівництва (суб'єкти спеціальної компетенції (Служба безпеки України, Національна поліція України, Державна прикордонна служба України, Державна служба спеціального зв'язку та захисту інформації України); 4) суб'єкти спеціальної компетенції (розвідувальні та контррозвідувальні органи, Центр протидії дезінформації, відповідні служби та підрозділи суб'єктів спеціального керівництва) та досліджено їх повноваження.

Здійснено деталізацію властивостей гарантій механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. З'ясовано, що гарантії, по-перше, мають публічно-правовий характер і орієнтовані на забезпечення національної безпеки; похідні від конституційних прав і свобод; реалізуються в адміністративно-правовому порядку, мають правореалізаційний та правоохоронний зміст; є інструментом, завдяки якому створюються умови для ефективного функціонування OSINT у сфері національної безпеки; законодавчо закріплені у законах та підзаконних правових актах, які визначають адміністративно-правовий статус відповідних суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки; мають організаційний, правовий, правоохоронний та матеріально-технічний зміст.

Висвітлено міжнародний досвід механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та запропоновано напрями його імплементації у законодавство та діяльність суб'єктів здійснення OSINT, зокрема обґрунтовано доцільність: створення спеціального законодавства, яке чітко врегульовуватиме питання здійснення розвідки, у тому числі з відкритих джерел, а також завдання,

повноваження, межі діяльності розвідувальних і правоохоронних органів у цій сфері; впровадження ефективної системи парламентського та цивільного контролю за функціонуванням OSINT у сфері національної безпеки; створення незалежних наглядових органів контролю за розвідкою з відкритих джерел; створення умов для заохочення партнерства з ІТ-компаніями, іншими суб'єктами приватного права з метою поширення використання новітніх технік та технологій зі здійсненням розвідки з відкритих джерел; впровадження системи навчання та підвищення кваліфікації суб'єктів, які здійснюють OSINT; покращення міжнародного співробітництва та створення спільних платформ з обміну інформацією між розвідувальними та правоохоронними органами інших держав і Україною у питаннях здійснення розвідки з відкритих джерел.

Ключові слова: адміністративно-правове забезпечення, адміністративно-правове регулювання, механізм адміністративно-правового забезпечення, розвідка з відкритих джерел, OSINT, національна безпека, загрози у сфері національної безпеки, розвідувальні органи, правоохоронні органи, гарантії прав людини, міжнародний досвід.

SUMMARY

Martyniuk S.O. Administrative and legal support for the functioning of OSINT in the field of national security. – *Qualifying scientific work on manuscript rights.*

Dissertation for the degree of Doctor of Philosophy in specialty 081 – Law. – PJSC «Higher Educational Institution» Interregional Academy of Personnel Management». – Kyiv, 2025.

The dissertation is one of the first comprehensive studies of the administrative and legal support for the functioning of OSINT in the field of national security. As a result of the study, scientific propositions and conclusions containing scientific novelty are proposed, namely, it is substantiated that intelligence from open sources (OSINT) in the field of national security is a purposeful process of collecting, processing and transmitting information carried out by OSINT subjects for the purpose of detection, prevention, and neutralization of potential and actual threats to national security with subsequent transfer of information to authorized bodies for making management decisions aimed at protecting national interests, ensuring stability and security of society and the state; the concept of the mechanism of administrative and legal support for the functioning of OSINT in the field of national security is formulated, its purpose is highlighted and its characteristics are provided by identifying and researching its constituent elements, properties, principles and functioning; justified, the adoption of a special legislative act, which should regulate the activities of the relevant intelligence and law enforcement agencies in conducting intelligence from open sources; creation of an independent supervisory body for conducting intelligence from open sources; implementation of a unified information platform for information exchange between OSINT subjects; search for alternative sources of funding and investment in data collection and analysis technologies; expansion of international cooperation in the field of OSINT; professional development and training of specialists in conducting intelligence from open sources.

In the dissertation, national security is considered in a broad and narrow sense, the author's definition of the concept of «national security» is formulated, the functions and directions of the state in ensuring national security are proposed, and it is argued that the administrative and legal support for the functioning of OSINT in the field of national security should be based on an understanding of the factors, nature, degree, origin of dangers that may arise and affect those interests of man, society and the state that are important for normal existence and functioning, that is, about sources that pose a threat to the national safety. This is fundamental for understanding the essence of the administrative and legal support for the functioning of OSINT in the field of national security. Administrative and legal support for the operation of OSINT provides for the creation of legal, organizational, economic, technical and other means and conditions that will provide the relevant entities with effective activities in conducting intelligence from open sources with the aim of timely detection and subsequent elimination of threats and challenges to national security.

It was found that the administrative and legal regulation provides; regulation of the legal relationship between OSINT subjects, defining their tasks, functions and powers, interaction mechanisms; ensuring the activities of OSINT subjects at various levels; establishment of a mechanism for the implementation of powers by OSINT subjects (forms, methods of activity, use of information resources, means and tools for ensuring national security). It is substantiated that the regulatory and legal support for the functioning of OSINT in the field of national security has a multi-level structure that includes constitutional, legislative, institutional and international legal acts.

The thesis examines the essence of the administrative-legal means of the mechanism of administrative-legal support for the functioning of OSINT in the field of national security, under which it is proposed to understand the set of legal tools (methods, methods, etc.) established by the norms of administrative law, which are used to implement tasks aimed at ensuring national security through the implementation of intelligence from open sources and allow to effectively detect

and counter threats to national security thanks to the functioning of OSINT, their types have been clarified and their properties have been identified.

It was found that administrative and legal means are characterized by the following properties: regulatory certainty, complexity, purposefulness, functionality, efficiency and adaptability, legal influence. The proposed classification of administrative and legal means according to the following criteria: dependence on tasks of legal regulation in the field of OSINT (general and special); depending on the degree of complexity of OSINT tasks (primary (elementary) and complex (complex); for the purpose of carrying out OSINT (regulatory, security and procedural); on the subject of legal regulation in the field of OSINT; by nature (material and procedural); by consequences (ordinary and exceptional); by the time of implementation (permanent, temporary). It is emphasized that the key role in the implementation of OSINT is played by special administrative and legal means and their characteristics are provided.

The subjects of the mechanism of administrative and legal support for the functioning of OSINT in the field of national security have been characterized, and it has been clarified that the subjects of the mechanism of administrative and legal functioning of OSINT in the field of national security are a set of state and other authorized bodies (intelligence, law enforcement, counterintelligence), which perform a set of tasks for the detection, collection, analysis and processing of information from open sources in order to ensure the national security of the state.

It is proposed to group the subjects of the administrative and legal functioning of OSINT in the field of national security into the following organizational and functional levels: 1) subjects of general competence (the Verkhovna Rada of Ukraine, the President of Ukraine and the Cabinet of Ministers of Ukraine); 2) subjects of general management (National Security and Defense Council, Ministry of Information Policy of Ukraine, Ministry of Defense of Ukraine); 3) subjects of special management (subjects of special competence (Security Service of Ukraine, National Police of Ukraine, State Border Service of

Ukraine, State Service of Special Communications and Information Protection of Ukraine); 4) subjects of special competence (intelligence and counter-intelligence bodies, the Center for Combating Disinformation, relevant services and units of special management entities) and their powers were investigated.

Details of the properties of guarantees of the mechanism of administrative and legal support for the functioning of OSINT in the field of national security have been detailed. It was found that the guarantees, firstly, have a public-legal nature and are aimed at ensuring national security; derived from constitutional rights and freedoms; are implemented in the administrative and legal order, have law enforcement and law enforcement content; is a tool thanks to which conditions are created for the effective functioning of OSINT in the field of national security; legally enshrined in laws and by-laws, which determine the administrative-legal status of the relevant subjects of the mechanism of administrative-legal support for the functioning of OSINT in the field of national security; have organizational, legal, law enforcement and material and technical content.

The international experience of the mechanism of administrative and legal support for the functioning of OSINT in the field of national security is highlighted and directions for its implementation in the legislation and activities of OSINT subjects are highlighted, the expediency is justified: the creation of special legislation that will clearly regulate the issue of intelligence, including from open sources , as well as tasks, powers, limits of activity of intelligence and law enforcement agencies in this area; implementation of an effective system of parliamentary and civil control over the functioning of OSINT in the field of national security; creation of independent supervisory bodies for control of intelligence from open sources; creation of conditions to encourage partnership with IT companies, other subjects of private law in order to spread the use of the latest techniques and technologies with the implementation of intelligence from open sources; implementation of a system of training and advanced training of subjects conducting OSINT; improvement of international cooperation and

creation of joint platforms for exchange of information between intelligence and law enforcement agencies of other states and Ukraine in matters of conducting intelligence from open sources.

Key words: administrative and legal support, administrative and legal regulation, mechanism of administrative and legal support, intelligence from open sources, OSINT, national security, threats in the field of national security, intelligence agencies, law enforcement agencies, guarantees of human rights, international experience.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Мартинюк С. О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал.* 2021. № 9. С. 332–334. DOI: https://doi.org/10.32782/2524-0374/2021-9/82.

2. Мартинюк С. О. Адміністративно-правове регулювання забезпечення функціонування OSINT у сфері національної безпеки. *Аналітично-порівняльне правознавство.* 2023. Випуск 5. С. 355–358. DOI: https://doi.org/10.24144/2788-6018.2023.05.63.

3. Мартинюк С. О. Зарубіжний досвід функціонування OSINT у сфері національної безпеки: адміністративно-правовий аспект. *Наукові перспективи.* 2025. № 3 (57). С. 1061–1071. DOI: https://doi.org/10.52058/2708-7530-2025-3(57)-1061-1071.

4. Мартинюк С. О. Національна безпека, як об'єкт адміністративно-правового забезпечення: поняття та зміст у працях вітчизняних дослідників. 2025. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. № 2(74) (2025). С. 78-83. DOI: https://doi.org/10.32689/2522-4603.2025.2.12

Статті у зарубіжних періодичних наукових виданнях:

5. Lata N., Martyniuk S., Minka T., Ilchyshyn N., Yurakh V. Administrative and legal security of public information services in the activities of bodies of legislative and judicial power: Seguridad administrativa y jurídica de los servicios de información pública en las actividades de los órganos del poder legislativo y judicial. *Cuestiones Políticas*. 2022. Vol. 40 (72). P. 656–669. DOI: https://doi.org/10.46398/cuestpol.4072.38.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Мартинюк С. О. Щодо змісту поняття адміністративно-правового забезпечення OSINT у сфері національної безпеки України. *Актуальні завдання та напрями розвитку юридичної науки у XXI столітті*: матеріали Міжнародної науково-практичної конференції (м. Львів, 15–16 жовтня 2021 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», 2021. С. 77–79.

7. Мартинюк С. О. Забезпечення прав людини при використанні OSINT у сфері національної безпеки. *Права людини: методологічний, гносеологічний та онтологічний аспекти:* матеріали Міжнародної науково-практичної конференції присвяченої 75-річчю проголошення Загальної декларації прав людини (м. Дніпро, 5 грудня 2023 р.). Дніпро, 2023. С. 213–215.

8. Мартинюк С. О. Організаційно-правові засоби адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. *Український правовий вимір: пошук відповідей на глобальні міжнародні виклики*: матеріали VI Міжнародної науково-практичної конференції (м. Дніпро, 24 травня 2024 р.) / Університет митної справи та фінансів. Дніпро, 2024. С. 66–69.

9. Мартинюк С. О. Роль OSINT для безпеки бізнесу: організаційно-правовий аспект. *Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності*: матеріали X Міжнародної науково-практичної конференції (м. Київ, 20–22 травня 2025 р.). Київ: Міжрегіональна Академія управління персоналом, 2025. С. 572–574.

ЗМІСТ

ВСТУП

Обґрунтування теми дослідження. Україна, як демократична та соціально орієнтована держава, активно зміцнює свою безпеку в умовах інтенсивної європейської та євроатлантичної інтеграції. Однак цей шлях супроводжується низкою серйозних викликів і загроз як внутрішнього, так і зовнішнього характеру, серед яких – збройна агресія з боку російської федерації, окуповані території, терористичні загрози, економічна криза та ін. Усі ці фактори підкреслюють необхідність розробки й упровадження нових підходів і технологій, спрямованих на ефективне забезпечення національної безпеки.

Одним із перспективних напрямів забезпечення національної безпеки є використання OSINT (Open Source Intelligence) – розвідки на основі відкритих джерел, яка демонструє високий потенціал для підвищення оперативності та ефективності виявлення й аналізу загроз. OSINT забезпечує не лише швидкий доступ до великого обсягу інформації з відкритих джерел, але й сприяє розробці ефективних стратегій реагування та прийняття рішень на державному рівні. Водночас для реалізації повного потенціалу OSINT у процесі виявлення й усунення загроз національній безпеці необхідне впровадження дієвого адміністративно-правового механізму. Такий механізм має забезпечити вдосконалення правового регулювання, процедур і координації діяльності відповідних суб’єктів.

Законодавець вже здійснив низку важливих кроків у цьому напрямі, зокрема розробив державні стратегії, концепції та програми, які сприяють впровадженню сучасних розвідувальних технологій для зміцнення національної безпеки. Утім, наявні прогалини та недоліки в правовому й організаційному забезпеченні обмежують можливості повноцінного використання OSINT. У зв’язку з цим нагальним завданням є створення ефективного адміністративно-правового механізму функціонування OSINT, що

сприятиме своєчасному виявленню й усуненню загроз у сфері національної безпеки.

Відсутність ґрунтовних наукових досліджень з питань адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки свідчить як про складність цих питань, так і про недостатню увагу з боку вчених, що загалом позначається на якості правового регулювання та правозастосовної діяльності. Єдине монографічне дослідження, що певним чином стосується проблем функціонування OSINT в Україні, належить В. Д. Щербаню, який у своїй монографічній праці на тему: «Концепція адміністративно-правового забезпечення функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах України» (2020 р.), висвітлив питання функціонування OSINT, проте винятково у сфері антикорупційної діяльності та стосовно правоохоронних органів.

Проблематика гарантування державної безпеки України неодноразово виступала предметом наукових досліджень спеціалістів у сфері адміністративного законодавства. Значний внесок у цю галузь зробили такі вчені: В. О. Антонов, О. М. Бандурка, Д. О. Беззубов, О. І. Безпалова, О. О. Бригінець, А. Л. Борко, С. М. Гусаров, І. М. Доронін, В. Ф. Загурська-Антонюк, І. В. Каріх, В. Ю. Кобринський, А. Т. Комзюк, І. В. Кременовська, А. М. Куліш, В. А. Ліпкан, К. Б. Левченко, С. О. Лисенко, Ю. П. Лісовська, М. В. Лошицький, О. А. Моргунов, О. М. Музичук, А. М. Мурашко, Т. С. Перун, А. В. Рубан, О. Ю. Салманова, І. В. Сервецький, В. В. Сокуренко, В. І. Теремецький, Т. Ю. Ткачук, Н. П. Христинченко, З. В. Чуйко, Р. В. Шаповал та ін. Їхні наукові роботи стали базою для подальшого розвитку теоретичних і практичних підходів до вдосконалення адміністративно-правового забезпечення функціонування OSINT у сфері державної безпеки.

Водночас, хоча результати досліджень цих та інших науковців є вагомим підґрунтям для нашого аналізу, питання адміністративно-правового забезпечення OSINT у контексті національної безпеки все ще потребують глибшого вивчення та подальшого опрацювання.

Наведене вище, а також сучасні загрози та виклики у сфері національної безпеки, стрімкий розвиток інформаційних технологій, потреби удосконалення діяльності відповідних суб'єктів, що здійснюють розвідку з відкритих джерел, й обумовлюють актуальність теми дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Проблематика дисертації пов'язана із Переліком пріоритетних тематичних наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затвердженого Постановою Кабінету Міністрів України від 30.04.2024 р. № 476; та виконана відповідно до Плану наукових досліджень ПрАТ «ВНЗ Міжрегіональна Академія управління персоналом» за темою: «Дослідження теоретико-методологічних основ розвитку української державності в контексті світових модернізаційних процесів формування національних громадянських суспільств: політичний, юридичний, економічний, соціальний, психологічний та управлінський аспекти» (ДР № 0119U100492).

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає у комплексному аналізі теоретико-правових та практичних аспектів адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, а також у формулюванні науково обґрунтованих пропозицій та рекомендацій щодо удосконалення чинного законодавства та діяльності суб'єктів, які здійснюють розвідку з відкритих джерел.

Для реалізації зазначеної мети, необхідно виконати такі *завдання*:

– висвітлити стан наукових досліджень адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– розкрити сутність національної безпеки як об'єкта адміністративно-правового забезпечення;

– з'ясувати особливості адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– сформулювати поняття та розкрити зміст механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– охарактеризувати суб’єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– здійснити аналіз адміністративно-правових засобів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– розкрити зміст гарантій механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– висвітлити міжнародний досвід механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та запропонувати напрями його імплементації;

– запропонувати шляхи удосконалення адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Об’єктом дослідження є відносини, що виникають у зв’язку з адміністративно-правовим забезпеченням національної безпеки.

Предмет дослідження – адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки.

Методи дослідження. Методологічну основу дисертації складають загальнонаукові та спеціальнонаукові методи пізнання. *Діалектичний підхід* дав змогу дослідити зміст суспільних відносин у сфері адміністративно-правового забезпечення функціонування OSINT у контексті їхнього сучасного стану та тенденцій розвитку. За допомогою *логіко-семантичного методу* сформульовано авторські поняття та запропоновано тлумачення термінам та категоріям у досліджуваній сфері (розділ 2). *Метод порівняльного правознавства* сприяв дослідженню змісту законодавства інших країн щодо функціонування OSINT та розробці шляхів його імплементації (підрозділ 3.1). *Системно-структурний* та *системно-функціональний методи* дали змогу розкрити зміст складових механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, з’ясувати функціональні зв’язки між його елементами (розділи 1–2). За допомогою *спеціально-юридичного* і *емпіричних методів* було здійснено збір і аналіз інформації щодо

адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки (підрозділи 1.1, 1.3, 2.1–2.4, 3.2), а *структурно-логічний метод* дав змогу сформулювати шляхи вирішення проблем щодо забезпечення національної безпеки з використанням OSINT (розділ 3).

Теоретичну основу дослідження становили наукові праці фахівців у галузях філософії, загальної теорії держави та права, адміністративного, інформаційного, військового права та інших галузей правових наук (монографії, дисертації, наукові статті тощо).

Нормативну основу роботи склали Конституція України, закони та підзаконні нормативно-правові акти, що регулюють адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки.

Емпіричною основою дисертації слугували матеріали узагальнень практики адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, аналітичні огляди, довідкова література та статистичні дані.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших комплексних досліджень адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. У результаті дослідження запропоновано наукові положення та висновки, які містять наукову новизну, зокрема:

вперше:

– обґрунтовано, що розвідка з відкритих джерел (OSINT) у сфері національної безпеки – це цілеспрямований процес збору, обробки й передачі інформації, що здійснюється суб’єктами OSINT з метою виявлення, попередження й нейтралізації потенційних і актуальних загроз національній безпеці з подальшим переданням інформації уповноваженим органам для ухвалення управлінських рішень, спрямованих на захист національних інтересів, забезпечення стабільності та безпеки суспільства й держави;

– сформульовано дефініцію терміна «адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки», під яким

доцільно розуміти діяльність уповноважених суб'єктів OSINT, що здійснюється в межах правового поля адміністративного законодавства із застосуванням специфічного адміністративно-правового інструментарію (методів, способів, засобів, процедур тощо), спрямованого на правове впорядкування та регламентацію суспільних відносин у зазначеній сфері, що пов'язані з виявленням і усуненням загроз у сфері національної безпеки за допомогою розвідки з відкритих джерел та висвітлено його властивості: державно-владний характер, цільове спрямування, системність, структурованість, регулювання нормами адміністративного права; наявність спеціальних правових засобів;

– сформульовано поняття механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, висвітлено його мету та надано характеристику шляхом виокремлення і дослідження складових елементів, властивостей, принципів та функціонування;

– аргументовано прийняття спеціального законодавчого акту, що має врегульовувати діяльність відповідних розвідувальних та правоохоронних органів зі здійснення розвідки з відкритих джерел; створення незалежного наглядового органу за здійсненням розвідки з відкритих джерел; впровадження єдиної інформаційної платформи для обміну інформацією між суб'єктами OSINT; пошук альтернативних джерел фінансування та інвестування у технології збору та аналізу даних; розширення міжнародної співпраці у сфері OSINT; підвищення кваліфікації та підготовки спеціалістів зі здійснення розвідки з відкритих джерел;

удосконалено:

– теоретичні підходи до розуміння змісту поняття «національна безпека» та її складових. Національну безпеку розглянуто в широкому і вузькому розумінні, сформульовано авторське визначення поняття «національна безпека», запропоновано функції та напрями держави у забезпеченні національної безпеки та аргументовано, що адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки має

виходити з розуміння чинників, характеру, ступеню, походження небезпек, що можуть виникнути та впливати на ті важливі для нормального існування та функціонування інтереси людини, суспільства та держави, тобто про джерела, які становлять загрозу національній безпеці. Це є принциповим для сприйняття сутності адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– теоретичні уявлення щодо напрямів та рівнів адміністративно-правового регулювання забезпечення функціонування OSINT у сфері національної безпеки. З'ясовано, що адміністративно-правове регулювання передбачає: регулювання правовідносин між суб'єктами OSIN, визначаючи їх завдання, функції та повноваження, механізми взаємодії; забезпечення діяльності суб'єктами OSINT на різних рівнях; установлення механізму реалізації повноважень суб'єктами OSINT (форми, методи діяльності, використання інформаційних ресурсів, засоби та інструменти забезпечення національної безпеки). Обґрунтовано, що нормативно-правове забезпечення функціонування OSINT у сфері національної безпеки має багаторівневу структуру, яка охоплює конституційні, законодавчі, інституційні та міжнародно-правові акти;

– зміст поняття «адміністративно-правові засоби механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки», під яким запропоновано розуміти сукупність правових інструментів (способів, методів тощо), закріплених нормами адміністративного права, які використовуються для реалізації завдань, що спрямовані на забезпечення національної безпеки, шляхом здійснення розвідки з відкритих джерел і дозволяють ефективно виявляти та протидіяти загрозам національній безпеці завдяки функціонуванню OSINT. З'ясовано їх види та виокремлено властивості;

– деталізацію напрямів запозичення позитивного досвіду Великобританії, США, Німеччини у законодавство і діяльність суб'єктів, що здійснюють розвідку з відкритих джерел;

дістали подальшого розвитку:

– підходи до групування та класифікації наукових джерел дослідження. Наукові джерела поділено на системні та фундаментальні праці, де розглядаються різні аспекти управління, розвитку і функціонування сектору безпеки та оборони, а також на ті, що фокусуються на окремих аспектах правового регулювання, зокрема стосовно адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. У глобальному масштабі ці дослідження поділяються на вітчизняні та іноземні, що стосуються адміністративно-правових аспектів адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– характеристика суб'єктів механізму адміністративно-правового функціонування OSINT та підходи до їх класифікації. За змістом правосуб'єктності суб'єктів OSINT поділено на суб'єктів загальної і спеціальної компетенції, за характером адміністративно-правового регулювання – на тих, які мають владні повноваження, та на тих, що здійснюють правозастосовну діяльність;

– розгляд загальних принципів функціонування OSINT у сфері національної безпеки, таких як законність, верховенство права, повага до прав і свобод людини та спеціальних принципів, що визначають засади здійснення розвідки з відкритих джерел, – конфіденційність, прозорість, пропорційність та незалежність;

– деталізація властивостей гарантій механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. З'ясовано, що гарантії, по-перше, мають публічно-правовий характер і орієнтовані на забезпечення національної безпеки; похідні від конституційних прав і свобод; реалізуються в адміністративно-правовому порядку, мають правореалізаційний та правоохоронний зміст; є інструментом, завдяки якому створюються умови для ефективного функціонування OSINT у сфері національної безпеки; законодавчо закріплені у законах та підзаконних правових актах, які визначають адміністративно-правовий статус відповідних

суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки; мають організаційний, правовий, правоохоронний та матеріально-технічний зміст.

Практичне значення одержаних результатів полягає в тому, що положення, висновки, пропозиції і рекомендації, сформульовані у дисертації, можуть бути використані у:

– *науково-дослідній діяльності* – для подальших загальнотеоретичних та галузевих досліджень адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки;

– *правотворчості* – як теоретичне підґрунтя для вдосконалення чинного законодавства, яке регулює адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки;

– *правозастосовній сфері* – для покращення правозастосовної діяльності суб'єктів OSINT у сфері національної безпеки;

– *освітньому процесі* – для підготовки навчально-методичних матеріалів, проведення лекцій, під час викладання таких дисциплін як: «Адміністративне право України», «Проблеми адміністративного права», у процесі підготовки навчально-методичних комплексів дисциплін, підручників, навчальної та прикладної літератури.

Особистий внесок здобувача. Дисертацію виконано здобувачем самостійно, з використанням останніх досягнень теорії права і адміністративного права, а усі викладені у роботі наукові положення, узагальнення та висновки базуються на власних аналітичних напрацюваннях автора. Ідеї, результати та фрагменти текстів, запозичені з праць інших науковців, належним чином оформлені з посиланням на відповідні джерела. Усі наукові публікації за темою дисертації здійснені без участі співавторів.

Апробація результатів дослідження. Основні теоретичні положення, їх новизна та практична значущість дослідження були оприлюднені на таких міжнародних науково-практичних конференціях: «*Актуальні завдання та напрями розвитку юридичної науки у XXI столітті*» (м. Львів, 15–16 жовтня

2021 р.); «*Права людини: методологічний, гносеологічний та онтологічний аспекти*» (м. Дніпро, 5 грудня 2023 р.); «*Український правовий вимір: пошук відповідей на глобальні міжнародні виклики*» (м. Дніпро, 24 травня 2024 р.); *Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності* (м. Київ, 20–22 травня 2025 р.).

Публікації. Основні результати дослідження, висновки та пропозиції висвітлено у 9 наукових працях, з яких 4 статті – опубліковані у наукових фахових виданнях України, 1 стаття – у зарубіжному періодичному виданні, а також 4 – тези доповідей на міжнародних науково-практичних конференціях.

Структура та обсяг дисертації. Робота складається з анотації, вступу, трьох розділів, логічно об’єднаних у 9 підрозділів, висновків, списку використаних джерел та додатку. Загальний обсяг дисертації становить 250 сторінок, з них основного тексту – 213 сторінок. Список використаних джерел налічує 204 найменування і займає 21 сторінку. Додаток розміщено на 2 сторінках.

РОЗДІЛ 1
ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ OSINT У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Стан наукових досліджень адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки

Питання адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки неможливо розглядати без урахування управління сектором безпеки, оскільки він є складовою частиною державного управління у сфері забезпечення національної безпеки. Тому тематика адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки розглядається у наукових дослідженнях різних галузей.

Варто зазначити, що питання адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки розглядаються не лише в рамках адміністративно-правових досліджень, але й у працях з інформаційного права та інших аспектів управління сектором безпеки, де аналізуються правові аспекти цього питання як з теоретичної, так і з практичної точок зору.

Перед тим як представити аналіз досліджень науковців, які висвітлювали загальні питання адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, доцільно здійснити класифікацію наукових джерел за кількома критеріями. З огляду на форму подачі, використані джерела можна класифікувати на дисертаційні праці, наукові монографії, підручники та навчально-методичні посібники, що цілком або частково присвячені проблематиці адміністративно-правового забезпечення у сфері національної безпеки, а також загальнотеоретичним аспектам безпеки та оборони.

Окрім того, це можуть бути наукові статті в періодичних виданнях, які досліджують різні аспекти національної безпеки, а також тези конференцій, присвячені вищезгаданим темам.

Крім цього, наукові праці можна поділити на компіляції нормативно-правових актів, які регулюють суспільні відносини у сфері адміністративно-правового забезпечення функціонування OSINT, та на докторські та кандидатські дисертації, автореферати, монографії та статті, в яких розглядається адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки. Окремо слід виділити довідкові матеріали, тези конференцій або інші матеріали наукових заходів.

Окрім згаданих раніше категорій наукових джерел, важливо зазначити, що в кожній з цих груп є особливості, які стосуються глибини дослідження і специфіки охоплення проблематики адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Наприклад, дисертації та монографії зазвичай розглядають питання детально, з урахуванням широкого спектра правових і адміністративних аспектів функціонування OSINT, тоді як наукові статті можуть висвітлювати окремі конкретні питання або нові підходи до адміністративно-правового регулювання та управління функціонуванням OSINT у сфері національної безпеки.

Також варто зосередити увагу на тезах наукових конференцій, які часто є джерелом нових ідей і підходів, оскільки науковці у такому форматі представляють свої попередні результати або пропонують інноваційні рішення. Це важливий компонент наукового доробку, оскільки конференції забезпечують платформу для обміну думками, обговорення сучасних викликів та формування нових напрямів досліджень адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Довідкові та енциклопедичні видання мають інший характер – вони призначені для надання узагальненої інформації про нормативно-правове регулювання, управлінські та адміністративні аспекти, але зазвичай не містять глибокого аналізу чи нових наукових висновків. Їх роль полягає в

систематизації і доступному поданні чинного законодавства та наукового знання, що робить їх зручним інструментом для практичного використання.

Крім того, компіляції нормативно-правових актів – це особливий вид наукових джерел, оскільки вони надають інформацію і аналіз чинного законодавства, яке регулює адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки. Ці джерела є важливими для правозастосовної практики, оскільки допомагають структурувати правові акти, визначити ключові норми та зрозуміти їхню взаємодію у системі адміністративно-правового забезпечення.

Варто також згадати про наукові праці, присвячені міжнародному досвіду. Зокрема, дослідження іноземних правових систем і моделей адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки можуть бути корисними для України у контексті адаптації та вдосконалення власної правової системи. Закордонні приклади, з урахуванням різних історичних умов та специфіки кожної держави, можуть містити важливі уроки щодо реформування, структури управління і правового забезпечення сектору безпеки загалом, та адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки зокрема.

У контексті цього важливим напрямом є порівняльне правознавство, яке дозволяє аналізувати різні моделі та підходи до адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки в інших країнах, що може допомогти у розробці ефективної системи управління в Україні. Це також сприяє інтеграції кращих практик у вітчизняну правову систему, враховуючи специфіку міжнародних безпекових загроз та викликів, з якими стикаються різні держави.

Таким чином, науковий доробок у сфері адміністративно-правового забезпечення функціонування OSINT у національній безпеці можна класифікувати за різними ознаками: формою джерел, глибиною аналізу, а також національною чи міжнародною специфікою. Такий підхід дозволяє отримати всебічне розуміння адміністративно-правового забезпечення

функціонування OSINT, охоплюючи як теоретичні, так і практичні аспекти розвитку безпеки та оборони в Україні.

Отже, за формою наукові джерела, використані в цьому дослідженні, доцільно розподілити на такі групи: 1) монографії, дисертаційні дослідження, автореферати, підручники та навчальні посібники; 2) наукові статті, опубліковані у фахових виданнях з правознавства; 3) матеріали наукових конференцій, зокрема тези доповідей і виступів; 4) довідкові видання, енциклопедичні джерела та систематизовані збірники нормативно-правових актів, які регламентують адміністративно-правові засади функціонування сектору безпеки та оборони України.

Ці джерела можна додатково поділити на: 1) ті, що присвячені винятково адміністративно-правовому забезпеченню функціонування OSINT у сфері національної безпеки; 2) ті, в яких адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки згадуються частково у контексті інших проблем.

Загалом наукові дослідження можна розділити на системні та фундаментальні праці, де розглядаються різні аспекти управління, розвитку і функціонування сектору безпеки та оборони, а також на ті, що фокусуються на окремих аспектах правового регулювання, зокрема стосовно адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. У глобальному масштабі ці дослідження можна поділити на вітчизняні та іноземні, що стосуються адміністративно-правових аспектів адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Цей поділ залежить від історичних умов, загроз національній безпеці, форми державного управління та адміністративно-територіального устрою конкретних країн.

Огляд теоретичних праць адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки потрібно розглядати насамперед через аналіз досліджень тих учених, що приділяли увагу питанням забезпечення національної безпеки України. І це не випадково, адже питання

забезпечення національної безпеки України є одним із найбільш важливих для нашої держави через низку соціальних, економічних та політичних викликів. Водночас, це питання залишалося актуальним для України з моменту здобуття незалежності в 1991 році, що сприяло постійному інтересу науковців-юристів до тематики національної безпеки. Вона неодноразово ставала предметом досліджень у дисертаціях, монографіях, наукових статтях і доповідях, охоплюючи різні галузі та сфери суспільних наук.

Так, О. Феденко (2002 р.) у своїй праці висвітлив військово-політичні аспекти становлення та розвитку системи національної безпеки [161]. Г. Пономаренко (2007 р.) у монографії «Управління у сфері забезпечення внутрішньої безпеки держави: адміністративно-правові засади» дослідила актуальні питання управління внутрішньою безпекою держави та висвітлила особливості адміністративної діяльності відповідних органів влади [108]. Стратегічне планування національною безпекою було предметом дисертаційного дослідження А. Семенченко (2008 р.) [143].

У наукових розвідках, присвячених національній безпеці України, суттєву роль відіграли праці таких учених як: В. А. Ліпкан, З. В. Чуйко та В. Ю. Кобринський, які здійснили вагомий внесок у розвиток адміністративно-правових та конституційно-правових засад забезпечення національної безпеки.

Дисертаційна праця В. А. Ліпкана (2008 р.) стала вагомим кроком у становленні наукових підходів до формування адміністративно-правових засад забезпечення національної безпеки України. У межах свого дослідження автор уперше системно виокремив та обґрунтував адміністративно-правові закономірності формування системи національної безпеки, зокрема: 1) вторинний характер адміністративних правовідносин, що виникають на основі формування окремих сфер національної безпеки; 2) взаємозв'язок об'єктів адміністративних правовідносин з об'єктами національної безпеки як такими, що взаємно зумовлюють один одного; 3) кореляція між суб'єктами адміністративних правовідносин і суб'єктами національної безпеки, що

свідчить про органічну єдність їх функціонування; 4) наявність як вертикальних, так і горизонтальних взаємозв'язків між суб'єктами адміністративно-правових відносин у сфері безпеки; 5) автономний розвиток системи забезпечення національної безпеки в межах адміністративно-правового регулювання, що відрізняється від класичних державно-управлінських механізмів.

Важливим аспектом стало формулювання основних напрямів удосконалення адміністративно-правового регулювання національної безпеки, серед яких: створення нової Концепції національної безпеки, розробка на її основі відповідних доктрин і законодавчих актів, гармонізація законодавства з європейськими нормами та вдосконалення правової бази суб'єктів національної безпеки [77].

Значний внесок у вивчення конституційних засад національної безпеки здійснила З. В. Чуйко. Метою її дослідження було обґрунтування конституційно-правових основ національної безпеки та аналіз нормативно-правової бази України й іноземних країн. Учена відзначила, що механізм забезпечення національної безпеки має складну правову природу, яка включає конституційні норми, поточне законодавство та сукупність дій органів державної влади й громадських структур, спрямованих на захист національних інтересів. Одним із ключових висновків З. В. Чуйко є те, що оптимізація цього механізму вимагає не лише законодавчих змін, але й підвищення ролі громадянського суспільства, а також підвищення професіоналізму й правової культури державних службовців [169].

Зі свого боку, В. Ю. Кобринський зосередив увагу на проблемі державного контролю у сфері національної безпеки. Він підкреслив відсутність єдиного законодавчого акту, що систематизував би основи контрольної політики в цій сфері. Система забезпечення національної безпеки включає численні суб'єкти, кожен з яких керується власними нормативними актами, що ускладнює координацію і контроль. Основні тенденції розвитку державного контролю, запропоновані дослідником, включають: підвищення

ефективності контролю, централізація контролюючих органів, своєчасне виявлення порушень та професіоналізація цієї сфери. Крім того, В. Ю. Кобринський розробив Концепцію державного контролю у сфері національної безпеки, яка має стати основою для подальшого реформування цієї важливої функції державного управління [56].

У монографії «Система і компетенція державних органів зі спеціальним статусом у сфері національної безпеки України», виданій того ж року, авторський колектив у складі В. Пилипчука, О. Дзьобаня та В. Настюк здійснив глибокий аналіз чинних правових актів та документів у сфері національної безпеки. Учені висвітлили категоріальний апарат, що використовується в безпековій та оборонній сферах, а також дослідили систему державних органів, залучених до забезпечення безпеки та оборони України. Особливої уваги заслуговує їхній аналіз правових актів НАТО та країн Європейського Союзу, що стосуються сектору безпеки та оборони. Окрім того, автори надали рекомендації щодо вдосконалення правової науки в галузі безпеки, що може бути корисним для досліджень у рамках адміністративного права [104].

Таким чином, ці наукові праці є вагомим внеском у розвиток теорії та практики забезпечення національної безпеки України, а також у вдосконалення правової та організаційної бази державної безпеки, враховуючи сучасні виклики та загрози, що мали місце під час проведення зазначених досліджень.

У 2010 році І. В. Кременовська успішно захистила дисертаційну роботу на тему: «Правові та організаційні засади діяльності суб’єктів виконавчої влади у сфері забезпечення національної безпеки України» [70]. У своєму дослідженні авторка зосередила увагу на тому, що як теоретичне осмислення, так і нормативне регулювання діяльності суб’єктів виконавчої влади у сфері гарантування національної безпеки України залишаються недостатньо розробленими. Зокрема, у вітчизняній та іноземній адміністративно-правовій науці ці питання розглядаються фрагментарно і не піддаються комплексному

підходу. Правові й організаційні механізми функціонування органів виконавчої влади як учасників системи забезпечення національної безпеки залишаються малодослідженими. Крім того, І. В. Кременовська наголосила на відсутності цілісної концепції побудови системи таких органів у межах української адміністративно-правової доктрини. На думку І. В. Кременовської, для підвищення ефективності забезпечення національної безпеки потрібно більше уваги приділяти людському аспекту, оскільки це сприятиме захисту життєво важливих інтересів не тільки окремих громадян, але й суспільства та держави загалом [70].

Значний внесок у дослідження управління у сфері національної безпеки зробив Г. Ситник. У 2012 році вийшла його монографія під назвою «Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади)», в якій автор детально розглянув категоріальний апарат сектору безпеки і оборони, а також визначив роль, місце, суб'єкти та об'єкти державного управління в галузі національної безпеки [146]. У роботі акцентовано увагу на функціях і завданнях державного управління, що стосуються забезпечення національної безпеки України, включаючи організаційно-правові та інституційні основи розробки безпекової політики.

Одним із важливих аспектів монографії є дослідження правової основи діяльності суб'єктів державної політики у сфері національної безпеки, а також їх компетенції. Особливу увагу учений приділяє питанням демократичного цивільного контролю за сектором безпеки та оборони, хоча визнає, що аналізується застаріла законодавча база. Незважаючи на це, дослідник пропонує цінні теоретичні підходи до визначення предмета і принципів цивільного контролю, зокрема, використовуючи досвід країн Європейського Союзу [145; 146].

О. О. Бригінець у своїй науковій праці розглянув правові аспекти забезпечення фінансової безпеки України. Науковець слушно зауважив, що, незважаючи на постійні зусилля щодо внесення змін до законодавчих актів, стан правового регулювання фінансової безпеки залишається недосконалим,

що негативно впливає на економічну незалежність країни та залучення інвестицій. На думку вченого, зволікання з впровадженням реформ, рекомендованих Європейським Союзом, у сферах державного управління, судової системи та правоохоронної діяльності також негативно впливає на фінансову безпеку. О. О. Бригінець розробив проєкт Закону України «Про основи фінансової безпеки України», який покликаний забезпечити комплексне правове підґрунтя для формування цієї сфери. У цьому законопроєкті виділено основні положення, що визначають терміни, правовий статус суб'єктів фінансової безпеки, національні інтереси та принципи забезпечення фінансової безпеки держави [12].

У 2016 році була опублікована наукова праця О. С. Власюка під назвою «Національна безпека України: еволюція проблем внутрішньої політики», в якій особливу увагу приділено питанням трансформації сектору безпеки, зокрема в розділі 8. У цьому контексті автор здійснив ґрунтовний аналіз реалізації положень Державної програми реформування та розвитку Збройних сил України, а також запропонував конкретні напрями оптимізації державного контролю за процесами планування та фінансування діяльності сектору безпеки й оборони. Окремо досліджуються питання запровадження ефективного механізму цивільного нагляду над діяльністю спеціальних служб України та іншими ключовими суб'єктами сектору безпеки [18].

Того ж року вийшов навчальний посібник «Соціально-економічна безпека», де колектив авторів звертає увагу на аспекти економічної безпеки на загальнодержавному рівні. У першому розділі розглядаються законодавчі та підзаконні акти, що стосуються сектору безпеки та оборони України, у контексті генези економічної та національної безпеки [150].

У 2017 році була опублікована фундаментальна монографія «Сектор безпеки і оборони України: теорія, стратегія, практика». У першому розділі цього дослідження розкриваються ключові поняття, такі як «сектор безпеки» та «сектор безпеки і оборони держави», що в літературі можуть розглядатися як різні категорії. Автори також наводять правові ознаки цього сектору,

зокрема його об'єкти, суб'єкти (складові елементи), межі та суб'єктивні ознаки [142, с. 12–19]. Крім того, у 2017 році А. Б. Качинський видав монографію «Індикатори національної безпеки: визначення та застосування їх граничних значень», у якій дослідив теоретичні аспекти національної безпеки та навів нормативно-правові акти, що стосуються управління сектором безпеки і оборони [52].

В. О. Антонов у своїй монографічній роботі 2017 року досліджував конституційно-правові та методологічні основи національної безпеки України [6]. Автор проаналізував національну безпеку як конституційно-правову категорію, підкресливши, що розвиток цієї сфери відображає певні етапи розвитку суспільства і державності України. Учений приділив особливу увагу конституційно-правовому аспекту системи національної безпеки, її сутності, змісту та структурі. Він запропонував конституційно-правове визначення поняття «система національної безпеки» – це сукупність елементів, що забезпечують захист життєво важливих інтересів людини, суспільства та держави від зовнішніх і внутрішніх загроз [6].

Серед дисертаційних досліджень, що зосереджуються на адміністративно-правових аспектах регулювання та управління сектором безпеки і оборони України, варто особливо виділити докторську дисертацію В. В. Сокуренка «Публічне адміністрування сферою оборони в Україні», захищену у 2016 році, в якій автор основну увагу приділяє військовій та оборонній складовій, аналізуючи законодавчу базу, яка регулює публічне адміністрування у сфері оборони. Адміністративно-правового регулювання в цій сфері дослідник потлумачив як «цілеспрямований і впорядковувальний вплив на відносини, що виникають у сфері оборони, здійснюваний публічною адміністрацією через застосування правових засобів, таких як юридичні норми, правовідносини, індивідуальні приписи тощо, і пов'язаний із встановленням конкретних прав та обов'язків суб'єктів відповідних відносин» [148].

У 2018 році Т. Ю. Ткачук присвятив своє дослідження інформаційній безпеці, що є важливою складовою національної безпеки. Автор зазначав, що забезпечення інформаційної безпеки є пріоритетом державної політики, оскільки воно впливає на саме існування держави, її соціально-економічний розвиток та міжнародний статус. Основними цілями державної політики в цій сфері, на думку науковця, є захист інформаційного суверенітету, забезпечення доступності інформації для прийняття рішень та реалізація прав і свобод громадян на інформацію. Крім того, учений окреслив перспективні напрями подальших наукових досліджень, включаючи оцінку загроз інформаційній безпеці, управління ризиками, розвиток інформаційного суспільства та правові аспекти функціонування штучного інтелекту [158].

Т. С. Перун звернув увагу на проблеми інформаційної безпеки, присвятивши своє дослідження адміністративно-правовому механізму її забезпечення. Він акцентував на новизні свого дослідження в контексті сучасних умов інформаційної війни, яку веде росія проти України, а також розвитку інформаційного суспільства в умовах євроінтеграції. Автор здійснив аналіз доктрин країн ЄС і практики Європейського суду з прав людини, запропонувавши низку змін до чинного законодавства, зокрема до Законів «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державне-приватне партнерство» та інших нормативно-правових актів [103].

Серед важливих наукових джерел, що суттєво вплинули на формування адміністративно-правових підходів до функціонування сектору безпеки і оборони України, варто окремо згадати дисертаційне дослідження С. П. Пономарьової «Адміністративно-правове забезпечення діяльності сектору безпеки і оборони України» (2018 р.) [109], яке стало ґрунтовним внеском у розробку теоретико-правових основ цієї сфери. Т. Стукалін у своїх наукових працях порушує фундаментальні питання функціонування системи державного управління в оборонній сфері [156], акцентуючи на необхідності комплексного підходу до її модернізації. В. Столбовий (2019 р.) здійснив значущий аналіз нормативно-правового регулювання службових

правовідносин у контексті забезпечення національної безпеки, що є важливим елементом правового механізму функціонування відповідної сфери [151]. О. Шевчук розглядає сектор безпеки і оборони як цілісний об'єкт публічного адміністрування. Дослідник підкреслює актуальність розробки нових законодавчих ініціатив, спрямованих на врегулювання відносин у сфері публічного управління сектором безпеки і оборони, з урахуванням взаємозв'язку з розвитком державної, економічної, воєнної та інших складових національної безпеки [170, с. 138]. Н. Цибульник у своїй публікації зазначає, що сучасний стан сектору безпеки і оборони України характеризується наявністю широкого спектра проблем у сфері управління та адміністративно-правового забезпечення, що вимагає негайного наукового осмислення й практичного вдосконалення [155, с. 33].

Дисертаційне дослідження А. В. Рубана «Державне управління у сфері національної безпеки України» (2019) заслуговує на особливу увагу, оскільки воно базується на актуальній нормативно-правовій базі, що регулює управління сектором безпеки і оборони України. Хоча дисертація була захищена за спеціальністю «державне управління у сфері державної безпеки та охорони громадського порядку», автор розглядає також важливі питання управління сектором безпеки з адміністративно-правової точки зору. У своєму дослідженні він узагальнює досвід іноземних країн у цій сфері та окреслює низку проблем, серед яких: недостатній розвиток національного сектору безпеки й оборони, слабка інституційна база, відсутність професійного кадрового корпусу, структурна незбалансованість державних органів, недостатність ресурсів та неефективне їх використання, а також неефективність міжнародних гарантій безпеки для України [141].

І. В. Каріх здійснив ґрунтовне дослідження інституційних та правових засад формування й реалізації державної політики у сфері національної безпеки України в сучасних умовах. Ключовою метою його дисертаційного дослідження було визначення ступеня впливу чинних політико-правових механізмів на стан безпеки в гуманітарному вимірі, а також напрацювання

пропозицій щодо вдосконалення нормативно-правової та інституційної основ відповідної державної політики. Підкреслено, що політика національної безпеки в гуманітарній сфері є одним із пріоритетних напрямів діяльності як державних органів, так і громадянського суспільства. Вона спирається на чіткі концептуальні підвалини, законодавчу базу та відповідні інституційні механізми реалізації. Форми цієї політики формувалися впродовж тривалого історичного періоду, відображаючи як загальноцивілізаційні тенденції розвитку гуманітарного простору, так і особливості національного державотворення [51].

У свою чергу, А. М. Мурашко у 2021 році також присвятила своє наукове дослідження проблематиці формування та реалізації державної політики у сфері національної безпеки, акцентуючи на сучасних викликах та необхідності комплексного підходу до зміцнення національної безпеки в умовах трансформаційних процесів [88].

Учена обґрунтувала теоретичний підхід до формування української стратегії національної безпеки, систематизувала її компоненти в контексті інтеграції політичних і правових норм, інститутів, процедур та дій, спрямованих на забезпечення національної безпеки. Дослідниця також акцентувала увагу на нейтралізації недоліків цієї політики та запропонувала вдосконалення понятійно-категоріального апарату дослідження [88].

Після 2022 року було написано низку монографічних праць, в яких досліджувалися проблеми забезпечення національної безпеки в умовах військової агресії, зокрема це роботи: М. П. Стрюк (2022 р.) на тему: «Формування системи управління сектором безпеки і оборони України: адміністративно-правовий аспект» [155]; Є. В. Кобко (2023 р.) «Адміністративно-правовий механізм забезпечення національної безпеки держави» [54]; І. В. Наконечна (2023 р.) «Адміністративно-правовий механізм забезпечення національної безпеки в умовах євроінтеграції: питання теорії і практики» [90].

Дисертаційні дослідження в галузі юриспруденції, військових та інших соціальних наук відіграють ключову роль у формуванні та розвитку національної безпеки України. Вони є важливим джерелом наукового знання щодо адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та надають рекомендації для практичного вдосконалення державної політики в цій сфері, що має велике значення в умовах сучасних глобальних і регіональних викликів.

Одним із важливих аспектів цих досліджень є теоретичне та практичне обґрунтування правових механізмів забезпечення національної безпеки. Учені-юристи проводять глибокий аналіз чинного законодавства та виявляють його недоліки, що дозволяє розробляти пропозиції для вдосконалення нормативно-правової бази України. Ці дослідження мають значення не лише для розвитку теорії національної безпеки, а й для створення конкретних рекомендацій для відповідних суб'єктів щодо покращення адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Крім того, такі наукові праці сприяють розвитку нового понятійного апарату та вдосконаленню юридичної термінології, що використовується у сфері функціонування OSINT та національної безпеки. Це є важливим елементом уніфікації нормативних актів, а також їхнього тлумачення у контексті правозастосування.

Наприклад, у роботі, присвяченій інформаційній безпеці, Т. Ю. Ткачук [158] аналізує виклики, що виникають у зв'язку з глобалізацією інформаційного простору та його впливом на національну безпеку та функціонування OSINT. Це дозволяє формулювати стратегії протидії загрозам інформаційної війни, що стає дедалі актуальнішим в умовах сучасних гібридних конфліктів та війни в Україні.

Наукові розвідки на рівні дисертацій також сприяють розвитку інституційної спроможності держави, допомагають удосконалювати інституційний механізм адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, пропонуючи

рекомендації щодо покращення координації між різними органами влади, що відповідають за захист держави.

Таким чином, дисертаційні дослідження проблем національної безпеки є важливим підґрунтям дослідження адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Вивчення проблем національної безпеки дає автору дисертації фундаментальні знання про загальну концепцію національної безпеки, її принципи, механізми і структуру. Це важливо для розуміння того, як OSINT (відкриті джерела інформації) інтегрується у ширший контекст безпеки держави. Дослідження національної безпеки також дозволяють виявити можливі загрози та виклики, на які OSINT може ефективно реагувати. Дослідження проблем національної безпеки, зокрема в адміністративно-правовій сфері, допомагають визначити, які саме правові механізми та інституційні структури необхідні для регулювання OSINT у контексті національної безпеки. Адміністративно-правове забезпечення включає визначення правового статусу суб'єктів, що здійснюють OSINT, їхніх повноважень, обов'язків, а також законодавчі норми, які регулюють їх діяльність.

Отже, дослідження проблем національної безпеки забезпечують теоретичне та практичне підґрунтя для створення ефективної адміністративно-правової бази функціонування OSINT. Вони дозволяють врахувати сучасні виклики, які стоять перед державою, та виробити механізми правового регулювання, що гарантують ефективне використання відкритих джерел інформації у сфері безпеки України.

Водночас важливим є й те, що на рівні монографічних досліджень використання OSINT досліджувалося В. Д. Щербанем, який у 2020 році захистив дисертацію на тему: «Концепція адміністративно-правового забезпечення функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах України». Дисертацію присвячено комплексному та ґрунтовному аналізу проблематики концептуальних основ адміністративно-правового забезпечення функціонування OSINT у сфері антикорупційної

діяльності в правоохоронних органах України. У роботі з'ясовано специфіку інформаційно-правового забезпечення протидії корупції в правоохоронних органах, а також здійснено ретроспективний аналіз цього правового явища. Досліджено роль адміністративно-правового забезпечення функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах у сучасних умовах. Ученим запропоновано повну класифікацію ключових проблем адміністративно-правового забезпечення функціонування OSINT у сфері антикорупційної діяльності, зокрема: 1) відсутність в Україні спеціального законодавства, яке урегульовує здійснення розвідки з відкритих джерел; 2) відсутність дефініції OSINT у законодавстві, внаслідок чого сутність розвідки з відкритих джерел та її значення для антикорупційної діяльності залишаються невстановленими для широкого загалу; 3) функціонування OSINT у діяльності суб'єктів антикорупційної діяльності не урегульоване у спеціальному порядку. Здобутком праці є з'ясування тенденцій функціонування OSINT у сфері антикорупційної діяльності, які або здійснюють безпосередній вплив на адміністративно-правове забезпечення функціонування OSINT у сфері антикорупційної діяльності, або ж обумовлюють необхідність в адміністративно-правовому регулюванні: 1) набуває популярності метод збирання розвідувальної інформації з комп'ютерних соціальних мереж, як різновид OSINT; 2) поява різноманітних відкритих державних інформаційних баз в Україні; 3) співпраця правоохоронних органів України з громадськими організаціями та журналістами, які проводять незалежні розслідування та оперують широким спектром інформаційних ресурсів [176].

Водночас Хоча вказана праця безумовно слугує основою нашого дослідження, питання адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки залишилися у ній поза увагою.

Незважаючи на майже відсутність комплексних монографічних досліджень адміністративно-правового забезпечення функціонування OSINT

у сфері національної безпеки, його використання висвітлюється у наукових статтях, серед яких варто виділити наступні праці:

– В. Ю. Калугін «Основні методи OSINT, шо використовуються у кримінальному аналізі» (2023 р.) [50]. Ця наукова стаття присвячена використанню OSINT у кримінальному аналізі. У ній розглядаються переваги та обмеження використання цього методу під час розслідування злочинів. Серед переваг OSINT відзначено можливість доступу до інформації, яка не завжди є доступною через традиційні методи, швидкість отримання даних, а також збір інформації з різноманітних джерел, що дозволяє скласти повнішу картину злочину. Водночас окреслено обмеження, як-от ненадійність деяких даних, трудомісткість процесу, вимоги до високих навичок аналітиків, а також юридичні обмеження, пов’язані із захистом персональних даних. Стаття також підкреслює важливість гнучкості та адаптації OSINT-фахівців до швидко змінюваного інформаційного середовища. Це особливо актуально у кримінальних розслідуваннях, де нові джерела даних та інформаційні технології постійно з’являються і розвиваються. Важливо, щоб аналітики були в курсі нових інструментів і методів збору інформації, таких як аналіз «темних куточків» інтернету або застосування штучного інтелекту для обробки великих обсягів даних. Особливу увагу приділено питанню безпеки самих OSINT-аналітиків. В умовах сучасних конфліктів, таких як ситуація в Україні, фахівці з розвідки за відкритими джерелами стають пріоритетними цілями для противника. Вони піддаються кіберзагрозам, можливості стеження та навіть фізичній загрозі, що вимагає від них бути надзвичайно уважними до інформаційної гігієни та безпеки.

Відповідні дослідження використання OSINT у галузі кримінального права здійснили В. В. Білоус у праці «OPEN DATA І OSINT як актуальні категорії інформаційного забезпечення розслідування злочинів» [11] та інші вчені [48; 53; 57];

– Т. С. Яровий «OSINT, як перспективний інструмент контролю за лобістською діяльністю у контексті державної безпеки». Ця наукова стаття

присвячена дослідженню механізмів отримання розвідувальної інформації з відкритих джерел (OSINT) як перспективного інструменту для контролю лобістської діяльності в контексті державної безпеки. Автор аналізує як українські, так і міжнародні підходи до розуміння процесу збору інформації з відкритих джерел та пропонує власне визначення OSINT. Зосереджено увагу на класифікації джерел, які можуть бути використані в OSINT. У дослідженні окреслено переваги використання OSINT для наглядової діяльності Національної ради України з питань регулювання лобізму (НРУРЛ). Серед них: економія часу та ресурсів завдяки збору інформації з відкритих джерел; можливість надання аналітичної інформації керівництву країни щодо потенційно небезпечної діяльності лобістів; можливість публічного викриття порушень суб'єктів лобіювання, що може допомогти відбивати інформаційні атаки та запобігати звинуваченням у недемократичних діях НРУРЛ [178];

– А. В. Серватовський, Ю. М. Онищенко, П. В. Макаренко: «Міжнародний досвід використання OSINT» та О. О. Кожушко: «Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США» висвітлили досвід США, Великобританії та Ізраїлю у використанні OSINT [57; 144];

– А. Л. Главацька, О. В. Ангельська, І. Р. Опірський «Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет-просторі» [26].

Проблемні питання використання OSINT на рівні наукових статей досліджувалися також Т. П. Пащенко [102], О. В. Мінько [85], Н. В. Ржевською [140], І. В. Панченко [100] та ін.

Таким чином, можемо констатувати, що за останні роки з'явилося чимало наукових праць, в яких висвітлюються проблемні аспекти, пов'язані із забезпеченням національної безпеки України, зокрема за допомогою OSINT-фахівцями з різних галузей права – конституційного, кримінального та інформаційного, а також інших наукових галузей, таких як теорія управління, економіка тощо. Важливо відзначити, що науковці зробили суттєвий внесок у

розвиток цього інституту, однак залишається чимало питань, які ще потребують дослідження, зокрема в аспекті адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Серед перспективних напрямів для наукових досліджень можна виокремити: аналіз правових основ забезпечення національної безпеки за допомогою OSINT та визначення ролі адміністративного права в цій сфері; встановлення рівнів, напрямів та меж адміністративно-правового забезпечення національної безпеки, з використанням OSINT; дослідження адміністративно-правових форм і методів забезпечення безпеки, з використанням OSINT; узагальнення міжнародного досвіду; удосконалення адміністративного законодавства, що регулює цю сферу.

Адміністративне право відіграє ключову роль у створенні нормативної бази та визначенні чітких меж і механізмів функціонування OSINT у сфері національної безпеки. Це передбачає розробку правових основ для збору, аналізу та використання відкритих джерел інформації, з дотриманням законності та прав людини. З огляду на стрімкий розвиток інформаційних технологій, ефективне використання OSINT стає важливою складовою сучасної розвідки. Використання даних з відкритих джерел – інтернету, соціальних мереж, публічних баз даних – потребує врегулювання на адміністративно-правовому рівні для забезпечення прозорості та законності. Необхідно поглибити дослідження правових основ національної безпеки через OSINT, зокрема щодо визначення ролі адміністративного права. Перспективними напрямами є розробка нових форм та методів адміністративно-правового регулювання у цій сфері. Безумовно, для вирішення цих завдань потрібні спеціальні комплексні дослідження у галузі адміністративного права.

Зазначене обумовлює гостроту наукового дослідження адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Безумовно, хоча науковий інтерес до питання OSINT зростає, існує брак комплексних досліджень, присвячених саме адміністративно-правовому

забезпеченню функціонування цієї системи у сфері національної безпеки. Сучасна державна безпека значною мірою залежить від розвідки, і OSINT стає дедалі важливішим джерелом інформації завдяки швидкому розвитку інформаційних технологій та доступу до відкритих джерел, таких як інтернет, соціальні мережі, новинні ресурси, публічні бази даних тощо. Для забезпечення ефективного функціонування системи національної безпеки необхідно вивчити організаційно-правові основи, які забезпечать належне правове регулювання збору, аналізу та використання відповідних даних, а також запропонувати шляхи удосконалення діяльності уповноважених суб'єктів.

Відповідно, адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки потребує подальших комплексних досліджень фахівцями з адміністративного права. Це дозволить створити цілісну нормативно-правову базу для ефективного використання відкритих джерел інформації в умовах зростаючих викликів і загроз.

1.2 Національна безпека як об'єкт адміністративно-правового забезпечення: поняття та зміст

Національна безпека є однією з ключових категорій сучасної державної політики, безпосередньо пов'язаною з існуванням держави, її територіальною цілісністю, суверенітетом, політичною стабільністю, економічним розвитком, соціальним добробутом та правами громадян. В умовах війни в Україні та глобальних викликів, таких як тероризм, кіберзагрози, екологічні катастрофи та інформаційна війна, питання забезпечення національної безпеки набуває особливого значення. Відповідно до цього виникає необхідність не лише чіткого розуміння концепту національної безпеки, але й розробки ефективних механізмів адміністративно-правового забезпечення за допомогою функціонування OSINT у сфері національної безпеки.

Поняття національної безпеки, попри його широке використання в науковій та правовій практиці, залишається предметом активних наукових дискусій. Це обумовлено різноманітними тлумаченнями національної безпеки, а також підмін понять окремими дослідниками терміну «національна безпека» з іншими суміжними категоріями. У своїх дослідженнях учені-юристи намагаються визначити сутність поняття «національна безпека» та «державна безпека», вивчити складові елементи національної безпеки. Важливим є розуміння того, що національна безпека є ширшою категорією, яка включає не тільки захист державних інтересів, але й захист суспільних цінностей та прав громадян. Таке розширене розуміння дозволяє розглядати національну безпеку як комплексне явище, яке охоплює економічні, політичні, соціальні та екологічні аспекти життя суспільства і держави.

Національна безпека – це комплексна категорія, що включає в себе систему заходів, спрямованих на забезпечення безпеки держави в усіх сферах її існування: політичній, економічній, соціальній, екологічній, інформаційній тощо. З юридичної точки зору, національна безпека є як складовою відповідної державної політики, так і об’єктом адміністративно-правового забезпечення.

В. В. Макарчук зазначає, що термін «національна безпека» застосовується в різних контекстах і досі не має однозначного тлумачення в правовій літературі, законодавчій та юридичній практиці. Українські вчені-адміністративісти визначають безпеку країни переважно крізь призму виконавчої діяльності правоохоронних органів, які забезпечують її реалізацію [81, с. 5–8].

Феномен «національної безпеки» набув значної уваги в науково-юридичному середовищі із моменту здобуття Україною незалежності, що стало відправною точкою для всебічного дослідження цієї категорії. Актуальність цієї тематики помітно зросла в умовах військової агресії проти України, що стимулює перегляд підходів до національної безпеки та її правового забезпечення. Науковці досліджують це поняття крізь призму його

становлення та розвитку в різні історичні епохи, а також трансформацій у системі права.

Безпека як універсальна категорія супроводжувала розвиток людської цивілізації від найдавніших часів, коли людина стикалася з загрозами своєму життю, здоров'ю та інтересам. Усвідомлення необхідності попередження та мінімізації загроз породило правові й організаційні заходи, спрямовані на збереження цінностей та стабільності. Ці заходи стали передумовою для утворення соціальних об'єднань, які з часом еволюціонували у суспільні та державні інститути. Такий процес забезпечив основу для виникнення й розвитку механізмів правового регулювання, що сприяють захисту прав та інтересів особи, громади й держави.

Однією з ключових характеристик безпеки як правової категорії є її всеохопність та інтегрованість у всі сфери суспільних відносин, що підкреслює її значення для правотворчості та регуляторної діяльності. Безпека органічно пов'язана з життєдіяльністю суспільства, а оцінка стану безпеки різних соціальних об'єктів (особи, соціальних груп та держави) стає основою для розробки й реалізації ефективних правових механізмів. Враховуючи ці аспекти, погоджуємося з науковцями, які вважають, що правове забезпечення безпеки виникло одночасно з утворенням перших суспільних і державних інститутів. Відтоді забезпечення безпеки стало ключовим напрямом діяльності як держави, так і суспільства загалом.

Отже, правова природа безпеки розкриває її інституційну роль у розвитку держави та суспільства, оскільки саме на основі юридично оформлених норм і механізмів можливе ефективне забезпечення стабільності, порядку та захисту фундаментальних прав і свобод.

Потреба у безпеці є фундаментальною складовою існування людини та відіграє ключову роль у її взаємодії з природою, суспільством і державою. Із розвитком суспільних відносин значення безпеки невпинно зростало, що зумовило її поступове перетворення на пріоритетний обов'язок як окремих індивідів, так і суспільних та державних інститутів. Аналіз історичних

правових і соціальних практик дозволяє сформувати дієві механізми забезпечення безпеки та сприяє розширенню правового розуміння цього явища як комплексної соціально-правової категорії, що охоплює всі аспекти життєдіяльності людини. При цьому центральним об’єктом правового захисту в межах безпеки залишається особа та її права, свободи й інтереси, що мають бути гарантовані як на національному, так і на міжнародному рівнях.

Сучасні наукові дослідження свідчать про тенденцію до уніфікації поняття «безпека». У більшості юридичної літератури поняття «національна безпека» розглядається не лише як фактична відсутність загроз, а передусім як стан забезпеченої, гарантованої захищеності ключових життєвих інтересів особи, суспільства та держави від впливу зовнішніх і внутрішніх чинників небезпеки. При цьому підкреслюється багатовимірний характер таких загроз, серед яких виокремлюють політичні, економічні, соціальні, воєнні, екологічні, інформаційні та інші прояви.

Це розуміння включає необхідність забезпечення політичної, економічної та соціальної стабільності в державі, неухильного дотримання законодавства й підтримання правопорядку, а також розвитку міжнародного співробітництва на засадах партнерства та взаємної довіри.

Хоча інтерпретації поняття безпеки змінюються відповідно до історичного контексту, його політична сутність зберігає сталу орієнтацію на досягнення стану захищеності й стабільності у взаєминах між державою, суспільством та людиною. Ця концепція охоплює не лише короткострокові заходи реагування на загрози, а й довгострокові стратегічні цілі, спрямовані на забезпечення розвитку та збереження стабільності правової системи та соціального порядку.

У концентрованому вигляді концепція безпеки представляє собою сукупність офіційно затверджених державою та суспільством принципових положень щодо державних інтересів і цінностей суспільства, а також щодо засобів і механізмів їх захисту від потенційних та реальних загроз. Відтак, ефективність державної політики значною мірою залежить не лише від чіткого

юридичного визначення та соціальної легітимації національних цінностей, інтересів і стратегічних цілей, але й від належного усвідомлення правових шляхів, засобів, методів та інструментів їх реалізації в межах державного управління системою національної безпеки [93, с. 35].

В. А. Ліпкан акцентує увагу на багатогранній природі феномена «безпеки», трактуючи його як фундаментальну характеристику, що визначає стан захищеності держави та її здатність адаптивно реагувати на динаміку внутрішніх і зовнішніх умов функціонування. Безпека у цьому контексті, на думку вченого, передбачає системний комплекс конституційних, нормативно-правових та організаційно-практичних заходів, спрямованих на забезпечення захисту життєво важливих інтересів об'єкта від потенційних загроз та ризиків, незалежно від їхньої природи та джерела походження. Ключові характеристики безпеки, згідно з В. А. Ліпканом, включають такі положення: стан об'єкта (безпека відображає поточний стан захищеності, що забезпечує стабільність і збереження функціонування об'єкта); здатність до стійкості та самозбереження (безпека передбачає здатність системи або явища зберігати свою сутність та цілісність в умовах цілеспрямованого руйнівного впливу як зовнішнього, так і внутрішнього. Ця характеристика прирівнює безпеку до гомеостатичної рівноваги); системна властивість (безпека як властивість системи базується на принципах структурної стійкості, самоорганізації та цілісності. Порушення хоча б одного з цих принципів може спричинити дисфункцію чи повний колапс системи); гарантія життєдіяльності: безпека виступає необхідною умовою для функціонування особи, суспільства та держави, забезпечуючи збереження і примноження духовних та матеріальних цінностей. Отже, безпека характеризується не лише як відсутність загроз, а й як постійна готовність системи до управління ризиками та адаптації до мінливих обставин. З огляду на це, – робить висновок В. А. Ліпкан, – вона має перманентний характер і вимагає безперервного моніторингу та управлінських рішень [78, с. 57–61].

Прийнятною є позиція В. Баліцького, який вважає, що у процесі аналізу й дослідження проблем державної, національної та зовнішньополітичної безпеки України, зокрема в контексті її зовнішньої діяльності, вихідною категорією має бути саме поняття «небезпека». На думку дослідника, доцільно надавати цьому терміну таке визначення: небезпека – це об'єктивно наявна ймовірність негативного впливу на соціальний організм, його функціонування та організаційні структури (служби), що може спричинити ушкодження або завдати шкоди, унаслідок чого відбувається погіршення загального стану, а також виникає небажана динаміка чи зміна параметрів його розвитку (характер, темпи, форми тощо) [68, с. 15]. Далі учений уточнює, що небезпека полягає саме в об'єктивній можливості такого впливу, який може негативно відобразитися на стабільності та ефективності функціонування соціального організму, включаючи його інституції та управлінські структури. Такий підхід дозволяє логічно обґрунтувати необхідність активної участі органів Служби безпеки України та розвідувальних структур у контррозвідувальному забезпеченні зовнішньополітичної діяльності держави за кордоном, оскільки рівень їхньої залученості прямо залежить від реальних і потенційних зовнішніх небезпек, ризиків і загроз [8].

На наш погляд, знання про навколишнє середовище, тенденції розвитку суспільства, держави й людства, а також про стан функціонування соціальної системи дають змогу глибше розуміти рівень «безпеки» та характер загроз, що її підривають. Це сприяє своєчасному виявленню потенційних небезпек і дозволяє ефективно їх мінімізувати або усувати.

Т. В. Тихий зазначає, що поняття «безпека» фіксує домінантний спосіб існування об'єкта як стан, за якого він не піддається небезпеці. Визначення безпеки ґрунтується на співвіднесенні предмета з можливими загрозами, що дозволяє класифікувати його стан як безпечний або небезпечний. При цьому основна увага приділяється саме відношенню об'єкта до небезпеки, не враховуючи його властивостей в інших контекстах. Таке розуміння дає змогу

охарактеризувати безпеку як одну із загальних та суттєвих характеристик об’єкта, що домінують у певних умовах його існування [157].

У соціальному вимірі «безпека» розглядається як збалансований стан функціонування соціальних систем різного рівня – від окремої особи до держав та міжнародної спільноти. Цей стан забезпечується завдяки здатності суб’єктів, спираючись на знання про природне й антропогенне середовище, своєчасно виявляти та мінімізувати потенційні й реальні загрози. Таким чином, забезпечення безпеки не лише сприяє збереженню соціальних і культурних цінностей, а й створює умови для їх сталого розвитку. Ключовим елементом такого підходу є превентивні дії, спрямовані на уникнення негативного впливу загроз на систему та її складові [67, с. 71].

Отже, безпека виступає не лише як характеристика стабільності системи, а й як процес взаємодії суб’єкта з оточенням, що дозволяє прогнозувати та запобігати ризикам, зберігаючи і розвиваючи внутрішні ресурси системи.

Тому адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки має виходити з розуміння чинників, характеру, ступеню, походження небезпек, що можуть виникнути та впливати на ті важливі для нормального існування та функціонування інтереси людини, суспільства та держави, тобто про джерела, які становлять загрозу національній безпеці. Це є принциповим для розуміння сутності адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

За сучасних умов динамічних змін у внутрішньому середовищі України та на міжнародній арені національна безпека потребує систематичних і ефективних зусиль держави для протидії різноманітним загрозам, зокрема через забезпечення ефективного функціонування OSINT. Мінлива безпекова обстановка, що охоплює як внутрішні, так і зовнішні фактори впливу, безпосередньо позначається на стані національної безпеки. У цьому контексті необхідно розглянути зміст поняття «національна безпека», яке виступає

об’єктом забезпечення функціонування OSINT. Національну безпеку слід трактувати як стан і умову захищеності життєво важливих інтересів особи, суспільства та держави. Це означає, що навіть за наявності загроз різного характеру держава повинна забезпечувати їх подолання, збереження життєздатності системи та створення умов для подальшого прогресивного розвитку.

Важливим аспектом дослідження проблем національної безпеки є її структура, оскільки саме вона визначає ефективність вибору правових форм, методів та організаційних заходів, спрямованих на виявлення, попередження та нейтралізацію загроз і які використовуються для забезпечення функціонування OSINT. Крім того, дослідження правових механізмів забезпечення національної безпеки повинно враховувати складність взаємодії суб’єктів безпеки на всіх рівнях, а також адаптивність системи до нових викликів і ризиків.

Поняття «національна безпека» є динамічним і змінюється залежно від наявних джерел небезпеки, а також відповідно до політичної, економічної та соціальної ситуації в державі та світі. Його сутність не є статичною, а зміст постійно трансформується з урахуванням нових викликів і загроз.

У сучасній науковій літературі поняття «національна безпека» розглядається з урахуванням багатовимірності цього феномена. Дослідники трактують її як: стан та ступінь захищеності національних цінностей, що забезпечує стабільне функціонування суспільства, держави та окремої особи; відсутність загроз або ефективне зниження їх впливу до допустимого рівня; головну умову життєдіяльності людини, суспільства і держави, яка дозволяє забезпечити їхній розвиток і захист інтересів; сукупність заходів і механізмів, що спрямовані на попередження та нейтралізацію внутрішніх і зовнішніх загроз, а також підтримання стабільності; здатність об’єкта безпеки (держава, суспільство або інший суб’єкт) зберігати свої сутнісні риси та функціональні характеристики навіть в умовах потенційних або реальних загроз; систему, що

складається з елементів, взаємодія яких побудована на принципах цілісності, стійкості, взаємодоповнюваності та саморегуляції [31; 44; 55; 73; 74; 77].

У контексті юридичних досліджень особлива увага приділяється аналізу нормативно-правових основ національної безпеки, структурі безпекових інститутів та правових механізмів взаємодії суб'єктів, які забезпечують стабільність у суспільстві. Національна безпека розглядається не тільки як політична чи соціальна категорія, але й як система правових відносин, що покликана забезпечувати баланс між правами та свободами людини і необхідністю захисту суспільного та державного порядку.

У науковій праці О. С. Власюка «Національна безпека України: еволюція проблем внутрішньої політики» національна безпека розглядається як комплексне соціально-державне явище, що в широкому розумінні виступає способом самозбереження українського народу, який досяг рівня державної організації у формі незалежної України [18]. Такий спосіб, за твердженням автора, створює умови для вільного існування, всебічного саморозвитку народу та ефективного захисту від як зовнішніх, так і внутрішніх викликів і загроз. Згідно з визначенням О. С. Власюка, національна безпека України – це система державних, правових і соціальних гарантій, які забезпечують стабільність життєдіяльності та розвитку як усього українського народу, так і кожного громадянина зокрема. Така система має за мету захист основних цінностей, законних інтересів, а також джерел духовного й матеріального прогресу від потенційних і наявних загроз незалежно від їхнього походження – внутрішнього чи зовнішнього [18, с. 25].

Г. О. Пономаренко визначає національну безпеку як стан захищеності життєво важливих інтересів людини, суспільства та держави від внутрішніх загроз [108, с. 127]. Особливу роль у забезпеченні цієї безпеки відіграють органи спеціального призначення. Їхня діяльність спрямована на попередження, виявлення та припинення злочинних або інших протиправних дій, які становлять безпосередню загрозу національним інтересам України. Задля цього ці підрозділи наділені повноваженнями використовувати

оперативно-розшукові методи та засоби [108, с. 127]. З юридичної точки зору, таке визначення акцентує увагу на значенні оперативно-службової діяльності як ключового механізму протидії внутрішнім загрозам. Важливою є правова регламентація повноважень та функцій органів СБУ, що забезпечує баланс між захистом національної безпеки та дотриманням прав і свобод громадян. Оперативно-розшукова діяльність повинна здійснюватися у межах правового поля, з дотриманням принципів законності, пропорційності та необхідності, що забезпечує легітимність втручання держави у приватне життя громадян заради захисту загальнонаціональних інтересів. Цілком прийнятним є те, що забезпечення функціонування OSINT у сфері національної безпеки відбувається за допомогою певного інституціонального механізму, суб'єктів, які здійснюють розвідку з відкритих джерел.

Інші вчені, зокрема В. І. Булавін та З. Д. Чуйко, трактують національну безпеку як сукупність ключових факторів, що забезпечують сприятливі умови для розвитку держави, її життєздатність, збереження та поступальний розвиток фундаментальних цінностей і традицій. У наведених визначеннях особлива увага приділяється гармонійним та неконфліктним відносинам між особою та державою. Однією з основних характеристик національної безпеки є здатність держави ефективно протидіяти зовнішнім і внутрішнім загрозам, приймати стратегічні рішення, що відповідають національним інтересам, а також успішно досягати поставлених національних цілей [169].

З погляду права таке визначення національної безпеки вимагає розробки та впровадження комплексної нормативно-правової бази, яка забезпечуватиме сталий розвиток держави та ефективний захист її цінностей у межах законності. Юридичне забезпечення національної безпеки передбачає не лише протидію загрозам, але й створення інституційних та правових механізмів для управління кризовими ситуаціями та реалізації національних інтересів у внутрішній і зовнішній політиці. Важливо також підкреслити необхідність підтримання правової рівноваги між захистом безпеки держави та

дотриманням прав і свобод громадян, що є запорукою легітимності державної політики у сфері безпеки.

До прикладу, укладачі аналітичного звіту на тему: «Концептуальні засади розвитку системи забезпечення національної безпеки України» виокремлюють дві базові інтерпретації терміна «національна безпека» – розширене та вузьке розуміння. Розширене тлумачення охоплює всі ключові напрями функціонування соціуму та визначає національну безпеку як: забезпечення захисту ключових життєвих інтересів індивіда, громадянського суспільства та державного утворення від загроз внутрішнього й зовнішнього походження; відсутність небезпек для базових національних цінностей і законних прав громадян, що дозволяє зберігати соціальну рівновагу та державну стійкість; комплекс передумов та чинників, які сприяють формуванню безпечного середовища для довготривалого й динамічного розвитку країни та її інституційних структур.

Вузький підхід зосереджується на окремих сферах державної діяльності та визначає національну безпеку як: комбінацію державних політик, спрямованих на захист національних інтересів, зокрема у сферах зовнішньої та воєнної політики; як стан захищеності держави, за якого відсутні загрози війни, а також гарантується збереження суверенітету, незалежності та територіальної цілісності країни [66, с. 5].

З юридичної точки зору, кожен із цих підходів формує різне бачення правових засад забезпечення національної безпеки. Широке трактування передбачає необхідність створення комплексної нормативно-правової бази, яка регулює всі сфери суспільного життя та інтегрує різні аспекти безпеки – економічний, соціальний, екологічний, інформаційний тощо. Водночас звужений підхід акцентує увагу на стратегічних напрямах державної політики, які безпосередньо стосуються оборони, зовнішньої політики та територіальної цілісності, що потребує спеціальних законодавчих актів і міжнародних угод.

Таким чином, вибір підходу до визначення національної безпеки визначає не лише пріоритети державної політики, але й рамки правового

регулювання, що забезпечує її ефективність і відповідність сучасним викликам.

На наш погляд, національна безпека передбачає підтримання стану стабільності протягом тривалого періоду, що забезпечується розумною та динамічною захищеністю від ключових загроз і небезпек. Важливим компонентом цього поняття є не лише стійкість перед реальними викликами, а й здатність держави та суспільства вчасно ідентифікувати потенційні загрози та вживати превентивні заходи для їхньої нейтралізації. Такий підхід до розуміння національної безпеки акцентує увагу на необхідності ефективних правових механізмів моніторингу та попередження загроз. Це вимагає створення гнучкої нормативно-правової бази, яка дозволяє державним інституціям своєчасно реагувати на виклики, забезпечуючи захист фундаментальних інтересів особи, суспільства та держави. Важливою є також здатність системи органів протидії цим загрозам адаптуватися до динамічних змін зовнішнього і внутрішнього середовища, що є запорукою довготривалої стабільності та правопорядку.

Водночас поняття національної безпеки є багатогранним, його дослідження потребує вивчення й норм законодавства, яке тлумачить цей термін, а також в якому містяться загрози, усунення яких мають виконувати відповідні суб’єкти.

Комплексний підхід до розуміння і визначення поняття безпеки застосовується у рамках європейських інституцій, й був чітко окреслений у підсумковому документі «Conference on Security and Cooperation in Europe» (ОБСЄ) від 1975 року [182]. У цьому документі безпека охоплює три ключові виміри: військово-політичний вимір – передбачає реформи систем оборони, поліції, розвідувальних структур та інших інститутів, відповідальних за захист державного суверенітету й територіальної цілісності; економічний та екологічний вимір – зосереджується на належному управлінні в секторі безпеки, включаючи адміністративний менеджмент та заходи щодо боротьби з корупцією, які забезпечують ефективне функціонування державних структур

у сфері безпеки; гуманітарний вимір – охоплює реформи системи правосуддя та пенітенціарної системи, а також забезпечення контролю з боку незалежних органів, що сприяє зміцненню верховенства права та дотриманню прав людини. Особливо важливим у підсумковому документі є акцент на міжвимірному підході до забезпечення безпеки, який вимагає координації та взаємодії між цими вимірами, незалежно від того, до якого сектору вони належать за своєю інституційною природою [91].

На національному рівні принципи цього комплексного підходу відображаються в програмних документах, які визначають основи національної безпеки конкретної держави. Такі документи слугують правовою базою для формування стратегії безпеки, забезпечуючи узгодженість між військово-політичними, економічними та гуманітарними аспектами безпеки. Це дає змогу інтегрувати міжнародні зобов'язання держави з внутрішніми механізмами безпеки, зберігаючи при цьому баланс між захистом національних інтересів та дотриманням прав і свобод громадян.

Вітчизняне законодавство протягом незалежності України містило спеціальні нормативно-правові акти та стратегічні документи, спрямовані на формування цілісної системи забезпечення безпеки держави та суспільства. Одним із ключових документів став Закон України «Про основи національної безпеки», прийнятий у 2003 році [123], який пізніше втратив чинність після ухвалення нового Закону України «Про національну безпеку». Важливими нормативними актами також стали Концепція національної безпеки України та Стратегії національної безпеки України, а також Послання Президента України до Верховної Ради «Про внутрішнє і зовнішнє становище України», що окреслювало основні напрями реформування сектору безпеки у відповідні роки.

Примітно, що у Стратегіях національної безпеки, ухвалених у 2007 [152], 2012 [132], 2015 [131] та 2020 [129] роках, пряме визначення національної безпеки відсутнє, проте його зміст розкривається через відповідні супутні правові акти. Відповідно до положень Концепції

національної безпеки України від 16 січня 1997 року [121], національна безпека трактується як стан гарантованої охорони життєво значущих інтересів індивіда, суспільства й держави від загроз як внутрішнього, так і зовнішнього походження, що створює умови для збереження та розвитку духовних і матеріальних надбань.

Закон України «Про основи національної безпеки України» 2003 року розширив це визначення, підкреслюючи, що захищеність життєво важливих інтересів особи, громадянина, суспільства та держави є основою для сталого розвитку суспільства. Закон також окреслює необхідність виявлення, попередження та нейтралізації реальних і потенційних загроз у ключових сферах, зокрема: оборона та правопорядок; економічна стабільність і соціальний захист; екологічна безпека, кібербезпека, інформаційна безпека; фінансовий ринок, податкова і митна політика; енергетика та охорона довкілля.

Ці правові акти в різні часи розвитку нашої держави створили систему гарантій, що спрямовані на захист держави та суспільства від внутрішніх і зовнішніх загроз, забезпечуючи належний розвиток ключових сфер державного управління, економіки та права. На різних етапах становлення держави ці нормативно-правові акти відігравали важливу роль у формуванні інституційних механізмів для сталого функціонування суспільства та підтримання національної стабільності. Таким чином, правове забезпечення національної безпеки в Україні розвивається як комплексна система, здатна адаптуватися до нових викликів та загроз, забезпечуючи ефективний захист національних інтересів.

Згідно з нормами базового Закону України «Про національну безпеку» від 21 червня 2018 року [123], національна безпека трактується як стан убезпечення державного суверенітету, недоторканності територіальної єдності, демократичних засад конституційного устрою, а також інших стратегічно важливих інтересів України від наявних і можливих загроз.

Це визначення підкреслює необхідність координації зусиль як національних, так і міжнародних, зокрема європейських, інституцій. У сучасних умовах досягнення належного рівня національної безпеки стає неможливим без спільної та скоординованої діяльності всіх залучених суб'єктів [123].

Пункт 22 «Стратегії національної безпеки України», затвердженої Указом Президента України від 14 вересня 2020 р. № 392/2020, вказує на те, що однією з основних загроз незалежності, суверенітету та демократичним принципам в Україні є недостатня ефективність державних органів. Вона створює перешкоди у процесі розробки та реалізації дієвої державної політики [153]. З цього випливає, що неефективна діяльність відповідних державних органів може стати реальною загрозою для безпеки держави.

Аналіз політичних цілей, визначених в Угоді про асоціацію з Європейським Союзом, Законі України «Про національну безпеку» від 21 червня 2018 року [123] та інших нормативно-правових актах, що регулюють питання національної безпеки, свідчить про необхідність визначення подальших стратегічних кроків державної влади. Зокрема, ці кроки повинні бути спрямовані на: поглиблення політичної асоціації України з європейськими та міжнародними партнерами; зміцнення міжнародної стабільності та безпеки через активне співробітництво у сфері безпеки та управління кризами; досягнення миру та стабільності на Європейському континенті; утвердження принципів верховенства права та демократичних цінностей; захист прав людини та основоположних свобод; консолідацію внутрішніх політичних реформ для забезпечення належного функціонування державних інституцій [159].

Зважаючи на вищезазначені цілі та на те, що Конституція України проголошує безпеку людини найвищою соціальною цінністю, можна стверджувати, що безпекова політика повинна бути невід'ємною складовою як внутрішньої, так і зовнішньої політики держави. Інтеграція політики національної безпеки в загальну структуру державного управління сприятиме

посиленню стійкості держави до внутрішніх та зовнішніх загроз, забезпеченню дотримання міжнародних зобов'язань України та підтримці сталого розвитку на шляху до євроінтеграції.

Аналіз законодавчої бази, що регулює сферу національної безпеки, свідчить про її специфічний характер, обумовлений складністю та багатогранністю відносин, які охоплюються цими актами. Така специфіка часто є властивою для нормативно-правових актів, які регулюють безпековий простір.

Правове регулювання у сфері національної безпеки охоплює кілька важливих напрямів суспільних відносин, серед яких можна виокремити такі:

1. Державне стратегічне планування у сфері національної безпеки. Цей напрям охоплює питання управління на основі стратегічних пріоритетів, що стикається з організаційно-правовими проблемами: визначення суб'єктів, підстав та процедур планування, компетенції органів влади, а також порядок і межі контролю за виконанням державних рішень;

2. Оборона держави та економічне забезпечення оборонних заходів. До цього напряму належить реалізація оборонної політики, зокрема унормування діяльності органів оборонного сектору, а також особливих суб'єктів, які діють в умовах спеціальних адміністративно-правових режимів. Важливим є державне регулювання економіки для забезпечення потреб оборони та розвиток державно-цивільного партнерства;

3. Розвідувальна та контррозвідувальна діяльність. Цей напрям передбачає здобуття критично важливої інформації, протидію підривній діяльності та гібридним загрозам з боку іноземних держав. Регламентація цієї діяльності охоплює розвідувальні органи та спеціально уповноважені інституції, їх повноваження та методи діяльності.

4. Стратегічна комунікація та міжнародний вплив. Включає заходи стратегічної комунікації для впливу на політику інших держав, інформаційні операції, дипломатію та культурне співробітництво. Також передбачаються

заходи з підтримки контактів зі співвітчизниками за кордоном та просування національних інтересів України у міжнародній сфері;

5. Запровадження тимчасових (особливих, надзвичайних) обмежувальних заходів. Цей блок стосується правового регулювання запровадження надзвичайних режимів у ситуаціях, що створюють загрозу безпеці держави, для забезпечення швидкого реагування на кризові явища;

6. Протидія тероризму, сепаратизму та політичному екстремізму. Передбачає впровадження правових заходів для боротьби з терористичною діяльністю, сепаратизмом та іншими проявами політичного екстремізму, що становлять загрозу внутрішній стабільності;

7. Охорона державного кордону України. Регламентує діяльність з управління та захисту державного кордону, що є ключовим елементом у забезпеченні територіальної цілісності держави;

8. Воєнна безпека та спеціальні правові режими. Охоплює запровадження та регулювання правових режимів воєнного стану або інших спеціальних умов, що забезпечують підвищену готовність держави до загроз у сфері оборони;

9. Правове регулювання питань тимчасової окупації та реінтеграції територій. Цей напрям стосується підтримання зв’язків із громадянами на окупованих територіях, заходів деокупації та реінтеграції цих територій у правове поле України [36, с. 54–55].

Таким чином, зазначені напрями охоплюють широкий спектр суспільних відносин, які формують основу національної безпеки України. Ефективне правове регулювання цих відносин є критично важливим для забезпечення стабільності та стійкості держави, а також реалізації її національних інтересів у внутрішній та зовнішній політиці. Національна безпека охоплює такі ключові складові, як: державна безпека, внутрішня безпека, економічна безпека, громадська безпека, воєнна безпека, екологічна безпека, інформаційна безпека (зокрема кібербезпека) та зовнішньополітична безпека.

Більш глибоку сутність національної безпеки можна усвідомити через функції держави.

Прийнятною є позиція І. М. Дороніна, згідно з якою метою сучасної держави є забезпечення безпеки для кожної особи та суспільства загалом, що виступає основною умовою її існування та сталого розвитку [36, с. 391]. У цьому контексті забезпечення національної безпеки слід розглядати як ключову функцію держави, яка відображає її фундаментальне завдання – захист життєво важливих інтересів суспільства. На думку вченого, функції держави можна розуміти як властивості та напрями діяльності, що відображають основні цілі державного управління. Безпекова основа державних функцій визначає межі, підстави та обсяги державного регулювання, тобто втручання держави у суспільне та приватне життя. Водночас забезпечення національної безпеки слугує гарантією від надмірного втручання органів влади у суспільні процеси, оскільки втручання має бути обґрунтованим і пропорційним загрозам [36, с. 391].

Забезпечення національної безпеки є не лише ціллю державної політики, але й передумовою ефективного виконання інших функцій держави, кожна з яких також спрямована на захист ключових сфер суспільного життя. До основних взаємопов’язаних функцій, спрямованих на забезпечення безпеки, належать:

– функція забезпечення державної безпеки – зосереджується на захисті суверенітету, конституційного ладу та територіальної цілісності держави;

– функція забезпечення воєнної безпеки (оборони) – передбачає підготовку та реалізацію оборонних заходів, спрямованих на запобігання військовим загрозам та підтримання обороноздатності держави;

– функція забезпечення економічної безпеки – спрямована на захист економічних інтересів, стабільність фінансової системи та запобігання економічним кризам, що можуть підірвати розвиток держави;

– функція забезпечення громадської безпеки – передбачає створення умов для підтримання громадського порядку, захисту прав і свобод громадян, а також запобігання злочинності та іншим внутрішнім загрозам;

– функція забезпечення екологічної безпеки – зосереджується на захисті довкілля, запобіганні екологічним катастрофам та збереженні природних ресурсів для сталого розвитку суспільства;

– функція забезпечення інформаційної безпеки – спрямована на захист інформаційного простору держави, запобігання дезінформації, кібератакам та підривним інформаційним кампаніям [36, с. 391–392].

Таким чином, національна безпека інтегрує всі ці функції в єдину систему, де кожен з напрямів безпеки сприяє зміцненню стійкості держави та суспільства. Забезпечення безпеки у різних сферах діяльності держави є критично важливим для її ефективного функціонування, оскільки стабільність у цих сферах дозволяє забезпечувати верховенство права, захист прав людини та сталий розвиток держави [36, с. 391–392].

Сучасна безпекова ситуація, яка характеризується динамічними викликами та загрозами як на національному, так і на глобальному рівнях, вимагає перегляду змісту поняття «національна безпека». Нові ризики та трансформації у сфері безпеки ставлять перед державою завдання актуалізації підходів до національної безпеки, з урахуванням змінних умов зовнішнього та внутрішнього середовища. Від правильного та чіткого розуміння цього поняття залежить ефективність діяльності суб’єктів, залучених до забезпечення безпеки, зокрема тих, які здійснюють зовнішню розвідку на основі відкритих джерел (OSINT).

Юридичне розуміння національної безпеки визначає напрями роботи відповідних інституцій, об’єкти спостереження та виявлення потенційних небезпек. Суб’єкти, що здійснюють розвідувальну діяльність, мають чітко орієнтуватися у пріоритетах і напрямах протидії загрозам, які безпосередньо впливають на національні інтереси. Їхні завдання полягають у своєчасному виявленні, аналізі та оцінці ризиків з метою запобігання небажаним подіям,

що можуть поставити під загрозу суверенітет, безпеку та сталий розвиток держави.

Отож актуалізація концепції національної безпеки у відповідь на нові виклики має не лише нормативно-правове значення, але й впливає на функціонування системи безпеки загалом. Зміна змісту та структури цього поняття дозволяє сформувати ефективну стратегію роботи розвідувальних органів, забезпечуючи належну координацію їх діяльності з іншими суб'єктами безпеки. Це підвищує здатність держави своєчасно реагувати на потенційні загрози, залишаючись гнучкою у змінних умовах міжнародного середовища та внутрішньої політики.

Узагальнюючи викладене, варто підкреслити, що національна безпека держави охоплює комплекс заходів із захисту суверенітету, територіальної єдності, недоторканності державного кордону, прав і свобод громадян, а також забезпечення стратегічних інтересів країни та стабільного функціонування конституційного ладу. Такий підхід свідчить про те, що гарантування як внутрішньої, так і зовнішньої безпеки становить одну з ключових функцій державної влади. Ефективність механізмів забезпечення національної безпеки безпосередньо впливає на рівень незалежності держави та її міжнародний статус. У контексті розвитку сучасного інформаційного суспільства особливого значення набуває роль відкритих джерел розвідки (OSINT) як одного з інструментів інформаційної підтримки процесів національної безпеки. Варто наголосити, що національна безпека є невід'ємною складовою суспільного розвитку і не існує поза його межами. Розуміння безпеки держави повинно ґрунтуватися на усвідомленні її як результату консолідованої діяльності державних інституцій, органів місцевого самоврядування, інститутів громадянського суспільства та кожного громадянина зокрема [82, с. 356].

Поняття «національна безпека» має виразний міждисциплінарний характер і є ключовою складовою державної діяльності та соціального управління у суспільствах, об'єднаних у рамках певної держави. Це поняття

відображає не лише стан захищеності національних інтересів, а й процес постійного підтримання цієї захищеності через реалізацію державної політики та функціонування відповідних державних органів. Національна безпека у демократичних суспільствах не обмежується лише військовою складовою, але охоплює також політичну, економічну, інформаційну, екологічну та соціальну безпеку. Вона забезпечується через спільні зусилля держави і суспільства, де державні інституції та громадяни спільно працюють над підтримкою стабільності й розвитку.

Відповідно, національна безпека трактується як захищеність інтересів суспільства та держави, а також як процес безперервної адаптації державної політики та інституцій для запобігання і нейтралізації загроз, що можуть порушувати суспільний порядок чи підривати державний суверенітет. Це забезпечення охоплює не лише оборонні заходи, але й інші сфери управління, що сприяють стабільному розвитку країни.

У сучасній системі забезпечення національної безпеки особливе місце посідає зовнішня розвідка на основі відкритих джерел (OSINT). OSINT є важливим інструментом для збору та аналізу інформації з відкритих джерел, таких як: медіа (новинні ресурси, соціальні мережі); публічні звіти, бази даних та аналітичні огляди; наукові дослідження та академічні публікації; дані з урядових та міжнародних організацій; геопросторові дані (карти, супутникові знімки тощо).

Основна роль OSINT у сфері національної безпеки полягає у завчасному виявленні потенційних загроз та підвищенні обізнаності керівництва держави про поточну ситуацію як всередині країни, так і за її межами. Завдяки відкритим джерелам розвідка може: моніторити геополітичну ситуацію та виявляти тенденції, що становлять потенційну загрозу для безпеки держави; аналізувати поведінку іноземних держав та недержавних акторів, у тому числі терористичних угруповань та організацій, що застосовують гібридні методи впливу; виявляти дезінформаційні кампанії та пропаганду, що можуть дестабілізувати внутрішню ситуацію в країні; підтримувати стратегічну

комунікацію та інформаційний вплив, спрямований на захист національних інтересів на міжнародній арені; забезпечувати кризовий моніторинг та попередження у разі виникнення надзвичайних ситуацій чи загроз у різних сферах (економічній, екологічній, політичній тощо).

OSINT також відіграє важливу роль у підтримці державних і безпекових рішень через надання актуальної та достовірної інформації для прийняття стратегічних рішень. У сучасних умовах, коли інформаційне середовище стає дедалі більш насиченим та динамічним, використання OSINT дає змогу оперативно реагувати на загрози і зміцнювати національну безпеку без необхідності вдаватися до ресурсно-витратних заходів традиційної розвідки.

Отже, OSINT є важливим елементом інтегрованої системи національної безпеки, що сприяє підвищенню ефективності діяльності розвідувальних та аналітичних структур держави. Використання інформації з відкритих джерел дозволяє значно розширити спроможності державних органів у виявленні загроз та забезпеченні захисту національних інтересів, забезпечуючи дотримання законності та відповідність міжнародному праву.

1.3 Адміністративно-правове регулювання забезпечення функціонування OSINT у сфері національної безпеки

В умовах зростання сучасних викликів і загроз національній безпеці, які мають комплексний та непередбачуваний характер, дослідження механізмів адміністративно-правового забезпечення функціонування OSINT набуває особливої значущості. Інформація з відкритих джерел, зважаючи на її доступність, оперативність та значний обсяг, стає критично важливим інструментом для виявлення потенційних загроз та забезпечення національних інтересів.

Розвиток інформаційних технологій і глобалізація інформаційних потоків підвищують як потенціал, так і ризики використання OSINT у

державному управлінні. Водночас ефективне функціонування OSINT потребує належної правової регламентації, яка б забезпечувала баланс між свободою доступу до інформації та необхідністю захисту національної безпеки і прав людини. Це вимагає системного підходу до адміністративно-правового регулювання, що включає розробку відповідних норм, процедур та механізмів контролю.

З огляду на військову агресію та складність сучасних загроз – від терористичних актів до кібератак та гібридної війни, дослідження адміністративно-правових аспектів OSINT є актуальним як на національному, так і на міжнародному рівнях. Зокрема, необхідність впровадження ефективних механізмів координації та співпраці між державними органами, приватним сектором та міжнародними партнерами стає ключовим фактором у забезпеченні ефективності OSINT як інструмента безпеки.

Таким чином, актуальність дослідження адміністративно-правового регулювання механізму адміністративно-правового забезпечення функціонування OSINT зумовлена необхідністю створення чіткої нормативно-правової бази, яка сприятиме ефективному використанню інформаційних ресурсів для забезпечення національної безпеки та водночас запобігатиме зловживанням правами і свободами громадян.

Дослідження такого багатовимірного та значущого феномена, як забезпечення ефективного функціонування OSINT у системі національної безпеки, набуває особливої актуальності для сучасної української адміністративно-правової науки. У цьому контексті виникає об’єктивна необхідність у визначенні правової природи та змістового наповнення понять «адміністративно-правове регулювання у сфері національної безпеки» та «адміністративно-правове регулювання функціонування OSINT у системі гарантування національної безпеки». За умов збройної агресії, зовнішнього тиску та внутрішніх викликів реалізація державою своїх функцій із гарантування національної безпеки, відновлення територіальної цілісності та зміцнення обороноздатності неможлива без впровадження ефективних

механізмів, серед яких важливе місце займає організація та правове забезпечення функціонування відкритих джерел розвідки (OSINT). Ці процеси вимагають належного адміністративно-правового врегулювання відповідних суспільних відносин.

Адміністративна діяльність органів та суб'єктів, відповідальних за реалізацію політики національної безпеки, потребує чіткого нормативного регламентування. Така регламентація здійснюється за допомогою нормативно-правових актів різного рівня, включаючи закони України, укази Президента, постанови та розпорядження Кабінету Міністрів України, накази профільних міністерств та інших центральних органів виконавчої влади. Суспільні відносини, які формуються у процесі забезпечення функціонування OSINT у сфері національної безпеки, регулюються нормами адміністративного права, що визначають порядок, форми та межі діяльності уповноважених суб'єктів у відповідній сфері. Отже, адміністративно-правове регулювання виступає ключовим інструментом упорядкування, легітимації та підвищення ефективності управлінських процесів, пов'язаних з інформаційною безпекою та загальною стратегією національної безпеки держави.

Одним із ключових інструментів у системі адміністративно-правового регулювання функціонування OSINT у сфері національної безпеки виступають норми адміністративного права, які охоплюють широкий спектр регулятивних засобів, зокрема: обов'язки, приписи, заборони та дозволи. Особливо вагоме значення у цьому контексті мають норми-приписи, що формулюють вимоги до обов'язкових дій з боку уповноважених суб'єктів, відповідальних за впровадження і підтримання ефективного функціонування систем OSINT. Адміністративно-правове регулювання забезпечення діяльності OSINT у сфері національної безпеки варто розглядати як систему заходів, інструментів і правових механізмів, що реалізуються компетентними органами з метою впорядкування, контролю та координації суспільних відносин у відповідній сфері. Такий підхід забезпечує чіткість управлінських

процедур, визначеність повноважень та відповідальність учасників правовідносин, які беруть участь у збиранні, аналізі та використанні відкритої розвідувальної інформації.

Для більш глибокого розуміння специфіки та внутрішньої структури засобів адміністративно-правового регулювання функціонування OSINT, необхідно звернутися до загальнотеоретичних основ адміністративного права, а саме – до категорій «адміністративно-правове регулювання» і «адміністративно-правове забезпечення». Їх аналіз дозволяє з'ясувати співвідношення між правовим впливом і організаційно-правовим супроводом, що в сукупності утворює нормативну й інституційну базу для ефективного використання OSINT у системі національної безпеки.

Адміністративно-правове впорядкування є складним феноменом, який, з огляду на сучасні зміни в суспільстві, набуває оновленого значення та предметності дослідження в межах правознавчої науки і вимагає постійного теоретичного осмислення. Варто наголосити, що адміністративно-правове впорядкування становить один із компонентів загального юридичного регулювання, що розглядається крізь призму систематизації, погодження та пристосування різних елементів правової дійсності.

Цілком виправданою є позиція А. Т. Комзюка, відповідно до якої юридичне регулювання – це особлива форма впливу, що здійснюється правом як специфічним нормативно-організаційним механізмом. При цьому правове регулювання має цілеспрямований, структурований та ефективний характер і реалізується шляхом застосування цілісної сукупності інструментів, що втілюють сутність права як нормативного утворення – регулюючого механізму [60, с. 47]. Водночас адміністративно-правове впорядкування – це спрямований вплив норм адміністративного права на суспільні взаємовідносини з метою гарантування за допомогою адміністративно-правових інструментів прав, свобод і легітимних публічних інтересів як фізичних, так і юридичних осіб, а також належного функціонування інститутів громадянського суспільства та державного апарату [2, с. 323–324; 82].

Слід підкреслити, що юридичне впорядкування завжди охоплює встановлення конкретизованих правомочностей і обов'язків суб'єктів правових відносин, а також формулювання однозначних норм щодо належної поведінки. Тоді як правовий вплив може виявлятися менш очевидно. Адміністративно-правове впорядкування передбачає втілення норм адміністративного права через відповідні правовідносини та водночас здійснює нормативний вплив, який не завжди супроводжується усвідомленим упорядкуванням суспільних процесів [82].

У контексті гарантування національної безпеки завдяки використанню інструментів OSINT, призначення правової системи полягає у забезпеченні виконання відповідними учасниками визначених функцій, дотримання встановлених положень, закріплених у нормах адміністративного права. У зв'язку з цим актуалізується питання розкриття змісту поняття «адміністративно-правове забезпечення» та визначення його співвідношення з категорією «адміністративно-правове регулювання» [82].

Теоретичне осмислення дефініції «адміністративно-правове забезпечення» вимагає від дослідників комплексного підходу до вивчення цієї категорії. Це охоплює розгляд співвідношення між поняттями «адміністративно-правове забезпечення» і такими термінами, як «адміністративно-правове регулювання», «юридичне регулювання» та «правове забезпечення». Додатково доцільним є аналіз змісту вказаних понять крізь призму таких правових категорій, як «право» і «забезпечення», «правовий режим» тощо.

Зокрема, К. В. Барсуков трактує термін «забезпечення» у двох аспектах: як діяльність органів державної влади, уповноважених на виконання покладених на них функцій; а також як наслідок цієї діяльності, що виявляється у практичному втіленні правових норм, а також у реалізації прав та свобод осіб [10, с. 7; 82].

І. М. Шопіна трактує адміністративно-правове регулювання як вплив адміністративно-правового характеру на суспільні взаємовідносини, що

здійснюється шляхом застосування комплексу правових інструментів адміністративного спрямування та інших юридичних елементів, які разом утворюють механізм адміністративно-правового впливу [174, с. 55]. Дослідниця наголошує, що адміністративно-правове регулювання формулює загальну мету упорядкування суспільних зв'язків з боку органів державної влади шляхом використання імперативного підходу, тоді як адміністративно-правове забезпечення конкретизує правову норму в межах публічного управління. У зв'язку з цим адміністративно-правове забезпечення варто розглядати як систему адміністративно-правових інструментів, методів і процедур їх впровадження, спрямовану на створення передумов для повноцінного здійснення прав, свобод і законних інтересів особи, інститутів громадянського суспільства, суб'єктів господарювання, а також інших учасників адміністративно-правових відносин. У межах свого наукового дослідження І. М. Шопіна зосереджує увагу саме на адміністративно-правових інструментах і методах, підкреслюючи, що нормативно-правові акти становлять лише один із елементів у структурі адміністративно-правового забезпечення [82; 175, с. 143–144].

Беручи до уваги специфіку сфери національної безпеки, адміністративно-правове врегулювання функціонування OSINT слід розуміти як діяльність, що чітко регламентується нормами адміністративного права та здійснюється уповноваженими суб'єктами із застосуванням визначених способів, інструментів і заходів, спрямованих на гарантування безпеки держави [82, с. 358]. Така діяльність підпорядковується вимогам спеціалізованого нормативно-правового регулювання.

Належне адміністративно-правове регулювання забезпечення функціонування OSINT та механізмів її реалізації дозволяє ефективно здійснювати розвідку з відкритих джерел з метою забезпечення національної безпеки.

Законодавче забезпечення діяльності у сфері OSINT здійснюється за такими напрямами:

1. Регулювання правовідносин між суб’єктами OSIN, визначаючи їх завдання, функції та повноваження, механізми взаємодії;

2. Забезпечення діяльності суб’єктами OSINT на різних рівнях: держава, суспільство, особи;

3. Визначення механізмів реалізації повноважень суб’єктами OSINT (форми, методи діяльності, використання інформаційних ресурсів, засоби та інструменти забезпечення національної безпеки).

Одним із ключових завдань адміністративно-правового регулювання OSINT є гармонізація національного законодавства з міжнародними нормами у сфері інформаційної безпеки. Наприклад, це включає дотримання стандартів, установлених міжнародними угодами щодо захисту прав на інформацію та персональні дані, таких як Будапештська конвенція про кіберзлочинність та Загальний регламент про захист даних (GDPR). Вітчизняне законодавство також має забезпечити належний баланс між вільним доступом до інформації та захистом інтересів національної безпеки.

Законодавство, що регулює функціонування відкритих джерел інформації (OSINT) у сфері національної безпеки, доцільно розглядати з урахуванням сфери його застосування та наявної ієрархії нормативно-правових актів. Цей ієрархічний підхід забезпечує чітке розуміння правових підстав та напрямів регулювання OSINT як частини загальної системи забезпечення національної безпеки держави.

На найвищому рівні нормативно-правової системи знаходиться Конституція України, яка закріплює основоположні принципи забезпечення національної безпеки держави. Вона має обов’язки щодо захисту державного суверенітету, територіальної цілісності, а також безпеки громадян. Конституційні норми є базою для формування національної політики у сфері безпеки, включаючи положення про військову, кібербезпеку, інформаційну безпеку та, як її складову, забезпечення функціонування OSINT. Доповнюють конституційні положення стратегічні концептуальні документи, зокрема

Стратегія національної безпеки України, Стратегія кібербезпеки, що окреслюють загальні засади державної політики в цій сфері.

Другий рівень становлять законодавчі акти, які деталізують ключові положення національної безпеки та регулюють питання використання OSINT у рамках безпекової діяльності. Закони України «Про національну безпеку України», «Про основні засоби забезпечення кібербезпеки України», «Про інформацію» закріплюють основні принципи та механізми правового регулювання інформаційної діяльності, включаючи питання використання відкритих джерел інформації для національної безпеки.

На третьому рівні знаходиться інституційне законодавство, що регулює діяльність окремих органів і суб'єктів у сфері національної безпеки. Це нормативно-правові акти, які визначають функції, завдання, повноваження та відповідальність органів державної влади у сфері кібербезпеки, розвідки та інші структури, що застосовують діяльність з використанням OSINT. Наприклад, положення про функціонування Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства оборони України та інші суб'єкти розробляють взаємодію цих установ із забезпеченням безпеки за допомогою відкритих джерел.

Четвертий рівень складають міжнародно-правові акти, що регулюють використання відкритих джерел інформації в контексті забезпечення національної безпеки. До таких актів належать міжнародні угоди та конвенції, що встановлюють стандарти щодо захисту персональних даних, боротьби з кіберзлочинністю, а також забезпечення прав людини в інформаційному середовищі. Також Будапештська конвенція про кіберзлочинність [63], Загальний регламент ЄС про захист даних (GDPR) [138], міжнародні резолюції ООН є основними документами, які регулюють взаємодію держави у сфері OSINT на міжнародному рівні.

Таким чином, нормативно-правове забезпечення функціонування OSINT у сфері національної безпеки має багаторівневу структуру, яка охоплює конституційні, законодавчі, інституційні та міжнародно-правові

акти. Такий підхід забезпечує ефективне правове регулювання цієї сфери з урахуванням національних та міжнародних інтересів і стандартів.

Як уже зазначалося вище, об'єктом механізму адміністративно-правового забезпечення функціонування OSINT є національна безпека. Тому діяльність уповноважених суб'єктів OSINT у цій сфері також буде визначатися межами законодавства, яке є правовою основою національної безпеки та стратегічними документами, які визначають загрози та небезпеки, а також окреслюють напрями та завдання діяльності відповідних органів у сфері з усунення таких загроз і небезпек.

Правові засади забезпечення національної безпеки України закріплені в низці нормативно-правових актів різної юридичної сили. Основу цієї сфери становить Конституція України. Відповідно до статті 17 Конституції захист суверенітету, територіальної цілісності та забезпечення економічної й інформаційної безпеки є ключовими функціями держави та спільною справою всього народу України [65]. Таким чином, забезпечення національної безпеки інтегрується в загальнодержавну діяльність, підкреслюючи її пріоритетність як фундаментального обов'язку всіх громадян і державних інституцій.

В адміністративно-правовому регулюванні національної безпеки ключовими засадами, що спрямовують правотворчу діяльність у сфері національної безпеки та функціонування відповідних органів публічної влади, є конституційні положення щодо дотримання принципів, закріплених у статті 1 Конституції України, яка визначає державу як суверенну, незалежну, демократичну, соціальну та правову. Крім того, пункт 17 статті 92 Конституції України містить положення, яким установлено винятковий характер законів у визначенні основ національної безпеки [65]. Цей конституційний припис виключає можливість регулювання цих питань указами чи підзаконними актами, підкреслюючи необхідність чіткого законодавчого підходу.

Реалізація конституційних принципів національної безпеки відображена в Законі України «Про національну безпеку України» [123]. Цей закон визначає повноваження державних органів у сфері безпеки та оборони,

забезпечує інтеграцію політики та процедур різних відомств, регулює координацію між силами безпеки та оборони. Він також запроваджує систему командування та контролю і забезпечує демократичний цивільний контроль над сектором безпеки. Цей нормативний акт належить до спеціального законодавства, спрямованого на врегулювання суспільних відносин у сфері національної безпеки.

У першій частині статті 12 Закону України «Про національну безпеку» окреслено складові елементи сектора безпеки й оборони, до якого належать органи безпеки, військові формування, оборонно-промислова галузь, а також громадяни й інститути громадянського суспільства, що здійснюють підтримку у сфері забезпечення національної безпеки.

Розділ III цього закону встановлює механізми демократичного контролю, який здійснюють центральні органи влади (Президент, Верховна Рада, Кабінет Міністрів), Рада національної безпеки і оборони, органи місцевого самоврядування, судова система та громадські інституції [123].

Закон України «Про національну безпеку» слугує правовою основою для функціонування OSINT у контексті національної безпеки, встановлюючи нормативні межі для збору та аналізу даних з відкритих джерел. Він визначає повноваження органів державної влади у сфері безпеки та оборони, забезпечує координацію дій між ними та впроваджує принципи демократичного цивільного контролю. Закон підтримує комплексний підхід до інформаційної безпеки, що дозволяє використовувати OSINT для виявлення загроз і прийняття стратегічних рішень у рамках правових процедур. Закон також забезпечує дотримання демократичного цивільного контролю, що важливо для використання OSINT відповідно до правових норм. Таким чином, OSINT стає інструментом для виявлення загроз і ухвалення рішень у межах законодавчої бази, сприяючи ефективності сектору безпеки.

Стратегія національної безпеки України [153] є ключовим стратегічним документом, який визначає напрями державної політики у сфері безпеки та оборони. Вона формує правові й організаційні основи для функціонування

OSINT – розвідки на основі відкритих джерел, що зараз є важливим інструментом виявлення та нейтралізації сучасних загроз. Цей документ узгоджується із Законом України «Про національну безпеку» та встановлює стратегічні пріоритети щодо інформаційної безпеки, кіберзахисту, боротьби з гібридними загрозами та дезінформацією. Функціонування OSINT підпорядковується цим пріоритетам, оскільки використання відкритих джерел дозволяє оперативно збирати інформацію про внутрішні та зовнішні загрози. Стратегія передбачає залучення до процесу не лише державних органів, а й приватних інституцій та громадян, сприяючи інтеграції суспільства у забезпечення національної безпеки.

У межах Стратегії визначаються також підходи до міжнародного співробітництва у сфері безпеки. Це створює умови для використання OSINT як інструменту в координації з міжнародними партнерами для обміну інформацією та спільного аналізу загроз. Важливим компонентом є контроль і моніторинг інформаційних ризиків, що сприяє своєчасному виявленню дезінформаційних кампаній і попередженню їхніх негативних наслідків. Крім того, Стратегія національної безпеки підкреслює важливість розвитку технологій та аналітичних інструментів для підвищення ефективності OSINT. Вона спрямована на створення сприятливих умов для використання сучасних інформаційних технологій, що дозволяють оптимізувати процеси збору та аналізу даних із відкритих джерел.

Наступним нормативно-правовим актом, який визначає стратегічні пріоритети діяльності суб’єктів з питань забезпечення національної безпеки, є Указ Президента України № 447/2021, яким було затверджено Стратегію кібербезпеки [129] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України».

Згідно зі Стратегією кібербезпеки України забезпечення кібербезпеки є ключовим напрямом у системі національної безпеки України, що відповідає сучасним викликам у глобальному цифровому середовищі. Ефективна реалізація цього стратегічного пріоритету забезпечує посилення спроможності

національної системи кібербезпеки, яка покликана протидіяти ескалації кіберзагрози та забезпечити захист критичної інфраструктури, інституцій та громадянських прав у кіберпросторі. З огляду на швидку еволюцію технологій та зростання стійкості кіберзагроз, удосконалення нормативно-правового забезпечення та впровадження міжнародних стандартів є необхідними складними інтегрованими підходами до забезпечення національної кібербезпеки [129].

Актуальні виклики кіберпростору охоплюють збільшення кількості кібератак на критичну інфраструктуру, що спрямовані на підрив енергетичної, фінансової та інформаційної стабільності держави. В умовах гібридних конфліктів кіберпростір стає полем для реалізації як традиційних військових стратегій, так і нових форм інформаційної війни. Державні органи повинні бути спроможними оперативно реагувати на кібератаки та розробляти попереджувальні заходи, що забезпечують зменшення негативних ризиків та відновлення роботи інфраструктури після інцидентів.

У Стратегії кібербезпеки України [129] акцентовано увагу на тому, що для створення ефективної системи кібербезпеки держава має діяти комплексно, залучаючи ресурси як з державного, так і приватного секторів. Це включає формування національних центрів моніторингу загроз, розвиток системи кіберрозвідки та співпрацю з міжнародними партнерами. Значну роль у цьому відіграє розвиток правових механізмів, зокрема завдяки законодавчим актам, які регламентують порядок взаємодії між органами державної влади та суб’єктами приватного сектору з питань кібербезпеки. Крім того, правове забезпечення кібербезпеки має передбачати механізми швидкого реагування на нові виклики, зокрема шляхом впровадження процедур кібердипломатії та забезпечення участі України в міжнародних ініціативах з протидією.

Виконання вказаних завдань потребує створення дієвої системи нормативно-правових актів, що має врегульовувати порядок взаємодії, форми і методи діяльності, процедури діяльності відповідних інституцій, що здійснюють розвідку з відкритих джерел.

У сучасних умовах необхідним є перехід від реактивного підходу до проактивної моделі управління кіберризиками. Це означає не лише виявлення загрози на ранніх етапах, але й формування політики та стратегії, що забезпечує довготривалу стійкість національного кіберпростору. Важливим аспектом є також підвищення обізнаності суспільства щодо загроз у кіберпросторі та стимулювання розвитку компетенцій у сфері кібербезпеки серед широких верств населення.

Аналіз положень Стратегії кібербезпеки України [129] дозволяє зробити висновок, що кібербезпека в сучасному контексті потребує системного та міждисциплінарного підходу, що охоплює не лише технологічні та організаційні аспекти, але й розвиток правових механізмів, тобто відповідного спеціального законодавства. Формування відповідної нормативно-правової бази та комплексної національної системи кібербезпеки, здатної ефективно реагувати на динамічні виклики кіберпростору, є важливою умовою для збереження суверенітету та стабільності.

Національна система кібербезпеки України є комплексною інституційною та правовою основою, що забезпечує державну політику у сфері кібербезпеки відповідно до вимог Стратегії кібербезпеки України [129]. З огляду на виклики сучасного глобального інформаційного середовища та гібридних загроз, ефективне функціонування цієї системи має за мету захист національних інтересів та забезпечення кіберстійкості критичної інфраструктури. Успішна розбудова національної системи кібербезпеки передбачає гармонізацію правових, організаційних та технічних механізмів, що сприяють запобіганню, виявленню та нейтралізації кіберзагрози.

Наступним нормативно-правовим документом, що формує адміністративно-правову основу механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, є Закон України «Про основні засади забезпечення кібербезпеки України» [129].

Закон України «Про основні заходи забезпечення кібербезпеки України» [126] встановлює базові юридичні та інституційні принципи гарантування

захисту ключових інтересів особистості, суспільства та держави в умовах інформаційного середовища. У зазначеному законі закріплюються стратегічні орієнтири та принципи реалізації державної політики у сфері кіберзахисту, яка має за мету оборону національних інтересів України у кіберпросторі, а також визначаються повноваження основних учасників цього процесу.

Цим нормативно-правовим актом установлюються базові положення щодо розподілу компетенцій між органами державної влади, підприємствами, установами, організаціями та громадянами, які беруть участь у забезпеченні кібербезпеки. Відповідно, він використовує форму їхньої взаємодії та координації для запобігання та протидії кіберзагрозам. Закон також закріплює обов'язок державних інституцій розробляти та реалізовувати комплексні заходи протидії кіберзагрозам, водночас сприяючи співпраці між державним і приватним секторами та міжнародними партнерами.

Ключовим елементом цього правового акта є визначення системи державних органів, уповноважених функцій управління у сфері кібербезпеки. Такі органи, як Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України та Міністерство цифрової трансформації, наділені широкими повноваженнями для координації діяльності в цьому напрямі. Закон також зобов'язує суб'єкти господарювання та громадян дотримуватися встановлених вимог і стандартів безпеки з метою запобігання загрозам.

Окремої уваги заслуговують положення закону щодо принципів кібербезпеки, серед яких виділяється верховенство прав, відповідальність суб'єктів за забезпечення безпеки, відкритість і прозорість діяльності у сфері кіберзахисту, а також відповідність національної політики міжнародним стандартам та практикам. Ці принципи забезпечують інтеграцію України у світовий кіберпростір і сприяють підвищенню стійкості національної кіберінфраструктури до загроз різного характеру [126].

Таким чином, Закон України «Про основні заходи забезпечення кібербезпеки України» [126] формує цілісний правовий механізм, який

регулює взаємодію суб'єктів у сфері кібербезпеки, визначає напрями державної політики та сприяння інтеграції України в міжнародну систему протидії кіберзагрозам. Він закладає правову основу для побудови ефективної системи захисту національних інтересів у кіберпросторі, водночас стимулюючи розвиток співпраці між усіма суб'єктами, залученими до забезпечення кіберстійкості держави.

Вказані нормативно-правові акти слугують основою, яка визначає пріоритети на напрями діяльності відповідних суб'єктів, що здійснюють розвідку на основі відкритих джерел, з метою виявлення та усунення загроз національній безпеці.

В Україні функціонування OSINT регулюється також низкою інших нормативно-правових актів, спрямованих на забезпечення правомірного збору, використання та обробки інформації з відкритих джерел у контексті національної безпеки та оперативно-розшукової діяльності. До таких законодавчих актів можна віднести:

1. Закон України «Про Службу безпеки України» регулює діяльність СБУ, яка виконує розвідувальні та контррозвідувальні функції, зокрема із застосуванням OSINT для виявлення загрози національної безпеки [134];

2. Закон України «Про розвідку» визначає завдання та повноваження розвідувальних органів, які можуть використовувати відкриті джерела інформації для збору та аналізу розвідувальних даних [133];

3. Закон України «Про основні засоби забезпечення кібербезпеки України» оцінює завдання у сфері кібербезпеки, які виконує Державна служба спеціального зв'язку та захисту інформації України, включаючи моніторинг загроз із використанням OSINT [126];

4. Закон «Про інформацію» регулює порядок отримання та використання інформації, включаючи інформацію з відкритих джерел. Він визначає права і обов'язки суб'єктів інформаційної діяльності та обмеження, пов'язані з доступом до певних категорій інформації (наприклад, конфіденційної чи державної таємниці) [118];

5. Закон «Про захист персональних даних» вводить обмеження на збір та обробку персональних даних, що є критично важливим під час використання OSINT. Це законодавство забезпечує баланс між необхідністю збору інформації для розвідувальних цілей та захистом прав людини, зокрема права на приватність, шляхом встановлення чітких вимог щодо обробки персональних даних та їхнього захисту [117];

6. Закон «Про оперативно-розшукову діяльність» визначає основи застосування розвідувальних методів для забезпечення національної безпеки та правопорядку. Він обмежує використання таких методів без належного відкриття оперативної справи, що стосується й OSINT у правоохоронній діяльності [125];

7. Кримінальний процесуальний кодекс України регламентує проведення слідчих дій та застосування розвідувальних інструментів, включаючи дані з відкритих джерел, у межах кримінальних проваджень. Використання OSINT для збору доказів допускається лише з дотриманням норм закону та процесуальних вимог [71];

8. Закон України «Про затвердження Положення про Державну службу спеціального зв’язку та захисту інформації України» – виконує функції та повноваження Держспецзв’язку, яка відповідає за кібербезпеку та захист державних інформаційних ресурсів. Закон передбачає застосування технологій збору даних з відкритих джерел для моніторингу загроз та забезпечення безпеки інформаційної інфраструктури держави [114];

9. Закон України «Про контррозвідувальну діяльність» [120] визначає правові та організаційні основи здійснення контррозвідувальних заходів органами СБУ та іншими уповноваженими структурами. Використання інформації з відкритих джерел у цьому контексті можливо для: виявлення загрози національної безпеці; зберігання додаткових даних про осіб або структури, які можуть бути залучені до шпигунства або диверсій; здійснення моніторингу публічних висловлювань або дій, які можуть свідчити про ворожу активність. Стаття 5 закону передбачає, що контррозвідувальні

заходи можуть включати збір інформації з різних джерел, у тому числі відкритих даних, якщо це відповідає завданням і цілям захисту державних інтересів.

Безумовно, вказаними законодавчими актами цей перелік не вичерпується. Крім того, діяльність державних органів, пов'язана із застосуванням OSINT, регулюється не тільки законами, але й низкою постанов Кабінету Міністрів України та іншими підзаконними актами. Ці документи встановлюють правила діяльності органів виконавчої влади, їх взаємодію та особливі вимоги до використання інформаційних ресурсів. До цих підзаконних правових актів можна віднести такі, як:

1. Постанова Кабінету Міністрів України «Про внесення змін до Положення про Міністерство цифрової трансформації України» [112]. Встановлює завдання та функції Мінцифри, зокрема у сфері управління інформаційною безпекою, впровадження інноваційних технологій та забезпечення моніторингу відкритих джерел інформації для підтримки урядових рішень у сфері цифрової трансформації та національної безпеки;

2. Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» [32]. Цією постановою створено механізм моніторингу кіберпростору, що включає використання OSINT для виявлення загроз в інтернеті та державних інформаційних системах;

3. Постанова Кабінету Міністрів України «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів» [33] – регулює обмін інформацією між державними органами через електронні системи, які можуть включати аналіз інформації з відкритих джерел для підтримки діяльності державних установ у сфері національної безпеки;

4. Указ Президента України «Про Національний координаційний центр кібербезпеки» [122] регулює діяльність Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України та визначає ключові завдання та роль центру в координації зусиль для

забезпечення кібербезпеки України, включно з використанням інструментів OSINT. Ключова роль OSINT у діяльності НКЦК полягає у збиранні публічної інформації для аналізу можливих загроз і планування реагування. Це включає моніторинг цифрового середовища, прогнозування наявних кіберінцидентів та співпрацю з іншими державними органами та міжнародними партнерами у сфері кібербезпеки;

5. Постанова Кабінету Міністрів України «Про затвердження Положення про організаційно-технічну модель кіберзахисту» від 29 грудня 2021 р. № 1426 – регулює організаційно-технічну модель кіберзахисту, яка включає кіберзагрозу з використанням аналітичних даних з відкритих джерел [116].

Ці та інші підзаконні акти спрямовані на координацію роботи органів державної влади та забезпечення правової основи для їх діяльності у сфері OSINT. Зазначені вище та інші нормативно-правові акти регламентують використання відкритих джерел інформації з питань забезпечення національної безпеки, кібербезпеки та моніторингу загроз в інформаційному просторі. Загалом інституційний рівень досліджуваного нами законодавства забезпечує комплексний підхід до використання OSINT, сприяючи підвищенню ефективності кібербезпеки та національної безпеки шляхом інтеграції розвідувальних інструментів у діяльність державних органів.

Застосування OSINT в Україні активно підтримується для цілей національної безпеки, зокрема для боротьби з корупцією та організованою злочинністю. Однак правовий контроль за цією діяльністю має забезпечити баланс між ефективністю збору розвідувальних даних і захистом прав громадян, що особливо важливо в умовах цифровізації суспільства та зростання кількості інформаційних загроз.

Наступним рівнем адміністративно-правового регулювання функціонування OSINT у сфері національної безпеки є міжнародне законодавство, і це не випадково, адже активне використання OSINT потребує чіткого міжнародно-правового регулювання, яке встановлює межі

використання відкритих джерел, забезпечує захист прав людини та координує діяльність держав у цій сфері на глобальному рівні.

Одним із ключових аспектів регулювання OSINT є забезпечення балансу між правом доступу до інформації та захистом прав людини, особливо в контексті захисту персональних даних та конфіденційної інформації. Основоположні міжнародні документи, такі як Міжнародний пакт про громадянські і політичні права [87] та Європейська конвенція з прав людини [39], гарантують право на отримання і поширення інформації. Однак це право не є абсолютним, особливо в умовах загрози національній безпеці. Стаття 19 Міжнародного пакту про громадянські і політичні права встановлює можливість обмеження свободи інформації, зокрема в ситуаціях, коли це необхідно для забезпечення національної безпеки, громадського порядку або захисту прав і свобод інших осіб. Це дозволяє державам вживати відповідних заходів для обмеження доступу до певної інформації в інтересах безпеки та стабільності суспільства [87].

Захист персональних даних, що є важливим аспектом діяльності з OSINT, регулюється такими міжнародними актами, як Загальний регламент ЄС про захист даних (GDPR) [43] та Конвенція Ради Європи № 108 про захист осіб у зв’язку з автоматизованою обробкою персональних даних [62]. Ці акти встановлюють стандарти обробки інформації та захисту конфіденційних даних, що мають важливе значення в контексті використання відкритих джерел інформації для національної безпеки.

Міжнародні організації, такі як Європейський Союз, НАТО та ООН, відіграють важливу роль у формуванні міжнародних стандартів з використанням OSINT для забезпечення національної безпеки. Європейська стратегія кібербезпеки (2020) [40] стимулює держав-членів до розробки національних підходів щодо використання відкритих джерел інформації для кіберрозвідки та аналізу загроз. У межах НАТО діяльність з використання OSINT є частиною оборонних операцій, спрямованих на підтримку безпеки союзників та моніторинг кримінальних загроз.

Регулювання OSINT у рамках забезпечення національної безпеки також пов’язане з міжнародними договорами у сфері кібербезпеки та інформаційної безпеки. Наприклад, Будапештська конвенція про кіберзлочинність (2001) є одним із важливих міжнародних документів, що регулює боротьбу з кіберзлочинністю та забезпечує можливість збору, обміну та аналізу інформації для протидії кіберзагрозам. OSINT стає елементом таких заходів, після чого відкриті джерела можуть використовуватися для ідентифікації та нейтралізації кібератак.

ООН також займає провідне місце у розробці рекомендацій щодо використання OSINT у контексті глобальної безпеки. Наприклад, Група урядових експертів ООН з питань інформаційної безпеки розробила низку рекомендацій для принципів державної влади щодо відповідної поведінки в кіберпросторі, у тому числі з використанням відкритих джерел інформації.

Важливим результатом співпраці держав у сфері інформаційної безпеки є резолюції Ради Безпеки ООН, зокрема резолюція 1373 (2001) [139], яка зобов’язує державу розробляти та впроваджувати заходи для запобігання тероризму, включаючи використання інформації з відкритих джерел для моніторингу терористичних загроз. Інші акти, такі як Резолюція 2178 (2014), закликають державу співпрацювати в обміні розвідувальною інформацією, що включає OSINT, для протидії загрозам, пов’язаним із тероризмом і насильницьким екстремізмом [204].

Так, у Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» від 4 грудня 1998 року [37] було ініційовано дискусію щодо формування принципово нової системи міжнародно-правового регулювання, одним із ключових компонентів якої в майбутньому мають стати інформація, інформаційні технології та способи їх застосування. У цьому документі міститься звернення до держав-членів сприяти розгляду на багатосторонньому рівні як наявних, так і потенційних викликів у сфері інформаційної безпеки, надати чіткі дефініції таких загроз, а також висловити власне бачення

проблематики, включаючи напрацювання міжнародних засад захисту глобальних інформаційних мереж [20].

Проблематика міжнародної інформаційної безпеки послідовно залишалася в центрі уваги наступних сесій Генеральної Асамблеї ООН, що підтверджується прийнятими резолюціями: A/RES/55/63 від 4 грудня 2000 р. та A/RES/56/121 від 19 грудня 2001 р. щодо протидії злочинному використанню інформаційних технологій; A/RES/57/239 від 20 грудня 2002 р. щодо формування глобальної культури кібербезпеки; A/RES/58/199 від 23 грудня 2003 р. і A/RES/64/211 від 21 грудня 2009 р. щодо створення глобальної культури кіберзахисту та охорони критичної інформаційної інфраструктури; A/RES/62/17 від 5 грудня 2007 р. щодо підтримки багатостороннього обговорення актуальних і потенційних загроз у сфері інформаційної безпеки; A/RES/71/28 від 5 грудня 2016 р. щодо прогресу у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки [20].

Міжнародні правові акти, що регулюють застосування OSINT у сфері національної безпеки, встановлюють основні принципи співпраці між державами, підтримки прав людини та захисту персональних даних. відповідно, такі акти, як Будапештська конвенція про кіберзлочинність, GDPR та резолюції Ради Безпеки ООН, забезпечують правову базу для ефективного та законного використання відкритих джерел інформації в інтересах національної безпеки.

Крім того, міжнародні правові акти встановлюють нормативні межі та етичні стандарти для використання OSINT у сфері національної безпеки. Вони забезпечують баланс між свободою доступу до інформації та захистом персональних даних, сприяють міжнародній співпраці у боротьбі з кіберзагрозами та тероризмом. Для ефективного застосування OSINT держава повинна гармонізувати національне законодавство з міжнародними стандартами, що дозволяє забезпечити правову визначеність та прозорість у цій сфері.

Таким чином, розбудова правової основи функціонування OSINT вимагає постійного оновлення національного законодавства, що має адаптуватися до швидко змінюваного характеру кіберзагроз. Ключовим елементом цього процесу є імплементація норм міжнародного права у сферах кібербезпеки та інформаційної безпеки, врахування глобальних загроз, а також забезпечення відповідності українських правових актів вимогам Європейського Союзу. Співпраця в межах Будапештської конвенції та інших міжнародних угод сприяє зміцненню національної безпеки, створюючи правові механізми для забезпечення ефективного функціонування OSINT.

Підсумовуючи вищенаведене, можемо загалом констатувати, що адміністративно-правове регулювання механізму адміністративно-правового забезпечення функціонування OSINT представляє собою взаємодіючу, комплексну багаторівневу систему, яка складається з таких елементів: конституційні положення та стратегічні документи; законодавчі акти, які регулюють правові аспекти забезпечення національної безпеки та направляють функціонування OSINT у цій сфері; інституційні нормативно-правові акти, які регулюють адміністративно-правовий статус суб'єктів здійснення OSINT, їх функцій, форми, методи та засоби діяльності і взаємодії; міжнародно-правові акти, які регулюють використання відкритих джерел інформації (OSINT) у контексті міжнародної безпеки та співпраці.

Ієрархічна структура нормативно-правових актів, що регулюють використання OSINT у сфері національної безпеки, забезпечує узгодженість між стратегічними, законодавчими та інституційними підходами. Вона створює чіткі правові рамки для координації діяльності державних органів та інших суб'єктів, залучених до функціонування OSINT, а також сприяння інтеграції України в міжнародну систему безпеки.

Ефективне функціонування OSINT (розвідки з відкритих джерел) потребує оновлення правової бази України, з урахуванням міжнародних стандартів і національних потреб. Одним із ключових напрямів удосконалення є розробка спеціалізованого закону про OSINT, який би визначав правові межі

збору, обробки та використання інформації з відкритих джерел з метою національної безпеки. Це дозволить уникнути правових колізій із законами про захист персональних даних та доступ до публічної інформації.

Необхідно запровадити механізми державного контролю за діяльністю суб'єктів OSINT, зокрема шляхом створення реєстрів та систем звітності для органів, що використовують такі дані. Важливим є встановлення чітких критеріїв відповідальності за неправомірне використання інформації, що може порушувати права людини та загрожувати національній безпеці.

Крім того, слід адаптувати законодавство до сучасних технологічних викликів, таких як використання штучного інтелекту та автоматизованих систем аналізу даних. Розширення міжнародної співпраці у сфері OSINT також вимагає імплементації норм міжнародного права та участі в угодах про обмін інформацією. Такі заходи сприятимуть підвищенню ефективності національної системи безпеки в умовах сучасних кіберзагроз.

Отже, ефективне функціонування системи OSINT у сфері національної безпеки України вимагає комплексного підходу, що охоплює як внутрішні, так і зовнішні загрози. Розвиток та вдосконалення правових і інституційних механізмів, які регулюють використання OSINT, є необхідною умовою забезпечення інформаційної безпеки держави та гарантією її сталого розвитку в умовах сучасного інформаційного середовища. Зважаючи на зростаючу важливість розвідки з відкритих джерел у протидії кіберзагрозам та підтримці стратегічних рішень, ключовими завданнями залишаються удосконалення нормативно-правової бази, що регулює функціонування OSINT, оптимізація координації між державними органами та підвищення рівня технологічної готовності до використання OSINT-інструментів.

Висновки до Розділу 1

У розділі проаналізовано загально-теоретичні засади адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Установлено, що наукові дослідження, присвячені функціонуванню OSINT у сфері національної безпеки, мають велике значення для розвитку адміністративного права та забезпечення державної безпеки. Вони сприяють формуванню ефективного механізму використання відкритих джерел інформації, що дає змогу оперативно реагувати на загрози національній безпеці. У сучасних умовах швидкого розвитку інформаційних технологій наукове обґрунтування адміністративно-правових засад функціонування OSINT у сфері національної безпеки стає надзвичайно актуальним. Дослідження у цій сфері дозволяють удосконалити методи управління та забезпечити системний підхід до забезпечення національної безпеки з використання розвідки з відкритих джерел.

Важливим напрямом подальших досліджень є розробка нових форм і методів адміністративно-правового регулювання OSINT у сфері національної безпеки, які б відповідали реаліям глобалізації та цифрової ери, імплементації міжнародного досвіду та розробки єдиних стандартів у правовому регулюванні здійснення OSINT суб’єктами забезпечення національної безпеки.

Національна безпека, як об’єкт адміністративно-правового забезпечення, охоплює кілька важливих напрямів і складових, таких як політична, економічна, інформаційна, соціальна, екологічна та військова безпека. Її стійкість забезпечується через оперативний моніторинг, запобігання загрозам та нейтралізацію факторів, що можуть порушити стабільність держави. Національна безпека та її адміністративно-правове забезпечення через функціонування OSINT є необхідною умовою для вчасного виявлення загроз та прийняття ефективних управлінських рішень з метою їх усунення.

Використання OSINT дає змогу державним органам здійснювати превентивні заходи для виявлення і вчасного усунення загроз у сфері національної безпеки, дозволяючи державі бути готовою до реагування на потенційні виклики і зміцнювати свою стійкість у сучасному інформаційному середовищі.

Адміністративно-правове регулювання функціонування OSINT у сфері національної безпеки України представляє собою комплексну багаторівневу систему законодавства. Вона охоплює конституційні положення, законодавчі акти, що визначають засади національної безпеки, а також нормативні документи, які регулюють діяльність суб'єктів OSINT. Важливим компонентом є міжнародні правові акти, які формують основи співпраці у сфері безпеки та регламентують доступ і використання відкритих джерел інформації. Така ієрархічна структура забезпечує узгодженість дій усіх суб'єктів, залучених до функціонування OSINT, та сприяє ефективній реалізації національних і міжнародних безпекових завдань. Забезпечення надійного функціонування OSINT потребує вдосконалення правової бази України, з урахуванням світових стандартів.

Особливо важливим є розроблення спеціалізованого законодавства, яке б регламентувало правові межі збору й використання інформації з відкритих джерел. Таке законодавство дозволить уникнути правових колізій з нормами про захист персональних даних та доступ до публічної інформації. Ефективне функціонування OSINT як інструмента національної безпеки вимагає адаптації до сучасних технологій і викликів. Це включає імплементацію норм міжнародного права, вдосконалення технологічної інфраструктури, впровадження штучного інтелекту для аналізу великих обсягів даних, а також посилення співпраці з міжнародними партнерами.

РОЗДІЛ 2
ХАРАКТЕРИСТИКА МЕХАНІЗМУ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ OSINT У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

2.1 Поняття механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки

На сьогодні вже сформовано певну теоретичну, методологічну та емпіричну базу для дослідження сутності та механізмів адміністративно-правового забезпечення різних складників національної безпеки, з урахуванням системного, інституційного, функціонального та інших підходів. Проте сучасні виклики, пов’язані з внутрішньополітичною ситуацією та зовнішньою геополітичною динамікою, а також особливості розвитку міжнародної, регіональної та глобальної безпеки вимагають безперервного оновлення та вдосконалення підходів до вивчення відповідних механізмів.

Актуальність дослідження механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки обумовлюється зростаючою роллю відкритих джерел інформації в сучасних умовах. Використання OSINT стає одним із ключових інструментів для перевірки загроз, аналізу ризиків та формування адекватних управлінських рішень у сфері національної безпеки. Однак необхідність оптимізації та вдосконалення функціонування OSINT у сучасних умовах потребує ретельного дослідження та розробки ефективного механізму адміністративно-правового забезпечення цієї сфери суспільних відносин. Одним із найбільш актуальних питань є впровадження єдиних стандартів збору, обробки та використання відкритої інформації. Крім того, важливим є забезпечення ефективної взаємодії між державними органами в процесі використання OSINT, що вимагає чіткого нормативного регулювання та розробки механізмів координації. Такий підхід дозволить вирішити низку інших проблем, зокрема

щодо удосконалення процедур і підвищення ефективності управлінських рішень.

Тому дослідження механізму адміністративно-правового забезпечення OSINT має за мету не лише заповнити наукові прогалини в цій галузі, але й сприяти досконалому законодавчому регулюванню та підвищенню ефективності функціонування здійснення розвідки з відкритих джерел в умовах сучасних викликів.

Забезпечення національної безпеки представляє собою комплексний процес, який потребує належного адміністративно-правового механізму його ефективної реалізації. Ця діяльність є важливою функцією держави, змістом якої є забезпечення функціонування системи національної безпеки. Система національної безпеки виступає як інституційно-правовий регулятор, що забезпечує створення умов для підтримки і захисту основних національних інтересів, а також управління та нейтралізацію наявних і потенційних загроз безпеці суспільства та держави [147, с. 355–357; 160, с. 126].

При цьому «підтримка стабільності та захисту» вказує на досягнення встановленого рівня захисту, що вимагає не лише збереження цього стану, але і його забезпечення на постійній основі [14, с. 32]. Це означає, що механізм забезпечення національної безпеки має включати не лише реагування на загрози, але й на здійснення превентивних заходів, спрямованих на їх попередження та мінімізацію ризиків.

Функціонування OSINT у сфері національної безпеки є важливим складником загального механізму адміністративно-правового забезпечення національної безпеки. Однак специфіка його мети, завдань, функцій та інших елементів визначає його самостійне і особливе значення в забезпеченні національної безпеки, зокрема в контексті швидкості реагування на загрози та ефективності обробки відкритої інформації для прийняття управлінських рішень.

Ключовим терміном досліджуваного нами механізму є поняття «забезпечення». Це змістовне поняття стало об’єктом досліджень багатьох

вчених, однак досі не існує єдиного його трактування. І це є закономірним, оскільки його інтерпретація залежить від конкретної сфери суспільних відносин, яка підлягає «забезпеченню». Відповідно, зміст цього поняття буде обумовлюватися змістом суспільних відносин. Важливість дослідження поняття «забезпечення» в межах нашої роботи зумовлена тим, що його змістовне наповнення безпосередньо впливатиме на сутність та складові механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Дослідження наукових джерел засвідчує, що термін «адміністративно-правове забезпечення» може тлумачитися з позицій двох основних підходів: розширеного та звуженого. У широкому сенсі адміністративно-правове забезпечення охоплює організацію суспільних зв'язків з боку уповноважених суб'єктів державної влади, їх нормативне закріплення через правові приписи, гарантування, втілення в практику та подальший розвиток. Натомість у вузькому розумінні зміст цього поняття варіюється залежно від характеру та специфіки суспільних відносин, які стають предметом правового регулювання [29, с. 48; 46; 167, с. 174].

У науковому дискурсі також представлені інші концептуальні підходи до трактування категорії «забезпечення», які відображають різні аспекти її змісту, зокрема:

– як упорядкування суспільних взаємин, що здійснюється державою через спеціально створений механізм, включаючи їх нормативне оформлення, охорону, реалізацію та подальший розвиток [58, с. 434];

– як наявність адміністративно-правових приписів і фактичний рівень їх втілення у практику суб'єктами, наділеними владно-управлінськими повноваженнями [46, с. 42];

– як діяльність органів, уповноважених державою, з виконання покладених на них функцій, а також результат цієї діяльності, який виражається у практичному втіленні правових норм, прав і свобод громадян [10, с. 7];

– як владний вплив держави на суспільні зв'язки з використанням усіх юридичних засобів з метою впорядкування, закріплення, охорони та розвитку, а також як вплив на поведінку та правосвідомість громадян через встановлення їх прав, обов'язків, дозволів, заборон і прийняття відповідних нормативних актів [110, с. 369];

– як упорядкування суспільних відносин за допомогою адміністративно-правових норм і комплексу відповідних засобів, спрямованих на нормативне закріплення, охорону, реалізацію й розвиток прав і свобод осіб у межах діяльності державних органів та органів місцевого самоврядування [76, с. 8];

– як адміністративно-правову базу впливу суб'єктів публічної влади на суспільні відносини у сфері державного управління, а також їхню діяльність, спрямовану на формування, застосування та вдосконалення цієї бази задля реалізації завдань адміністративного права [167, с. 178];

– як постійну фахову діяльність суб'єктів публічної адміністрації, яка здійснюється шляхом застосування адміністративно-правових методів та інструментів і спрямована на забезпечення належних умов для ефективної реалізації, захисту, охорони й поновлення прав і свобод громадян [154].

Крім того, у науці розглядають структуру адміністративно-правового забезпечення, виділяючи його ключові елементи: об'єкт адміністративно-правового забезпечення – ті суспільні відносини, на які спрямоване правове регулювання; суб'єкт адміністративно-правового забезпечення – органи або установи, уповноважені діяти адміністративно-правове регулювання; норми права, зокрема норми адміністративного права, що застосовують правила поведінки в цій сфері; адміністративно-правові відносини та їх зміст, що забезпечується процесом регулювання; гарантії, заходи, засоби, форми та методи адміністративно-правового забезпечення, що забезпечують ефективність цього механізму [29, с. 48; 46; 167, с. 174].

На наш погляд, під адміністративно-правовим супроводженням OSINT у контексті національної безпеки доцільно тлумачити діяльність уповноважених суб'єктів, що здійснюється на підставі норм

адміністративного законодавства, із застосуванням специфічного адміністративно-правового арсеналу (методів, прийомів, інструментів, процедур тощо), за допомогою яких реалізується адміністративно-правове впорядкування та нормативне унормування суспільних взаємовідносин у відповідній сфері, що підлягає такому регуляторному впливу [84].

У наведених підходах до тлумачення поняття «забезпечення» можна виділити кілька ключових аспектів:

1. Державний характер адміністративно-правового забезпечення. Більшість підходів визначають забезпечення як процес, що здійснюється саме державою, яка використовує відповідний правовий та адміністративний інструментарій для впорядкування суспільних відносин. Це означає, що адміністративно-правове забезпечення не є самостійним процесом, це частина більш широкої державної діяльності;

2. Цільове спрямування. Різні вчені виділяють як цілі адміністративно-правового забезпечення – юридичне закріплення, охорону, реалізацію та розвиток суспільних відносин. Це підкреслює не лише регуляторну, але й стабілізаційну функції адміністративно-правового забезпечення, що дозволяє праву ефективно діяти та реалізовуватися в суспільстві;

3. Адміністративно-правові норми. У кількох визначеннях акцентується на адміністративно-правових нормах та засобах, які формують юридичну основу забезпечення. Це свідчить про те, що саме адміністративне право є центральним у системі забезпечення, особливо коли йдеться про взаємодію органів влади із суспільством та громадянами;

4. Роль уповноважених органів. Поняття адміністративно-правового забезпечення охоплює діяльність уповноважених органів держави, які здійснюють свої функції, сприяючи реалізації правових норм і забезпеченню прав та свобод громадян. Така діяльність не лише формує, але й структурує суспільні відносини, забезпечуючи їх належний правовий порядок;

5. Владний вплив. Адміністративно-правове забезпечення розглядається як владний вплив держави на суспільні відносини, який реалізується через правові акти, проголошення прав і обов'язків громадян, встановлення дозволів та заборон. Це вказує на регулятивний характер забезпечення, який поєднує адміністративні та правові механізми.

Отже, адміністративно-правове забезпечення – це комплексний процес, що охоплює діяльність держави і її органів через використання правових та адміністративних інструментів для організації, захисту та реалізації суспільних відносин, прав і свобод громадян у правовому полі.

У контексті безпекового спрямування адміністративно-правове забезпечення орієнтоване на нейтралізацію та усунення загроз і викликів, що створюють передумови для виникнення небезпеки. У цьому процесі ключову роль відіграють державні інституції, наділені відповідними повноваженнями для здійснення цієї діяльності. Таким чином, адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки нерозривно пов'язане з діяльністю відповідних суб'єктів, регульованою нормами адміністративного права. Це забезпечення здійснюється за допомогою певних форм і засобів, що визначають його мету та завдання. З огляду на це, формою здійснення адміністративно-правового забезпечення є відповідний механізм.

Необхідно зосередити увагу і на тому, що зміст поняття «механізм адміністративно-правового забезпечення» передбачає обов'язкову наявність інституційної складової, що випливає з наведеної вище дефініції поняття адміністративно-правового забезпечення. Вивчаючи юридичні механізми, слід акцентувати на позицію науковців, які структурують їх у два основні взаємопов'язані елементи: правову основу, що охоплює комплекс правових засобів, та інституційний блок, до якого входять відповідні органи і владні структури, що здійснюють адміністративно-правове забезпечення.

У сфері науки адміністративного права існують різноманітні підходи до розуміння механізму адміністративно-правового забезпечення, які зокрема інтерпретуються як:

– сукупність інструментів, що становлять елементи впливу цієї правової галузі на суспільні взаємини та закріплені її нормативною базою гарантії реалізації прав (зокрема поновлення прав у виконавчих органах і судах, захист через адміністративну відповідальність і прокурорський контроль) [47];

– упорядкована система правових засобів, які надають компетентним суб'єктам змогу належно розвивати та результативно реалізовувати покладені на них функції через організаційно-правові дії та адміністративний примус [2, с. 7; 60, с. 41];

– комплекс, сформований юридичними й фізичними особами, завдяки діям яких забезпечення набуває форми, функціонує та вдосконалюється, а також включає принципи, підходи, методи адміністративного регулювання та управлінські механізми [167, с. 174];

– сукупність суб'єктів, наділених владними повноваженнями (державними органами та управлінськими структурами), які застосовують правові інструменти з метою впливу на соціальні відносини в інтересах громадян і юридичних осіб [98, с. 145];

– набір правових засобів, які дозволяють узгоджувати поведінку учасників суспільних зв'язків із вимогами та дозволами, визначеними нормами чинного права [41, с. 218–220];

– система адміністративно-правових інструментів, орієнтованих на впорядкування суспільних зв'язків, що функціонує як послідовний процес з визначеними етапами реалізації та структурними компонентами [38, с. 14];

– особливі адміністративно-правові інструменти, зокрема норми адміністративного права, адміністративно-правові відносини, акти тлумачення адміністративно-правових норм, а також акти їх реалізації, що впливають на відповідні відносини в межах здійснення функцій державної виконавчої влади [79, с. 37].

Аналіз наведених підходів до трактування механізму адміністративно-правового забезпечення свідчить про багатовимірний характер цього поняття, що відображає різні аспекти правового впливу адміністративного права на суспільні відносини. Ключовими характеристиками механізму адміністративно-правового забезпечення виступають його системність, структурованість, наявність правових засобів, що використовуються уповноваженими суб'єктами, а також визначення цільового спрямування дії таких засобів.

З наведених вище визначень можна виокремити кілька основних підходів до тлумачення досліджуваного поняття, що дозволяє глибше розкрити його сутність та значення в контексті адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Так, одні вчені розглядають цей механізм як систему засобів впливу, спрямованих на гарантування реалізації прав громадян, забезпечених відповідними нормами адміністративного права. Сюди відносяться засоби поновлення в правах через органи виконавчої влади та суди, а також механізми адміністративної відповідальності та прокурорського нагляду. Це трактування акцентує увагу на захисній функції механізму забезпечення.

Другий підхід визначає механізм як систему правових інструментів, організованих для забезпечення ефективної діяльності уповноважених суб'єктів за допомогою організаційно-правових заходів та адміністративного примусу. Такий підхід підкреслює організаційну складову механізму, де центральне місце відведене інструментам, що полегшують функціонування державних інституцій.

Третє визначення розглядає механізм як комплексну систему суб'єктів та інструментів, до складу якої входять не лише державні органи, а й фізичні та юридичні особи, діяльність яких сприяє реалізації адміністративно-правового забезпечення у відповідній сфері. Тут важливими компонентами є принципи, форми та методи адміністративного регулювання, а також

управлінські технології, що створюють основу для правового впливу. Цей підхід зосереджує увагу на суб'єктно-інституційному складі механізму.

Четверте визначення зосереджено на системі суб'єктів, що наділені владними повноваженнями. Такий механізм включає органи державної влади, що впливають на суспільні відносини в інтересах фізичних та юридичних осіб. Сюди входять повноваження органів державного управління, які мають забезпечувати адміністративно-правовий вплив на суспільні відносини.

Наступний підхід розглядає механізм як сукупність правових засобів, за допомогою яких поведінка суб'єктів узгоджується з вимогами права. Це визначення звертає увагу на регулятивну роль правових норм, які дисциплінують і контролюють суспільні відносини.

Нарешті, механізм адміністративно-правового забезпечення розглядається як система правових засобів, організованих у процес із визначеними стадіями. Це трактування підкреслює етапність та структурованість процесу реалізації адміністративно-правового впливу, що дозволяє забезпечити комплексний підхід до регулювання суспільних відносин.

Отже, механізм адміністративно-правового забезпечення є багатокомпонентною системою, що включає правові та інституційні елементи, а також засоби впливу на суспільні відносини з метою захисту прав громадян та забезпечення ефективного функціонування державних інституцій. При цьому такий вплив здійснюється з використанням адміністративно-правового інструментарію, норм адміністративного права та у зв'язку із здійсненням відповідними суб'єктами публічно-владної діяльності.

З урахуванням вищевикладеного, механізм адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки можна визначити як комплекс правових і організаційних засобів, через які здійснюється вплив адміністративного права на суспільні відносини в сфері безпеки. Цей механізм включає сукупність правових інструментів, спрямованих на забезпечення виконання завдань, що постають перед

уповноваженими суб'єктами – органами, які здійснюють правоохоронну діяльність, розвідувальними та контррозвідувальними органами, силами безпеки та оборони та іншими інституціями, наділеними відповідними повноваженнями здійснення розвідки з відкритих джерел. Він охоплює системні засоби, що регулюють діяльність вищеназваних суб'єктів, правові гарантії, форми та методи адміністративно-правового регулювання, заходи адміністративного примусу тощо.

Таким чином, механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки притаманні наступні властивості. По-перше, правові засоби, тобто набір правових норм та інструментів, що формують правове підґрунтя для функціонування OSINT, визначають правомірну поведінку суб'єктів, а також установлюють способи адміністративного примусу та правового захисту у разі порушень. По-друге, інституційний блок – система державних органів та інших інституцій, що мають повноваження в галузі національної безпеки та забезпечують реалізацію норм адміністративного права в контексті діяльності OSINT. По-третє, організаційно-правові заходи – структурування і координація дій суб'єктів, що реалізують адміністративно-правове забезпечення OSINT, а також управлінські технології та методи, що забезпечують узгоджене функціонування системи. По-четверте, відповідна сфера суспільних відносин – національна безпека.

Відповідно, механізм адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки – це складна система взаємопов'язаних правових, організаційних і процедурних засобів, спрямованих на підтримку національної безпеки шляхом впорядкування, регулювання та контролю діяльності суб'єктів, що здійснюють розвідку з відкритих джерел.

Наступним важливим моментом є питання структури досліджуваного механізму та його складових елементів, які визначають функціонування і ефективність усієї системи адміністративно-правового забезпечення.

Структура адміністративно-правового механізму не має однозначного визначення. Кожен дослідник пропонує власний склад елементів, що призводить до різноманіття поглядів, багато з яких є дискусійними. Аналізуючи наукові джерела, можна дійти висновку, що найбільш поширеними є підходи, в яких дослідники виокремлюють кілька масштабних груп елементів: об'єкт адміністративно-правового забезпечення; суб'єкти адміністративно-правового забезпечення; принципи права, норми права, правовідносини, їх зміст, види, структура та особливості реалізації; гарантії, заходи, засоби форми, принципи та методи правового забезпечення [23].

Зокрема, З. С. Гладун у структурі адміністративно-правового регулювання пропонує розрізняти елементи механізму та його функціональні складові. Серед елементів він виокремлює: норми права – загальнообов'язкові правила поведінки, встановлені для регулювання адміністративно-правових відносин; акти реалізації норм права – процес фактичного втілення нормативних приписів у практичну діяльність суб'єктів адміністративного права; правові відносини – вольові суспільні зв'язки, що створюються на основі чинних правових норм. До функціональних складових частин адміністративно-правового механізму З. С Гладун пропонує відносити: юридичні факти – обставини, що зумовлюють виникнення, зміну або припинення правових відносин; правову свідомість і правову культуру – рівень розуміння і прийняття права суб'єктами правовідносин; законність – принцип неухильного дотримання правових норм усіма учасниками правових відносин; акти тлумачення норм права – офіційні роз'яснення змісту правових норм; акти застосування норм права – окремі рішення органів влади, спрямовані на реалізацію конкретних правових норм у певних ситуаціях [27, с. 10].

Таким чином, підхід З. С. Гладуна дозволяє комплексно охарактеризувати механізм адміністративно-правового регулювання, враховуючи як його структурні, так і функціональні елементи, що забезпечує

всебічне розуміння процесу регулювання та його ефективність у конкретних умовах.

Аналогічний підхід пропонує й Т. О. Коломоєць, яка структурує складові механізми адміністративно-правового регулювання на дві групи: органічні та функціональні. До органічних складових учена відносить: норми права – засадничі правила, що виконують поведінку учасників адміністративних відносин; акти реалізації норм права – практична реалізація правових приписів суб'єктами адміністративного права; правові відносини – суспільні зв'язки, що забезпечують взаємодію у процесі суб'єктів на основі норм адміністративного права. Натомість до функціональних складових, на думку Т. О. Коломоєць, відносяться: юридичні факти – сутності, що породжують, змінюють або припиняють правові відносини; правова свідомість суб'єктів – рівень відомості та внутрішнього прийняття правових норм суб'єктами адміністративно-правових відносин; законність – принцип дотримання правових норм у процесі регулювання суспільних відносин; акти тлумачення норм права – офіційні роз'яснення змісту та обсягу правових норм; акти застосування норми права – індивідуально-конкретні рішення, що забезпечують реалізацію норми права в конкретних випадках [4, с. 24].

О. М. Гумін та Є. В. Пряхін пропонують власне бачення структури механізму адміністративно-правового забезпечення, яка включає п'ять ключових елементів: об'єкт адміністративно-правового забезпечення – сфера чи суспільні відносини, на які спрямоване адміністративно-правове регулювання; суб'єкт адміністративно-правового забезпечення – органи чи особи, уповноважені виконувати адміністративно-правове регулювання та контроль; норми адміністративного права – правові приписи, які встановлюють порядок взаємодії суб'єктів та об'єктів адміністративного права; адміністративно-правові відносини та їх зміст – зв'язки між суб'єктами, що створюються на основі норм адміністративного права, включаючи їх права, обов'язки та юридичні наслідки; гарантії, заходи, засоби, форми та методи адміністративно-правового забезпечення – механізми та інструменти, що

забезпечують ефективність правозастосування й досягнення цілей адміністративно-правового регулювання [29, с. 49].

Отже, така структуризація відображає комплексний підхід до адміністративно-правового забезпечення, підкреслюючи взаємозв'язок між нормативною базою, суб'єктами й об'єктами правовідносин та інструментами їх реалізації.

Інші дослідники виокремлюють у механізмі адміністративно-правового забезпечення відносно статичні елементи (норми права; державні органи та органи місцевого самоврядування) та динамічні (реалізація, охорона та захист) [172, с. 69]. Водночас існує підхід, який пропонує структуру юридичних механізмів, що включає два тісно взаємопов'язані елементи: правову основу, сформовану із сукупності правових засобів, та інституційний блок, до якого входить структура і діяльність відповідальних органів та державно-владних установ [9].

К. Г. Волинка вважає за доцільне виділяти такі складові категорії забезпечення прав і свобод: нормативно-правові передумови – закріплені в правових актах права, свободи та обов'язки особи, що вступає в її правовий статус; нормативно-правові засоби забезпечення прав і свобод, до яких належать юридичні гарантії, що сприяють реалізації та захисту цих прав; загальносоціальні умови – фактори, що впливають на реалізацію, охорону та захист прав і свобод особи в суспільстві [21, с. 65].

Аналіз наукових підходів до структури адміністративно-правового механізму свідчить про наявність різноманіття думок серед дослідників, що дозволяє виділити два основні напрями. Перший полягає у виокремленні статичних і динамічних елементів механізму адміністративно-правового забезпечення (норми, органи, форми реалізації та захисту), як це роблять З. С. Гладун та Т. О. Коломоєць. Другий підхід, представлений роботами О. М. Гуміна, Є. В. Пряхіна та К. Г. Волинки, акцентує увагу на комплексному, взаємопов'язаному механізмі, що включає об'єкти, суб'єкти, правові норми, правовідносини, гарантії та засоби правозастосування. Цей

підхід відображає прагнення систематизувати механізм через виокремлення взаємодіючих компонентів, що сприяють реалізації адміністративно-правових відносин.

Існують також і інші альтернативні погляди на механізм адміністративно-правового забезпечення. Зокрема, К. В. Барсуков пов'язує цей термін із діяльністю органів державної влади, завдяки якій забезпечується правозастосування та захист прав, свобод і інтересів громадян [10, с. 7]. На нашу думку, такий підхід акцентує перевагу правореалізації над правотворчістю, що обумовлено специфікою предмета дослідження, пов'язаного з відносинами, які виникають у процесі роботи правоохоронних органів у складі міжнародних миротворчих підрозділів. Натомість «класичні» підходи до визначення досліджуваного нами поняття ґрунтуються на владному впливі держави на суспільні відносини та їх учасників, шляхом установлення певних правил і обмежень задля впорядкування цих відносин [42, с. 327; 110, с. 369; 173]. Як бачимо, альтернативні погляди дослідників акцентують увагу на діяльності державних органів як забезпечувальному чиннику адміністративно-правових відносин.

Виходячи з аналізу вищевикладеного та базуючись на загальних положеннях адміністративного права України, розглянемо структуру механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Предметом регулювання адміністративного права виступають суспільні відносини, що формуються між представниками публічної адміністрації та приватними особами, а зміст цього регуляторного впливу полягає у наданні адміністративних послуг, реалізації адміністративних процедур і здійсненні виконавчо-розпорядчих функцій з боку органів публічної влади.

Адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки можна визначити як комплекс заходів і правових інструментів, що здійснюються з метою регулювання та захисту відносин, пов'язаних з обробкою відкритих джерел інформації для забезпечення

державної безпеки. Цей механізм включає систему норм, що регламентують допустимі методи збору та аналізу інформації, правовий статус суб'єктів OSINT, а також процедури захисту інформаційних прав громадян.

Структурно адміністративно-правовий механізм забезпечення OSINT у сфері національної безпеки складається з таких елементів: нормативна основа – правові акти, норми та принципи, що регулюють порядок збору та використання інформації з відкритих джерел; суб'єкти регулювання – органи національної безпеки, правоохоронні органи, а також інші уповноважені суб'єкти, що мають повноваження здійснювати розвідку з відкритих джерел; правовідносини – взаємовідносини між суб'єктами та об'єктами OSINT, які забезпечують законне використання інформації в інтересах національної безпеки; забезпечувальні засоби та заходи – спеціальні адміністративні процедури, методи та технології, що сприяють ефективному виконанню OSINT-операцій, включаючи інформаційні та технічні ресурси; гарантії дотримання прав та свобод – заходи, що гарантують законність застосування OSINT та захист інформаційних прав громадян, зокрема право на приватність та захист персональних даних.

Важливим елементом структури механізму функціонування OSINT у сфері національної безпеки є об'єкт адміністративно-правового забезпечення, яким зазвичай виступають суспільні відносини.

Ці суспільні відносини виникають у процесі здійснення діяльності з пошуку, аналізу та використання з відкритих джерел інформації, спрямованої на виявлення та оцінку загроз національній безпеці. Ці суспільні відносини, що є об'єктом адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, можна поділити на такі напрями:

1. Правовідносини у сфері інформаційної діяльності: охоплюють регулювання прав та обов'язків суб'єктів, що здійснюють збір, аналіз та обробку інформації з відкритих джерел, а також відповідальність за недотримання стандартів у цій сфері. Ці відносини включають, зокрема,

питання доступу до інформації, її збереження, конфіденційності та правомірного використання даних;

2. Організаційні відносини у сфері координації діяльності суб'єктів OSINT: мають за мету забезпечити ефективну взаємодію між державними органами, уповноваженими на здійснення діяльності у сфері національної безпеки, а також їх координацію з іншими організаціями, які можуть брати участь у діяльності з відкритих джерел (аналітичні центри, наукові установи тощо). Важливим аспектом цих відносин є забезпечення чіткого розподілу функцій, відповідальності та каналів комунікації;

3. Відносини контролю та нагляду: охоплюють питання нагляду за дотриманням норм і стандартів у процесі здійснення OSINT-діяльності. Механізми контролю та відповідальності сприяють дотриманню законодавчих вимог щодо збереження приватності, захисту персональних даних, а також відповідальності суб'єктів за порушення правових норм;

4. Відносини правового захисту та безпеки: включають заходи, спрямовані на забезпечення захисту суб'єктів OSINT від потенційних зовнішніх загроз, таких як кібератаки, спроби втручання або маніпуляцій з відкритими джерелами інформації. Ці відносини спрямовані на забезпечення інформаційної стійкості та безпеки в умовах кібернетичних ризиків.

Таким чином, суспільні відносини, що складають об'єкт адміністративно-правового забезпечення OSINT у сфері національної безпеки, є складною системою, яка охоплює різноманітні напрями діяльності. У своїй сукупності ці напрями спрямовані на забезпечення ефективного та належного функціонування OSINT у зазначеній сфері, враховуючи специфіку завдань і загроз, що постають перед національною безпекою.

Відповідно до наведеного визначення основні елементи механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки включають: нормативні засади адміністративно-правового регулювання OSINT (принципи та норми права, що визначають правила використання відкритих джерел інформації); об'єкт адміністративно-

правового забезпечення OSINT (правовідносини, що виникають у процесі використання відкритої інформації, їх зміст, типи та особливості реалізації); суб'єктів адміністративно-правового забезпечення OSINT (органи, уповноважені на здійснення відповідної діяльності); а також засоби адміністративно-правового забезпечення OSINT (методи і заходи, спрямовані на ефективне функціонування цієї системи в інтересах національної безпеки).

Запропонований механізм дозволяє, по-перше, створити ефективну систему адміністративно-правового забезпечення виконання завдань у сфері національної безпеки, пов'язаних із здійсненням розвідки з відкритих джерел, з урахуванням потреб сучасного суспільства та етичних вимог щодо збереження приватності в умовах глобалізованого інформаційного простору; по-друге, забезпечувати системність і всебічне врахування факторів, необхідних для ефективного функціонування OSINT у сфері національної безпеки.

Нормативні засади адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки є фундаментальним елементом досліджуваного механізму. Вони формують правове підґрунтя для організації й функціонування OSINT, а також визначають межі правомірної діяльності у сфері використання відкритих джерел інформації з метою забезпечення національної безпеки. До основних складових нормативних засад можна віднести наступне:

1. Принципи права, які встановлюють загальні правові орієнтири для функціонування OSINT, що включають принципи законності, пропорційності, відкритості та інших засад, пов'язаних з дотриманням прав людини. Принцип законності вимагає, щоб діяльність у сфері OSINT була чітко врегульована законодавчими нормами, що визначають права й обов'язки суб'єктів цієї діяльності. Принцип пропорційності забезпечує баланс між національною безпекою та правами громадян, передбачаючи, що заходи з використання відкритих джерел не повинні порушувати основоположні права та свободи.

Принцип відкритості передбачає, що основні аспекти діяльності OSINT мають бути зрозумілими та передбачуваними для суспільства;

2. Норми права спрямовані конкретизувати правила, обов'язки і процедури функціонування OSINT, визначають, хто має право використовувати відкриті джерела для збору інформації, які методи дозволено застосовувати, а також які обмеження та заборони діють у цій сфері. До основних видів правових норм у цій галузі можна віднести: матеріальні норми: визначають права та обов'язки суб'єктів, які здійснюють OSINT, зокрема щодо доступу до відкритих джерел, способів обробки отриманої інформації та зобов'язань щодо захисту конфіденційної або персональної інформації; процесуальні норми: встановлюють процедурні аспекти здійснення OSINT, включаючи порядок збору, обробки та передачі даних, а також вимоги до звітності й надання результатів аналітичної обробки;

3. Правовий статус та повноваження суб'єктів OSINT, визначені нормами адміністративного права, забезпечують органам і організаціям можливість здійснювати OSINT у сфері національної безпеки. Ці норми регламентують обсяг їхніх прав, повноважень і відповідальності. Важливим аспектом є також чітке розмежування функцій і повноважень між різними органами, що сприяє уникненню дублювання завдань і підвищенню ефективності їхньої діяльності в цій сфері;

4. Міжнародні стандарти та правові акти є важливою складовою механізму, оскільки у зв'язку з глобальним характером сучасної інформаційної діяльності, правове регулювання OSINT має враховувати міжнародні стандарти та угоди, що регламентують питання використання відкритих джерел, обміну даними, захисту прав людини й забезпечення безпеки інформації. Імплементація міжнародних стандартів у національне законодавство є важливим кроком для підвищення легітимності та результативності OSINT у забезпеченні національної безпеки.

Таким чином, нормативні засади адміністративно-правового регулювання OSINT у сфері національної безпеки включають принципи,

матеріальні й процесуальні норми, що регулюють діяльність із відкритими джерелами інформації, а також норми міжнародного права. Ці засади сприяють забезпеченню законності та прозорості OSINT, створюють умови для його ефективного функціонування та дозволяють дотримуватися балансу між захистом національних інтересів і правами громадян.

Суб'єкти адміністративно-правового забезпечення OSINT, до яких належать органи державної влади та інші інституції, уповноважені здійснювати діяльність у сфері збирання, аналізу й обробки інформації з відкритих джерел, відіграють ключову роль у функціонуванні механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки. Їхня діяльність спрямована на виявлення, прогнозування та нейтралізацію загроз, що можуть створювати загрози національній безпеці. Кожен суб'єкт OSINT має власні повноваження та компетенції, визначені законодавством, що дозволяє уникнути дублювання функцій і підвищити ефективність взаємодії між ними. До основних суб'єктів здійснення OSINT можна віднести:

1. Службу безпеки України (СБУ) – центральний орган, який здійснює розвідувальну діяльність з використанням OSINT для виявлення загроз національній безпеці, зокрема таких, що пов'язані з тероризмом, кіберзлочинністю, контррозвідувальною діяльністю та зовнішніми загрозами. Основними повноваженнями СБУ у сфері OSINT є: здійснення збору та аналізу інформації з відкритих джерел, зокрема соціальних мереж, медіа, наукових та аналітичних ресурсів; проведення інформаційного моніторингу для раннього виявлення потенційних загроз і прогнозування їх впливу на національну безпеку; забезпечення взаємодії з іншими розвідувальними службами на національному та міжнародному рівнях для обміну OSINT-даними, що мають значення для безпеки України;

2. Міністерство внутрішніх справ України. Діяльність МВС України у сфері OSINT спрямована на забезпечення правопорядку, протидію злочинності, особливо організованій та транснаціональній, а також забезпечення публічної безпеки. Повноваженнями МВС України щодо OSINT

є: здійснення моніторингу відкритих джерел, що можуть містити інформацію про кримінальні або екстремістські загрози; використання OSINT для розробки профілактичних заходів щодо злочинності та прогнозування криміногенної ситуації; взаємодія з іноземними правоохоронними органами для обміну інформацією з відкритих джерел, що може допомогти у розслідуванні злочинів міжнародного характеру;

3. Національна поліція України – ключовий суб'єкт, відповідальний за профілактику правопорушень, а також за оперативне реагування на злочини, що становлять загрозу для громадського порядку. Використання OSINT є важливим інструментом для забезпечення публічної безпеки та здійснення діяльності, пов'язаної з розкриттям та розслідуванням кримінальних правопорушень. Основні повноваження Національної поліції включають: здійснення моніторингу соціальних мереж, інтернет-ресурсів та інших публічних джерел для виявлення злочинної діяльності або її ознак; використання OSINT у кримінальних розслідуваннях для збору доказів і визначення кола підозрюваних; забезпечення обміну інформацією з іншими державними та міжнародними структурами, що використовують OSINT для боротьби зі злочинністю;

4. Розвідувальні органи України (зокрема, Головне управління розвідки Міністерства оборони України). З огляду на військові загрози, які постійно стоять перед Україною, розвідувальні органи активно використовують OSINT для отримання даних про стан і переміщення збройних сил потенційних противників, а також для моніторингу інформаційного простору. Основні повноваження цих органів включають: збір і аналіз відкритих даних про діяльність збройних сил інших держав, зокрема, інформації з військових ресурсів, офіційних заяв і відкритих міжнародних джерел; моніторинг медіапростору з метою ідентифікації пропагандистських кампаній, дезінформації, яка може впливати на національну безпеку; взаємодія з міжнародними розвідувальними партнерами для обміну OSINT, що сприяє своєчасному виявленню військових загроз;

5. Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) – відіграє ключову роль у забезпеченні інформаційної безпеки та захисту інформаційних систем. У сфері OSINT ДССЗЗІ здійснює: моніторинг публічних джерел для виявлення інформаційних загроз, зокрема у вигляді кіберзагроз, що можуть бути спрямовані на державні інформаційні ресурси; розробку рекомендацій щодо захисту інформаційних систем і ресурсів, які використовують OSINT, від потенційних загроз; взаємодію з національними та міжнародними організаціями для запобігання кіберзлочинам, які можуть загрожувати безпеці інформаційної інфраструктури України;

6. Інші державні та недержавні установи, до яких можна віднести науково-дослідні установи, аналітичні центри та комерційні організації, що беруть участь у наданні даних з відкритих джерел на підставі укладених договорів чи партнерських відносин. Їхні повноваження включають: проведення досліджень і надання аналітичної інформації для державних органів з використанням OSINT; взаємодія з державними структурами для забезпечення безперервного потоку даних та інформаційної підтримки аналітичних процесів.

Таким чином, суб'єкти адміністративно-правового забезпечення OSINT в Україні представляють собою складну систему органів та посадових осіб цих органів, що мають повноваження на здійснення правоохоронної, розвідувальної та контррозвідувальної діяльності, а також включають в себе спеціалізовані наукові та аналітичні центри. Повноваження цих суб'єктів охоплюють збір, аналіз та обробку інформації з відкритих джерел, що створює комплексну систему моніторингу та реагування на загрози у сфері національної безпеки.

Засоби адміністративно-правового забезпечення OSINT складаються із методів, прийомів та способів, використання яких дозволяє забезпечувати ефективний збір, аналіз, обробку тощо інформації з відкритих джерел, а також функціонування самої системи OSINT. Відповідні засоби та методи формують практичну основу для організації процесів збору, обробки та аналізу відкритої

інформації з метою своєчасного виявлення потенційних загроз національної безпеки. До основних засобів адміністративно-правового забезпечення OSINT належать:

1. Організаційно-правові заходи – передбачають створення спеціалізованих підрозділів або відділів, які займаються діяльністю OSINT у державних органах, відповідальних за національну безпеку. Вони також охоплюють нормативне забезпечення процедури взаємодії між різними органами, які використовують OSINT. Організаційно-правові заходи можуть включати визначення функцій і повноважень кожного суб'єкта OSINT, що сприяє ефективній координації діяльності, уникненню дублювання функцій і підвищенню результативності аналітичної роботи;

2. Інформаційно-аналітичні методи – забезпечують оперативний збір, систематизацію, аналіз та перевірку інформації, що отримується з відкритих джерел. Серед найбільш поширених методів можна виділити такі, як: по-перше, методи збору даних, наприклад такі, як сканування відкритих баз даних, медіаресурсів, соціальних мереж, наукових та аналітичних джерел для отримання необхідної інформації, що стосується загроз національній безпеці. По-друге, методи аналізу даних, які включають застосування алгоритмів машинного навчання та штучного інтелекту, і які допомагають визначати закономірності, прогнозувати загрози й виявляти потенційно небезпечні тенденції. Крім того, використовуються методи порівняльного аналізу, що дозволяють зіставляти інформацію з різних джерел для перевірки її достовірності та виявлення можливих розбіжностей. По-третє, інструменти візуалізації даних, такі як графічне відображення інформації та створення інфографік, що підвищує зручність і швидкість сприйняття складної інформації, яка може бути корисною для прийняття управлінських рішень у сфері національної безпеки;

3. Методи контролю та моніторингу – забезпечують здійснення постійного моніторингу інформаційного середовища з метою виявлення нових загроз і ризиків, що можуть створити небезпеку. До цих методів належать

моніторинг медіапростору, соціальних мереж, форумів та інших відкритих платформ, що здійснюється з метою фіксації та аналізу інформації, яка може свідчити про загрози національній безпеці. Використання цих методів дозволяє побудувати систему раннього попередження загроз у сфері національної безпеки, та забезпечити оперативне реагування на потенційні небезпеки шляхом своєчасного збору та обробки даних;

4. Забезпечення захисту інформаційної безпеки. Ця особлива група методів включає заходи з охорони інформаційних ресурсів і даних, отриманих у процесі OSINT, від несанкціонованого доступу, маніпуляцій або кібератак. Ці методи є важливою складовою забезпечення захисту інформації, адже OSINT передбачає роботу з великою кількістю інформації, зокрема такої, що може містити дані про загрози національній безпеці. Засоби захисту включають використання шифрування, захисту від вірусів та шкідливих програм, а також обмеження доступу до конфіденційної інформації;

5. Міжнародні методи співпраці та обміну даними. У зв'язку з тим, що загрози національній безпеці можуть мати міжнародний характер, ефективне функціонування OSINT вимагає тісної співпраці з міжнародними партнерами. Це включає обмін інформацією з закордонними розвідувальними органами, участь у міжнародних інформаційних мережах та узгодження стандартів OSINT. Міжнародна співпраця також сприяє підвищенню ефективності аналітичної діяльності за рахунок отримання актуальних даних та обміну передовими практиками.

Таким чином, засоби адміністративно-правового забезпечення OSINT у сфері національної безпеки є сукупністю організаційних, інформаційно-аналітичних, контрольних та захисних заходів, що сприяють належному функціонуванню механізму OSINT.

Вони створюють умови для ефективного й правомірного використання відкритих джерел інформації та забезпечення належного захисту національних інтересів в умовах сучасних інформаційних викликів.

Підсумовуючи вищенаведене, можемо зробити такі висновки і узагальнення.

Зростаюча роль здійснення розвідки з відкритих джерел інформації обумовлює необхідність ефективного правового регулювання цієї діяльності, особливо в умовах наявних загроз та викликів у сфері національної безпеки. Використання OSINT дозволяє своєчасно виявляти потенційні загрози та аналізувати ризики, а тому відповідна діяльність повинна бути ефективною, чіткою та злагодженою. Це можливо досягти завдяки відповідному механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Важливість розробки та використання ефективного механізму адміністративно-правового забезпечення OSINT полягає у тому, що він завдяки комплексності та системному функціонуванню елементів, передбачає належне нормативно-правове регулювання, повноваження відповідних суб’єктів, інституційні зв’язки та засоби контролю, а також методи реагування на загрози та виклики. Це дає змогу створити дієву систему, яка не лише захищає інтереси держава та права громадян від загроз та викликів, але й забезпечує ефективну діяльність та координацію суб’єктів у сфері національної безпеки.

Адміністративно-правове забезпечення функціонування OSINT у сфері національної безпеки представляє собою багатовекторну діяльність уповноважених державних органів, що мають повноваження здійснювати розвідку з відкритих джерел, спрямовану на впорядкування, юридичне закріплення, охорону та реалізацію процесів збирання, аналізу та використання відкритих джерел інформації з метою захисту національних інтересів. Вона включає адміністративно-правові норми і засоби, що встановлюють правові основи для збору, обробки та використання відкритих даних, а також забезпечують нагляд та контроль за їх відповідністю цілям національної безпеки і правам громадян.

Механізм адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки можна розглядати як комплексну систему правових, організаційних, технічних та інформаційно-аналітичних заходів, що застосовуються компетентними органами публічної адміністрації з метою створення умов для ефективного здійснення розвідки з відкритих джерел. Ці заходи спрямовані на регулювання суспільних відносин, пов'язаних із використанням відкритих джерел інформації з метою своєчасного виявлення загроз національній безпеці та забезпечення охорони життєво важливих інтересів держави та суспільства, прав і свобод громадян у цій сфері. Структура механізму адміністративно-правового забезпечення визначається специфікою суспільних відносин, які виникають у процесі використання OSINT у контексті забезпечення національної безпеки.

Основними елементами механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки визначено: нормативні засади, які включають принципи та норми права, що регулюють здійснення розвідки з відкритих джерел інформації; об'єкт адміністративно-правового забезпечення функціонування OSINT, тобто правовідносини, що виникають у процесі здійснення розвідки з відкритих джерел, їх зміст, види та специфіка реалізації, яка обумовлена сферою національної безпеки; суб'єкти адміністративно-правового забезпечення, які уповноважені забезпечувати ефективне функціонування OSINT, та ті, що здійснюють розвідку з відкритих джерел; а також засоби та методи, що забезпечують здійснення розвідки з відкритих джерел, а також збір, аналіз, обробку, зберігання та використання інформації, отриманої внаслідок здійснення такої розвідки.

2.2 Суб'єкти механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки

Механізм адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки виступає складною правовою та організаційною системою, яка включає різноманітні елементи, що забезпечують її ефективність. Серед ключових компонентів такого механізму особливе місце займають суб'єкти, які прямо чи опосередковано беруть участь у забезпеченні процесів збору, обробки, аналізу та використання інформації з відкритих джерел. У контексті національної безпеки ці суб'єкти є не просто технічними чи виконавчими елементами, а відіграють системотвірну роль, що визначає ступінь організованості та ефективності відповідної функції держави із забезпечення національної безпеки.

Суб'єкти механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки можна поділити на кілька основних категорій. До першої групи належать державні органи, які здійснюють правове регулювання та визначають засади державної політики у сфері національної безпеки. До таких суб'єктів можна віднести Верховну Раду України, Президента України та Кабінет Міністрів України.

Другу групу становлять суб'єкти, які здійснюють загальне керівництво та спрямовують діяльність системи суб'єктів, що здійснюють розвідку з відкритих джерел. До цих суб'єктів відносяться: Рада національної безпеки і оборони, Міністерство інформаційної політики України, Міністерство оборони.

До третьої групи належать державні органи (посадові особи), уповноважені безпосередньо здійснювати збір, обробку та аналіз інформації з відкритих джерел. До таких суб'єктів відносяться, зокрема, підрозділи спеціальних служб, правоохоронних органів та органів виконавчої влади, які мають відповідні повноваження на підставі законодавства. Четверта група включає суб'єктів приватного права, тобто органи, установи та фахівців, що

спеціалізуються на інформаційному аналізі, виконують завдання з моніторингу відкритих джерел і можуть діяти за контрактом з державою. Окрім них, існують також міжнародні та громадські організації, які можуть надавати необхідну аналітичну підтримку або здійснювати самостійний моніторинг загроз.

Отже, в Україні функціонування OSINT – розвідки з відкритих джерел – у сфері національної безпеки забезпечується низкою державних органів, які виконують певні завдання у сфері моніторингу, збору та аналізу інформації. Кожен із цих органів наділений специфічними повноваженнями та функціями, що регулюються законодавчими актами. Система цих суб'єктів є розгалуженою, їх адміністративно-правовий статус визначається низкою законодавчих актів, які регулюють відповідні заходи і повноваження із забезпечення національної безпеки, у тому числі шляхом здійснення розвідки з відкритих джерел.

Розглянемо суб'єктів першої групи адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Так, Верховна Рада України відіграє ключову роль у системі адміністративно-правового забезпечення функціонування розвідки з відкритих джерел (OSINT) у сфері національної безпеки. Як вищий представницький орган державної влади, вона має повноваження, які безпосередньо впливають на законодавче регулювання діяльності органів безпеки та оборони, а також на правове регулювання механізмів та процедур збору, аналізу та використання інформації з відкритих джерел.

Згідно зі статтею 85 Конституції України Верховна Рада має право: ухвалювати закони, що регулюють питання національної безпеки, зокрема в контексті використання OSINT [65]. Законом України «Про основи національної безпеки України» передбачено, що парламент здійснює контроль за реалізацією державної політики у цій сфері, що включає в себе моніторинг та оцінку ефективності використання відкритих джерел інформації [123].

Крім того, Верховна Рада має повноваження затверджувати бюджет національної безпеки, що включає фінансування програм та проєктів, спрямованих на розвиток технологій збору та обробки інформації з відкритих джерел. Це сприяє створенню необхідних умов для ефективної роботи органів, відповідальних за національну безпеку, і забезпечує їх оперативність у реагуванні на загрози, що виникають у сучасному інформаційному просторі.

Таким чином, Верховна Рада України, виконуючи свої законодавчі та контрольні функції, є важливим суб'єктом адміністративно-правового забезпечення функціонування OSINT, забезпечуючи правове підґрунтя для ефективної діяльності відповідних суб'єктів у сфері національної безпеки.

Президент України – головний суб'єкт у системі забезпечення національної безпеки держави. Згідно зі статтею 102 Конституції України Президент виступає гарантом державного суверенітету, територіальної цілісності, дотримання Конституції та прав і свобод громадян. У межах цієї конституційної функції Президент має широкі повноваження, спрямовані на забезпечення безпеки та стабільності держави [65].

Відповідно до статті 106 Конституції України Президент визначає основні напрями національної безпекової політики та здійснює керівництво у цій сфері через систему відповідних органів, зокрема Раду національної безпеки і оборони України (РНБО). Президент головує на засіданнях РНБО та має право видавати укази, які є обов'язковими до виконання на всій території України після їх затвердження парламентом. Завдяки цьому Президент координує діяльність органів виконавчої влади щодо захисту національної безпеки, зокрема в інформаційній, економічній та воєнній сферах [65].

Законом України «Про національну безпеку України» передбачено, що Президент у межах своїх повноважень здійснює стратегічне керівництво діяльністю державних органів і визначає пріоритети безпеки. Це включає можливість введення надзвичайного або воєнного стану у разі виникнення загроз державному суверенітету чи конституційному ладу (згідно зі статтями 106 та 112 Конституції). Президент також уповноважений приймати рішення

про використання Збройних сил України та інших військових формувань для відсічі збройній агресії [123].

Повноваження Президента України в забезпеченні національної безпеки мають значний вплив на функціонування системи розвідки з відкритих джерел (OSINT), яка є важливою складовою сучасної безпекової стратегії держави. Президент як Верховний Головнокомандувач Збройних сил України та голова Ради національної безпеки і оборони (РНБО) здійснює керівництво органами, що використовують OSINT для виявлення та аналізу загроз з боку іноземних держав, а також для відслідковування критичних змін у політичних, економічних та інформаційних умовах.

Відповідно до Закону України «Про національну безпеку України» Президент затверджує основні напрями і завдання у сфері національної безпеки, зокрема щодо створення та підтримки потужної інформаційної системи, що дозволяє забезпечити оперативний доступ до відкритих даних. Ці повноваження Президента дозволяють визначати, які напрями моніторингу та розвідувальної діяльності у сфері OSINT є пріоритетними для держави та потребують особливої уваги. Зокрема, Президент може ініціювати прийняття рішень РНБО, спрямованих на підсилення здатності органів безпеки використовувати OSINT для запобігання деструктивним інформаційним впливам та іншим загрозам [123].

Президент також уповноважений видавати укази, які регулюють функціонування органів виконавчої влади у сфері національної безпеки. Це включає ініціацію програм розвитку технічних і аналітичних засобів, що дозволяють використовувати OSINT для моніторингу відкритих джерел, аналізу інформації та виявлення ризиків у цифровому просторі. Така діяльність сприяє адаптації розвідувальних підходів України до умов інформаційної епохи, що особливо важливо для забезпечення національної безпеки в контексті гібридних загроз.

Таким чином, повноваження Президента України у сфері національної безпеки мають вирішальне значення для функціонування системи OSINT,

оскільки вони визначають стратегічні та оперативні завдання розвідки з відкритих джерел, сприяють її розвитку та забезпечують необхідні ресурси для її ефективного функціонування в інтересах національної безпеки.

Кабінет Міністрів України, як головний орган системи виконавчої влади, відіграє ключову роль у забезпеченні функціонування системи розвідки з відкритих джерел (OSINT) у сфері національної безпеки. Виконуючи функції вищого органу виконавчої влади, Кабінет Міністрів реалізує державну політику у стратегічно важливих напрямах, зокрема в галузі інформаційної безпеки та кібербезпеки, що є складовими загальної системи національної безпеки.

Згідно зі статтею 116 Конституції України [65] Кабінет Міністрів України забезпечує виконання законів України, зокрема тих, що стосуються національної безпеки. Суттєве значення має також Закон України «Про національну безпеку України», який окреслює компетенцію Кабінету Міністрів України щодо формування та впровадження державної політики у сфері забезпечення інформаційної безпеки. Він відповідальний за створення та забезпечення умов для функціонування OSINT, зокрема через розробку відповідних підзаконних нормативно-правових актів.

Кабінет Міністрів України також координує діяльність центральних органів виконавчої влади, що здійснюють моніторинг і аналіз відкритих джерел інформації, що є критично важливим для своєчасного виявлення загроз національній безпеці. Він має повноваження затверджувати програми та плани дій, що сприяють розвитку технологій збору інформації з відкритих джерел, а також їх інтеграції у систему національної безпеки.

Крім того, Кабінет Міністрів України наділений повноваженнями щодо формування та реалізації інформаційної політики держави, спрямованої на забезпечення інформаційного суверенітету. Відповідно до положень Стратегії інформаційної безпеки Кабінет Міністрів України здійснює програмне фінансування заходів, пов’язаних з інформаційною безпекою, зокрема надає кошти для розвитку OSINT-спроможностей державних органів. Крім того,

Кабінет Міністрів розробляє і затверджує план заходів з реалізації Стратегії, на підставі якого виконавчі органи здійснюють заходи щодо забезпечення інформаційної безпеки, включаючи використання розвідувальних даних з відкритих джерел для підвищення готовності до інформаційних загроз [119; 130].

Отож Кабінет Міністрів України, виконуючи свої функції, відіграє важливу роль в адміністративно-правовому забезпеченні функціонування OSINT, що забезпечує ефективність реагування на сучасні виклики у сфері національної безпеки, спрямовуючи діяльність органів виконавчої влади.

Щодо другої групи суб'єктів, які здійснюють загальне керівництво та координують діяльність системи суб'єктів, що займаються розвідкою з відкритих джерел, то передусім проаналізуємо Раду національної безпеки та оборони України. Як орган, що забезпечує інтеграцію та координацію діяльності інших суб'єктів у цій сфері, РНБО формулює стратегії та політики, що сприяють ефективному використанню інформації з відкритих джерел для забезпечення національних інтересів.

Відповідно до статті 107 Конституції України [65] та Закону України «Про національну безпеку України» [123] РНБО має повноваження з розробки пропозицій щодо забезпечення національної безпеки, зокрема в частині виявлення загроз, що можуть виникати в інформаційному просторі. Однією з основних функцій РНБО є проведення моніторингу та аналізу стану інформаційної безпеки, а також вироблення рекомендацій для органів виконавчої влади стосовно стратегій протидії дезінформації.

Рада національної безпеки і оборони України, виконуючи конституційно визначену функцію координації діяльності органів виконавчої влади щодо забезпечення національної безпеки, є органом загального керівництва та стратегічного планування. Зокрема, РНБО координує діяльність виконавчої гілки влади та правоохоронних органів, з урахуванням спроможностей Центру протидії дезінформації, діяльність якого має за мету нейтралізацію інформаційних загроз та посилення здатності держави виявляти та протидіяти

дезінформації. Діяльність РНБО, у контексті OSINT, також полягає у координації збору, аналізу та використання даних з відкритих джерел для оцінки ризиків та прогнозування загроз у сфері інформаційної безпеки [128; 130].

У складі Ради національної безпеки і оборони діє Апарат Ради національної безпеки і оборони України, який здійснює координацію між різними суб'єктами безпеки та оборони. Відповідно до статті 3 Закону України «Про національну безпеку України» він формує пропозиції щодо реалізації державної політики в сфері безпеки, що включає управління інформацією з відкритих джерел для ефективного реагування на загрози [106].

Крім того, РНБО здійснює контроль за реалізацією заходів у сфері національної безпеки, що включає в себе діяльність, пов'язану з моніторингом та аналізом відкритих джерел. Це дозволяє не лише виявляти потенційні загрози, але й формувати належну інформаційну політику, яка відповідає сучасним викликам. Отже, РНБО є ключовим суб'єктом у забезпеченні функціонування системи OSINT в Україні, здійснюючи координацію та взаємодію відповідних органів.

Центральні органи виконавчої та місцевої влади у межах повноважень спільно з органами місцевого самоврядування, Центром протидії дезінформації та інститутами громадянського суспільства, забезпечують виконання планів заходів, які затверджуються Кабінетом Міністрів України з питань забезпечення національної безпеки. У контексті OSINT, їх діяльність може включати моніторинг місцевих відкритих джерел, виявлення та передачу інформації про потенційні інформаційні загрози до центральних органів для подальшої оцінки та реагування. Завдяки такій взаємодії, забезпечується ефективний горизонтальний обмін інформацією та координація заходів з інформаційної безпеки на національному і місцевому рівнях [130].

Важливими повноваженнями у сфері адміністративно-правового забезпечення функціонування OSINT наділене Міністерство інформаційної політики України.

Так, згідно зі Стратегією інформаційної безпеки відповідальним за формування та реалізацію державної політики в інформаційній сфері та її нормативно-правове регулювання є відповідний центральний орган виконавчої влади, а саме Міністерство інформаційної політики України [130]. Міністерство інформаційної політики України визначає ключові напрями та перспективи розвитку цієї сфери, а також спільно з Міністерством закордонних справ формує позитивний імідж України на міжнародному рівні для захисту її політичних, економічних та соціально-культурних інтересів. Цей орган є основним координатором у сфері інформаційної політики, спрямованої на підтримку інформаційного суверенітету України. Завдяки цьому забезпечується не лише популяризація української позиції, а й посилення стійкості України в інформаційному просторі перед зовнішніми загрозами [105].

Міністерство оборони України [115] разом із силами безпеки і оборони забезпечують моніторинг інформаційного простору для виявлення загроз у воєнній сфері, що становить важливу частину національної безпеки. Вони проводять заходи інформаційної підтримки оборони та координують залучення інших суб'єктів національної безпеки до цих заходів.

Міністерство оборони України, маючи у своїй структурі спеціальні органи, здійснює функції із забезпечення військової безпеки, з використанням розвідки з відкритих джерел шляхом здійснення постійного моніторингу військових загроз. Міністерство оборони України активно використовує OSINT для збору розвідувальних даних про військову діяльність потенційних противників. Проводить аналіз інформаційних загроз у кіберпросторі, особливо в контексті оборони інформаційної інфраструктури та стратегічних об'єктів, а також розбудовує систему стратегічних комунікацій і підтримує інформаційну безпеку власного інформаційного середовища, особливо в місцях розташування військових формувань. Крім того, спеціальні служби міністерства працюють із засобами масової інформації, забезпечуючи прозорість висвітлення ситуації в районах, де здійснюються оборонні заходи.

Це дозволяє швидко ідентифікувати деструктивні інформаційні впливи та оперативно реагувати на них.

Тепер перейдемо до розгляду спеціальних суб'єктів механізму адміністративно-правового забезпечення OSINT. Їх доцільно класифікувати відповідно до повноважень, які вони здійснюють у різних складових сфери національної безпеки. Такий підхід дозволить детально визначити функції, роль та значення кожного суб'єкта у забезпеченні ефективного функціонування OSINT.

Ключовим нормативно-правовим документом, що визначає коло суб'єктів, відповідальних за гарантування національної безпеки, є Закон України «Про національну безпеку». Відповідно до п. 16 ч. 1 ст. 1 цього Закону, суб'єкти забезпечення національної безпеки входять до складу сектору безпеки і оборони та охоплюють систему органів державної влади, Збройні сили України, інші військові формування, створені відповідно до чинного законодавства, правоохоронні й розвідувальні структури, державні органи з правоохоронними функціями, сили цивільного захисту, а також суб'єкти оборонно-промислового комплексу України. Їхня діяльність підлягає демократичному цивільному контролю та здійснюється відповідно до Конституції та законів України з метою захисту національних інтересів від внутрішніх і зовнішніх викликів. Крім того, у процесі забезпечення національної безпеки можуть брати участь і громадяни України, а також громадські об'єднання, які залучаються до цієї діяльності на добровільних засадах [123].

Таке розуміння дозволяє визначити сектор безпеки і оборони як сукупність державних і недержавних суб'єктів, функціонально орієнтованих на збереження та захист національних інтересів, шляхом вжиття відповідних правових, організаційних та інших заходів у межах їх повноважень, установлених законодавством України.

Закон України «Про національну безпеку України» класифікує органи сектору безпеки і оборони на дві основні категорії: сили безпеки та сили

оборони. Відповідно до п. 17 ч. 1 ст. 1 цього нормативного акта, до складу сил безпеки відносяться правоохоронні органи, розвідувальні служби, органи спеціального призначення, що виконують правоохоронні функції, підрозділи цивільного захисту, а також інші державні інституції, на які Конституцією та законами України покладено завдання щодо гарантування національної безпеки [123]. Таке визначення охоплює широке коло суб'єктів, чия діяльність спрямована на підтримання правопорядку та захист національних інтересів держави від потенційних і реальних загроз.

Водночас відповідно до п. 18 ч. 1 ст. 1 цього самого Закону до сил оборони належать Збройні сили України, інші військові формування, утворені відповідно до законів України, а також окремі правоохоронні та розвідувальні органи і органи спеціального призначення з правоохоронними функціями, наділені повноваженнями щодо оборони держави [123].

Крім того, у п. 2 ст. 12 Закону України «Про національну безпеку» надано перелік органів, які входять до складу безпеки та оборони: Міністерство оборони України, Збройні сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Антитерористичний центр при Службі безпеки України, Служба судової охорони, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику [123].

Безумовно, діяльність не всіх перелічених вище органів безпосередньо пов'язана із здійсненням розвідки з відкритих джерел (OSINT), оскільки їхні функції охоплюють значно ширший спектр завдань у сфері національної безпеки. Деякі органи виконують регуляторні, наглядові чи координаційні

функції, спрямовані на забезпечення правопорядку, захист інформаційної інфраструктури чи протидію кіберзагрозам. Наприклад, Міністерство оборони України здійснює стратегічне планування, тоді як Служба безпеки України зосереджується на контррозвідці та боротьбі з тероризмом, використовуючи OSINT як допоміжний інструмент. Натомість спеціалізовані підрозділи розвідки активно залучені до збору, аналізу та використання відкритої інформації. Таким чином, хоча не всі органи займаються OSINT напряму, кожен із них відіграє важливу роль у забезпеченні національної безпеки.

У межах подальшого вивчення функціональних обов'язків суб'єктів, відповідальних за гарантування національної безпеки України в аспекті розвідувальної діяльності, що здійснюється на основі відкритої інформації, доцільно акцентувати увагу на роботі Міністерства внутрішніх справ України, Державної прикордонної служби України, Антитерористичного центру при Службі безпеки України, а також Державної служби спеціального зв'язку та захисту інформації України. Зазначені структури виступають невід'ємними елементами системи органів, що реалізують завдання у сфері національної безпеки та оборони.

Міністерство внутрішніх справ України, відповідно до ст. 1 Закону України «Про Національну поліцію», має повноваження щодо забезпечення публічної безпеки та порядку, а також запобігання та виявлення злочинів [124]. Зокрема, МВС здійснює моніторинг інформаційного простору з метою виявлення загроз, пов'язаних із кримінальною діяльністю, яка може негативно вплинути на національну безпеку. Правові основи діяльності МВС також включають збори та аналіз інформації з відкритих джерел для оцінки рівня злочинності та формування заходів реагування.

Державна прикордонна служба України, згідно зі ст. 2 Закону України «Про Державну прикордонну службу України», відповідає за охорону державного кордону та контролює порядок перетину кордону. У своїй діяльності служба використовує інформацію з відкритих джерел для моніторингу загроз національній безпеці, пов'язаних із контрабандою,

нелегальною міграцією та іншими загрозами, що можуть виникнути на прикордонних територіях [113].

Згідно з чинним українським законодавством, зокрема положеннями Законів України «Про розвідку» та «Про оперативно-розшукову діяльність», Державна прикордонна служба України реалізує функції у сфері розвідувальної, інформаційно-аналітичної та оперативно-розшукової роботи з метою забезпечення охорони та оборони державного кордону.

Реалізуючи ці завдання, ДПСУ активно залучається до моніторингу та аналізу інформації з відкритих джерел для виявлення загроз на державному кордоні. Це передбачає оцінку даних, що стосуються транскордонних злочинів, нелегальної міграції, а також можливих терористичних актів. У межах своїх повноважень ДПСУ бере участь у боротьбі з організованою злочинністю. Використовуючи інформацію з відкритих джерел, прикордонники можуть виявляти та документувати злочинну діяльність, що здійснюється на прикордонних територіях, що, водночас, сприяє формуванню цілісної картини злочинності в Україні. Крім того, ДПСУ забезпечує виконання заходів, спрямованих на протидію незаконній міграції. Це передбачає здійснення аналізу відкритих джерел, які містять інформацію про маршрути мігрантів, організовані злочинні угруповання та їхні методи роботи.

Таким чином, повноваження Державної прикордонної служби України як суб’єкта механізму адміністративно-правового забезпечення OSINT є важливими для реалізації державної політики у сфері національної безпеки, зокрема що стосується безпеки державного кордону. ДПСУ не лише виконує функції з охорони державного кордону, але й активно впроваджує інструменти інформаційного моніторингу, що дозволяє своєчасно реагувати на загрози та забезпечувати захист національних інтересів. Залучення відкритих джерел інформації є критично важливим елементом у боротьбі з викликами, які постають перед Державною прикордонною службою України в умовах війни, сучасних геополітичних реалій на державному кордоні.

Антитерористичний центр при Службі безпеки України, згідно з Законом України «Про боротьбу з тероризмом» [111], а також Положення про Антитерористичний центр координує діяльність державних органів у сфері протидії тероризму [127]. У зв'язку з цим Антитерористичний центр є вагомим і надзвичайно важливим суб'єктом адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки України, оскільки розвідка з відкритих джерел може ефективно доповнювати традиційні методи боротьби з тероризмом. Створений з метою координації діяльності державних органів у запобіганні терористичним актам, цей центр функціонує як суб'єкт збирання, аналізу та використання інформації з відкритих джерел для захисту держави від зовнішніх і внутрішніх загроз.

Згідно із Законом України «Про боротьбу з тероризмом» [111] та іншими нормативно-правовими актами Антитерористичний центр наділений широким колом повноважень, що дозволяють йому ефективно інтегрувати OSINT у систему національної безпеки. Ключовими його завданнями є координація дій органів виконавчої влади та організація заходів з профілактики терористичних актів, що може включати моніторинг і аналіз інформації з відкритих джерел для виявлення потенційних загроз.

Надзвичайно важливим аспектом роботи Антитерористичного центру є проведення постійного моніторингу соціальних мереж, медіаресурсів, публікацій у відкритому доступі та інших джерел інформації для виявлення небезпечних тенденцій, поширення радикальних ідей та ідентифікації підозрілих осіб і груп. Завдяки цьому процесу центр здійснює раннє виявлення можливих загроз, що є основою для оперативного реагування та прийняття управлінських рішень.

Повноваження Антитерористичного центру як суб'єкта механізму адміністративно-правового забезпечення OSINT, включають надзвичайно важливі функції, по-перше, планування та координація антитерористичних заходів – центр має право розробляти плани дій для запобігання терористичним актам, узгоджуючи їх з іншими державними установами та

відомствами. Ця діяльність передбачає створення міжвідомчих груп для оперативного обміну інформацією, зокрема й тією, що отримана через OSINT. По-друге, аналіз та оцінка інформації – один з найбільш значущих аспектів роботи Антитерористичного центру. Аналітики центру обробляють отримані з відкритих джерел дані, надаючи уряду важливі аналітичні звіти про ризики терористичних актів та можливі варіанти реагування. Інформація з відкритих джерел особливо важлива для моніторингу діяльності різноманітних організацій та осіб, що потенційно можуть бути причетними до терористичної діяльності. По-третє, реагування на терористичні загрози. Антитерористичний центр у разі виявлення терористичної загрози центр ініціює заходи оперативного реагування, зокрема організацію і проведення антитерористичних операцій. Такий алгоритм дій включає як відкритий доступ до інформації з OSINT, так і співпрацю з іншими органами безпеки для здійснення спільних операцій. По-четверте, співпраця з міжнародними структурами, Так, Антитерористичний центр активно співпрацює з міжнародними розвідувальними структурами, організаціями та агенціями, обмінюючись OSINT-даними та передовими методами моніторингу загроз. Така співпраця дозволяє запроваджувати новітні технології у протидії тероризму.

Залучення OSINT як механізму отримання відкритої інформації дозволяє Антитерористичному центру своєчасно та ефективно ідентифікувати та локалізувати потенційні загрози на ранніх стадіях їх формування, що забезпечує своєчасність реагування і, врешті-решт, безпеку громадян і держави.

Державна служба спеціального зв’язку та захисту інформації України, як ключовий суб’єкт сил безпеки і оборони, виконує особливі функції у сфері захисту інформації, забезпечення кібербезпеки та спеціального зв’язку, що робить її незамінним інструментом у протидії сучасним загрозам, зокрема у кіберпросторі. Її діяльність регламентована Законом України «Про Державну службу спеціального зв’язку та захисту інформації України» [114], а також

Законом України «Про національну безпеку України», які визначають повноваження цього органу у забезпеченні національної безпеки.

До основних завдань Держспецзв'язку, як суб'єкта сил безпеки і оборони, належать:

1. Захист державних інформаційних ресурсів та об'єктів критичної інфраструктури. Держспецзв'язку забезпечує захист від несанкціонованого доступу, зловмисних дій та кібератак на державні ресурси, що є критичними для функціонування держави, що має особливе значення в умовах гібридної війни;

2. Забезпечення функціонування урядового зв'язку та інших спеціальних мереж. Важливим аспектом діяльності є створення, експлуатація та захист спеціальних каналів зв'язку, які використовуються державними органами для безпечної передачі інформації, зокрема конфіденційної та секретної;

3. Кіберзахист та реагування на інциденти кібербезпеки. Держспецзв'язку уповноважена здійснювати моніторинг і аналіз кіберзагроз, а також забезпечувати захист інформаційних систем від таких загроз. Це охоплює, зокрема, запобігання, виявлення, реагування та відновлення після кіберінцидентів;

4. Стандартизація та технічний контроль у сфері інформаційної безпеки. Держспецзв'язку має право розробляти та затверджувати нормативи та стандарти інформаційної безпеки для державних органів, а також здійснювати технічний контроль за їх дотриманням, забезпечуючи єдину політику в сфері захисту інформації.

Здійснення OSINT не є основною функцією Держспецзв'язку, однак у сучасних умовах вона отримує дедалі більше значення як інструмент для забезпечення кібербезпеки. Основна роль Держспецзв'язку у цьому контексті зосереджена на: моніторингу відкритих джерел на предмет потенційних кіберзагроз; виявлення критичних уразливостей в інформаційних системах (OSINT дозволяє Держспецзв'язку ідентифікувати потенційно небезпечні

уразливості, які можуть бути використані кіберзлочинцями або ворожими розвідувальними службами); аналіз кіберінцидентів та прогнозування загроз; забезпечення інформаційного обміну з міжнародними партнерами (з метою підвищення кіберзахисту, Держспецзв'язку здійснює обмін інформацією з міжнародними організаціями, такими як ENISA, НАТО та інші структури, які також використовують OSINT для моніторингу загроз).

Роль Держспецзв'язку як суб'єкта національної безпеки і оборони в умовах цифрової трансформації значно розширюється, охоплюючи не лише захист критичних державних ресурсів, але й кіберрозвідку, у тому числі використання OSINT для здійснення моніторингу кіберзагроз та запобігання потенційним атакам.

Таким чином, аналіз повноважень зазначених органів показує, що їхня діяльність є важливою складовою системи забезпечення національної безпеки України, яка включає в себе різноманітні аспекти, пов'язані з моніторингом, аналізом та реагуванням на загрози з відкритих джерел. Синергія між цими органами забезпечує комплексний підхід до виявлення і нейтралізації загроз національної безпеки.

У контексті здійснення розвідки з відкритих джерел також серед суб'єктів забезпечення національної безпеки особливу роль відіграють Служба безпеки України (СБУ), розвідувальні органи України та Апарат Ради національної безпеки і оборони України.

Служба безпеки України, відповідно до ст. ст. 1, 2 та 21 Закону України «Про Службу безпеки України», виконує функції, що включають протидію загрозам національній безпеці, зокрема через моніторинг інформаційного простору [134]. Вона має повноваження щодо здійснення моніторингу засобів масової інформації та інтернет-ресурсів для виявлення потенційних загроз інформаційній безпеці, що передбачено статтею 6 зазначеного закону. СБУ проводить аналіз і оцінку інформації з відкритих джерел для запобігання інформаційним операціям, що можуть бути спрямовані проти держави.

Розвідувальні структури України, зокрема Головне управління розвідки Міністерства оборони України та органи військової контррозвідки, функціонують з метою забезпечення контррозвідувального супроводу діяльності Збройних сил України, Державної прикордонної служби України, а також інших військових формувань, розміщених на території держави. Зазначені інституції виконують завдання, спрямовані на оперативне реагування на зовнішні загрози національній безпеці.

Вони також займаються збором та аналізом інформації з відкритих джерел для оцінки стану міжнародної безпеки та можливих загроз, що відображено в Законі України «Про розвідку». Ці органи забезпечують національні інтереси, проводячи моніторинг і аналіз інформації з міжнародних медіа, наукових публікацій та інших джерел [133].

Отже, діяльність зазначених органів у сфері розвідки з відкритих джерел є невід'ємною складовою системи національної безпеки України. Вони забезпечують своєчасне виявлення загроз, формування стратегій протидії дезінформації та підтримку національних інтересів. Згуртована робота цих структур дозволяє оперативно реагувати на виклики, з якими стикається Україна в умовах війни.

З наведених визначень стає очевидним, що повноваження на забезпечення національної безпеки, зокрема на здійснення розвідувальної діяльності, належать саме до компетенції сил безпеки. У цьому контексті суб'єкти, віднесені до складу сил безпеки, мають право на проведення заходів з розвідки з відкритих джерел (OSINT) у рамках забезпечення національних інтересів і реагування на відповідні загрози. Таким чином, правові підстави для реалізації OSINT у сфері національної безпеки зосереджені саме у правовому полі, що регулює діяльність органів, які належать до сил безпеки. Повноваження таких органів у сфері OSINT випливають із їхньої компетенції забезпечувати правопорядок і реагувати на загрози національним інтересам України. Використання відкритих джерел інформації, як складової розвідувальної діяльності, дає змогу органам безпеки отримувати, аналізувати

та використовувати актуальні дані, що не підлягають державній або комерційній таємниці, але мають значення для прогнозування ймовірних ризиків.

Як уже зазначалося, складовою національної безпеки є інформаційна безпека та кібербезпека. Відповідно, забезпечення інформаційної безпеки та кібербезпеки покладено на спеціальні органи, що також мають повноваження на здійснення розвідки з відкритих джерел.

Відповідно до ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [126] національна система кібербезпеки – це сукупність суб'єктів забезпечення кібербезпеки, а також заходів політичного, науково-технічного, освітнього, інформаційного, організаційного, правового, оперативно-розшукового, розвідувального, контррозвідувального, оборонного та інженерно-технічного характеру, спрямованих на захист національних інформаційних ресурсів і критичної інформаційної інфраструктури.

Згідно з положеннями Закону України «Про основні засади забезпечення кібербезпеки України» [126] система кібербезпеки включає низку суб'єктів, кожен з яких має особливі повноваження у забезпеченні безпеки держави в кіберпросторі, зокрема в аспекті розвідки з відкритих джерел (OSINT). Використання OSINT дає змогу цим суб'єктам здійснювати моніторинг, аналіз та протидію кіберзагрозам, що може мати значення для своєчасного реагування на інциденти й захисту об'єктів критичної інформаційної інфраструктури. Розглянемо детальніше повноваження основних суб'єктів кібербезпеки у здійсненні розвідки з відкритих джерел.

Основними суб'єктами, що забезпечують кібербезпеку на державному рівні, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [126], є:

1. Державна служба спеціального зв'язку та захисту інформації України – відповідає за формування і реалізацію політики кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної

інфраструктури, здійснює контроль за їхньою захищеністю, проводить аудит інформаційної безпеки та координує діяльність інших суб'єктів кібербезпеки. Для ефективного виконання цих завдань ДССЗЗІ може використовувати OSINT, зокрема для моніторингу загроз у кіберпросторі, виявлення вразливостей об'єктів критичної інфраструктури та розробки рекомендацій з кіберзахисту [114];

2. Національна поліція України – забезпечує захист прав та інтересів громадян, держави і суспільства у кіберпросторі, протидіє кіберзлочинності шляхом виявлення, попередження, розкриття та припинення кіберзлочинів. Вона займається запобіганням, виявленням та розслідуванням кіберзлочинів, що вимагає доступу до інформації з відкритих джерел, зокрема для ідентифікації потенційних загроз, збирання доказів кіберзлочинів та підвищення обізнаності громадян щодо безпеки в кіберпросторі [124].

3. Служба безпеки України – здійснює контррозвідувальну і оперативно-розшукову діяльність, спрямовану на боротьбу з кібертероризмом, кібершпигунством, кіберзлочинністю, що створює загрозу державній безпеці, та проводить розслідування кіберінцидентів, які загрожують життєво важливим інтересам держави. Враховуючи значну роль СБУ у протидії кіберзлочинності, використання OSINT стає важливим для збору даних про можливі атаки, виявлення кібершпигунських дій та аналізу загроз щодо критичних об'єктів інфраструктури [134].

4. Міністерство оборони України та Генеральний штаб Збройних сил України – здійснюють заходи з кібероборони та співпрацюють з НАТО й іншими міжнародними суб'єктами задля захисту від кіберзагроз. Здійснення OSINT у межах їх діяльності дозволяє вчасно виявляти та аналізувати кіберзагрози, пов'язані з воєнною агресією, а також встановлювати потенційні вразливості, які можуть використовуватись під час гібридних воєнних дій [123].

5. Розвідувальні органи України – проводять розвідувальну діяльність, що охоплює моніторинг загроз у кіберпросторі, які можуть

створити небезпеку для національних інтересів OSINT у цьому контексті є невід'ємним інструментом для відстеження тенденцій розвитку кіберзагроз, прогнозування атак та ідентифікації дій суб'єктів, які можуть становити загрозу національній безпеці.

Таким чином, кожен із зазначених суб'єктів кібербезпеки володіє правом використовувати розвідку з відкритих джерел (OSINT) як важливий інструмент для ідентифікації загроз, запобігання кібератакам і захисту критичної інформаційної інфраструктури, що є складовою забезпечення національної безпеки України в кіберпросторі.

Для забезпечення інформаційної безпеки в державі створені та функціонують спеціальні органи, що мають повноваження застосовувати розвідку з відкритих джерел. Згідно зі Стратегією інформаційної безпеки [130] суб'єктами забезпечення інформаційної безпеки є суб'єкти, які можна поділити на два рівня: суб'єкти забезпечення інформаційної безпеки центрального рівня і спеціальні суб'єкти, які мають особливі повноваження, забезпечуючи інформаційну безпеку, здійснювати розвідку з відкритих джерел. При цьому, повноваження першої групи суб'єктів полягають у здійсненні правового регулювання цієї сфери, стратегічного планування та виконання координаційної функції по відношенню до інших суб'єктів здійснення розвідки з відкритих джерел у сфері інформаційної безпеки.

У контексті дослідження суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки доцільно деталізувати повноваження суб'єктів центрального рівня, що забезпечують інформаційну безпеку України, відповідно до положень Стратегії інформаційної безпеки України.

Важливим суб'єктом, що має повноваження у здійсненні розвідки з відкритих джерел, є Центр протидії дезінформації – робочий орган Ради національної безпеки і оборони України, утворений відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про

створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106 [135].

Відповідно до Положення про Центр протидії дезінформації, цей орган відіграє ключову роль у забезпеченні національної інформаційної безпеки, здійснюючи системну протидію дезінформації, деструктивним інформаційним кампаніям та спробам маніпулювання суспільною думкою. Згідно з законодавством головними завданнями Центру є: по-перше, аналіз та моніторинг інформаційного простору. Центр здійснює постійний моніторинг інформаційного середовища України, аналізуючи події, явища та загрози в контексті інформаційної безпеки, а також оцінює місце і роль України у глобальному інформаційному просторі. По-друге, виявлення та оцінка загроз. Центр займається виявленням і прогнозуванням актуальних і потенційних загроз національній інформаційній безпеці, оцінює чинники їх формування, визначає наслідки цих загроз для безпеки національних інтересів України. По-третє, інформаційне забезпечення керівництва РНБО. Центр надає Раді національної безпеки і оборони України, включаючи її Голову, аналітичні матеріали, що стосуються інформаційної безпеки України, ефективного реагування на дезінформаційні атаки та пропаганду, деструктивні інформаційні впливи та кампанії. По-четверте, формування пропозицій з протидії дезінформації. Центр готує та подає до РНБО пропозиції щодо концептуальних підходів у сфері боротьби з дезінформацією, деструктивними інформаційними впливами та запобігання маніпулюванню суспільною свідомістю. Центр також координує взаємодію між органами виконавчої влади для забезпечення цілісної та ефективної інформаційної політики в умовах загроз [107].

Центр також сприяє підвищенню здатності сектору безпеки, оборонних і правоохоронних органів до ефективного забезпечення інформаційної безпеки шляхом підготовки рекомендацій з удосконалення національної інфраструктури інформаційної безпеки. У рамках своїх повноважень Центр надає пропозиції щодо удосконалення правової та наукової бази, необхідної

для забезпечення ефективної протидії дезінформаційним кампаніям і деструктивним інформаційним впливам. Центр відіграє важливу роль у побудові системи стратегічних комунікацій держави та координації заходів, спрямованих на її розвиток, для посилення національної стійкості до інформаційних загроз. Крім того, Центр працює над створенням інтегрованої системи оцінки інформаційних загроз і оперативного реагування на них [107].

Отже, Центр протидії дезінформації при Раді національної безпеки і оборони України відіграє важливу роль у забезпеченні національної інформаційної безпеки, зокрема у реалізації розвідки з відкритих джерел (OSINT) як елемента сучасної системи захисту від інформаційних загроз. Головною цінністю Центру є можливість застосування аналітичного підходу до збору, оцінки та аналізу даних з відкритих джерел для оперативного виявлення загрозливих інформаційних явищ, прогнозування потенційних ризиків та ефективного попередження дезінформаційних атак.

Завдяки систематичному моніторингу інформаційного простору, Центр формує аналітичні матеріали для Ради національної безпеки і оборони України, що забезпечує якісне інформаційне забезпечення керівництва держави. Діяльність Центру з виявлення, класифікації та аналізу деструктивних інформаційних впливів на основі OSINT-технологій сприяє підвищенню обізнаності суспільства про дезінформаційні загрози та розвитку медіаграмотності.

До спеціальних суб’єктів, які відіграють ключову роль у забезпеченні інформаційної безпеки України шляхом здійснення розвідки з відкритих джерел (OSINT), належать декілька основних державних органів, кожен з яких виконує конкретні функції в межах своєї компетенції.

Так, Служба безпеки України має спеціалізовані повноваження з моніторингу медіапростору та інтернет-ресурсів для виявлення загроз національній безпеці. Вона зосереджує свою діяльність на протидії інформаційним операціям, що спрямовані на дестабілізацію України, порушення суверенітету та цілісності держави [134].

Отже, Служба безпеки України є одним з ключових суб'єктів у забезпеченні національної безпеки, володіючи широкими повноваженнями в таких сферах, як інформаційна безпека, контррозвідка, боротьба з тероризмом та кіберзагрози. Важливим напрямом її діяльності є здійснення розвідки з відкритих джерел, що дозволяє своєчасно виявляти загрози національній безпеці, а також ефективно аналізувати та оцінювати інформаційні ризики, зберігаючи при цьому відповідність до законодавчих вимог і міжнародних стандартів.

СБУ здійснює OSINT на підставі Закону України «Про Службу безпеки України» [134] та Закону України «Про національну безпеку України» [123].

Так, у статті 24 Закону «Про Службу безпеки України» закріплено чисельні повноваження на проведення спеціальних заходів для захисту національної безпеки, включаючи заходи в інформаційній сфері [134]. Безумовно, реалізація багатьох розвідувальних та контррозвідувальних заходів Служби безпеки України здійснюється з використанням розвідки з відкритих джерел. Згідно з Законом України «Про національну безпеку України» на СБУ покладено завдання забезпечувати безпеку національних інтересів в інформаційній сфері, шляхом запобігання та протидії дезінформаційним кампаніям, інформаційним атакам, підбурюванню до порушення конституційного ладу та суверенітету держави, що також не можливо здійснити без використання OSINT.

До основних повноважень СБУ у сфері OSINT належить моніторинг засобів масової інформації, інтернет-ресурсів і соціальних мереж для виявлення загрозливих дезінформаційних матеріалів, які можуть негативно вплинути на стан національної безпеки. Згідно з вищезгаданими законодавчими актами СБУ має право на застосування спеціальних технічних методів для аналізу відкритих джерел, що дозволяє ефективно виявляти інформаційні загрози та заздалегідь попереджати деструктивні впливи. Крім того, Служба безпеки України здійснює аналітичну обробку зібраних

матеріалів і надає рекомендації органам державної влади з метою запобігання дестабілізаційним впливам.

Використання OSINT є ефективним інструментом для зниження ризиків, пов’язаних із зовнішніми та внутрішніми інформаційними загрозами. Завдяки широкому колу повноважень і правовому забезпеченню, Служба безпеки України здатна оперативно реагувати на загрози національній безпеці, забезпечуючи захист національних інтересів України у тому числі в інформаційному просторі.

Розвідувальні органи України виконують стратегічну роль у забезпеченні національної безпеки, зокрема через виявлення та нейтралізацію зовнішніх інформаційних загроз. Завдяки використанню розвідки з відкритих джерел (OSINT), ці органи можуть ефективно отримувати та аналізувати інформацію про зовнішні загрози, що впливають на безпеку держави в політичній, економічній, військовій та інформаційній сферах. Їхня діяльність є критично важливою для запобігання іноземним інформаційним впливам, які можуть підірвати національні інтереси та стабільність України. У процесі здійснення OSINT вони здатні не лише виявляти деструктивні інформаційні потоки, а й вчасно вживати заходів для попередження зовнішніх впливів. Використання OSINT дозволяє цим органам проводити системний аналіз даних з відкритих джерел, що значно розширює їхню можливість діяти ефективно у сучасному інформаційному просторі.

Основними розвідувальними органами України є Служба зовнішньої розвідки України (СЗРУ), Головне управління розвідки Міністерства оборони України (ГУР МОУ) та розвідувальні підрозділи інших спеціальних органів, що діють у рамках правового поля, закріпленого Законом України «Про розвідку» [133]. Відповідно до статті 3 цього Закону розвідувальні органи здійснюють збір та аналітичне опрацювання інформації з метою реалізації національних інтересів, включаючи забезпечення суверенітету, територіальної цілісності та запобігання терористичним загрозам.

Серед повноважень розвідувальних органів у здійсненні OSINT – моніторинг міжнародних та національних відкритих інформаційних ресурсів, включаючи іноземні засоби масової інформації, соціальні мережі та аналітичні платформи. Згідно з Законом України «Про національну безпеку України» [123] розвідувальні органи мають право здійснювати збір інформації у відкритих джерелах з метою попередження зовнішніх загроз, що може включати як організацію системного спостереження за інформаційними потоками, так і подальший аналіз отриманої інформації для оцінки ризиків. Особливе значення надається прогнозуванню розвитку подій у країнах, що можуть становити загрозу для національної безпеки України, або в регіонах, де активні антагоністичні інтереси.

Діяльність розвідувальних органів у сфері OSINT має неоціненне значення в умовах сучасної гібридної війни, де інформаційні загрози є невід'ємним компонентом. Зібрана інформація забезпечує ефективну комунікацію з іншими суб'єктами сектору безпеки й оборони, сприяючи координації дій в інтересах захисту держави. Зважаючи на розширення спектра зовнішніх інформаційних впливів, можливість оперативного доступу до аналітичної інформації та її обробки з відкритих джерел є важливою складовою інформаційної безпеки України.

Кожен із цих органів, виконуючи повноваження в межах своєї компетенції, використовує розвідку з відкритих джерел для збору, аналізу та оцінки інформації. Це забезпечує координацію та системність у виявленні, запобіганні й протидії загрозам національній безпеці, роблячи внесок у загальну стратегію інформаційної безпеки України. Це сприяє підвищенню національної безпеки та стійкості країни до деструктивних інформаційних впливів у сучасних умовах гібридної агресії.

Отже, діяльність суб'єктів, що забезпечують функціонування OSINT у механізмі адміністративно-правового забезпечення національної безпеки, має важливе значення для своєчасного виявлення загроз і належного реагування на них. OSINT є ефективним інструментом, що передбачає збір, обробку та

аналіз інформації з відкритих джерел, і дозволяє створити підґрунтя для прийняття управлінських рішень з питань захисту національних інтересів, протидії загрозам та викликам у сфері національної безпеки.

Ефективність діяльності зазначених вище суб'єктів значною мірою залежить від якості правового забезпечення їхнього функціонування у здійсненні розвідки з відкритих джерел. Відповідна правова база має враховувати сучасні вимоги у сфері кібербезпеки та інформаційної розвідки, забезпечуючи чіткий розподіл повноважень, стандарти інформаційного обміну та координаційні механізми. Удосконалення нормативно-правового регулювання діяльності суб'єктів, які здійснюють розвідку з відкритих джерел дозволить гармонізувати взаємодію суб'єктів, зменшити дублювання функцій та збільшити швидкість обміну критичною інформацією, що є важливим в умовах динамічного інформаційного простору. Крім того, розвиток правової бази має враховувати співпрацю з міжнародними партнерами, що дозволить Україні інтегруватися у глобальну систему кіберзахисту та обміну OSINT, підвищуючи спроможність реагування на транснаціональні загрози.

Аналіз системи суб'єктів механізму адміністративно-правового функціонування OSINT у сфері національної безпеки дозволяє зробити деякі узагальнення. Як бачимо, вони представляють собою систему органів державної влади різного рівня, які мають різні повноваження, права та обов'язки щодо здійснення розвідки з відкритих джерел. Одні суб'єкти, з проаналізованих вище, мають загальну компетенції, наділені повноваженнями здійснювати правове регулювання, координацію та взаємодію (Верховна Рада України, Рада національної безпеки і оборони тощо), інші безпосередньо займаються розвідкою з відкритих джерел (наприклад, розвідувальні органи тощо). За місцем в ієрархічній структурі вказані суб'єкти також мають різний адміністративно-правовий статус. Одні наділені повноваженнями здійснювати керівництво іншими (наприклад, МВС України відносно Національної поліції, або Служба безпеки України відносно розвідувальних органів).

Отже, суб'єкти механізму адміністративно-правового функціонування OSINT у сфері національної безпеки – це сукупність державних та інших уповноважених органів, що виконують комплекс завдань з виявлення, збору, аналізу та обробки інформації з відкритих джерел з метою забезпечення національної безпеки держави. Ці суб'єкти мають особливий адміністративно-правовий статус і діють у межах установленої компетенції, яка надає їм законодавчо закріплені повноваження для забезпечення функціонування OSINT у сфері національної безпеки. Суб'єктам механізму адміністративно-правового функціонування OSINT у сфері національної безпеки притаманні такі властивості: наявність адміністративно-правового статусу та компетенції на забезпечення функціонування OSINT у сфері національної безпеки; інституційна належність до системи органів забезпечення національної безпеки і її складових; виконання функцій із забезпечення OSINT.

Суб'єкти механізму адміністративно-правового функціонування OSINT у сфері національної безпеки представляють собою багаторівневу систему. Система суб'єктів механізму адміністративно-правового функціонування OSINT у сфері національної безпеки є цілісною та синергетичною сукупністю складових, які перебувають у взаємодії, обумовленій завданнями із забезпечення національної безпеки. Елементи цієї системи, тобто суб'єкти, поєднані спільними інтересами та потребами в контексті здійснення адміністративно-правового регулювання застосування розвідки з відкритих джерел у сфері національної безпеки, яке визначає особливості їх адміністративно-правового статусу, форм і методів діяльності.

Система суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки охоплює різні організаційно-функціональні рівні: 1) суб'єкти загальної компетенції (Верховна Рада України, Президент України та Кабінет Міністрів України); 2) суб'єкти загального керівництва (Рада національної безпеки і оборони, Міністерство інформаційної політики України, Міністерство оборони України); 3) суб'єкти спеціального керівництва (суб'єкти спеціальної

компетенції (Служба безпеки України, Національна поліція України, Державна прикордонна служба України, Державна служба спеціального зв'язку та захисту інформації України); 4) суб'єкти спеціальної компетенції (розвідувальні та контррозвідувальні органи, Центр протидії дезінформації, відповідні служби та підрозділи суб'єктів спеціального керівництва). Кожен з цих суб'єктів має визначені адміністративно-правовими актами повноваження і завдання щодо здійснення розвідки з відкритих джерел та функціонування OSINT у сфері національної безпеки, які спрямовані на запобігання, виявлення та нейтралізацію загроз на основі даних, отриманих з відкритих джерел.

Системі суб'єктів механізму адміністративно-правового функціонування OSINT у сфері національної безпеки характерні такі властивості: цілісність та взаємодія; функціональна спеціалізація та взаємодія; координація; чітка регламентація повноважень; адаптивність до змінного інформаційного середовища.

На підставі аналізу системи суб'єктів механізму адміністративно-правового функціонування OSINT у сфері національної безпеки запропоновано класифікувати їх за такими критеріями:

1) за змістом правосуб'єктності вони поділяються на: суб'єктів загальної компетенції, до яких належать органи, що поряд із забезпеченням національної безпеки виконують широкий спектр завдань у різних сферах суспільного життя (наприклад, Верховна Рада України, Кабінет Міністрів України, Президент України, МВС України); суб'єкти спеціальної компетенції, які мають повноваження на здійснення розвідки з відкритих джерел (Національна поліція, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України).

2) за характером адміністративно-правового регулювання: суб'єкти, що мають владні повноваження для прийняття управлінських рішень та здійснення адміністративно-правового регулювання; суб'єкти, відповідальні за забезпечення національної безпеки шляхом здійснення розвідки з відкритих джерел.

Запропонована класифікація дозволяє чітко окреслити функції, повноваження, а також специфіку взаємодії між цими суб'єктами, що підвищує ефективність адміністративного регулювання у сфері безпеки.

Для забезпечення ефективності діяльності суб'єктів механізму адміністративно-правового функціонування OSINT у сфері національної безпеки України ключову роль відіграють професіоналізація та спеціалізація кадрів, які безпосередньо здійснюють розвідку з відкритих джерел. Відповідна підготовка та спеціалізація фахівців дають змогу підвищити точність аналізу, ефективність обробки інформації з відкритих джерел та покращують здатність виявляти приховані загрози, які могли б бути проігноровані внаслідок недостатньої кваліфікації. Професіоналізація також сприяє адаптації до нових викликів, оскільки постійне навчання і вдосконалення компетенцій дозволяють кадровому складу своєчасно реагувати на зміни у цифровому середовищі та появу нових загроз.

Ефективне розподілення завдань і повноважень серед суб'єктів адміністративно-правового забезпечення OSINT є важливим аспектом підвищення продуктивності їх діяльності. В умовах сучасних загроз чітке розмежування повноважень між суб'єктами, такими як СБУ, Держспецзв'язку, Збройні сили України тощо, дозволяє уникнути дублювання зусиль і забезпечує оптимальне використання ресурсів. Це, натомість, сприяє підвищенню оперативності та точності заходів з виявлення та нейтралізації потенційних загроз.

Адаптація механізму OSINT до нових викликів і загроз є важливою складовою сучасної національної безпеки. Технологічні інновації, поява нових платформ і способів комунікації вимагають гнучкого підходу до методів збору та аналізу інформації з відкритих джерел та ефективного механізму підготовки та навчання відповідних суб'єктів. Крім того, це зобов'язує державні органи регулярно оновлювати аналітичні підходи та залучати нові технології, такі як штучний інтелект та автоматизовані системи аналізу великих масивів даних, що дозволяють значно підвищити якість та швидкість обробки інформації.

Отже, професіоналізація кадрів, чіткий розподіл завдань і повноважень, адаптація до нових викликів та ефективна координація на національному й міжнародному рівнях є ключовими елементами для забезпечення ефективної діяльності суб'єктів механізму адміністративно-правового забезпечення OSINT.

2.3 Адміністративно-правові засоби механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки

Забезпечення національної безпеки є однією з головних функцій держави, яка передбачає реалізацію комплексу заходів для ефективного реагування на сучасні виклики, пов'язані з різноманітними, у тому числі інформаційними та кіберзагрозами, що набувають глобального поширення. У цьому контексті важливою складовою виступають адміністративно-правові засоби, що слугують основою для адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Дослідження цих засобів є вкрай актуальним, адже саме ці адміністративно-правові інструменти забезпечують належну правову основу для організації та координації діяльності суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. Крім того, вони дозволяють ефективно реалізовувати функції державного управління у сфері національної безпеки та здійснювати правове регулювання, забезпечення діяльності відповідних суб'єктів щодо обробки, аналізу та використання інформації, отриманої з відкритих джерел.

Адміністративно-правові засоби є важливим інструментом діяльності суб'єктів, які займаються розвідкою з відкритих джерел, адже саме за їх допомогою забезпечується функціонування OSINT та, власне, розвідка з

відкритих джерел. Зокрема, такі засоби дозволяють встановити межі правомірного використання відкритої інформації, що зменшує ймовірність порушення прав громадян і забезпечує дотримання принципів прозорості та законності. Адміністративно-правові засоби включають такі елементи, як нормативні акти, накази, процедури та стандарти, що регламентують роботу суб'єктів розвідувальної діяльності, спрямованої на збирання та обробку інформації з відкритих джерел. Їх значення в процесі захисту національної безпеки важко переоцінити, оскільки вони допомагають уникнути ризиків, пов'язаних з обмеженням прав і свобод громадян, що є надзвичайно актуальним у контексті сучасних викликів безпеці, та забезпечити вчасне виявлення та усунення загроз національної безпеки.

Варто зазначити, що в юридичній науці категорії «правові засоби» та «адміністративно-правові засоби» хоча й досліджувалися на сторінках наукових праць, однак досі не мають однозначного визначення, що зумовлює потребу у детальному аналізі їх змісту та структури. Невизначеність термінології ускладнює ефективну реалізацію правових норм, що регулюють діяльність суб'єктів здійснення розвідки з відкритих джерел, і ставить під питання правову визначеність та передбачуваність їх функціонування у рамках національної безпеки. Сучасні правознавці підходять до цих понять по-різному, що може спричиняти колізії та неоднакове тлумачення норм у практиці застосування права. Відтак, дослідження сутності адміністративно-правових засобів у контексті забезпечення функціонування OSINT набуває не лише теоретичного, але й практичного значення, оскільки сприяє уніфікації термінології та підвищує ефективність адміністративно-правового регулювання у сфері національної безпеки.

Термін «засіб» за етимологією охоплює такі аспекти, по-перше, як прийом, спосіб або спеціальна дія, що сприяє досягненню певної мети чи реалізації певної діяльності. Це може бути як інструмент, так і знаряддя чи комплекс пристроїв, що полегшують досягнення результатів [15, с. 326]; по-друге, як особлива дія, що дозволяє реалізувати щось або досягти певної мети.

По-третє, засіб означає знаряддя, що сприяє виконанню певної справи. І нарешті, «засіб» визначається як прийом чи спосіб дій для досягнення певного результату, а також як предмет або сукупність пристроїв, що використовуються для здійснення певної діяльності [15, с. 420; 45, с. 145; 94, с. 96]. Усі значення цього терміну об'єднує спільна ознака: можливість використання для вирішення конкретних завдань, тобто функціональне призначення.

Таким чином, категорія «правові засоби» дає змогу узагальнити явища, які слугують для досягнення цілей, закріплених у законодавстві. Ця категорія об'єднує ідеальне та реальне: з одного боку, вона включає інструменти, що представляють собою певну правову ідею або мету; з іншого боку, охоплює практичні методи та процедури, які перетворюють цю ідею на результат. У цьому контексті правові явища, хоча і різнорідні за своєю природою, набувають спільної якості засобів, оскільки забезпечують досягнення законодавчо визначених завдань, об'єднуючи в собі як концептуальні, так і практичні компоненти.

У юридичній літературі під правовими засобами тлумачать систему субстанціональних і діяльнісних правових явищ, через які учасники правовідносин досягають як приватних, так і публічних цілей [97, с. 14–15]. Такий підхід до розуміння правових засобів відповідає поглядам більшості науковців у сфері філософії, які вважають, що поняття «засіб» включає не лише набір інструментів, але й процес їхнього застосування для досягнення бажаного результату.

Інші вчені «правові засоби» визначають як юридичні явища, які відображаються в інструментах (установленнях) та діяннях (технологіях), завдяки яким задовольняються інтереси суб'єктів права та забезпечується досягнення соціально значущих цілей. До таких правових засобів належать норми й принципи права, правозастосовні акти, договори, юридичні факти, суб'єктивні права, юридичні обов'язки, заборони, пільги та акти реалізації прав [99].

Науковці також трактують правові засоби як об’єктивовані юридичні явища, що мають стабільні властивості та забезпечують можливість реалізації потенціалу права, його ефективність і силу. Прихильники діяльнісного підходу акцентують, що розуміння правових засобів лише як субстанціональних явищ є обмеженим, оскільки воно не охоплює діяльнісні феномени і, відповідно, представляє лише частину суті цього поняття. Заборони, дозволи, приписи та інші елементи правової системи, разом із джерелами права, формують статичну складову правового механізму. Ця складова є лише початковою основою для правового регулювання, яка обов’язково доповнюється динамічним елементом – технологіями, тобто діяннями, спрямованими на застосування правових інструментів. На підставі цього правові засоби можна розглядати як сукупність інструментів (установлень) і діянь (технологій), завдяки яким забезпечується реалізація інтересів суб’єктів права та досягнення соціально корисних цілей. Згідно з першим підходом, правові засоби відображаються у нормах права, а згідно з другим – у діяльності суб’єктів правовідносин [86].

Зокрема, П. М. Рабінович розглядає правові засоби як інституційні утворення (установлення та форми) правової дійсності, що в процесі їхнього функціонування та застосування в спеціальній правовій діяльності сприяють досягненню конкретного результату. Це визначення охоплює широкий спектр завдань, включаючи соціально-економічні, політичні, моральні та інші цілі, що постають перед державою та суспільством на сучасному етапі [137, с. 55].

Розвиваючи ідеї П. М. Рабіновича, О. О. Ганзенко вказує, що правові інструменти становлять базову категорію інструментального підходу до права, і в найзагальнішому вигляді «правові засоби» визначаються як система способів, методів і прийомів, встановлених правовими нормами, що використовуються суб’єктами правовідносин для досягнення індивідуальних або суспільних цілей [24, с. 39–40]. У свою чергу, А. Денисова формулює власне трактування поняття «правові способи» (синонімічне до «правові засоби»), під яким розуміє правові феномени, що проявляються через

інструментарій (постанови) та дії (технології), спрямовані на реалізацію інтересів учасників правовідносин і досягнення як особистих, так і загальносуспільних результатів [30, с. 190–191].

Запропонована ученою класифікація правових засобів є раціональною й структурованою. Зокрема, дослідниця розподіляє правові засоби на субстанціональні (засоби-постанови, інструменти) та дієві (засоби-дії, технології). До першої групи вона зараховує правові дозволи, обов'язки, заборони, стимули, привілеї, а також правові норми і принципи. Натомість до дієвих правових засобів включаються акти реалізації та застосування права, акти тлумачення правових норм та всі інші процеси, що належать до юридичної діяльності [30, с. 191–192]. Як бачимо, вказані науковці охоплюють у межах поняття «правові засоби» майже всі складові механізму правового регулювання: правові норми, правовідносини, дії щодо реалізації та застосування норм, судову та адміністративну практику, мовчазні (конклюдентні) правові акти, інтерпретаційні процедури, а також правові звичаї й традиції. Такий підхід є цілком обґрунтованим, оскільки в теорії держави та права механізм правового регулювання розглядається саме як система правових засобів. Таким чином, «правові засоби» виступають універсальною правовою категорією, яка дає змогу оцінювати право не лише як сукупність державних заборон, зобов'язань і дозволів, а як систему активних інструментів, спрямованих на досягнення певних цілей та задоволення публічних або приватних інтересів учасниками суспільних відносин [80].

Щодо розуміння адміністративно-правових засобів, то в науці адміністративного права переважає таке тлумачення: це сукупність способів, методів, прийомів та інструментів, що перебувають у розпорядженні органів державної влади та застосовуються ними для виконання своїх функцій і завдань згідно з вимогами адміністративного та інших галузей права [25].

В. Т. Комзюк та О. Ю. Салманова вважають, що адміністративно-правові засоби об'єднують функції прийомів і способів, закріплених

адміністративним правом, за допомогою яких суб’єкти публічної адміністрації здійснюють вплив на суспільні відносини у визначеній сфері. Метою такого впливу є забезпечення належного функціонування цих відносин, припинення правопорушень і притягнення винних до відповідальності. Серед властивостей зазначених правових інструментів можна виокремити такі ознаки: вони поєднують різноманітні способи та механізми правового впливу, зокрема дозвільні, заборонні, зобов’язальні й стимулювальні засади, що реалізуються через практику застосування адміністративно-правових норм, зокрема шляхом використання, виконання та дотримання владних розпоряджень; вони передбачають активну управлінську діяльність суб’єктів публічної влади, спрямовану на забезпечення належного функціонування об’єктів адміністративного регулювання; ці засоби реалізуються на підставі чинного законодавства з можливістю застосування примусових заходів, зокрема адміністративної відповідальності для осіб, що вчиняють правопорушення [61].

Існують також інші підходи до сутності адміністративно-правових засобів. Так, О. А. Куций розглядає їх як системну категорію, що складається з правових інститутів, які забезпечують досягнення певної мети та задоволення інтересів суб’єктів права, з акцентом на конкретні сфери публічної діяльності. Учений акцентує, що такі засоби реалізуються через систему дозволів, заохочень, заборон і обмежень [75].

В. К. Колпаков, зі свого боку, відносить до адміністративно-правових засобів приписи, заборони й дозволи. Згідно з визначенням ученого, приписи встановлюють юридичне зобов’язання виконувати певні дії за умов, передбачених правовою нормою; заборони – це юридичні обов’язки утримуватись від певних дій за аналогічних умов; а дозволи надають право вибору – вчиняти або не вчиняти дії, які дозволені нормою, на власний розсуд [59, с. 56–57].

З урахуванням вищенаведеного, пропонуємо під адміністративно-правовими засобами механізму адміністративно-правового забезпечення

функціонування OSINT у сфері національної безпеки розуміти сукупність правових інструментів (способів, методів тощо), закріплених нормами адміністративного права, які використовуються для реалізації завдань, що спрямовані на забезпечення національної безпеки шляхом здійснення розвідки з відкритих джерел і дозволяють ефективно виявляти та протидіяти загрозам національній безпеці завдяки функціонуванню OSINT. Ці засоби призначені для здійснення визначеного кола заходів з боку суб'єктів механізму забезпечення функціонування OSINT у сфері національної безпеки, і дозволяють здійснювати розвідку з відкритих джерел, моніторинг, аналіз та узагальнення відповідної інформації, а також реагувати на ризики й загрози у сфері національної безпеки.

На нашу думку, адміністративно-правовим засобам забезпечення функціонування OSINT у сфері національної безпеки притаманні такі властивості:

1. Нормативна визначеність. Адміністративно-правові засоби функціонування OSINT закріплені у нормах адміністративного права та регулюються законодавчими та підзаконними правовими актами, що встановлює правові підстави та процедури для здійснення OSINT;

2. Цілеспрямованість засобів полягає у їх спрямованості на досягнення конкретних публічних цілей, а саме – забезпечення національної безпеки шляхом ефективного використання інформації з відкритих джерел для запобігання, виявлення й протидії загрозам у сфері національної безпеки;

3. Комплексність. Адміністративно-правові засоби включають різні методи правового регулювання, такі як дозволи, заборони, приписи, зобов'язання та заохочення, що разом утворюють систему заходів і процедур для збору та аналізу інформації;

4. Функціональність означає, що засоби забезпечують виконання адміністративно-правових функцій суб'єктами здійснення розвідки з відкритих джерел, і є необхідними для ефективної організації роботи OSINT;

5. Оперативність і адаптивність. Адміністративно-правові засоби є інструментами, здатними до швидкого реагування на нові загрози та виклики. Вони адаптовані для динамічних умов інформаційного середовища, швидкі зміни у якому вимагають прийняття негайних і гнучких рішень;

6. Є елементами адміністративно-правового впливу. Оскільки ці засоби мають адміністративно-правовий характер, їх застосування може супроводжуватися заходами адміністративного примусу, зокрема застосуванням заходів адміністративного попередження (контроль, нагляд, моніторинг), які спрямовані на вчасне виявлення загроз національній безпеці з метою виявлення та притягнення осіб, які створюють такі загрози до відповідальності.

Багатоманітність засобів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки дозволяє провести їх класифікацію, що дає змогу детальніше розглянути їхні особливості та ефективність у забезпеченні національної безпеки.

Вітчизняні науковці пропонують різні підходи до класифікації адміністративно-правових засобів, враховуючи їхню природу, функції та сферу застосування. В. Б. Авер'янов запропонував поділ адміністративно-правових засобів на регулятивні та охоронні. Регулятивні засоби спрямовані на створення, зміну або припинення прав і обов'язків суб'єктів адміністративного права, до них відносяться нормативно-правові акти, адміністративні договори та інші форми правового регулювання, які застосовуються до поведінки суб'єктів у конкретних правовідносинах. Охоронні засоби, натомість, передбачають захист правопорядку та забезпечення правомірної поведінки, зокрема, через адміністративні притягнення, заходи адміністративного примусу, контрольні та наглядові повноваження органів виконавчої влади.

Адміністративно-правові інструменти становлять один із різновидів правових засобів поряд із кримінально-правовими, цивільно-правовими, дисциплінарними тощо. Щодо змістовного наповнення категорії

адміністративно-правових засобів, варто зазначити, що в науковій літературі відсутній усталений підхід до їхнього визначення. Зосередимо увагу на окремих теоретичних позиціях стосовно розуміння цієї правової категорії. Так, за В. К. Колпаковим, до адміністративно-правових засобів належать приписи, заборони та дозволи. Приписи розглядаються як встановлення безпосереднього юридичного обов'язку вчиняти певні дії в межах, визначених правовою нормою. Заборони, у свою чергу, передбачають юридичне зобов'язання утримуватись від конкретних дій за умов, окреслених нормативним приписом. Дозволи – це надання правової можливості діяти або не діяти в межах, установлених нормою, за власним розсудом [59, с. 56–57].

Варто також зауважити, що залежно від конкретної сфери суспільних відносин та об'єкта адміністративно-правового впливу, виокремлюються й інші типи адміністративно-правових засобів.

В. М. Кондратенко пропонує наступну класифікацію адміністративно-правових засобів гарантування прав і свобод осіб з обмеженими можливостями: за формами впровадження: регуляторні юридичні засоби – комплекс норм адміністративного законодавства, які регламентують питання формування необхідних соціальних умов для втілення та охорони прав і свобод осіб з обмеженими можливостями; структурні юридичні засоби – легітимні діяння державних інституцій, на які покладено функції щодо забезпечення реалізації та захисту прав і свобод осіб з обмеженими можливостями; за суб'єктами впровадження: юридичні засоби, що застосовуються органами виконавчої гілки влади; юридичні засоби, що використовуються виконавчими структурами місцевого самоврядування; юридичні засоби, що задіюються державними правозахисними органами; за способами впровадження: юридичні засоби безпосередньої дії – прямо здійснюють владний вплив на адміністративно-правові взаємини з відповідних аспектів обмежених можливостей; юридичні засоби опосередкованої дії – формують передумови для адміністративно-правового гарантування прав і свобод осіб з обмеженими можливостями через

використання юридичних засоби; за напрямами впровадження: юридичні засоби, що застосовуються у нормотворчій діяльності; юридичні засоби, що використовуються під час адміністративно-виконавчої діяльності; за функціональними рівнями впровадження: організаційно-регулятивні юридичні засоби – відображають форми адміністративно-правового забезпечення прав і свобод осіб з обмеженими можливостями через встановлення дозволеної, забороненої та обов'язкової поведінки для учасників відповідних суспільних правовідносин; контрольно-інспекційні юридичні засоби – використовуються органами публічної адміністрації при здійсненні своїх контрольних (наглядових) владних повноважень органами публічного управління у сфері забезпечення дотримання і виконання вимог законодавства з питань обмежених можливостей у суспільстві; охоронні юридичні засоби – реалізація заходів адміністративного примусу з метою запобігання правопорушенням, які протиправно зазіхають на права і свободи осіб з обмеженими можливостями, припинення таких правопорушень, а також залучення винних осіб до адміністративної відповідальності; за сферами впровадження: юридичні засоби у галузі громадянських суб'єктивних прав осіб з обмеженими можливостями; адміністративно-правові засоби у сфері політичних суб'єктивних прав осіб з обмеженими можливостями; юридичні засоби у сфері економічних суб'єктивних прав осіб з обмеженими можливостями; адміністративно-правові засоби у галузі соціальних суб'єктивних прав осіб з обмеженими можливостями; юридичні засоби в контексті культурних суб'єктивних прав осіб з обмеженими можливостями; за ступенями впровадження: елементарні юридичні інструменти – застосовуються самостійно або в комбінації з іншими, не пов'язаними між собою юридичними засобами в окремій сфері реалізації прав і свобод осіб з обмеженими можливостями; комплексні юридичні засоби – системне поєднання юридичних інструментів для досягнення спільної мети щодо правового забезпечення прав і свобод осіб з обмеженими можливостями; за часом дії впровадження: постійні юридичні засоби – включені до основного

системного адміністративно-правового арсеналу охорони та захисту прав і свобод осіб з обмеженими можливостями; тимчасові юридичні засоби – застосовуються за необхідності та наявності умов і підстав, передбачених законодавством [64].

До кола адміністративно-правових засобів Ю. В. Гаруст відносить адміністративну нормотворчість, контроль, адміністративне переконання, адміністративний примус [25].

Так, на думку Р. В. Мазурика, адміністративно-правовими засобами організації прокурорської діяльності є: визначення правового статусу прокурора та органів прокуратури в Україні через адміністративно-правові норми; нормативно-правове регулювання функціонування прокуратури; адміністративно-правові взаємовідносини всередині органів прокуратури; загальні концептуальні підходи, доктрини, а також інші науково-дослідні матеріали, що формують теоретичний фундамент у сфері організації прокурорської діяльності; адміністративна практика та процедурна діяльність, які є практичною реалізацією нормативних положень і теоретичних напрацювань у процесі організації функціонування прокуратури в Україні [80].

Проаналізувавши вищенаведене, можемо зазначити, що особлива сфера суспільних відносин, пов’язана зі здійсненням розвідки з відкритих джерел, потребує особливих адміністративно-правових засобів, ґрунтується на її винятковій значущості для національної безпеки. Використання OSINT дає змогу ефективно виявляти, аналізувати й оцінювати потенційні загрози, що виникають у різних сферах суспільного життя, зокрема в інформаційній та кіберпросторовій. Ця діяльність є багатокомпонентною і охоплює збір, обробку, аналіз та зберігання інформації, отриманої з відкритих джерел, що здійснюється завдяки комплексу адміністративно-правових засобів.

Зазначений механізм адміністративно-правового забезпечення має передбачати нормативне визначення повноважень державних органів, що здійснюють OSINT, а також установлення чітких правил і процедур доступу

до відкритих джерел інформації, їх обробки та захисту. Національні нормативні акти, що регулюють діяльність у сфері OSINT, повинні враховувати вимоги як внутрішньої правової системи, так і міжнародного законодавства, зокрема положення Європейської конвенції про права людини, яка закріплює право на приватність. Крім того, необхідно забезпечити баланс між потребами у зборі інформації та правами і свободами громадян, встановлюючи адміністративно-правові обмеження на збирання і використання персональних даних, як передбачено Законом України «Про захист персональних даних».

Отже, особливість цієї сфери суспільних відносин обумовлює необхідність створення ефективного адміністративно-правового інструментарію (засобів), який забезпечить результативну діяльність розвідувальних органів України з одночасним дотриманням основоположних прав і свобод громадян.

У сфері здійснення розвідки з відкритих джерел адміністративно-правові засоби можуть бути класифіковані залежно від специфіки завдань, які вони вирішують, а також від їхньої складності. Така класифікація дозволяє визначити особливості та цільове призначення кожного засобу, що підвищує ефективність функціонування системи OSINT в умовах динамічних загроз національній безпеці.

І. Залежно від завдань правового регулювання у сфері OSINT, можна виділити:

1. Загальні адміністративно-правові засоби, які спрямовані на вирішення універсальних завдань адміністративно-правового регулювання на всіх етапах здійснення OSINT. Завдяки цим засобам здійснюється адміністративно-правове регулювання діяльності з розвідки з відкритих джерел, зокрема забезпечення доступу до інформації, її обробки та захисту, створюються правові підстави та умови для цієї діяльності;

2. Спеціальні адміністративно-правові засоби у сфері OSINT, які можуть бути поділені на два підвиди:

– засоби, що дозволяють виконувати специфічні завдання у сфері OSINT. Вони забезпечують реалізацію окремих правових режимів, необхідних для роботи з відкритою інформацією, як-от правовий режим захисту персональних даних та конфіденційної інформації, правовий режим доступу до інформаційних ресурсів державних і приватних структур тощо. Цей блок адміністративно-правових засобів створює умови для формування ефективного механізму роботи з даними, що впливає на якість та надійність розвідки з відкритих джерел;

– засоби, спрямовані на виконання окремих оперативних завдань у сфері OSINT. Ці засоби є специфічними правовими інструментами, що забезпечують виконання конкретних завдань, наприклад, процедури збору інформації через запити до державних органів, подання скарг на відмову у доступі до публічної інформації, юридичне закріплення угод про співпрацю з міжнародними організаціями тощо.

II. Залежно від ступеню складності, адміністративно-правові засоби у сфері OSINT можна розділити на:

1. Первинні (елементарні) засоби, що охоплюють базові, неподільні приписи, такі як суб'єктивні права та обов'язки органів, що здійснюють OSINT, правила доступу до публічних даних, адміністративні заборони на збір персональних даних без згоди осіб тощо;

2. Комплексні (складні) засоби, що складаються з комбінації первинних засобів і передбачають розробку та реалізацію комплексних нормативно-правових актів, планів, вказівок. До них належать норми, які регулюють міжнародне співробітництво у сфері обміну даними, встановлюють інституційні зв'язки між розвідувальними органами, а також механізми міжвідомчої координації в процесі розвідки з відкритих джерел.

III. За призначенням адміністративно-правові засоби у сфері OSINT поділяються на:

– регулятивні засоби, які встановлюють порядок та способи здійснення розвідки з відкритих джерел, регулюючи діяльність суб'єктів, що здійснюють

OSINT. Вони створюють правове підґрунтя для збирання, обробки та зберігання інформації з відкритих джерел, а також доступ до публічної інформації;

– охоронні засоби, спрямовані на захист правопорядку та недоторканність особистих даних та інформації, що є особливо важливим у контексті використання відкритих джерел та забезпечення національної безпеки. Ці засоби забезпечують: контроль над правомірністю збирання та обробки інформації, а також передбачають механізми відновлення порушених прав; контроль за збереженням інформації, доступу до неї та використання, з метою забезпечення національної безпеки; засоби недопущення витоку інформації та доступу до неї третіх осіб;

– процесуальні (процедурні) засоби, які визначають порядок реалізації регулятивних та охоронних засобів у сфері OSINT. Вони окреслюють стадії процесу збору, обробки та зберігання інформації, способи фіксації інформації, що дозволяє забезпечити ефективне функціонування системи OSINT у правовому полі.

IV. За предметом правового регулювання адміністративно-правові засоби у сфері OSINT можуть бути:

– конституційно-правові – пов’язані з основоположними правами та свободами, зокрема правом на інформацію та забезпечення державної таємниці;

– адміністративні – що регулюють відносини між органами, які здійснюють OSINT, та іншими державними або приватними суб’єктами у питаннях здійснення розвідки з відкритих джерел;

– цивільно-правові – які регулюють взаємодію з приватними структурами у питаннях надання або використання відкритих даних;

– кримінально-правові – що застосовуються у випадках порушення порядку збирання, обробки чи захисту інформації, отриманої з відкритих джерел, якщо таке порушення тягне за собою заходи кримінальної відповідальності.

V. За характером адміністративно-правові засоби можуть бути поділені на:

– матеріально-правові (наприклад, пов’язані із матеріально-правовим, фінансовим, технічним забезпеченням діяльності щодо розвідки з відкритих джерел, щодо зберігання, обробки та використання даних з відкритих джерел);

– процедурні (наприклад, регламентують правотворчі, правозастосовні та правоохоронні процедури здійснення розвідки з відкритих джерел. Тобто, це ті інструменти та методи OSINT, що необхідні для отримання пошукової інформації. Вони включають в себе стадії та етапи здійснення пошукової роботи, алгоритми пошукової діяльності).

VI. За значенням наслідків:

– звичайні (засоби, які пов’язані із застосуванням заходів адміністративної та дисциплінарної відповідальності за порушення у сфері здійснення розвідки з відкритих джерел, зокрема що стосується сфери конфіденційної інформації, та інформації, що містить державну таємницю);

– виняткові (передбачають застосування кримінальної відповідальності за вчинення кримінальних правопорушень при здійсненні розвідки з відкритих джерел).

VII. За часом дії:

– постійні (наприклад, постійне здійснення розвідки з відкритих джерел з метою забезпечення національної безпеки);

– тимчасові (наприклад, заходи, які застосовуються для вирішення локальних завдань з метою виявлення та запобігання окремим загрозам у сфері національної безпеки).

VIII. За типом правового регулювання:

– нормативні засоби (заборони або дозволи, встановлені в нормах права, наприклад, обмеження доступу до певної конфіденційної інформації чи інформації, яка становить державну таємницю);

– індивідуальні засоби (акти застосування права, як-от дозволи на збір інформації з окремих джерел).

IX. За інформаційно-психологічною належністю:

– стимулюючі (надання додаткових пільг або ресурсів для органів, що займаються OSINT);

– обмежуючі (призупинення доступу до певних ресурсів у випадках порушення законодавства).

X. За методами, способами та типами правового регулювання:

– імперативні засоби (обов'язкові норми щодо збереження та захисту зібраних даних);

– диспозитивні засоби (норми, що надають певну свободу вибору у визначенні методів обробки інформації).

Запропонована класифікація адміністративно-правових засобів у сфері OSINT дає змогу забезпечити системний підхід до правового регулювання цієї діяльності, враховуючи її значення для захисту національних інтересів та дотримання прав громадян.

Спеціальні адміністративно-правові засоби у сфері OSINT відіграють ключову роль у регулюванні діяльності суб'єктів, які здійснюють розвідку з відкритих джерел. Ці засоби сприяють забезпеченню належного правового режиму для роботи з інформацією, а також уможливлюють виконання оперативних завдань, спрямованих на забезпечення національної безпеки. Залежно від особливостей і призначення, ці засоби можна поділити на два основні підвиди: засоби для виконання специфічних завдань і засоби для реалізації оперативних функцій.

До засобів, що дозволяють виконувати специфічні завдання у сфері OSINT, належать адміністративно-правові засоби, що забезпечують реалізацію правових режимів, необхідних для ефективної роботи з відкритими джерелами інформації. Суб'єкти, що здійснюють OSINT, використовують ці засоби для створення безпечних і прозорих умов у процесі обробки даних.

Важливою характеристикою спеціальних засобів є дотримання вимог захисту інформації та персональних даних. Зокрема, правовий режим захисту персональних даних передбачає обмеження доступу до інформації, яка може ідентифікувати особу, встановлює обов'язок анонімізації або деперсоналізації даних, якщо вони будуть використовуватись у розвідувальних цілях. Правовий режим доступу до інформаційних ресурсів державних і приватних структур, натомість, визначає порядок і підстави доступу до інформації, яка є у розпорядженні цих суб'єктів. Особливість використання цих засобів полягає в тому, що суб'єкти OSINT зобов'язані дотримуватися встановлених процедур доступу до даних, документування та зберігання інформації, що забезпечує надійність одержаних результатів і мінімізує ризики порушення прав громадян.

До засобів, спрямованих на виконання окремих оперативних завдань у сфері OSINT, відносяться спеціальні правові інструменти, що забезпечують оперативну діяльність у сфері OSINT. Їхня мета – забезпечити можливість швидкого доступу до потрібної інформації, оперативного реагування на загрози та виконання конкретних розвідувальних функцій. Наприклад, використання правового інструмента у вигляді запиту до державних органів дозволяє суб'єктам OSINT отримувати актуальну інформацію з офіційних джерел, що є особливо важливим для формування повної розвідувальної картини.

Іншим прикладом є процедура подання скарг у випадках відмови у доступі до інформації, яка може міститися в публічних базах даних або ресурсах, що перебувають у розпорядженні державних органів. Така скарга є ефективним інструментом захисту права на інформацію, забезпечуючи суб'єктам OSINT змогу оперативного відновлення доступу у разі необґрунтованих відмов.

На рівні міжнародного співробітництва правові засоби включають також юридичне закріплення угод про співпрацю з іноземними організаціями та партнерами. Це важливо для розширення можливостей збору даних та

обміну інформацією, що, зі свого боку, є ключовим для оцінки міжнародних загроз та забезпечення національної безпеки. Особливість таких угод полягає у визначенні порядку обміну інформацією, рівня доступу до неї, а також заходів щодо захисту конфіденційності даних відповідно до вимог міжнародного законодавства.

До цих засобів також можна віднести особливі інструменти, способи, методи та процедури здійснення OSINT, з метою отримання пошукової інформації, використання програмного забезпечення тощо.

Зокрема, автори видання «Використання інструментів та методів OSINT для отримання пошукової інформації» [16, с. 6] зазначають, що розвідка з відкритих джерел має здійснюватися за певним алгоритмом. Класичний алгоритм пошукової діяльності у сфері розвідки з відкритих джерел забезпечує чітку послідовність дій для збору та аналізу інформації, спрямованих на досягнення конкретних розвідувальних цілей. Його дотримання дозволяє суб'єктам OSINT не лише ефективно структурувати пошуковий процес, але й мінімізувати ризики отримання неповної чи недостовірної інформації.

Алгоритм пошукової діяльності в сфері розвідки з відкритих джерел (OSINT) можна деталізувати наступним чином:

1. Визначення вихідних даних та формулювання мети пошуку. Перший етап полягає у чіткому визначенні мети дослідження та аналізі наявних даних про об'єкт (наприклад, ім'я, вік, контактні дані, фотографії, посада тощо). Важливо також ідентифікувати інформаційні прогалини, тобто визначити, яких даних бракує для досягнення поставленої мети, як-от установлення місця перебування особи або ідентифікація реального власника компанії;

2. Визначення необхідних інструментів та методів OSINT. Після формулювання мети дослідження визначається набір інструментів для проведення розвідки. Через різноманіття інформаційних ресурсів та індивідуальність завдань у сфері OSINT універсального набору інструментів

не існує. Вибір пошукових слів, платформ та алгоритмів залежить від конкретного об’єкта та інформаційних потреб;

3. Здійснення пошуку інформації та аналіз зібраних відомостей. Пошук може бути *пасивним* (збір інформації через загальнодоступні джерела: соціальні мережі, блоги, форуми, відкриті бази даних, аналіз персональних даних та активності користувачів) або *активним* (використання платних баз даних, спеціалізованих інструментів, методів соціальної інженерії, сканування відкритих портів). Активні методи часто вимагають специфічних дозволів та інструментів для виявлення слабких місць у захисті об’єкта;

4. Систематизація отриманих даних та формулювання висновків. На основі зібраної інформації створюється структурована картина, яка може бути візуалізована за допомогою діаграм, таблиць або інтелект-карт. Важливим аспектом є документування знайденої інформації та збереження її для подальшого аналізу, зокрема через офлайн-архівування, скріншоти або збереження сторінок у форматі PDF з позначенням дати, часу та джерела;

5. Додаткові пошукові заходи та формування підсумкового звіту. Після аналізу початкових результатів може виникнути потреба у додаткових пошукових заходах. Для цього використовуються додаткові ключові слова, переглядається більша кількість сторінок у пошуковій видачі, застосовуються інші синоніми чи абревіатури. Підсумковий звіт повинен містити верифіковані та надійні дані, що дозволяють обґрунтувати висновки щодо об’єкта дослідження [16, с. 6].

Застосування такого алгоритму підвищує ефективність розвідки з відкритих джерел, сприяючи комплексному аналізу даних і забезпечуючи інформаційну підтримку для ухвалення обґрунтованих рішень у сфері національної безпеки [16, с. 6].

Таким чином, специфічні адміністративно-правові засоби, спрямовані на виконання особливих і оперативних завдань у сфері OSINT, є необхідними інструментами для забезпечення законності, прозорості та ефективності діяльності суб’єктів, що здійснюють розвідку з відкритих джерел. Вони

створюють юридичну основу для роботи з інформацією, що сприяє формуванню надійної системи національної безпеки, адаптованої до сучасних викликів і загроз.

Отже, адміністративно-правові засоби забезпечення функціонування OSINT у сфері національної безпеки можна визначити як сукупність правових інструментів, закріплених нормами адміністративного права, що використовуються для виконання завдань із забезпечення національної безпеки шляхом збору й аналізу інформації з відкритих джерел. Ці засоби спрямовані на виявлення, запобігання та нейтралізацію загроз, забезпечуючи державу інструментами, необхідними для виконання завдань з розвідки та моніторингу інформаційного простору.

Властивостями адміністративно-правових засобів забезпечення функціонування OSINT у сфері національної безпеки є: нормативна визначеність як основа правового регулювання OSINT; цілеспрямованість; комплексність і системність правових інструментів; функціональність та ефективність організації OSINT; оперативність та адаптивність; забезпеченість засобами адміністративного впливу.

Адміністративно-правові засоби забезпечення функціонування OSINT у сфері національної безпеки класифіковано за такими критеріями: залежно від завдань правового регулювання (загальні і спеціальні: засоби, що дозволяють виконувати специфічні завдання у сфері OSINT та засоби, спрямовані на виконання окремих оперативних завдань у сфері OSINT); залежно від ступеня складності: (первинні та комплексні); за призначенням (регулятивні, охоронні та процедурні); за предметом правового регулювання (конституційно-правові, адміністративні, кримінально-правові та цивільно-правові); за характером (матеріально-правові та процесуальні); за наслідками (звичайні та виняткові); за часом дії (постійні і тимчасові); за типом правового регулювання (нормативні і індивідуальні); за інформаційно-психологічною належністю (стимулюючі та обмежувальні); за методами (імперативні та диспозитивні).

Згідно з аналізом адміністративно-правові засоби у сфері OSINT поділяються на регулятивні та охоронні. Регулятивні засоби забезпечують правові основи для здійснення збору, обробки та зберігання інформації, тоді як охоронні засоби зосереджуються на захисті прав громадян, правопорядку та забезпеченні недоторканності особистих даних. Важливо, що використання регулятивних засобів дає змогу створити правові гарантії доступу до інформації, тоді як охоронні засоби запобігають витоку та несанкціонованому доступу до даних, що має особливу значущість в умовах кібербезпеки.

Чіткі процедурні правила є необхідними для ефективного застосування регулятивних та охоронних засобів, що забезпечує впорядкованість і послідовність дій державних органів. Відсутність належної процесуальної основи може призвести до зловживань або недоліків у зборі, зберіганні та використанні інформації.

Ефективне забезпечення національної безпеки потребує тісної координації з міжнародними організаціями та партнерами. Комплексні адміністративно-правові засоби, що включають інституційні зв’язки та механізми співпраці з іншими країнами, сприяють обміну даними та інформацією, необхідними для глобальної боротьби з загрозами національній безпеці.

Адміністративно-правові засоби у сфері OSINT мають відповідати вимогам захисту прав людини, зокрема права на приватність і захист персональних даних. Надмірне втручання держави в особисте життя громадян може порушувати конституційні права і викликати суспільний спротив. Тому важливо, щоб адміністративно-правові засоби забезпечення OSINT були пропорційними до рівня загрози та узгодженими з основоположними правами людини.

Адміністративно-правовий механізм OSINT може включати як постійні заходи, що забезпечують стабільний моніторинг загроз, так і тимчасові заходи, які застосовуються для реагування на конкретні інциденти або кризові

ситуації. Це дозволяє адаптувати правові інструменти до поточних умов та ризиків.

Адміністративно-правові засоби можуть бути імперативними (обов'язковими) або диспозитивними (надають певну свободу дій суб'єктам OSINT). Імперативні засоби, наприклад, встановлюють обов'язкові вимоги до зберігання та захисту даних, тоді як диспозитивні надають свободу вибору методів обробки інформації, що дозволяє суб'єктам OSINT більш гнучко адаптуватися до нових викликів.

Важливим аспектом адміністративно-правових засобів є їх здатність стимулювати суб'єктів OSINT до дотримання вимог безпеки через систему заохочень та обмежень. Стимулюючі заходи можуть передбачати надання пільг або ресурсів, що підвищують ефективність їхньої діяльності, тоді як обмежувальні заходи запобігають можливим порушенням, шляхом контролю за додержанням правових норм.

Ефективність адміністративно-правових засобів значною мірою залежить від наявності механізмів контролю за додержанням установлених правових норм. Такий контроль може здійснюватися як внутрішніми механізмами державних органів, так і через залучення громадських організацій або міжнародних структур.

2.4 Гарантії механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки

Використання OSINT дає змогу органам національної безпеки оперативно реагувати на потенційні загрози, своєчасно виявляти ризики та протидіяти незаконним діям, використовуючи доступні дані з відкритих джерел. Проте ефективність цього інструменту значною мірою залежить від наявності надійних адміністративно-правових гарантій, які дозволяють

забезпечити належне функціонування OSINT та захистити інтереси держави та громадян у сфері національної безпеки.

Національна безпека є основоположною цінністю будь-якої держави, що передбачає захист не лише від зовнішніх загроз, але й від внутрішніх викликів, які можуть вплинути на стабільність країни, її політичну, економічну, соціальну та інформаційну сфери. В умовах сучасних гібридних загроз, до яких входить також інформаційне та кібернетичне втручання, забезпечення безпеки потребує комплексного підходу, що включає різноманітні інструменти та методи розвідки, серед яких OSINT займає особливе місце.

OSINT, або розвідка з відкритих джерел, полягає в аналізі інформації, що є у вільному доступі, наприклад, у соціальних мережах, ЗМІ, на державних та приватних веб-сайтах. Незважаючи на свою відкритість, така інформація може мати стратегічне значення і забезпечувати об’єктивну основу для прийняття управлінських рішень у сфері національної безпеки. Проте, оскільки OSINT оперує відкритою інформацією, особливо важливим стає дотримання адміністративно-правових гарантій, які сприятимуть ефективному та правомірному застосуванню цього механізму.

Забезпечення функціонування OSINT у правовому полі передбачає наявність чітко визначених механізмів захисту прав і свобод громадян, що унеможливлює зловживання з боку органів, що здійснюють розвідку. Зокрема, адміністративно-правові гарантії є інструментами, які дозволяють врегулювати відносини між суб’єктами, що застосовують OSINT, і особами, чиї дані можуть бути предметом розвідки. Завдяки цьому забезпечується баланс між інтересами держави у збереженні безпеки та необхідністю захисту персональних даних громадян.

Дослідження гарантій механізму адміністративно-правового забезпечення OSINT є актуальним також у зв’язку з тим, що їх відсутність або недостатність може призводити до правових колізій, зловживань, або навіть порушення прав людини. На сьогоднішній день виникають нові виклики, зокрема у сфері кібербезпеки та інформаційної політики, які ускладнюють

процеси збору, аналізу та зберігання інформації з відкритих джерел. Тому обґрунтоване і системне регулювання, підкріплене належними адміністративно-правовими гарантіями, є запорукою безперебійної та законної роботи OSINT.

Гарантії адміністративно-правового механізму функціонування OSINT є важливими з кількох причин. По-перше, вони дозволяють упорядкувати правовідносини між державними органами, які здійснюють розвідку, та суб'єктами права, забезпечуючи при цьому дотримання прав і свобод громадян. По-друге, такі гарантії забезпечують прозорість діяльності розвідувальних органів, зокрема в питаннях дотримання правових норм під час обробки інформації з відкритих джерел. Враховуючи можливість отримання доступу до особистої інформації в ході OSINT, особливо важливим є забезпечення правової безпеки та прозорості процедур для запобігання порушенню прав осіб.

По-третє, правові гарантії сприяють зниженню ризиків, пов'язаних із безконтрольним використанням відкритих джерел. У цьому контексті адміністративно-правові гарантії включають такі важливі механізми, як правові регламенти, чіткі критерії доступу до даних, процедури захисту зібраної інформації та відповідальність за незаконне використання отриманої інформації. Зокрема, забезпечення дотримання таких гарантій дозволяє уникнути витоку або зловживання даними, які можуть бути використані не на користь національної безпеки.

По-четверте, ефективна система адміністративно-правових гарантій дозволяє досягти стабільності в правовому регулюванні сфери OSINT, що забезпечує правову визначеність та передбачуваність для суб'єктів розвідувальної діяльності. Це особливо важливо в умовах постійного розвитку технологій і змін у характері загроз національній безпеці, які вимагають оперативного та юридично обґрунтованого реагування.

Таким чином, адміністративно-правові гарантії механізму забезпечення функціонування OSINT є важливим аспектом діяльності державних органів у

сфері національної безпеки. Вони не тільки створюють правову основу для функціонування OSINT, але й забезпечують захист прав громадян та запобігають зловживанням з боку суб'єктів розвідувальної діяльності. Дослідження цих гарантій сприятиме вдосконаленню правового регулювання та забезпечить ефективну реалізацію завдань, пов'язаних із забезпеченням національної безпеки за допомогою OSINT.

Еволюція поглядів на правові гарантії в юридичній науці пройшла складний і тривалий шлях, що охоплює перехід від простого переліку окремих гарантій до формулювання загальної дефініції цієї категорії та розробки її систематизованих класифікацій до відповідної сфери суспільних відносин [1, с. 8–9]. Багатоманітність наукових підходів до визначення понять «юридичні гарантії захисту прав» і похідного від нього «адміністративно-правові гарантії захисту прав» вказує на відсутність єдиного підходу щодо їхнього розмежування з такими поняттями, як «юридичні гарантії», «гарантії прав», «гарантії реалізації прав». Це зумовлює необхідність ґрунтовного дослідження їхньої сутності та формулювання чітких дефініцій. У межах обраного напряму дослідження особливого значення набуває з'ясування змісту поняття адміністративно-правових гарантій механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки.

Поняття «гарантія» широко використовується не лише в юридичній науці, але й в інших галузях знань, зокрема в економіці та політології, що підкреслює його універсальний характер. У тлумачних словниках термін «гарантія» має кілька значень, серед яких виділяються наступні: 1) «запорука виконання зобов'язань, реалізації прав» [15, с. 173]; 3) «надання чи створення матеріальних засобів; охорона особи, об'єкта від небезпеки; гарантування чогось» [94, с. 42]. Відповідно до словника української мови «гарантія» означає «поруку у чомусь, забезпечення чого-небудь» [7, с. 29]. Водночас науковці трактують й етимологію цього терміна і пов'язують його походження з французьким словом «garantie» (від «garantir» – забезпечувати) [72, с. 519–523]. Таким чином, слово «гарантія» тісно пов'язане з процесами забезпечення

та охорони, а також із системою заходів, які сприяють захисту об’єкта, для якого ці гарантії встановлюються. Це підкреслює важливість гарантій як необхідних елементів правового регулювання, які забезпечують захист прав та свобод особистості, а також сприяють стабільності правовідносин у суспільстві.

Як бачимо, поняття «гарантії» охоплює собою не лише забезпечення реалізації прав і свобод, але й включає комплекс правових механізмів, спрямованих на захист прав суб’єктів права, що потребує подальшого дослідження та концептуалізації в межах адміністративно-правових відносин.

У науковій літературі адміністративного права термін «адміністративно-правові гарантії» вживається в різних контекстах. Він може стосуватися адміністративного права загалом, механізмів адміністративно-правового регулювання, специфічних адміністративно-правових режимів, а також характеристик адміністративно-правового статусу особи. Крім того, цей термін застосовується у рамках розгляду способів забезпечення законності в публічному управлінні та інших аспектах.

Поняття «адміністративно-правові гарантії» є узагальнюючим терміном для групи адміністративно-правових засобів, які забезпечують перетворення ідеальних та абстрактних моделей адміністративно-правових відносин у конкретні, реальні практики. Гарантії відіграють важливу роль у механізмі адміністративно-правового забезпечення прав як фізичних, так і юридичних осіб, особливо в контексті здійснення державного нагляду та контролю, у сфері реалізації прав і свобод людини, діяльності відповідних державних органів. Це підкреслює їх значущість як для науки адміністративного права, так і для сфери суспільних відносин, що регулюється нормами адміністративного права.

Беручи до уваги викладений матеріал, можна сформулювати низку попередніх висновків щодо сутності гарантій як правової категорії. По-перше, гарантії становлять собою необхідну складову, що включає різноманітні елементи, спрямовані на забезпечення реалізації та охорону базових

суспільних цінностей, зокрема прав і свобод людини. По-друге, гарантії завжди пов'язані з конкретним індивідом і його правовим становищем у державі. По-третє, змістовне наповнення гарантій змінюється залежно від характеру правового статусу особи, а також від правовідносин, у яких вона бере участь. По-четверте, ключовим призначенням закріплення гарантій є охорона і забезпечення прав та свобод особи, що реалізується через захисну і забезпечувальну складові; водночас вони виконують й упереджувальну роль, попереджаючи можливі правопорушення. По-п'яте, у межах механізму реалізації прав і свобод людини гарантії мають змінний характер, активізуючись у відповідь на певні обставини – зокрема, на порушення або посягання на права; до цього моменту вони, зазвичай, перебувають у стані потенційної готовності. По-шосте, дієвість гарантій неможлива без їх нормативного закріплення: у разі відсутності відповідного законодавчого регулювання вони втрачають юридичну силу і не здатні ефективно виконувати своє функціональне призначення. По-сьоме, реалізація гарантій не потребує створення окремих правових механізмів, оскільки їх дія забезпечується всією системою чинного права. Загальні гарантії прав і свобод особи набувають особливих рис залежно від виду правовідносин, учасником яких є особа, а також сфери, у межах якої ці правовідносини виникають [69].

Що стосується визначення адміністративно-правових гарантій, слід відзначити, що в наукових колах адміністративного права існує різноманітність підходів до їх трактування.

Зокрема, В. Б. Авер'янов визначає адміністративно-правові гарантії прав та свобод громадян як комплекс адміністративно-правових засобів, що забезпечують повноту, стійкість і стабільність прав і свобод у сфері державного управління [1].

О. І. Наливайко вказує на те, що адміністративно-правові гарантії прав і свобод людини є напрямом діяльності органів державної влади, місцевого самоврядування, громадських об'єднань і самих громадян, спрямованим на

забезпечення прав і свобод для їх законного та безперервного виконання і захисту [92].

В. З. Чорнописька визначає адміністративно-правові гарантії як умови, засоби та дії державних органів, уповноважених забезпечувати фактичну реалізацію прав та їх надійний захист [168, с. 61–62].

І. О. Ієрусалімова розглядає гарантії крізь призму адміністративно-правового механізму забезпечення прав і свобод людини як сукупність законодавчо встановлених засобів, які охороняють і захищають права громадян, а також припиняють і усувають порушення, надаючи можливості для їх поновлення [5]. Ю. С. Шемшученко – як умови, засоби і способи, які забезпечують реалізацію, всебічну охорону та захист прав особи, суб’єктів правовідносин [177].

На думку Е. О. Олефіренко, адміністративно-правові гарантії прав і свобод людини становлять самостійну сукупність елементів, закріплених у нормах адміністративного права. До цих елементів належать адміністративна правоздатність, яка визначається як здатність мати права, передбачені адміністративно-правовими нормами, та адміністративна дієздатність, що включає можливість громадян реалізувати свої конституційні права і обов’язки, конкретизовані в адміністративному законодавстві [95].

Таким чином, різноманітність підходів до визначення адміністративно-правових гарантій свідчить про складність та багатосторонність цього поняття, що потребує подальшого дослідження та уточнення в контексті гарантій механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Згідно з О. Навроцьким аналіз наукових поглядів дослідників-адміністративістів свідчить про те, що термін ««адміністративно-правові гарантії» слід розглядати крізь призму двох ключових аспектів. Перший – відповідає на запитання «як забезпечуються права», тоді як другий – «що саме забезпечується». Більшість учених, вивчаючи цю проблему, дотримуються думки про те, що, наприклад, права дитини забезпечуються за допомогою

конкретних засобів. Крім того, терміни «способи», «умови», «інститути», «принципи» та «норми» також використовуються в наукових дискусіях. При цьому важливо розглянути, чи є доцільним вживання всіх цих термінів …. На думку уже згаданого О. Навроцького, термін «засоби» є найбільш влучним, оскільки він оптимально відображає механізми, за допомогою яких гарантуються права дитини [89]. Водночас суперечливим, на наш погляд, є необґрунтоване обмеження «гарантій» способами забезпечення. Вважаємо, що «гарантії» включають в себе умови та засоби, які не тільки гарантують права осіб у визначеній сфері, але й створюють умови для ефективної діяльності органів державної влади та місцевого самоврядування, спрямовані на реалізацію своїх повноважень у відповідних сферах суспільних відносин. Цей підхід зосереджується на виконанні функцій і завдань органів державної влади, адже гарантії є тими умовами, що визначають спроможність їх здійснювати.

Отже, наявна різноманітність наукових поглядів щодо визначення адміністративно-правових гарантій підтверджує необхідність їх подальшого дослідження та систематизації в контексті специфіки функціонування OSINT. Визначення та реалізація цих гарантій є важливими для зміцнення правового порядку і забезпечення національної безпеки в умовах сучасних викликів і загроз. Систематизація вищезазначених поглядів дає підстави стверджувати, що адміністративно-правові гарантії в сфері національної безпеки, зокрема у контексті функціонування OSINT, мають бути комплексними і включати механізми, що забезпечують законність, прозорість і ефективність дій державних органів. Це, натомість, сприяє не лише захисту прав осіб, що беруть участь у процесі збору інформації, а й створює умови для більш ефективного використання відкритих джерел інформації в інтересах національної безпеки. Таким чином, визначення і розуміння гарантій механізму адміністративно-правового забезпечення функціонування OSINT є важливим кроком у розвитку теорії адміністративного права та практики забезпечення національної безпеки.

Загалом гарантії механізму адміністративно-правового забезпечення функціонування OSIN) у сфері національної безпеки представляють собою сукупність адміністративно-правових засобів, які створюють умови для ефективної реалізації, захисту та охорони прав і свобод суб'єктів, залучених до процесу збору та аналізу інформації з відкритих джерел.

Гарантії механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки охоплюють законодавчо закріплені механізми, які забезпечують стабільність і стійкість діяльності розвідувальних органів, а також сприяють захисту прав громадян і забезпечують їхнє право на доступ до інформації, що може бути використана в інтересах національної безпеки. Гарантії механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки є ключовими для формування правового середовища, яке дозволяє ефективно реалізовувати завдання з розвідки, забезпечуючи при цьому захист прав і законних інтересів громадян. Вони забезпечують не лише законність дій органів державної влади, але й створюють умови для об'єктивності та прозорості розвідувальної діяльності, сприяючи формуванню довіри суспільства до діяльності держави в сфері національної безпеки.

Як зазначає Д. О. Кошиков, усі гарантії суб'єктів у відповідній сфері закріплені в чинному законодавстві, що надає їм юридичної сили. Проте ці гарантії не мають чіткого упорядкування і часто розподілені між різними нормативно-правовими актами, як законодавчими, так і підзаконними. У зв'язку з цим у науковій літературі розробляються класифікації для систематизації цих гарантій. Однією з основних – є їх поділ на загальні та спеціальні. Загальні гарантії об'єднують соціальні, економічні, політичні та ідеологічні елементи, тоді як спеціальні – стосуються винятково юридичних аспектів [22, с. 202; 34, с. 99; 69].

Д. О. Іщук пропонує класифікувати гарантії реалізації адміністративно-правового статусу органів державної влади за кількома критеріями: по-перше, за сферою впливу: на юридичні, економічні, соціальні, ідеологічні, політичні

та інші; по-друге, за специфікою правового статусу, що дозволяє виділити гарантії, які забезпечують реалізацію статусу публічного службовця, а також гарантії, що регулюють статус конкретної посадової особи в системі публічної служби. Нарешті, за напрямом впливу на посадову особу виділяються позитивні гарантії, які сприяють ефективній діяльності, і негативні гарантії, що можуть призвести до негативних наслідків у разі неналежного виконання посадових обов'язків [49].

У своєму дослідженні В. М. Дожанин акцентує увагу на гарантіях адміністративно-правового забезпечення прав і свобод громадян у площині запобігання та протидії корупційним проявам. Він класифікує ці гарантії на загального характеру (до яких належать економічні, політичні, ідеологічні та соціальні чинники) та спеціальні, тобто юридичні. Останні, у свою чергу, поділяються на три основні групи: нормативні, інституційно-організаційні та організаційно-правові гарантії [34, с. 99–100].

Згідно з А. Чеможуровою гарантії це – принципи права, норми права, суб'єктивні права та юридичні обов'язки, юридична відповідальність, правові обмеження, правові стимули, правові заохочення, акти застосування норм права та інші [166]. На думку Л. В. Сороки, нагляд і контроль як елементи системи державних гарантій представляють собою комплекс правових, організаційних, інформаційно-інспекційних заходів [149, с. 176]. Ці засоби застосовуються у конструюванні адміністративно-правових гарантій. Їх набір дозволяє гарантувати дію прав фізичних і юридичних осіб при здійсненні державного нагляду та контролю, залежно від статусу суб'єкта гарантій, переслідуваних завдань та функцій, що виконуються [35].

Важливо акцентувати, що гарантії прав суб'єктів закріплені в чинному законодавстві, що забезпечує їх легітимність; проте вони не є упорядкованими і часто розосереджені в різних законах та підзаконних нормативно-правових актах. Це зумовлює потребу в їх систематизації, що часто реалізується через класифікацію в науковій літературі. Такий підхід також застосовується для визначення гарантій прав і суб'єктів у різних правовідносинах [69].

Таким чином, розуміння та систематизація адміністративно-правових гарантій у застосуванні розвідки з відкритих джерел є важливими для забезпечення правового регулювання в цій сфері, адже чітке класифікування гарантій дає змогу забезпечити їх ефективність і відповідність сучасним вимогам.

З огляду на багатовимірну участь суб'єктів адміністративно-правових правовідносин у реалізації державної політики у сфері забезпечення функціонування механізму OSINT у контексті гарантування національної безпеки, а також беручи до уваги особливості забезпечення їхніх правових гарантій, вбачається обґрунтованим здійснити систематизацію таких юридичних гарантій за такими критеріями:

1. За сферою дії:

1.1. Загальні гарантії – це такі, що створюють умови та підґрунтя для забезпечення прав всіх учасників правовідносин у сфері OSINT без винятку. Йдеться про принципи та норми права, які створюють умови щодо гарантування не порушення конституційних прав і свобод осіб у питаннях доступу до інформації і використання персональних даних. Наприклад, обов'язок державних органів нести юридичну відповідальність за неналежне використання відкритої інформації, що може загрожувати національній безпеці, або за порушення принципів законності та конфіденційності.

1.2. Спеціальні гарантії – ці гарантії є специфічними і стосуються суб'єктів, що здійснюють діяльність у рамках OSINT. Це ті гарантії, які створюють умови ефективної діяльності відповідних суб'єктів щодо збору, обробки та аналізу інформації, а також забезпечення незалежності цих суб'єктів у їхній професійній діяльності та прийнятті рішень. Наприклад, право окремих органів забезпечувати незалежність під час проведення аналітичних досліджень, що стосуються національної безпеки, або приймати обов'язкові для виконання рішення з питань аналізу та поширення відкритої інформації; матеріально-технічні та фінансові умови для здійснення OSINT тощо.

2. За суб’єктами реалізації гарантій:

2.1 Гарантії прав вищих органів державної влади. Наприклад, право Ради національної безпеки та оборони України (РНБО) здійснювати контроль за дотриманням вимог законності у діяльності суб’єктів OSINT.

2.2 Гарантії прав центральних органів виконавчої влади. Наприклад, право Служби безпеки України та Міністерства оборони України отримувати доступ до відкритої інформації, необхідної для аналізу загроз національній безпеці, з дотриманням обмежень щодо її поширення.

2.3 Гарантії прав інститутів громадянського суспільства. Наприклад, право громадських організацій брати участь у громадському контролі над діяльністю органів, що використовують OSINT, задля дотримання прав людини.

3. За змістом юридичні гарантії поділяються на:

3.1 Нормативні гарантії – включають прийняття нормативних актів, що регулюють діяльність суб’єктів OSINT, наприклад, ухвалення законів і підзаконних актів щодо доступу до відкритих джерел інформації з визначенням правових меж використання таких даних.

3.2 Організаційні гарантії – забезпечують незалежність організацій та аналітичних центрів, які займаються OSINT. Наприклад, право цих установ на доступ до відкритих даних, з урахуванням правових обмежень, участь у розробці державних стратегій та нормативно-правових актів з питань національної безпеки.

3.3 Матеріально-технічні гарантії – забезпечують належний рівень ресурсів для ефективного функціонування OSINT. Наприклад, державне фінансування для підтримки спеціалізованих аналітичних систем, необхідних для обробки та аналізу даних з відкритих джерел.

Запропонована класифікація юридичних гарантій механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки забезпечує системність і створює правову основу для ефективного

функціонування цього інструменту, спрямованого на виявлення та аналіз відкритих джерел інформації задля захисту національних інтересів.

На підставі систематизації вказаних гарантій ми можемо виокремити такі їх властивості: по-перше, вони мають публічно-правовий характер і орієнтовані на забезпечення національної безпеки; похідні від конституційних прав і свобод, які є універсальними у сфері захисту прав людини та діяльності органів державної влади, які здійснюють розвідку з відкритих джерел; реалізуються в адміністративно-правовому порядку, мають правореалізаційний та правоохоронний зміст; є інструментом, завдяки якому створюються умови для ефективного функціонування OSINT у сфері національної безпеки; законодавчо закріплені у законах та підзаконних правових актах, які визначають адміністративно-правовий статус відповідних суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки; мають організаційний, правовий, правоохоронний та матеріально-технічний зміст.

Безумовно, складовим елементом гарантій механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки є принципи, які визначають засади функціонування цього механізму та діяльності суб'єктів механізму.

Ключовими принципами, які визначають механізм формування державної політики у сферах національної безпеки та оборони, є:

1) пріоритетність принципу верховенства права, забезпечення підзвітності, законності, відкритості, а також дотримання основ демократичного цивільного нагляду за функціонуванням сектору безпеки й оборони та використанням сили;

2) неухильне дотримання положень міжнародного права, участь України у міжнародних ініціативах з підтримання миру та безпеки, а також у міждержавних системах і механізмах колективної безпеки;

3) послідовний розвиток сектору безпеки й оборони як базового інструмента реалізації державної стратегії у сфері національної безпеки та оборонної політики [123].

Зрозуміло, що ці принципи повинні становити основу функціонування OSINT у сфері національної безпеки. Проте вони не є вичерпними для цієї діяльності, оскільки функціонування OSINT у цій сфері охоплює й інші важливі аспекти. Перейдемо до детального аналізу цих принципів.

Одним із основних для механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки є принцип законності. Він вимагає суворого дотримання правових норм і обмежень при здійсненні OSINT, особливо в межах національної території. Проте у випадку OSINT у сфері національної безпеки цей принцип має певні особливості. В. В. Прощаєв у своєму дослідженні акцентував увагу на принципі законності як спірному у контексті діяльності розвідувальних органів, які часто працюють за межами національної юрисдикції, порушуючи законодавство інших держав [136, с. 100]. Дослідник підкреслював, що принцип законності може бути закріплений у нормативно-правовому документі, однак із певними застереженнями, наприклад: «у разі застосування розвідувальних методів та засобів на території власної держави» або «під час використання оперативно-розшукових заходів».

На думку дослідника, це саме стосується і принципу поваги до прав і свобод людини, який також обмежується національними кордонами. У розвідувальних операціях, що проводяться за межами держави, повага до прав громадян є часто неможливою, а тому застосування цього принципу є актуальним переважно в рамках національної території або у разі, коли використовуються методи, передбачені оперативно-розшуковим законодавством [136, с. 100].

Принцип дотримання прав і свобод людини передбачає обов’язок шанобливого ставлення до прав людини і громадянина та заборону їх обмеження без наявності належних правових підстав.

Захист прав і свобод громадян є ключовою вимогою для забезпечення здійснення OSINT. Реалізація цього принципу повинна здійснюватися з урахуванням законодавчих обмежень, які діють на території держави і яких мають дотримуватися суб'єкти здійснення розвідки з відкритих джерел. Важливо забезпечувати, щоб заходи, що вживаються в рамках OSINT, не порушували права на приватність та недоторканність приватного життя громадян. Дія цього принципу обмежена, оскільки повага до прав громадян стає значущою переважно в рамках національної юрисдикції та застосовується лише тоді, коли розвідувальні методи спрямовані на усунення загроз національній безпеці.

Наступним є принцип пропорційності, який передбачає, що заходи, вжиті для забезпечення національної безпеки через OSINT, повинні бути пропорційними меті, яка досягається, і не перевищувати необхідного обсягу втручання. OSINT має бути спрямований на мінімізацію негативного впливу на приватне життя осіб, забезпечуючи баланс між ефективністю аналітичної діяльності та захистом прав громадян.

Важливим у здійсненні розвідки з відкритих джерел є принцип конфіденційності, який передбачає, що діяльність, пов'язана з OSINT, має включати обов'язок держави і відповідних суб'єктів її здійснення, захищати зібрану інформацію від несанкціонованого доступу або витоку. Це стосується як захисту персональних даних, так і забезпечення охорони інформації, що має відношення до національної безпеки.

Сутність принципу прозорості та підзвітності полягає у тому, що діяльність, пов'язана зі здійсненням OSINT, має здійснюватися під контролем уповноважених органів з метою забезпечення підзвітності і дотримання законодавства. Це забезпечує можливість громадського контролю та розгляду випадків зловживання розвідувальними органами своїми повноваженнями. Прозорість і підзвітність знижують ризики перевищення повноважень та зловживань.

Принцип незалежності є важливим для отримання об’єктивної та неупередженої інформації. Він означає, що суб’єкти, що здійснюють діяльність у сфері OSINT, повинні бути незалежними від стороннього впливу під час аналізу даних, формування висновків і ухвалення рішень. Незалежність забезпечує об’єктивність та точність результатів діяльності у сфері національної безпеки.

Не можна ігнорувати й принцип верховенства права. Цей принцип передбачає, що жодна особа не стоїть понад законом, держава не має права притягати людину до відповідальності інакше як за вчинення правопорушення, передбаченого законом, і винятково у спосіб, встановлений чинним законодавством [171, с. 442].

Принцип верховенства права є фундаментальним для ефективного функціонування механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки. Він визначає пріоритет права над будь-якими іншими нормативними актами та гарантує, що держава, її органи та посадові особи діють винятково в межах, установлених правом, що дозволяє уникнути довільного втручання у права та свободи громадян.

Принцип верховенства права як гарантія механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки, охоплює декілька ключових аспектів. По-перше, всі дії, пов’язані з OSINT у сфері національної безпеки, мають базуватися на правових нормах, що забезпечує передбачуваність і прозорість діяльності державних органів. Це стосується як процедур збору та аналізу відкритих даних, так і засобів захисту інформації та дотримання прав людини. По-друге, дотримання прав і свобод людини. Верховенство права передбачає, що всі заходи з боку державних органів щодо забезпечення національної безпеки, включаючи OSINT, повинні відповідати міжнародним стандартам прав людини. Це особливо важливо, коли збір та обробка даних можуть зачіпати право на приватність або інші фундаментальні права. По-третє, принцип верховенства права вимагає, щоб усі учасники адміністративно-правових відносин у сфері OSINT були рівними перед

законом. Це стосується як державних органів, що здійснюють OSINT, так і суб'єктів, інформація про яких збирається. Усі рішення щодо збору та аналізу даних повинні бути обґрунтованими, а неупередженість має бути забезпечена на всіх етапах. По-четверте, державні органи, що здійснюють OSINT, повинні підлягати ефективному контролю, щоб забезпечити дотримання норм права. Це включає як внутрішній контроль, так і зовнішній – з боку судової системи та громадськості. Підзвітність сприяє уникненню зловживань з боку державних органів та створює умови для забезпечення ефективного нагляду за їх діяльністю. По-п'яте, пропорційність і розумність. Принцип верховенства права також передбачає дотримання вимог пропорційності, коли будь-які обмеження прав людини повинні бути виправдані реальними потребами національної безпеки. Заходи, вжиті для досягнення цих цілей, не повинні перевищувати необхідного обсягу і мають бути розумними та обґрунтованими.

Верховенство права виступає гарантією дотримання правового порядку в діяльності з OSINT. Воно обмежує дискрецію державних органів, вимагаючи від них обґрунтованих рішень, що базуються на законі. У разі порушень прав громадян під час збору або аналізу відкритих даних, принцип верховенства права забезпечує можливість звернення до суду та інших компетентних органів для відновлення справедливості.

В умовах застосування OSINT для забезпечення національної безпеки цей принцип стає фундаментом для забезпечення легітимності, прозорості та довіри до діяльності держави. Він установлює чіткі рамки для забезпечення правопорядку, захищає права громадян та сприяє ефективному функціонуванню механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки.

Отже, принципами функціонування OSINT у сфері національної безпеки є засади, визначальні ідеї та положення, на яких має ґрунтуватися функціонування OSINT і які мають спрямовувати діяльність суб'єктів її здійснення у цій сфері. Принципи функціонування OSINT у сфері

національної безпеки представляють собою систему закріплених у законодавстві положень, які визначають засади правового регулювання функціонування розвідки з відкритих джерел та діяльності правоохоронних органів, які здійснюють таку діяльність, у сфері національної безпеки [83].

Загалом принципи як основоположні гарантії механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки сприяють збереженню демократичних засад у діяльності розвідувальних та інших органів, підвищують легітимність та прозорість їх роботи. Це створює правові умови для ефективного функціонування OSINT, що, у свою чергу, дозволяє зберігати національну безпеку та водночас поважати права й свободи громадян у межах правового поля.

З врахуванням вищенаведеного можемо зробити наступні висновки і узагальнення з підрозділу.

Гарантії механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки – це сукупність юридичних і організаційних засобів, що забезпечують ефективне та правомірне функціонування розвідки з відкритих джерел для національної безпеки. Вони створюють умови для збору, обробки й аналізу інформації з відкритих джерел, забезпечуючи баланс між інтересами держави та захистом прав громадян.

Гарантіям адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки притаманні такі властивості: а) публічно-правовий характер, що спрямований на захист національної безпеки; б) похідність від конституційних прав і свобод; в) адміністративно-правовий порядок реалізації; г) орієнтація на забезпечення законності та запобігання зловживанням; д) закріпленість у законах і підзаконних актах, що визначають статус суб’єктів OSINT.

Гарантії адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки можна класифікувати за такими критеріями: а) за сферою дії: загальні та спеціальні (спрямовані на суб’єктів

OSINT); б) за суб'єктами гарантій: для органів влади, громадських інститутів та громадян; в) за характером юридичних гарантій: нормативні, організаційні та матеріально-технічні.

Принципи як гарантії адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки – це основоположні правові норми, що визначають засади функціонування OSINT та забезпечення національної безпеки. Вони спрямовані на підвищення легітимності й прозорості діяльності органів, що здійснюють OSINT, а також збереження демократичних цінностей у процесі розвідувальної діяльності.

Принципи адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки класифікуються наступним чином: а) загальні принципи (законність, верховенство права, повага до прав і свобод людини); б) спеціальні принципи, що регулюють розвідувальну діяльність (конфіденційність, прозорість, пропорційність та незалежність). Ця класифікація сприяє чіткому правовому забезпеченню OSINT в інтересах національної безпеки.

Висновки до Розділу 2

Розділ присвячено характеристиці механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Акцентовано, що механізм адміністративно-правового забезпечення функціонування OSINT в Україні повинен включати не тільки правові, але й організаційні, технічні та інформаційно-аналітичні заходи, що створюють умови для ефективного здійснення розвідки з відкритих джерел. Для цього необхідно чітко визначити суб'єктів, уповноважених на здійснення OSINT, їх функції, методи роботи, а також форми взаємодії між ними. Особливої уваги потребують питання контролю та відповідальності за використання отриманої інформації, аби уникнути порушення прав громадян та забезпечити її відповідність цілям національної безпеки. Лише скоординована та комплексна

реалізація адміністративно-правових заходів сприятиме створенню дієвого механізму захисту національної безпеки, який буде ефективним та відповідатиме викликам сучасного інформаційного середовища.

Констатовано, що з огляду на зростаючу роль розвідки з відкритих джерел у сфері національної безпеки, нагальною потребою є вдосконалення механізму адміністративно-правового забезпечення її функціонування. Ефективне здійснення OSINT можливе лише за наявності комплексної, чітко врегульованої системи правових норм, що регламентують діяльність відповідних суб'єктів, їх повноваження та методи реалізації заходів. Така система має враховувати як внутрішні загрози, так і сучасні виклики міжнародної безпеки. Нормативно-правова база OSINT повинна охоплювати принципи та засади діяльності, закріплені у конституційних, законодавчих та інституційних актах, що забезпечує узгодженість, захист національних інтересів і прав громадян. Розробка спеціальних законодавчих актів, що регулюватимуть OSINT, стане важливим кроком у забезпеченні прозорості, законності й ефективності даної діяльності.

Установлено, що суб'єкти механізму адміністративно-правового функціонування OSINT у сфері національної безпеки – це сукупність державних та інших уповноважених органів, що виконують комплекс завдань з виявлення, збору, аналізу та обробки інформації з відкритих джерел з метою забезпечення національної безпеки держави. Ці суб'єкти мають особливий адміністративно-правовий статус і діють у межах встановленої компетенції, яка надає їм законодавчо закріплені повноваження для: здійснення правового регулювання функціонування OSINT; прийняття управлінських рішень; здійснення безпосередньо функцій з розвідки з відкритих джерел.

Запропоновано групування суб'єктів адміністративно-правового функціонування OSINT у сфері національної безпеки на чотири організаційно-функціональні рівні, а також їх класифікацію. Дослідження повноважень суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки дозволило виявити

низку проблемних аспектів, що потребують вирішення, зокрема, професіоналізацію та спеціалізацію кадрів, удосконалення розподілу завдань і повноважень, а також підвищення ефективності взаємодії та координації діяльності.

Під адміністративно-правовими засобами механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки запропоновано розуміти сукупність правових інструментів (способів, методів тощо), закріплених нормами адміністративного права, які використовуються для реалізації завдань, що спрямовані на забезпечення національної безпеки шляхом здійснення розвідки з відкритих джерел, і дають змогу ефективно виявляти та протидіяти загрозам національній безпеці завдяки функціонуванню OSINT. Ці засоби призначені для здійснення визначеного кола заходів з боку суб'єктів механізму забезпечення функціонування OSINT у сфері національної безпеки, і дозволяють здійснювати розвідку з відкритих джерел, моніторинг, аналіз та узагальнення відповідної інформації, а також реагувати на ризики й загрози у сфері національної безпеки.

Зазначено, що це особлива сфера суспільних відносин, що стосується здійснення розвідки з відкритих джерел і вимагає застосування специфічних адміністративно-правових засобів, обумовлених її надзвичайною важливістю для забезпечення національної безпеки. Використання OSINT дає змогу ефективно виявляти, аналізувати й оцінювати потенційні загрози, що виникають у різних сферах суспільного життя, зокрема в інформаційній та кіберпросторовій. Ця діяльність є багатокомпонентною і охоплює збір, обробку, аналіз та зберігання інформації, отриманої з відкритих джерел, що здійснюється завдяки комплексу адміністративно-правових засобів.

Запропоновано адміністративно-правові засоби забезпечення функціонування OSINT класифікувати за різними критеріями, а саме: завдання правового регулювання, ступінь складності, призначення, предмет регулювання, характер правового регулювання та ін. Така класифікація

сприяє кращому розумінню структури та функцій цих засобів, а також дозволяє визначити найбільш оптимальні методи правового забезпечення на кожному етапі діяльності OSINT.

Підкреслено, що спеціальні адміністративно-правові засоби у сфері OSINT відіграють ключову роль у регулюванні діяльності суб'єктів, які здійснюють розвідку з відкритих джерел. Ці засоби сприяють забезпеченню належного правового режиму для роботи з інформацією, а також уможливлюють виконання оперативних завдань, спрямованих на забезпечення національної безпеки. Залежно від особливостей і призначення, ці засоби можна поділити на два основні підвиди: засоби для виконання специфічних завдань і засоби для реалізації оперативних функцій.

Ефективність механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та результативність відповідної діяльності залежать від гарантій, які дозволяють забезпечити належне функціонування OSINT та захистити інтереси держави та громадян у сфері національної безпеки. Гарантії механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки охоплюють законодавчо закріплені механізми, які забезпечують стабільність і стійкість діяльності розвідувальних органів, а також сприяють захисту прав громадян і забезпечують їхнє право на доступ до інформації, що може бути використана в інтересах національної безпеки. Гарантії механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки є ключовими для формування правового середовища, яке дозволяє ефективно реалізовувати завдання з розвідки, забезпечуючи при цьому захист прав і законних інтересів громадян. Вони забезпечують не лише законність дій органів державної влади, але й створюють умови для об'єктивності та прозорості розвідувальної діяльності, сприяючи формуванню довіри суспільства до діяльності держави в сфері національної безпеки.

Установлено, що принципи як гарантії адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки – це основоположні правові норми, що визначають засади функціонування OSINT та забезпечення національної безпеки. Вони спрямовані на підвищення легітимності й прозорості діяльності органів, що здійснюють OSINT, а також збереження демократичних цінностей у процесі розвідувальної діяльності.

РОЗДІЛ 3
НАПРЯМИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ OSINT У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

3.1 Міжнародний досвід адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки

У сучасному світі інформація стала ключовим ресурсом для забезпечення безпеки держави. Open Source Intelligence (OSINT) – це один з основних інструментів, що дозволяють країнам забезпечувати національну безпеку.

У Сполученому Королівстві Великої Британії та Північної Ірландії правове регулювання Open Source Intelligence (OSINT) є важливою складовою національної безпеки, яке охоплює кілька законодавчих актів. Основними з них є Закон про захист даних 2018 року (Data Protection Act 2018) [189] та Закон про слідство (Investigatory Powers Act 2016) [192]. Ці закони створюють правову основу для збору, аналізу та використання інформації з відкритих джерел, одночасно забезпечуючи дотримання прав і свобод громадян.

Так, Закон про захист даних 2018 року є основним нормативно-правовим актом, що імплементує Загальний регламент захисту даних (GDPR) у Сполученому Королівстві [43]. Цей закон регулює обробку персональних даних, включаючи дані, отримані з відкритих джерел. Згідно з ним будь-яке збирання та обробка даних повинні здійснюватися законно, справедливо та прозоро. Важливо зазначити, що при використанні OSINT державні органи повинні дотримуватись принципів обробки даних, які включають: законність, добросовісність і прозорість; обмеження цілей; мінімізація даних; точність; обмеження терміну зберігання; цілісність і конфіденційність.

Цей закон передбачає можливість проведення перевірок та аудитів, які можуть ініціюватися Національним офісом захисту даних (Information

Commissioner’s Office, ICO) для забезпечення дотримання норм щодо захисту даних.

Закон про слідство (Investigatory Powers Act 2016) є ще одним ключовим нормативним актом, що регулює використання відкритих джерел у контексті національної безпеки [192]. Цей закон надає право державним органам, таким як поліція та служби безпеки, отримувати дані з відкритих джерел для розслідувань. Закон визначає, які органи мають повноваження на проведення слідчих дій, а також установлює порядок отримання дозволів на доступ до інформації.

У Великобританії OSINT активно використовується в рамках національної безпеки, і здійснення розвідки з відкритих джерел є частиною роботи різних державних органів, включаючи такі як: Служба безпеки (MI5), яка відповідає за внутрішню безпеку та боротьбу з тероризмом, і активно використовує дані з відкритих джерел для виявлення загроз внутрішній безпеці [195]; Розвідувальна служба (MI6), займається зовнішньою розвідкою та також має право на використання OSINT у своїй діяльності [196]; Національне агентство боротьби з організованою злочинністю (NCA) займається протидією організованій злочинності та наркотрафіком, тому також використовує здійснення розвідки з відкритих джерел [197; 198]. Згідно з положеннями закону дані вищезазначеними органами можуть збиратися з різноманітних джерел, таких як соціальні мережі, новинні сайти, блоги та інші публічні ресурси.

Водночас законодавство Великобританії чітко окреслює повноваження органів, які здійснюють розвідку з відкритих джерел і сферу цієї розвідки. Так, якщо розвідку здійснюють служби національної безпеки, то вони мають законні повноваження для збору інформації, необхідної для виконання своїх функцій із забезпечення національної безпеки. Поліція, в свою чергу, та інші правоохоронні органи здійснюють розвідку з відкритих джерел з метою збору доказів у рамках кримінальних проваджень та розслідувань. Крім цих органів, розвідку з відкритих джерел можуть здійснювати спеціальні наукові та

дослідницькі установи, у разі, якщо вони здійснюють наукові дослідження у сфері безпеки, протидії тероризму та організованій злочинності. При цьому така діяльність усіх вищенаведених суб'єктів не повинна порушувати закони про захист даних.

Крім того, в Великобританії діяльність спецслужб, зокрема щодо збору та аналізу інформації з відкритих джерел, підлягає суворому контролю з боку держави і незалежних органів. Це здійснюється з метою для забезпечення дотримання прав людини та законності в розвідувальній діяльності.

Основними законодавчими актами, що регулюють діяльність спеціальних органів та поліції у питаннях дотримання законодавства про захист даних, є:

1. Закон про слідчі повноваження 2016 року (Investigatory Powers Act 2016). Він регулює повноваження, обов'язки та встановлює обмеження для органів, які проводять слідчі дії. У цьому законодавчому акті містяться підстави для здійснення розвідки з відкритих джерел у межах відповідних слідчих дій. Так, для здійснення розвідки з відкритих джерел слідчий, або інша уповноважена особа, яка здійснює слідчі дії, повинна отримати спеціальний дозвіл. А, наприклад, для здійснення спеціальних видів спостереження видається судовий дозвіл [192];

2. Закон про захист даних 2018 року (Data Protection Act 2018) регулює питання щодо захисту персональних даних, у тому числі під час здійснення розвідки з відкритих джерел. У положеннях закону передбачено принцип законності, дотримання якого необхідно під час доступу до персональних даних осіб, а також прозорості діяльності відповідних органів, які використовують персональні дані [183].

У Великобританії створені та функціонують незалежні органи, які мають право здійснювати контроль за розвідкою з відкритих джерел. Такий контроль здійснюється з метою недопущення порушень законів при доступі, використанні персональних даних та іншої інформації при здійсненні розвідки з відкритих джерел. Одним із суб'єктів здійснення такого контролю є

парламентський комітет з розвідки та безпеки (Intelligence and Security Committee of Parliament), який проводить нагляд за діяльністю британських розвідувальних служб, зокрема MI5, MI6, GCHQ, оборонною розвідкою, Національними кіберсилами, Групою внутрішньої безпеки Міністерства внутрішніх справ та іншими [190].

Важливою формою контролю є щорічне звітування комітету з питань законності діяльності розвідувальних та інших органів, зокрема щодо дотримання прав людини під час реалізації розвідувальних і контррозвідувальних заходів. Комітет під час підготовки звіту збирає свідчення від керівників розвідувальних та інших правоохоронних органів, свідків, експертів, науковців, журналістів та інших зацікавлених осіб, таким чином здійснюючи розвідку з відкритих джерел. Підготовка такого звіту відбувається у три етапи, а потім Комітет може надавати свої звіти парламенту лише після того, як Прем'єр-міністр підтвердить, що в них немає матеріалів, які б зашкодили виконанню функцій відповідними розвідувальними органами, спецслужбами та правоохоронними органами [190; 194].

Уповноважений з питань слідства (Investigatory Powers Commissioner – IPCO) здійснює нагляд за використанням слідчих повноважень, перевіряючи дотримання законодавства та правил, що визначені Законом про слідчі повноваження 2016 року [192]. Уповноважений з питань захисту даних (Information Commissioner) наглядає за використання повноважень для таємного збору інформації для слідчих або розвідувальних цілей понад за 600 органами державної влади. Він має право застосовувати різні заходи впливу до органів та суб'єктів, які порушують слідчі повноваження під час збору даних з відкритих джерел [193].

Цікавим є те, що Згідно з положеннями Закону про слідчі повноваження 2016 року фінансування IPCO забезпечує міністр внутрішніх справ. Однак IPCO виконує свої функції незалежно від уряду і не є частиною Міністерства внутрішніх справ [193].

Отже, у Великобританії розвідка з відкритих джерел є важливим компонентом національної безпеки, і включає в себе збирання та аналіз інформації з різних публічних джерел. Основні особливості, що характеризують здійснення розвідки з відкритих джерел полягають у наявності чіткої законодавчої основи, яка регулює діяльність спецслужб, правоохоронних, слідчих та інших органів щодо здійснення OSINT. Така чітка законодавча основа здійснення OSINT сприяє законності та прозорості в їхній діяльності. Крім того, у Великобританії функціонує ефективна система контролю, що включає як парламентський, так і незалежний нагляд, який здійснюють уповноважені з питань слідства, унаслідок чого реалізуються механізми перевірки дотримання прав людини та законності у діяльності розвідувальних та інших органів.

Попри позитивні аспекти, в організації функціонування OSINT у Великобританії існують певні проблеми, які пов'язані з дотриманням прав осіб при здійсненні розвідки з відкритих джерел. Зрозуміло, що використання OSINT підвищує ризики порушення доступу до персональних та інших приватних даних осіб, тому громадськість Великобританії постійно стурбована можливими зловживаннями з боку держави та її органів. Крім того, швидкий розвиток технологій ускладнює контроль за діяльністю спецслужб та правоохоронних органів у здійсненні розвідки з відкритих джерел. Постійно змінюються методи збору інформації, і це потребує оновлення норм і процедур регулювання здійснення розвідки з відкритих джерел та контролю за такою діяльністю. У деяких випадках недостатня фінансова підтримка або ресурсні обмеження можуть впливати на ефективність збору та аналізу даних.

Отже, Великобританія має багатий досвід в організації діяльності щодо збору та аналізу інформації з відкритих джерел (OSINT), який може бути корисним для України в контексті покращення національної безпеки та підвищення ефективності роботи розвідувальних та правоохоронних органів. Великобританія має розвинутий правовий механізм для регулювання діяльності спецслужб, який забезпечує збалансований підхід між безпекою та

правами людини. З урахуванням досвіду здійснення розвідки з відкритих джерел у Великобританії, для нашої держави може буде доцільним створення чіткого законодавства у питаннях прийняття прозорих та зрозумілих правил щодо збору інформації з відкритих джерел, які містяться в вищенаведених законодавчих актах Великобританії, і положення яких можуть стати основою для створення подібного законодавства в Україні.

Крім того, у Великобританії створена система органів, які здійснюють контроль за діяльність розвідувальних та інших органів у питаннях функціонування OSINT, тим самим забезпечується законність такої діяльності та її прозорість. Цей досвід може стати корисним для нашої держави теж. Для України доцільним буде створити незалежні наглядові органи для здійснення контролю за діяльністю, пов'язаною із розвідкою з відкритих джерел.

Цікавим є досвід Великобританії щодо використання новітніх технологій для збору та аналізу інформації. Для цього налагоджена співпраця з приватним сектором, а саме ІТ-компаніями. Для покращення цього напряму механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки в Україні доцільно вживати певних заходів щодо фінансування провідних технологій для здійснення розвідки з відкритих джерел. Зрозуміло, що це складно зробити в умовах війни, але можна реалізувати шляхом співпраці з технологічними ІТ-компаніями. Упровадження новітніх технологій, таких як штучний інтелект і аналітика великих даних, може суттєво підвищити ефективність збору інформації шляхом здійснення OSINT. Налагодження партнерств із приватним сектором, особливо з ІТ-компаніями, що спеціалізуються на зборі та аналізі даних, може допомогти Україні модернізувати свої можливості в цій сфері.

Важливим напрямом розвідки з відкритих джерел є співпраця з міжнародними партнерами для обміну розвідувальною інформацією. В Україні необхідно активно розвивати міжнародні партнерства та створювати спільні платформи для обміну інформацією з правоохоронними органами, що займаються розвідкою з відкритих джерел. Налагоджені спільні системи

обміну інформацією між вітчизняними розвідувальними і правоохоронними органами та міжнародними партнерами можуть значно підвищити швидкість реагування на загрози у сферах національної та військової безпеки, боротьби з тероризмом і організованою злочинністю.

Цікавим і корисним для України може стати досвід підготовки кадрів для здійснення розвідки з відкритих джерел. Великобританія цьому питанню приділяє значну увагу. Так, існують курси та програми для підготовки співробітників спецслужб у сфері OSINT. Упровадження такого досвіду в нашій державі можливо шляхом створення навчальних програм або курсів підготовки відповідних фахівців зі здійснення розвідки з відкритих джерел. Упроваджувати спеціальні курси та навчальні програми для співробітників розвідувальних і правоохоронних органів України можна з акцентом на врахування новітніх технологій у методах збору та аналізу інформації, шляхом створення експертних груп для обміну досвідом та знаннями між фахівцями в галузі розвідки з відкритих джерел, у тому числі із залученням таких фахівців з інших країн.

Запозичення досвіду Великобританії в галузі розвідки з відкритих джерел може значно посилити зусилля України щодо забезпечення національної безпеки. Впровадження цього досвіду передбачає комплекс заходів, спрямованих на удосконалення правового регулювання, підвищення ефективності системи контролю, інтеграцію новітніх технологій та зміцнення стратегічної співпраці на міжнародному рівні між спеціальними службами та правоохоронними органами. Такі кроки дозволять Україні адаптувати свої розвідувальні спроможності до сучасних викликів і загроз, забезпечуючи при цьому дотримання прав людини та прозорість діяльності відповідних органів.

Наступною країною є Німеччина, досвід якої може стати підґрунтям для запозичення в законодавство та практичну діяльність розвідувальних і правоохоронних органів у здійснення розвідки з відкритих джерел.

Основним правовим актом, що регулює засади здійснення розвідки з відкритих джерел у Німеччині, є Основний закон Німеччини (Grundgesetz),

який гарантує права людини та основоположні свободи. Зокрема, стаття 10 Основного закону забезпечує право на таємницю листування, а також на приватність особистого та іншого життя осіб. Ці положення Основного закону є фундаментальними принципами, які спрямовують діяльність розвідувальних і правоохоронних органів, забезпечуючи дотримання прав осіб і законності у зборі особистої інформації, зокрема даних з відкритих джерел [187].

Наступним слід вважати Закон про захист Конституції (Bundesverfassungsschutzgesetz) – ключовий нормативно-правовий акт, що регулює діяльність Федерального відомства захисту конституції (Bundesamt für Verfassungsschutz, BfV). Цей закон надає BfV повноваження збирати інформацію з відкритих джерел, щоб виявляти загрози національній безпеці, включаючи екстремізм і тероризм. Закон регулює такі напрями: збір інформації та обробку даних. Відповідно до статті 3 BfV має право збирати дані з відкритих джерел, таких як публікації, веб-сайти, соціальні мережі, а також інші матеріали, що можуть містити інформацію про загрози. Згідно зі статтею 4 усі зібрані дані повинні оброблятися відповідно до принципів захисту даних, що передбачає законність і справедливість збору [180].

Важливим законодавчим актом є Закон про захист даних (Bundesdatenschutzgesetz), який установлює правила використання та обробки персональних даних у Німеччині. Хоча цей закон не є спеціалізованим для OSINT, він має важливе значення для дотримання прав людини в процесі збору інформації. Основні положення закону передбачають: принципи обробки даних, до яких відносяться принципів законності, обмеження цілей і мінімізації даних та права суб’єктів даних, до яких належать громадяни, які мають право на доступ до своїх даних і можуть вимагати їх виправлення або видалення [179].

Щодо суб’єктів здійснення розвідки з відкритих джерел у Німеччині, то до них відносяться розвідувальні та правоохоронні органи. Є й спеціалізовані органи з певними повноваженнями у цій сфері. Наприклад, таким суб’єктом є Федеральне відомство захисту конституції (BfV) – відповідає за внутрішню

безпеку, виявлення загроз екстремізму, тероризму та шпигунства. Однією з його основних функцій є збір інформації з відкритих джерел для моніторингу активності груп, які можуть загрожувати конституційному порядку Німеччини. BfV має право доступу до різноманітних джерел, включаючи засоби масової інформації, соціальні мережі, публікації та онлайн-ресурси. Згідно з законом BfV може здійснювати спостереження за публічно доступними інформаційними ресурсами без необхідності отримання попереднього дозволу [163].

Федеральне управління кримінальної поліції Німеччини (Bundeskriminalamt, BKA) є ключовим суб'єктом у боротьбі з організованою злочинністю, тероризмом і кіберзлочинністю. У своїй діяльності BKA активно застосовує інструменти OSINT для збору доказів, ідентифікації загроз та підтримки розслідувань. Орган має законодавчо закріплене право на доступ до інформації з відкритих джерел, що стосується кримінальних проваджень, а також співпрацює з іншими правоохоронними органами як у Німеччині, так і на міжнародному рівні, забезпечуючи ефективність протидії сучасним викликам безпеки [164].

Певними повноваженнями у здійсненні розвідки з відкритих джерел володіє Федеральна розвідувальна служба (Bundesnachrichtendienst, BND). Вона відповідає за зовнішню розвідку і має завдання збору інформації, яка може вплинути на національну безпеку. Хоча основна діяльність BND зосереджена на закритих джерелах, вона також здійснює моніторинг відкритих джерел, особливо у випадках, коли йдеться про міжнародні загрози. BND має розширені повноваження для збору інформації, включаючи доступ до відкритих джерел, які можуть містити важливу інформацію для національної безпеки [162].

Правове регулювання OSINT у Німеччині забезпечує баланс між необхідністю забезпечення національної безпеки і дотриманням прав людини. Основні органи, відповідальні за збір інформації з відкритих джерел, мають

чіткі повноваження і підлягають контролю з боку відповідних державних органів.

У Німеччині контроль за законністю діяльності розвідувальних і правоохоронних органів, зокрема у використанні OSINT, здійснюється через комплексний механізм парламентського, судового та внутрішнього нагляду. Основні розвідувальні органи Німеччини – Федеральна розвідувальна служба (BND), Федеральне відомство з охорони конституції (BfV) та Військова контррозвідка (MAD) – зобов'язані дотримуватися принципів законності й забезпечення прав людини у своїй діяльності, а здійснення ефективного контролю за їх діяльність попереджає такі порушення.

Зокрема у цій країні створений Парламентський контроль за діяльністю розвідувальних органів, який здійснюється відповідним парламентським комітетом. Основні положення, що регулюють нагляд, містяться в Законі про парламентський контроль за діяльністю розвідувальних служб Союзу (Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, PKGrG). Відповідно до PKGrG Парламентський комітет з контролю наділений повноваженнями щодо нагляду за діяльністю Федеральної розвідувальної служби (BND), Федерального відомства з охорони конституції (BfV) та Військової контррозвідки (MAD). Контроль здійснюється з метою забезпечення дотримання законодавчих норм, прав людини та забезпечення законності в їхній діяльності, у тому числі щодо використання OSINT [186].

Згідно з PKGrG комітет має право вимагати інформацію про операції розвідувальних служб, включно з діяльністю у сфері OSINT. Повноваження з контролю Парламентського комітету здійснюються у формах: запитів щодо джерел та методів збору інформації; контролю за правомірністю збору інформації та використання розвідки відкритих джерел з метою недопущення порушень прав на конфіденційність; нагляду за відповідністю дій розвідувальних органів за дотриманням основних прав людини і законодавства при здійсненні розвідки з відкритих джерел [186].

Варто важливо акцентувати, що в багатьох країнах світу існують незалежні парламентські органи, зазвичай, це спеціальні комітети парламенту, які мають повноваження здійснювати контроль за діяльністю розвідувальних і правоохоронних органів у здійсненні ними розвідувальної діяльності, у тому числі розвідки з відкритих джерел (Албанія, Угорщина, Польща, Данія, Чехія та ін.) [165].

Комітети з нагляду за розвідкою можуть мати міцнішу правову базу, ніж інші комітети парламенту; їхня робота ґрунтується на спеціальному законі про парламентський нагляд за розвідкою (Німеччина, Словенія, Іспанія, Італія), на рішеннях парламенту, якими визначено їхні завдання та повноваження (Румунія, Польща), або на детальному регламенті парламенту (Нідерланди). У деяких випадках їх створення спирається навіть на конституцію (Німеччина). На відміну від інших парламентських комітетів, закон іноді вимагає, щоб комітети з нагляду за розвідкою затверджували власний регламент (Північна Македонія, Румунія) [165].

Також є різні методи визначення повноважень комітету з нагляду за розвідкою. За функціонального підходу один парламентський комітет відповідає за контроль усіх розвідувальних служб або всіх визначених розвідувальних функцій, незалежно від того, які державні органи їх виконують. Це дає змогу уникнути ризику, що деякі питання опиняться в компетенції двох чи більше комітетів. Крім комітетів з нагляду за розвідкою, деякі парламенти утворили комітети, що займаються винятково застосуванням прав на втручання для збирання інформації – це, зокрема, Північна Македонія і Болгарія, де є комітет з нагляду за перехопленням засобів зв’язку, або Німеччина з її комітетом G-10 (позапарламентським). У країнах, де повноваження комітетів з нагляду за розвідкою ґрунтуються на функціональному підході, їхні повноваження, зазвичай, також охоплюють воєнну розвідку. За організаційного підходу комітети створюють для нагляду за конкретними розвідувальними службами (зазвичай згаданими в назві комітету). Наприклад, такі комітети з нагляду за розвідкою працюють у

парламентах Румунії, Чехії, Північної Македонії та Словаччини. Це дає змогу наглядачам зосередитись на роботі конкретного відомства. Комітети з питань оборони та безпеки залишаються відповідальними за нагляд за меншими службами або міністерськими департаментами, що виконують розвідувальні функції, зокрема за воєнною розвідкою. Однак нагляд може втратити цілісність, якщо у ньому бере участь забагато комітетів [165].

У США здійснення розвідки з відкритих джерел є невід'ємною частиною національної безпеки. Правове регулювання збору та використання інформації з відкритих джерел (OSINT) у цій країні є важливим аспектом національної безпеки. Сполучені Штати мають комплексну систему законодавства, що регулює діяльність розвідувальних органів, а також права громадян. Це законодавство включає різноманітні акти, правила та положення, які визначають, як державні органи можуть використовувати інформацію з відкритих джерел.

Основними законодавчими актами, які регулюють здійснення розвідки з відкритих джерел у США є наступні:

1. Закон про національну розвідку (National Security Act of 1947) – є правовою основою регулювання діяльності розвідувальних органів США і визначає повноваження розвідувальних органів, їх завдання, методи та форми діяльності. Цей закон також регулює суб'єктів управління розвідкою та контролем за діяльністю відповідних розвідувальних органів. Наприклад, Національна розвідувальна служба, здійснює координацію діяльності різних розвідувальних агентств [199];

2. Закон про контроль за розвідувальними агентствами (Intelligence Reform and Terrorism Prevention Act of 2004). Він був ухвалений після терористичних атак 11 вересня 2001 року. Регулює питання підвищення ефективності діяльності розвідувальних органів, а також форми контролю за такою діяльністю [191];

3. Закон про свободу інформації (Freedom of Information Act, FOIA) регламентує питання доступу до інформації (персональних даних), що є

важливим для здійснення розвідки з відкритих джерел. Хоча FOIA не є безпосереднім правовим актом, який регулює здійснення OSINT, але він забезпечує функціонування механізму, за допомогою якого громадяни можуть отримувати інформацію про діяльність розвідувальних органів [185].

Якщо проаналізувати суб'єктів, які мають повноваження здійснювати розвідку з відкритих джерел, то до них відносяться:

1. Національна розвідувальна служба (Office of the Director of National Intelligence, ODNI), яка координує розвідувальну діяльність усіх агентств США, включаючи використання OSINT. Вона відповідає за формування державної політики у сфері розвідувальної діяльності. Ця служба має широкі повноваження у визначені пріоритетних напрямів розвідки з відкритих джерел, відповідає за їх аналіз та використання [202];

2. Центральне розвідувальне управління (Central Intelligence Agency, CIA) збирає інформацію з різних джерел, включаючи відкриті джерела, для забезпечення національної безпеки. CIA активно використовує OSINT з метою забезпечення національної безпеки. У рамках свого законодавчого мандату CIA має право збирати інформацію з відкритих джерел, таких як новини, медіа, публікації та онлайн-ресурси, щоб оцінити загрози для національної безпеки [181];

3. ФБР (Federal Bureau of Investigation, FBI) – виконує роль внутрішньої розвідки та забезпечення правопорядку. ФБР використовує OSINT для збору даних з метою протидії тероризму, організованій злочинності, торгівлі зброєю та кіберзлочинністю. ФБР має право здійснювати моніторинг публічно доступних інформаційних ресурсів, включаючи соціальні мережі та інші платформи, для виявлення загроз національній безпеці [184];

4. Агентство національної безпеки (National Security Agency, NSA) – відповідає за збір і аналіз інформації, що стосується національної безпеки, включаючи електронну розвідку та OSINT. Крім того, активно використовує технології для моніторингу публічно доступних даних. NSA має право збирати

та аналізувати дані з відкритих джерел, а також інтегрувати ці дані з інформацією, отриманою з інших розвідувальних джерел [200].

Щодо контролю над діяльністю розвідувальних органів, то в США створено, як і в інших країнах, спеціальні парламентські комітети нагляду за розвідкою. Це постійні спеціальні комітети з розвідки (один – у Палаті представників, один – у Сенаті), які наглядають за 17 службами: контролюють всі розвідувальні органи, зокрема воєнну розвідку. Комітети створені у 1976 (Сенат) та 1977 (Палата представників) роках після річного парламентського розслідування зловживань ЦРУ, АНБ, ФБР (Комісія Чорча). Членів призначають керівники Палати представників (22) і Сенату (15) [165].

Крім того, Законом про негласне спостереження за агентами іноземних розвідок 1978 року створений спеціалізований суд (FISA), що дає санкцію на таємне спостереження [165].

Сполучені Штати Америки мають розвинену систему збору та аналізу інформації з відкритих джерел (OSINT), яка може стати корисною для України в контексті покращення національної безпеки та ефективності роботи розвідувальних органів. З метою удосконалення механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки для України, доцільно: прийняти закони, подібні до Закону про національну розвідку та Закону про контроль за розвідувальними агентствами, які чітко визначають повноваження розвідувальних органів та принципи збору інформації з відкритих джерел та встановити механізми, які б забезпечували прозорість у діяльності спецслужб та підзвітність перед суспільством.

Важливим для впровадження в Україні є досвід створення незалежного демократичного цивільного контролю за здійсненням розвідки з відкритих джерел. Основні принципи побудови системи демократичного цивільного контролю за службами безпеки і правоохоронними органами визначені рекомендаціями Парламентської асамблеї Ради Європи від 1999 р. № 1402 та від 2005 р. № 1713 [17].

Крім парламентських комітетів, дедалі більше держав створюють позапарламентські експертні органи з нагляду за розвідкою. Прикладами можуть слугувати Бельгія, Данія, Німеччина, Греція, Норвегія, Нідерланди, Швеція, Хорватія, Північна Македонія, Швейцарія, Португалія та Фінляндія. Членами цих органів є відомі громадські діячі, активісти громадянського суспільства, нинішні й колишні судді або екс-політики, які зазвичай призначаються парламентом і підзвітні парламенту та/або виконавчій владі. Експертні органи загалом незалежні від парламенту та виконавчої влади, організаційно та оперативно. Вони автономні у прийнятті рішень, зокрема рішень про те, які питання розглядати й з яких звітувати, і часто мають власний бюджет, затверджений парламентом. Ці органи мають розвинений секретаріат та кваліфікований допоміжний штат, який функціонує на постійній основі, що забезпечує можливість здійснювати контроль безперервно та у форматі повної зайнятості. Експертні структури, як правило, наділені повноваженнями щодо контролю за дотриманням законності в діяльності розвідувальних служб і забезпеченням прав людини, проте їхній мандат нерідко охоплює також моніторинг ефективності проведення операцій, адміністративних процедур або методів збору даних, які передбачають елементи втручання [165].

Міжнародний досвід адміністративно-правового забезпечення функціонування OSINT демонструє, що ефективне використання відкритих джерел інформації є можливим лише за умов чіткого правового регулювання та захисту прав людини. Західноєвропейські країни та США демонструють цінний досвід, який може бути корисним для України в контексті вдосконалення механізму функціонування OSINT у сфері національної безпеки.

На шляху євроатлантичної інтеграції України, на наш погляд, важливим є встановлення належних партнерських зв’язків розвідок країн – членів НАТО для попередження й подолання регіональних і глобальних викликів та загроз. У контексті цього слід зазначити, що Служба зовнішньої розвідки України уже давно здійснює роботу в цьому напрямі. Зокрема, станом на сьогодні

встановлені і підтримуються робочі контакти з розвідувальними та спеціальними органами більшості держав – членів Альянсу, а також з Центром інформації та документації НАТО в Україні, Офісом безпеки та Спеціальним комітетом НАТО [165].

Тісна взаємодія військової розвідки з цивільними розвідувальними службами та правоохоронними органами інших країн відіграє особливо важливу роль в умовах зростання нових загроз безпеці, що потребують ефективного обміну розвідувальною інформацією. За останні два десятиліття значно активізувався транскордонний обмін даними, у тому числі з відкритих джерел (OSINT), який є важливим інструментом у запобіганні злочинам та забезпеченні національної безпеки. У такій взаємодії необхідним є чітке розмежування функцій військової розвідки, цивільних розвідувальних органів та правоохоронних структур, що сприяє підвищенню прозорості, підзвітності й забезпеченню законності [101].

У деяких правових системах законодавство встановлює чіткий поділ між розвідувальною та правоохоронною діяльністю, що забезпечує окремий правовий режим для використання OSINT у кожній із цих сфер. Однак ці межі в останні роки поступово розмиваються, що створює виклики для правозастосовної практики. Розмежування обміну OSINT для правоохоронних та розвідувальних цілей є необхідним, адже правові режими щодо обробки інформації, захисту даних і застосування її в операціях значно відрізняються [101].

Закони повинні передбачати чіткий поділ між завданнями військової розвідки, що включають збирання й аналіз інформації, та рішеннями щодо її практичного застосування, що запобігає можливим порушенням прав громадян і забезпечує демократичний нагляд. Задля належного контролю та підзвітності, функції військової розвідки у сфері OSINT повинні бути окреслені в законодавстві таким чином, щоб чітко відрізнятися від повноважень інших розвідувальних та правоохоронних структур. Така правова конструкція сприяє демократичному контролю та посиленню

підзвітності органів національної безпеки, забезпечуючи водночас ефективність державної політики у сфері протидії сучасним загрозам [101].

На основі міжнародного досвіду адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки в інших країнах, зокрема у США, Великій Британії та Німеччині, можна запропонувати низку заходів для імплементації в законодавство України та діяльність суб'єктів, які здійснюють розвідку з відкритих джерел.

Упровадження міжнародного досвіду законодавчого регулювання розвідки з відкритих джерел для України буде доцільним за такими напрямами. По-перше, це створення спеціалізованого законодавства. Як показує досвід Великої Британії, США, Німеччини та інших країн Західної Європи, чітке правове регулювання меж діяльності та повноважень органів зі здійснення розвідки з відкритих джерел є основою для їх ефективного функціонування і взаємодії, з одного боку, та захисту прав громадян – з іншого. У зв'язку з цим необхідно розробити і прийняти окремий закон, який регулюватиме процедури діяльності зі збирання та використання інформації з відкритих джерел. Цей законодавчий акт повинен містити визначення термінології, правові рамки для збору даних, а також обов'язки та відповідальність органів, що займаються OSINT.

По друге, спрямування діяльності системи суб'єктів, які здійснюють розвідку з відкритих джерел, на засадах прозорості і підзвітності. Це передбачає включення у відповідне законодавство норм, що забезпечують прозорість у діяльності органів, які здійснюють OSINT, а також механізми підзвітності перед громадськістю (йдеться про механізми демократичного цивільного контролю) та парламентом.

По-третє, доцільним є створення незалежних наглядових органів за здійсненням розвідки з відкритих джерел. У багатьох країнах діють незалежні наглядові органи, які здійснюють контроль за діяльністю спецслужб. Великобританія та Німеччина мають ефективні моделі незалежного контролю та парламентського нагляду за OSINT. Це підвищує довіру громадськості до

розвідувальної діяльності та зменшує ризик зловживань. Зокрема, доцільно створити незалежні комісії або органи наглядового контролю, які б забезпечували моніторинг діяльності суб'єктів, що займаються розвідкою з відкритих джерел. Ці органи повинні мати повноваження для перевірки дотримання законодавства та стандартів етики. Слід також установити механізми для забезпечення парламентського контролю за діяльністю спецслужб і розвідувальних органів, що займаються здійсненням OSINT.

По-четверте, це чітке визначення повноважень між суб'єктами здійснення OSINT. Законодавство повинно містити чітке визначення повноважень органів, що здійснюють розвідку з відкритих джерел, а також обмеження на їх використання. Це допоможе запобігти можливим зловживанням. Слід також передбачити механізми для координації діяльності між різними державними органами, які займаються збором і аналізом інформації, отриманою шляхом розвідки з відкритих джерел. Така координація діяльності може бути здійснена шляхом створення спільних робочих груп або платформ для обміну інформацією.

По-п'яте, це впровадження та використання новітніх технологій. У США, Великобританії, Німеччині активно використовуються новітні технології для збору та аналізу відкритих даних, зокрема штучний інтелект і аналітика великих даних. Це дозволяє оперативно обробляти великі обсяги інформації та забезпечує високий рівень точності аналізу загроз. Тому вітчизняне законодавство повинно передбачати бюджетні видатки на дослідження і розробку новітніх технологій для збору та аналізу інформації з відкритих джерел, зокрема в галузі штучного інтелекту та обробки великих даних. Слід також розширити співпрацю з приватним сектором, наприклад з IT-компаніями, для цього потрібно заохочувати партнерство між державними органами та приватними компаніями.

По-шосте, підвищення професійної кваліфікації персоналу. У країнах із розвинутими системами OSINT значну увагу приділяють підготовці фахівців. Спеціалізовані курси з аналізу та збору інформації з відкритих джерел

підвищують ефективність роботи розвідувальних і правоохоронних органів в інших країнах. Тому для України доцільно розробити спеціалізовані навчальні програми, тренінги, курси підвищення кваліфікації для співробітників розвідувальних і правоохоронних органів, на яких би здійснювалося навчання новим методам пошуку, аналізу інформації з відкритих джерел. Крім цього, допомога у навчанні та підвищенні кваліфікації може здійснюватися на рівні експертних груп, представники яких зможуть обмінюватися досвідом та знаннями щодо здійснення розвідки з відкритих джерел. До складу таких груп можуть входити представники ІТ-компаній, досвідчені фахівці, які займаються OSINT, зокрема представники розвідувальних чи правоохоронних органів інших країн.

Імплементація цих заходів у законодавство та практику діяльності суб'єктів, які здійснюють розвідку з відкритих джерел в Україні, дозволить не лише підвищити ефективність діяльності зі здійснення розвідки з відкритих джерел, але й забезпечити правовий захист громадян та прозорість діяльності розвідувальних та правоохоронних органів в цій сфері.

3.2 Шляхи удосконалення адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки

У світі, де інформація стає критичним ресурсом для забезпечення державного суверенітету і стабільності, ефективне функціонування OSINT відіграє ключову роль у виявленні, оцінці та протидії потенційним загрозам. Унікальність OSINT полягає у доступі до масиву інформації з відкритих джерел, таких як соціальні мережі, публікації у ЗМІ, медіапростір, новинні ресурси, блоги та бази даних, що дає змогу формувати оперативну і достовірну картину ситуації без значних фінансових витрат та ризиків.

Зростання ролі OSINT у національній безпеці обумовлено низкою причин. По-перше, в умовах воєнної агресії проти України виникла потреба у

швидкому й точному виявленні загроз на інформаційному фронті, де відкриті джерела можуть стати інструментом виявлення фейкових новин, дезінформаційних кампаній та ворожих інформаційних впливів. По-друге, поширення технологій штучного інтелекту і великих даних (Big Data) сприяє застосуванню нових методів автоматизованого аналізу даних, що натомість підвищує швидкість і якість прийняття рішень у сфері безпеки.

Дослідження викликів і проблем OSINT у питаннях національної безпеки також є актуальним через правову й етичну складність цього напряму. Відсутність чіткої законодавчої бази та міжвідомчої координації створює ризики дублювання функцій різних відомств та порушення прав громадян, зокрема їхньої приватності. Вивчення досвіду інших країн, таких як США, Великобританія і Німеччина, які мають розвинену систему правового регулювання OSINT, може допомогти Україні адаптувати відповідні законодавчі акти і створити ефективні механізми контролю та прозорості.

Невідкладною є потреба у підготовці фахівців та розробці спеціальних програм підвищення кваліфікації для роботи з OSINT-інструментами, що сприятиме підвищенню ефективності національних служб у сфері безпеки. Дослідження таких аспектів, як технологічні та фінансові виклики, ризики кіберзлочинності й інформаційної безпеки, є важливим для стратегічного розвитку національної безпеки України, оскільки дозволить виявити слабкі місця і знайти способи їх усунення.

Таким чином, дослідження викликів і проблем OSINT у контексті національної безпеки є вкрай актуальним і своєчасним для забезпечення стійкості та обороноздатності України в умовах сучасних загроз. Це дослідження може закласти основу для розробки сучасних стратегій, ефективної правової бази та інноваційних технологічних рішень, що сприятимуть зміцненню національної безпеки.

Військова доктрина США «Field Manual Interim № 2-22.9» акцентує на тому, що основною відмінністю OSINT від інших видів розвідки є те, що в її

основі лежать джерело, інформація та способи їх збору, а не певна категорія технічних або людських ресурсів [13; 203].

Автори спеціального монографічного дослідження Ніхад А. Хассан і Рамі Хіджазі зазначають, що всі методології збору інформації з відкритих джерел, особливо OSINT, стикаються низкою проблем. По-перше, аналіз величезних обсягів неструктурованої інформації потребує спеціалізованого сучасного програмного забезпечення, розробка якого вимагає значних фінансових і людських ресурсів. По-друге, часто виникає проблема ненадійності джерел, які нерідко не відповідають розвідувальним стандартам; при цьому в багатьох країнах поширюється неточна або цілеспрямовано маніпулятивна інформація, спрямована на дезінформацію систем OSINT. І, нарешті, по-третє, навіть після автоматизованої обробки отриманих даних необхідно залучати висококваліфікованих фахівців вузького профілю для їхньої ретельної оцінки, інтерпретації та подальшої передачі кінцевому користувачеві [13; 201, с. 16–17].

Heather J. Williams та Ilana Blum наголошують, що лише незначна частина інформації, отриманої через OSINT, може бути використана як релевантна та достовірна. Процес трансформації неструктурованої розвідувальної інформації у звіти для політичного керівництва держави потребує обов’язкового проходження етапів перевірки законності та надійності кінцевого документа. У цьому контексті розвідка з відкритих джерел вимагає розробки інноваційних і більш досконалих спеціалізованих методик, здатних забезпечити якість та ефективність роботи в умовах сучасних викликів [13; 188, с. 12].

Одним із ключових чинників, що суттєво обмежує ефективність функціонування Системи забезпечення інформаційної безпеки Міністерства оборони України та Збройних сил України, є відсутність у підрозділах органів військового управління сучасних спеціалізованих програмних або апаратно-програмних засобів, призначених для добування, обробки, узагальнення та

аналізу інформації щодо потенційних загроз інформаційній безпеці держави у воєнній сфері [13].

Окреслені проблеми, безумовно, вимагають подальшого глибокого аналізу, системного розкриття причин їх виникнення та розробки ефективних шляхів вирішення.

Отже, станом на сьогодні існують певні технічні та фінансові обмеження щодо ефективного здійснення OSINT. Для ефективної роботи OSINT потрібні значні інвестиції в технології збору та аналізу інформації. Однак українські спецслужби та правоохоронні органи мають обмежені фінансові ресурси, що впливає на якість їхньої роботи у цьому напрямі. Брак сучасних автоматизованих систем, таких як аналітика великих даних та штучний інтелект, знижує можливості для швидкої обробки великих обсягів інформації.

На нашу думку, оптимізація фінансування та технічного удосконалення можлива таким чином. По-перше, слід запровадити спеціальне державне фінансування пріоритетних технічних програм для здійснення розвідки з відкритих джерел. Це може бути спеціальна державна програма підтримки розвідувальних і правоохоронних структур у сфері OSINT. По-друге, можна залучати міжнародні гранти та інвестиції у цю сферу. Можливо звернутися до міжнародних партнерів, таких як Європейський Союз, НАТО, США, для отримання грантів і технічної підтримки. Міжнародні організації надають ресурси на розвиток безпекових технологій, зокрема для протидії дезінформації та кіберзагрозам. Одним із джерел покращення технічного удосконалення є поширення партнерства з приватним сектором. Для цього слід забезпечити широке впровадження укладання угод з українськими і міжнародними IT-компаніями, які спеціалізуються на зборі та аналізі даних, щоб залучити їхній досвід, технології та інфраструктуру. Це зменшить витрати держави на розвиток власних рішень і сприятиме швидшому оновленню технічного забезпечення.

Процес роботи з відкритими джерелами інформації (OSINT) умовно можна розкласти на послідовність логічних стадій або етапів, які постійно

повторюються, формуючи замкнений цикл: «Початкове формулювання завдання – накопичення відомостей – перевірка – оброблення (систематизація) – інтерпретація – розповсюдження (підготовка звітної документації, оглядів, аналітичних матеріалів) – вторинна перевірка», після чого процес знову запускається по колу. Для оптимізації процесу добування даних з відкритих інформаційних ресурсів на державному рівні застосовується широкий спектр інструментів автоматизації. Зокрема, програмне забезпечення Octoparse (www.octoparse.com) дозволяє здійснювати витяг веб-контенту; Microsoft Defender Threat Intelligence представляє собою платформу, що акумулює відомості про різноманітні онлайн-ресурси і забезпечує їх структуроване оброблення та оцінювання; Hunchly (hunch.ly) і Kuiper (github.com/DFIRKuiper/Kuiper) слугують для автоматизованого збирання, аналізу даних, а також для організації інформаційного обміну між фахівцями й керівними структурами. Окремі програмні комплекси ефективно використовуються для глибшого опрацювання здобутої інформації. Зокрема, MS Excel, IBM i2 Analysts Notebook, Gephi, Pajek, Maltego – використовуються для розгорнутого аналізу даних у межах як криміналістичної розвідки (FORINT), так і розвідки на основі відкритих джерел (OSINT) тощо [96].

Дійсно, нині ефективність здійснення розвідки з відкритих джерел напряму залежить від впровадження сучасних технологій аналізу та обробки даних. Інвестувати в технології аналізу великих обсягів даних для виявлення закономірностей і ризиків, є актуальними напрямами розвитку OSINT для національної безпеки. Big Data дозволяє обробляти великі обсяги інформації, відстежувати тенденції і аналізувати поведінкові моделі. Впровадження інструментів штучного інтелекту для автоматизованого аналізу тексту, зображень і відео, полегшить і прискорить виявлення загроз. Наприклад, штучний інтелект може допомогти виявляти ключові слова чи фрази, що вказують на загрози або підозрілі активності.

Але для роботи з вищенаведеними та іншими технічними та інформаційними ресурсами потрібні відповідні фахівці, що актуалізує

наступну проблему – підготовка кадрів для здійснення OSINT та впровадження відповідних навчальних програм.

Дійсно, станом на сьогодні в Україні недостатньо фахівців, які мають навички збору та аналізу інформації з відкритих джерел. Це обумовлено як обмеженим фінансуванням, так і відсутністю відповідних навчальних програм. В умовах швидких змін технологій працівникам необхідно постійно вдосконалювати свої навички. Однак в Україні мало розвинені системи безперервної освіти для працівників розвідувальних органів та інших суб'єктів, які займаються розвідкою з відкритих джерел. OSINT вимагає залучення різнопланових фахівців, включаючи аналітиків, IT-спеціалістів і лінгвістів.

Для вирішення цієї проблеми необхідно, по-перше, залучати заклади освіти до підготовки спеціалістів з інформаційних технологій, розвідки, аналітики та кібербезпеки. Ця співпраця дозволить розробляти нові методики аналізу інформації та впроваджувати їх у практичну діяльність зі здійснення розвідки з відкритих джерел. По-друге, одним із напрямів удосконалення підготовки відповідних кадрів у сфері OSINT можливо шляхом створення спеціалізованих навчальних курсів, з залученням IT-спеціалістів та міжнародних фахівців у цій сфері. Організувати навчальні курси та тренінги можливо на базі закладів освіти. Такі курси можуть бути корисними для підвищення кваліфікації та перепідготовки співробітників правоохоронних та розвідувальних органів, діяльність яких пов'язана із здійсненням розвідки з відкритих джерел. Це сприятиме розвитку навичок роботи з новими технологіями та програмним забезпеченням, обробки великого і різноманітного обсягу інформації, обробкою даних, кіберзахистом і роботою з аналітичними платформами.

Важливим напрямом також може стати міжнародне співробітництво з іноземними партнерами у питаннях навчання та стажування відповідного персоналу. Наприклад, можливо організувати стажування для українських спеціалістів в іноземних структурах (компаніях, правоохоронних органах,

закладах освіти відповідного спрямування), які мають досвід навчання та проведення тренінгів з вивчення використання різноманітних технік та технологій у здійсненні OSINT.

Наступна проблема стосується захисту інформації. Широке впровадження комп'ютерних інформаційних технологій у сферах державної діяльності, економіки, фінансів, банківської справи тощо зумовило підвищення вимог до безпеки інформації в комп'ютерних системах [19; 28, с. 12].

Поняття «безпека інформації» охоплює такі складові: технічний або технологічний аспект, змістом якого є безпека змістовної частини інформації, що забезпечує стимулювання негативної поведінки в людини, захист від навмисно закладених механізмів негативного впливу на психіку людини або на інші інформаційні блоки (наприклад, від шкідливих програм, таких як комп'ютерні віруси). Правовий аспект: забезпечення захисту інформації від зовнішнього втручання, що включає захист від несанкціонованого копіювання, розповсюдження, модифікації (зміни змісту) або знищення [19].

Т. М. Войтешенко зазначає, що для захисту інформації законодавством застосовуються такі засоби: організаційно-технічні: вони передбачають створення фізичних бар'єрів для обмеження доступу сторонніх осіб з ненадійною поведінкою. Сюди входять зберігання носіїв і обладнання в захищених приміщеннях, використання фільтрів і екранів для апаратури, блокування клавіатури та екранів. Ці методи захищають лише від зовнішніх злочинців і не забезпечують захист від осіб, які мають доступ до приміщення; організаційно-правові засоби: базуються на законодавчих актах, які регламентують правила обробки інформації з обмеженим доступом та передбачають кримінальну відповідальність за порушення норм законодавства; організаційно-управлінські засоби: включення відбору, навчання, виховання персоналу, застосування стимулів і санкцій, пропускний режим, обмеження доступу до комп'ютерних приміщень тощо; організаційно-

технологічні засоби: криптографія, шифрування, програмний контроль доступу, цифровий підпис [19].

У питаннях захисту інформації не можна ігнорувати технологічні виклики та кіберзагрози, з якими стикаються суб'єкти, що здійснюють розвідку з відкритих джерел. Зокрема, під час проведення OSINT постає проблема протидії кібератакам і забезпечення надійного захисту інформації. Для її вирішення необхідно впроваджувати комплексні заходи, які включають використання сучасних засобів кіберзахисту, удосконалення відповідних технологій, а також залучення висококваліфікованого персоналу, здатного оперативно реагувати на виклики та нейтралізувати потенційні загрози.

Протидія технологічним викликам і кіберзагрозам є складним завданням, що потребує комплексного підходу. Впровадження таких стратегій, як, наприклад, планування дій у разі кібератак, формування команд «швидкого реагування», обрання платформ з багаторівневим захистом, адаптація до нових технологій захисту, впровадження принципів кібергігієни та заходів контролю доступу можуть підвищити безпеку даних суб'єктів здійснення розвідки з відкритих джерел, покращити здатність до оперативного реагування на кіберінциденти та зменшити ризик порушень у здійсненні розвідувальної діяльності з відкритих джерел.

Окремо слід зосередити увагу на питаннях планування та формування команд швидкого реагування на кіберзагрози. Так, одним із шляхів вирішення цієї проблеми є створення планів реагування, які передбачають конкретні кроки для відновлення роботи та мінімізації втрат у разі кіберінцидентів, а також створення внутрішніх (спеціальних) підрозділів для швидкого реагування на кіберінциденти та відновлення роботи з мінімальними втратами.

Розвідка з відкритих джерел (OSINT) стала одним із ключових інструментів у забезпеченні національної безпеки та реагуванні на сучасні загрози. Її ефективність ґрунтується на здатності суб'єктів національної безпеки оперативно отримувати та аналізувати інформацію з

загальнодоступних джерел, таких як соціальні мережі, новинні портали, форуми, бази даних тощо. Однак впровадження OSINT як повноцінного елемента системи національної безпеки вимагає налагодженої взаємодії між суб'єктами, що здійснюють розвідку з відкритих джерел. В Україні це питання є особливо актуальним через зростання кіберзагроз, військової агресії з боку російської федерації та інформаційних атак, спрямованих на дестабілізацію ситуації в державі.

Взаємодія суб'єктів механізму адміністративно-правового забезпечення здійснення OSINT – це система координації та співпраці між органами державної влади і правоохоронними, розвідувальними і контррозвідувальними органами, приватним сектором (IT-компаніями) та іншими зацікавленими суб'єктами, змістом якої є обмін інформацією, ресурсами і технологіями для ефективного збору, аналізу та використання відкритих джерел інформації з метою забезпечення національної безпеки. Ця взаємодія передбачає визначення прав і обов'язків суб'єктів, створення нормативно-правової бази, яка має врегульовувати форми і методи взаємодії, а також механізмів контролю за здійсненням OSINT.

Взаємодія суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки передбачає:

1. Спільні зусилля суб'єктів забезпечення національної безпеки з реалізації важливих завдань зі здійснення розвідки з відкритих джерел, з метою виявлення загроз національній безпеці. Формами такої взаємодії можуть бути спільна співпраця з реалізації конкретних заходів у межах спеціальних операції, спільне планування діяльності та виконання запланованих заходів з метою усунення локальних загроз тощо;

2. Обмін інформацією між відповідними суб'єктами, що дозволить забезпечувати оперативне інформування, і як наслідок – швидке реагування на виявлені загрози. Обмін інформацією між суб'єктами здійснення OSINT підвищує ефективність прийняття рішень на всіх рівнях управління;

3. Координацію дій між суб'єктами, які займаються аналізом та використанням OSINT, що включає в себе створення спільних робочих груп, проведення навчань та обмін досвідом.

Взаємодія між різними суб'єктами механізму адміністративно-правового забезпечення здійснення OSINT забезпечує більш широкий доступ до джерел інформації, яка стосується загроз національної безпеки. Це дозволяє їх вчасно виявляти, оперативно реагувати та ефективно усувати. Налагоджена комунікація та співпраця між суб'єктами дозволяє оперативно обмінюватися даними, що є критично важливим для швидкого реагування на потенційні загрози.

Взаємодія сприяє створенню єдиного інформаційного простору, в якому суб'єкти здійснення розвідки з відкритих джерел можуть координувати свої дії. Це допомагає уникнути дублювання зусиль і забезпечує більш цілісний підхід до аналізу інформації та прийняття своєчасних управлінських рішень. Завдяки спільному аналізу даних з різних джерел, суб'єкти можуть робити обґрунтовані та комплексні аналітичні висновки про наявні та потенційні загрози у сфері національної безпеки. Це сприяє кращому розумінню ситуації у сфері національної безпеки та прийняттю своєчасних управлінських рішень.

Таким чином, взаємодія суб'єктів механізму адміністративно-правового забезпечення здійснення OSINT є важливим чинником для забезпечення національної безпеки, оскільки вона підвищує ефективність збору і аналізу інформації, дозволяє оперативно реагувати на загрози та забезпечує комплексний підхід до управління ризиками.

Сучасна система OSINT в Україні знаходиться на етапі становлення, і наразі існує чимало суттєвих проблем у сфері міжвідомчої співпраці між суб'єктами OSINT, до яких належать державні органи, які здійснюють загальне керівництво, розвідувальні та правоохоронні органи, які здійснюють розвідку з відкритих джерел. В Україні OSINT-завдання, як зазначалося в попередніх розділах, можуть виконувати різні суб'єкти, що часто призводить до дублювання зусиль, конкуренції за ресурси та недостатньої взаємодії між

ними. Відсутність належної координації діяльності цих суб'єктів у сфері національної безпеки суттєво знижує ефективність реалізації розвідувальних завдань з відкритих джерел і створює додаткові ризики для досягнення поставлених цілей.

Крім того, в нашій державі відсутня єдина платформа для обміну даними між суб'єктами, що здійснюють OSINT. Це ускладнює доступ до інформації, сповільнює процеси аналізу та оперативного реагування на загрози. Через це різні відомства часто працюють автономно, що знижує можливості для комплексного аналізу ситуації.

Для подолання зазначених проблем необхідно розробити та впровадити низку заходів, таких як створення єдиної законодавчої бази для суб'єктів OSINT, забезпечення технологічної підтримки через залучення інвестицій і міжнародних партнерів, а також створення освітніх програм для підготовки кваліфікованих кадрів.

Для покращення взаємодії та координації між суб'єктами, які здійснюють розвідку з відкритих джерел, важливо розробити чіткий механізм співпраці, що дозволить уникати дублювання функцій, забезпечити своєчасний обмін інформацією та підвищить ефективність розвідувальної діяльності. Для цього, наприклад, можна створити постійний міжвідомчий орган, до якого входитимуть представники основних державних органів, що займаються OSINT (розвідувальні служби, правоохоронні органи, Міністерство оборони, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації, інші суб'єкти).

Основним завданням такого органу може стати забезпечення оперативного обміну інформацією, узгодження стратегій збору і аналізу даних, встановлення єдиних стандартів та координацію заходів у сфері OSINT, а також вирішення нагальних питань, пов'язаних з розподілом завдань, аналізом нових загроз і розробкою напрямів для їх усунення.

Крім того, можна створити єдину електронну платформу для обміну інформацією, доступ до якої матимуть суб'єкти здійснення OSINT відповідно

до своїх повноважень. Завдяки цій системі, можливо забезпечити швидкий і безпечний обмін інформацією та інтеграцію даних, які надходять від різних відомств, для комплексного аналізу загроз національній безпеці.

Важливим кроком у напрямі удосконалення механізму адміністративно-правового забезпечення OSINT у сфері національної безпеки є реформування та розвиток адміністративно-правового регулювання цієї діяльності. Для цього доцільно розробити й ухвалити Закон України про розвідку з відкритих джерел (OSINT), який має стати ключовим нормативно-правовим актом, що визначатиме основи організації та функціонування діяльності державних органів у сфері OSINT. Цей закон повинен встановлювати чіткі повноваження суб'єктів OSINT, принципи їх взаємодії, правові гарантії захисту інформації та механізми забезпечення дотримання прав людини.

Крім того, Закон має чітко визначити, які органи державної влади можуть здійснювати OSINT, і окреслити їхні повноваження в цьому напрямі, встановити порядок збору, аналізу та використання даних, отриманих з відкритих джерел, з урахуванням захисту персональних даних і конфіденційної інформації, регулювати категорії даних, які можуть бути зібрані з відкритих джерел, і забезпечити дотримання принципів мінімізації даних, зокрема заборонити збір даних, які не мають значення для національної безпеки, передбачити запобіжні механізми для захисту прав громадян, зокрема у сфері приватності та конфіденційності персональних даних, та визначити, як громадяни можуть захистити свої права у разі порушення під час OSINT-діяльності, а також визначити правила зберігання і знищення зібраних даних, терміни їх зберігання та вимоги щодо анонімізації і псевдонімізації інформації, яка більше не потрібна для забезпечення національної безпеки.

Одним із важливих розділів цього закону має стати врегулювання питань незалежного контролю за діяльністю, що пов'язана з розвідкою з відкритих джерел. Закон повинен передбачати створення спеціального парламентського комітету у Верховній Раді, який здійснюватиме моніторинг та контроль за діяльністю органів, що займаються OSINT. Для забезпечення

прозорості та відповідальності, державні органи, які здійснюють OSINT, повинні регулярно надавати звіти цьому комітету. Звіти мають містити детальну інформацію про обсяг оброблених даних, заходи, що вживаються для захисту прав людини, а також результати перевірок та аудитів, що проводяться в рамках забезпечення законності їх діяльності.

У цьому законодавчому акті також необхідно окремо передбачити розділ, присвячений здійсненню міжнародної співпраці у сфері розвідки з відкритих джерел. Закон має визначати процедури та критерії обміну OSINT-даними з міжнародними партнерами, забезпечуючи при цьому належний рівень захисту національних інтересів та конфіденційної інформації. Крім того, закон повинен встановити вимоги щодо відповідності обробки даних міжнародним стандартам, що сприятиме спрощенню співпраці з іноземними партнерами та організаціями. Окремо слід вказати на необхідність включення положень, які визначатимуть, які дані можуть бути передані міжнародним партнерам, а які повинні залишатися обмеженими для національного використання. Також важливо встановити механізми співпраці з іншими державами у питаннях кіберзахисту та спільної протидії загрозам у сфері національної безпеки.

Висновки до Розділу 3

У розділі проаналізовано міжнародний досвід адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки.

Підкреслено, що запозичення досвіду Великобританії у сфері розвідки з відкритих джерел може значною мірою зміцнити Україну в її зусиллях щодо забезпечення національної безпеки. Впровадження цього досвіду передбачає комплекс заходів, спрямованих на удосконалення правового регулювання, посилення системи контролю, впровадження новітніх технологій та стратегічну співпрацю на міжнародному рівні між спеціальними службами та правоохоронними органами. Такі кроки сприятимуть адаптації розвідувальних спроможностей України та діяльності відповідних органів до сучасних

викликів і загроз, водночас забезпечуючи належне дотримання прав людини та прозорість їх діяльності.

Установлено, що ключові особливості, що характеризують здійснення розвідки з відкритих джерел у Великобританії, полягають у наявності чіткої законодавчої основи, яка регулює діяльність спецслужб, правоохоронних органів, слідчих та інших установ у сфері OSINT. Така законодавча база забезпечує законність та прозорість у їхній діяльності. Крім того, у Великобританії функціонує ефективна система контролю, яка включає як парламентський, так і незалежний нагляд, що здійснюється уповноваженими з питань слідства. Це дозволяє реалізувати механізми перевірки дотримання прав людини та законності у діяльності розвідувальних і правоохоронних органів.

З'ясовано, що правове регулювання OSINT у Німеччині забезпечує баланс між необхідністю забезпечення національної безпеки і дотриманням прав людини. Основні органи, відповідальні за збору інформації з відкритих джерел, мають чіткі повноваження і підлягають контролю з боку відповідних державних органів.

Акцентовано, що Сполучені Штати Америки мають розвинуту систему збору та аналізу інформації з відкритих джерел (OSINT), яка може стати корисною для України в контексті покращення національної безпеки та ефективності роботи розвідувальних органів. З метою удосконалення механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, для України доцільно: прийняти закони, подібні до Закону про національну розвідку та Закону про контроль за розвідувальними агентствами, які чітко визначають повноваження розвідувальних органів та принципи збору інформації з відкритих джерел, та встановити механізми, які б забезпечували прозорість у діяльності спецслужб та підзвітність перед суспільством.

Констатовано, що ефективність діяльності суб'єктів OSINT у сфері забезпечення національної безпеки напряму залежить від злагодженої

взаємодії. Під взаємодією суб'єктів механізму адміністративно-правового забезпечення здійснення OSINT запропоновано розуміти систему координації та співпраці між органами державної влади і правоохоронними, розвідувальними і контррозвідувальними органами, приватним сектором (IT-компаніями) та іншими зацікавленими суб'єктами, змістом якої є обмін інформацією, ресурсами і технологіями для ефективного збору, аналізу та використання відкритих джерел інформації з метою забезпечення національної безпеки.

До форм взаємодії запропоновано відносити: спільне планування та співпрацю у межах запланованих заходів чи виконання спеціальних операцій, обмін інформацією, координацію дій. Для покращення взаємодії та координації між суб'єктами, які здійснюють розвідку з відкритих джерел, важливо розробити чіткий механізм співпраці, що дозволить уникати дублювання функцій, забезпечити своєчасний обмін інформацією та підвищить ефективність розвідувальної діяльності.

Необхідно розробити та впровадити низку заходів, таких як створення єдиної законодавчої бази для суб'єктів OSINT, забезпечення технологічної підтримки через залучення інвестицій і міжнародних партнерів, а також створення освітніх програм для підготовки кваліфікованих кадрів.

Установлено, що використання OSINT вимагає залучення спеціалістів із різних сфер, таких як IT, аналітика, кібербезпека тощо. Констатовано, що станом на сьогодні існує потреба у створенні освітніх програм і курсів, які б надавали достатньо знань для діяльності зі здійснення розвідки з відкритих джерел, включаючи навички збору, обробки та аналізу інформації. Співпраця з закладами освіти та міжнародними партнерами може сприяти підвищенню якості підготовки кадрів. Крім того, вітчизняні заклади освіти, що готують фахівців для розвідувальних та правоохоронних органів, можуть розширити освітні програми з кібербезпеки та аналітики, що не тільки підвищить професійний рівень вітчизняних фахівців, але й сприятиме інтеграції міжнародних стандартів у діяльність зі здійснення OSINT, посилюючи

спроможності держави ефективно реагувати на сучасні виклики і загрози у сфері національної безпеки.

Для удосконалення правового регулювання діяльності з розвідки з відкритих джерел у сфері національної безпеки України доцільно розробити і прийняти Закон про розвідку з відкритих джерел (OSINT). Цей закон повинен стати основоположним нормативно-правовим актом, що регулює діяльність державних органів з розвідки з відкритих джерел у сфері національної безпеки.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та запропоновано нове вирішення наукового завдання щодо адміністративно-правового забезпечення OSINT у сфері національної безпеки. За результатами дослідження запропоновано такі висновки та рекомендації:

1. Висвітлено стан наукових досліджень адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та з'ясовано, що у наукових дослідженнях, що присвячені функціонуванню OSINT у сфері національної безпеки, можна виділити дві основні групи праць. Перша група охоплює монографії, дисертації, автореферати, підручники, де адміністративно-правове забезпечення OSINT є центральною темою. Друга група включає дослідження, де питання адміністративно-правового регулювання OSINT згадуються частково, в контексті інших правових або управлінських проблем національної безпеки. Ці праці також класифікуються на вітчизняні та іноземні, з урахуванням відмінностей у підходах та умовах забезпечення національної безпеки. Однак аналіз наукової літератури показує, що окремі напрями функціонування OSINT ще залишаються поза увагою вчених-юристів. Зокрема, мало досліджені правові аспекти визначення рівнів, меж та форм адміністративно-правового забезпечення національної безпеки за допомогою OSINT, а також відсутні цілісні узагальнення міжнародного досвіду. Потребує вивчення також нормативна база, яка регулює діяльність суб'єктів, що здійснюють розвідку з відкритих джерел, а також їх адміністративно-правовий статус.

2. Розкрито сутність національної безпеки як об'єкта адміністративно-правового забезпечення та встановлено, що вона є явищем, яке передбачає підтримання стану стабільності протягом тривалого періоду, що забезпечується розумною та динамічною захищеністю від ключових загроз і небезпек. Важливим компонентом цього поняття є не лише стійкість перед реальними викликами, а й здатність держави та суспільства вчасно

ідентифікувати потенційні загрози та вживати превентивні заходи для їхньої нейтралізації. Такий підхід до розуміння національної безпеки акцентує увагу на необхідності ефективних правових механізмів моніторингу та попередження загроз. OSINT у цьому процесі відіграє важливу роль, оскільки дозволяє використовувати відкриті джерела для ефективного моніторингу, аналізу та попередження загроз у сфері національної безпеки. Адміністративно-правове забезпечення функціонування OSINT передбачає створення правових, організаційних, економічних, технічних та інших засобів та умов, які забезпечать відповідним суб'єктам ефективну діяльність зі здійснення розвідки з відкритих джерел, з метою вчасного виявлення з подальшим усуненням загроз і викликів національній безпеці.

3. Адміністративно-правове регулювання функціонування OSINT представляє собою взаємодіючу, комплексну багаторівневу систему, яка складається з таких елементів: конституційні положення та стратегічні документи у сфері національної безпеки; законодавчі акти, які регулюють правові аспекти забезпечення національної безпеки та функції і завдання системи OSINT у цій сфері; інституційні нормативно-правові акти, які регулюють адміністративно-правовий статус суб'єктів здійснення OSINT, їх функції, форми, методи та засоби діяльності і взаємодії; міжнародно-правові акти, які регулюють використання відкритих джерел інформації у контексті забезпечення міжнародної безпеки та співпраці. Ефективне функціонування OSINT потребує оновлення правової бази України, з урахуванням міжнародних стандартів і сучасних викликів і загроз у сфері національної безпеки.

4. Механізм адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки розглянуто як комплексну систему правових, організаційних, технічних та інформаційно-аналітичних заходів, що застосовуються відповідними суб'єктами з метою створення умов для ефективного здійснення розвідки з відкритих джерел. Структуру адміністративно-правового механізму забезпечення OSINT у сфері

національної безпеки складають такі елементи: нормативні засади адміністративно-правового регулювання OSINT (принципи та норми права, що регулюють сферу національної безпеки та здійснення розвідки з відкритих джерел); об'єкт адміністративно-правового забезпечення OSINT (правовідносини, що виникають у процесі використання відкритої інформації, їх зміст, типи та особливості реалізації); суб'єкти адміністративно-правового забезпечення OSINT (органи, уповноважені на здійснення відповідної діяльності); а також засоби адміністративно-правового забезпечення OSINT (методи і заходи, спрямовані на ефективне функціонування цієї системи в інтересах національної безпеки).

5. Охарактеризовано суб'єктів механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та визначено, що цими суб'єктами є сукупність державних та інших уповноважених органів (розвідувальних, правоохоронних, контррозвідувальних), які виконують комплекс завдань з виявлення, збору, аналізу та обробки інформації з відкритих джерел з метою забезпечення національної безпеки держави. Ці суб'єкти мають особливий адміністративно-правовий статус і діють у межах встановленої компетенції, яка надає їм законодавчо закріплені повноваження для: здійснення правового регулювання функціонування OSINT; прийняття управлінських рішень; здійснення безпосередньо функцій з розвідки з відкритих джерел. Запропоновано групування суб'єктів адміністративно-правового функціонування OSINT у сфері національної безпеки на такі організаційно-функціональні рівні 1) суб'єкти загальної компетенції (Верховна Рада України, Президент України та Кабінет Міністрів України); 2) суб'єкти загального керівництва (Рада національної безпеки і оборони, Міністерство інформаційної політики України, Міністерство оборони України); 3) суб'єкти спеціального керівництва (суб'єкти спеціальної компетенції (Служба безпеки України, Національна поліція України, Державна прикордонна служба України, Державна служба спеціального зв'язку та захисту інформації України);

4) суб'єкти спеціальної компетенції (розвідувальні та контррозвідувальні органи, Центр протидії дезінформації, відповідні служби та підрозділи суб'єктів спеціального керівництва) та досліджено їх повноваження.

6. Проаналізовано адміністративно-правові засоби механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та запропоновано трактувати адміністративно-правові засоби як сукупність правових інструментів (способів, методів тощо), закріплених нормами адміністративного права, які використовуються для реалізації завдань щодо забезпечення національної безпеки шляхом здійснення розвідки з відкритих джерел, що дозволяють ефективно виявляти та протидіяти загрозам національній безпеці. З'ясовано, що адміністративно-правові засоби характеризують такі властивості: нормативна визначеність, комплексність, цілеспрямованість, функціональність, оперативність і адаптивність, правовий вплив. Запропоновано класифікувати адміністративно-правові засоби за такими критеріями: залежно від завдань правового регулювання у сфері OSINT (загальні та спеціальні); залежно від ступеня складності завдань OSINT (первинні (елементарні) та комплексні (складні); за призначенням для здійснення OSINT (регулятивні, охоронні і процедурні); за предметом правового регулювання у сфері OSINT; за характером (матеріальні та процедурні); за наслідками (звичайні та виняткові); за часом здійснення (постійні, тимчасові). Підкреслено, що ключову роль у здійсненні OSINT відіграють спеціальні адміністративно-правові засоби та надано їх характеристику.

7. Розкрито зміст гарантій механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та з'ясовано, що ефективність механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та результативність відповідної діяльності залежать від гарантій, які дозволяють забезпечити належне функціонування OSINT та захистити інтереси держави та громадян у сфері національної безпеки. Під гарантіями механізму

адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки запропоновано розуміти сукупність юридичних і організаційних засобів, що забезпечують ефективне та правомірне функціонування розвідки з відкритих джерел для національної безпеки. Вони створюють умови для збору, обробки й аналізу інформації з відкритих джерел, забезпечуючи баланс між інтересами держави та захистом прав громадян. Гарантії адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки класифіковано за такими критеріями: а) за сферою дії: загальні та спеціальні (спрямовані на суб'єктів OSINT); б) за суб'єктами гарантій: для органів влади та громадян; в) за характером юридичних гарантій: нормативні, організаційні та матеріально-технічні, та досліджено їх зміст.

8. Висвітлено міжнародний досвід механізму адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки та запропоновано напрями його імплементації у законодавство та діяльність суб'єктів здійснення OSINT, зокрема обґрунтовано доцільність: створення спеціального законодавства, яке чітко врегульовуватиме питання здійснення розвідки, у тому числі з відкритих джерел, а також завдання, повноваження, межі діяльності розвідувальних і правоохоронних органів у цій сфері; впровадження ефективної системи парламентського та цивільного контролю за функціонуванням OSINT у сфері національної безпеки; створення незалежних наглядових органів контролю за розвідкою з відкритих джерел; створення умов для заохочення партнерства з IT-компаніями, іншими суб'єктами приватного права з метою поширення використання новітніх технік та технологій зі здійсненням розвідки з відкритих джерел; впровадження системи навчання та підвищення кваліфікації суб'єктів, які здійснюють OSINT; покращення міжнародного співробітництва та створення спільних платформ з обміну інформацією між розвідувальними та правоохоронними органами інших держав і Україною у питаннях здійснення розвідки з відкритих джерел.

9. Запропоновано шляхи удосконалення адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки, а саме: прийняти Закон України про розвідку з відкритих джерел (OSINT), який повинен установлювати принципи та врегульовувати повноваження, сфери, форми та методи діяльності суб'єктів здійснення OSINT; створити незалежний парламентський комітет з питань здійснення контролю за діяльністю суб'єктів OSINT; для покращення взаємодії та координації діяльності суб'єктів OSINT, створити постійний міжвідомчий орган, до якого входитимуть представники основних державних органів, що займаються OSINT (розвідувальні служби, правоохоронні органи, Міністерство оборони, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації, інші суб'єкти); впровадити єдину інформаційну платформу між суб'єктами здійснення OSINT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авер'янов В. Адміністративне право України: доктринальні аспекти реформування. Право України. 1998. № 8. С. 8–13.

2. Адміністративне право України : підручник / В. В. Галунько та ін. Херсон : ХМД, 2013. Т. 1 : Заг. адміністративне право. Акад. курс. 393 с.

3. Адміністративне право України в сучасних умовах (виклики початку XXI століття) / за заг. ред. В. Галунька. Херсон : Херсон. міська друкарня, 2010. 378 с.

4. Адміністративне судочинство України : підручник / за заг. ред. Т. О. Коломоєць. Київ : Істина, 2008. 216 с.

5. Адміністративно-правове забезпечення прав і свобод людини та громадянина : навч. посіб. / І. О. Ієрусалімова та ін. Київ : Знання, 2007. 223 с.

6. Антонов В. О. Конституційно-правові засади національної безпеки України : монографія / наук. ред. Ю. С. Шемшученко. Київ : Талком, 2017. 576 с.

7. Бабій Б. М., Бурчак Ф. Г., Корецький В. М., Цветков В. В. Юридичний словник. Київ : УРЕ, 1983. 872 с.

8. Баліцький В. Гносеологія формування понять «безпека», «державна безпека» та «національна безпека». Літопис Волині. Всеукраїнський науковий часопис. 2023. Чис. 29. URL: http://litopys.volyn.ua/index.php/litopys/article/view/491/425.

9. Банк Р. О. Адміністративно-правові засади забезпечення безпеки підприємницької діяльності в Україні : дис. ... канд. юрид. наук : 12.00.07. Київ, 2014. 230 с.

10. Барсуков К. В. Адміністративно-правове забезпечення проходження служби працівниками органів внутрішніх справ у складі міжнародних миротворчих підрозділів : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2010. 20 с.

11. Білоус В. В. OPEN DATA І OSINT як актуальні категорії інформаційного забезпечення розслідування злочинів. Інформаційне забезпечення розслідування злочинів : матеріали ІІІ Міжнар. круглого столу. Одеса, 2015. С. 27–34.

12. Бригінець О. О. Правове забезпечення фінансової безпеки України : дис. ... д-ра юрид. наук : 12.00.07. Ірпінь, 2017. 415 с.

13. Бурба В. В. Організаційно-правові засади використання розвідки з відкритих джерел інформації (OSINT) в діяльності розвідувальних служб європейських країн. Юридичний бюлетень. 2019. Вип. 11(1). URL: http://www.lawbulletin.oduvs.od.ua/archive/2019/11/part_1/3.pdf.

14. Вархов А. Правовий концепт «забезпечення» у контексті безпекового спрямування. Виклики сучасності та наукові підходи до їх вирішення : матеріали міжнар. наук.-практ. конф. (м. Київ, 12–13 серп. 2020 р.). Київ, 2020. С. 32–34.

15. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : ВТФ «Перун», 2009. 1736 с.

16. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний порадник / Д. С. Зоренко та ін. Харків : ІПЮК для СБУ, 2023. 36 с.

17. Вічалківський І. В. Міжнародний досвід здійснення парламентського контролю за діяльністю розвідувальних та спеціальних служб. Державне управління: удосконалення та розвиток. 2014. № 7. URL: http://www.dy.nayka.com.ua/?op=1&z=750.

18. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : вибр. наук. праці. Київ : НІСД, 2016. 528 с.

19. Войтешенко Т. М. Правові аспекти охорони та захисту комп’ютерних систем. Інформація і право. 2010. № 1. URL: https://ippi.org.ua/sites/default/files/10vtmiks.pdf.

20. Войціховський А. В. Формування системи інформаційної безпеки в рамках ООН. Право і безпека в умовах сучасних викликів : матеріали міжнар.

наук.-практ. конф. (м. Харків, 17 трав. 2019 р.). Харків, 2019. URL: https://univd.edu.ua/general/publishing/konf/17_05_2019/pdf/17.pdf.

21. Волинка К. Г. Механізм забезпечення прав і свобод особи: питання теорії і практики : дис. ... канд. юрид. наук : 12.00.01. Київ, 2000. 177 с.

22. Волинка К. Г. Теорія держави і права : навч. посіб. Київ : МАУП, 2003. 240 с.

23. Галунько В., Діхтієвський П., Кузьменко О. та ін. Адміністративне право України. Повний курс : підручник / за ред. В. Галунька. Херсон : ОЛДІ-ПЛЮС, 2018. 446 с.

24. Ганзенко О. О. Теорія правових засобів у контексті інструментальної теорії права. Вісник Запорізького національного університету. Юридичні науки. 2016. № 3. С. 36–42.

25. Гаруст Ю. В. Адміністративно-правові засоби забезпечення прав громадян у податковій сфері. Правові горизонти. 2017. Вип. 5(18). URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/41787/1/Harust_Administrative_and_legal_means_to_ensure_the_rights_of_citizens_in_the_tax_area.pdf.

26. Главацька А. Л., Ангельська О. В., Опірський І. Р. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. Кібербезпека: освіта, наука, техніка. 2023. № 3(19). URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/647/500.

27. Гладун З. С. Адміністративне право України : навч. посіб.-довід. для підгот. до іспиту. Тернопіль : ТНЕУ, 2008. 172 с.

28. Голубєв В. О. Правові аспекти захисту інформації в автоматизованих системах. Юрист. 2007. № 5. С. 12–19.

29. Гумін О. М., Пряхін Є. В. Адміністративно-правове забезпечення: поняття та структура. Наше право. 2014. № 4. С. 46–50. URL: http://nbuv.gov.ua/UJRN/Nashp_2014_4_9.

30. Денисова А. Правові засоби: поняття та види. Право України. 2010. № 7. С. 190–195.

31. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення : монографія / М. Ф. Криштанович та ін. Львів : Сполом, 2020. 418 с.

32. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : Постанова Кабінету Міністрів України від 23 грудня 2020 р. № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF.

33. Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів : Постанова Кабінету Міністрів України від 10 травня 2018 р. № 357. URL: https://zakononline.com.ua/documents/show/373347___675526.

34. Дожанин В. М. Класифікація гарантій адміністративно-правового забезпечення прав і свобод громадян у сфері запобігання та протидії корупції. Visegrad Journal on Human Rights. 2015. № 1. С. 98–106.

35. Дозинський Ю. Р. Адміністративно-правові гарантії прав фізичних і юридичних осіб при здійсненні державного нагляду та контролю. Legal Science Electronic Journal. 2022. № 5. URL: http://lsej.org.ua/5_2022/91.pdf.

36. Доронін І. М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження : дис. ... д-ра юрид. наук. Київ, 2020. 539 с.

37. Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки : резолюція Генеральної Асамблеї ООН A/RES/53/70 від 4 груд. 1998 р. URL: https://undocs.org/ru/A/RES/53/70.

38. Дьомін І. Адміністративно-правові засади запобігання та протидії корупції міліцією України : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2011. 19 с.

39. Європейська конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року : офіц. текст зі змін. станом на 1 серпня 2021 р. / Рада Європи. Страсбург : Європейський суд з прав людини, Рада Європи, 2021. 63 с.

40. Європейська стратегія кібербезпеки (2020). URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

41. Загальна теорія держави і права : навч. посіб. / А. М. Колодій та ін. ; за ред. В. В. Копєйчикова. Київ : Юрінком Інтер, 2000. 320 с.

42. Загальна теорія держави і права : підручник / М. В. Цвік, В. Д. Ткаченко та ін. ; за ред. М. В. Цвіка. Харків : Право, 2002. 432 с.

43. Загальний регламент захисту даних (GDPR) в Сполученому Королівстві. URL: https://gdpr-text.com/uk/.

44. Загурська-Антонюк В. Ф. Державне управління національною безпекою в умовах геополітичних загроз : автореф. дис. ... д-ра наук з держ. упр. : 25.00.05. Київ, 2021. 45 с.

45. Івченко А. О. Тлумачний словник української мови. Харків : Фоліо, 2002. 543 с.

46. Ігонін Р. Проблема доктринального визначення поняття "адміністративно-правове забезпечення". Вісник Національної академії прокуратури України. 2015. № 2(40). С. 37–43. URL: http://nbuv.gov.ua/UJRN/Vnapu_2015_2_7.

47. Ієрусалімова І. О. Механізм адміністративно-правового забезпечення прав і свобод людини та громадянина : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2006. URL: http://mydisser.com/ru/avtoref/view/16746.html.

48. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. Південноукраїнський правничий часопис. 2016. № 2. С. 110–113.

49. Іщук Д. О. Гарантії реалізації адміністративно-правового статусу Національного антикорупційного бюро України. Порівняльно-аналітичне право. 2020. № 1. С. 324–327.

50. Калугін В. Ю. Основні методи OSINT, що використовуються у кримінальному аналізі. Кібербезпека в Україні: правові та організаційні

питання : матеріали міжнар. наук.-практ. конф. (м. Одеса, 17 листопада 2023 р.). Одеса : ОДУВС, 2023. 168 с.

51. Каріх І. В. Інституційно-правові засади політики національної безпеки в гуманітарній сфері : дис. ... канд. політ. наук : 21.01.01. Київ, 2018. 218 с.

52. Качинський А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень : монографія. Київ : НІСД, 2013. 101 с.

53. Кисельов А. О. Досвід використання підрозділами Національної поліції технологій «OSINT» у протидії кримінальним правопорушенням. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VI Міжнар. наук.-практ. конф. (м. Дніпро, 11 березня 2022 р.). Дніпро, 2022. С. 318–319.

54. Кобко Є. В. Адміністративно-правовий механізм забезпечення національної безпеки держави : дис. ... д-ра юрид. наук. Харків, 2023. 400 с.

55. Кобко Є. В. Актуальні проблеми реалізації державної політики у сфері забезпечення інформаційної безпеки України. Право і Безпека. 2021. № 2 (81). С. 104–109.

56. Кобринський В. Ю. Державний контроль у сфері національної безпеки України : дис. … канд. юрид. наук : 12.00.07. Київ, 2008. 209 с.

57. Кожушко О. О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. URL: http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/3217.

58. Колесников Є. Є. Поняття та особливості адміністративно-правового забезпечення захисту прав споживачів. Форум права. 2011. № 2. С. 432–438. URL: http://nbuv.gov.ua/UJRN/FP_index.

59. Колпаков В. К. Адміністративне право України : підручник. Київ : Юрінком Інтер, 1999. 736 с.

60. Комзюк А. Т. Заходи адміністративного примусу в правоохоронній діяльності міліції: поняття, види та організаційно-правові

питання реалізації : монографія / за заг. ред. О. М. Бандурки. Харків : Нац. ун-т внутр. справ, 2002. 336 с.

61. Комзюк А. Т. Адміністративно-правові засоби здійснення митної справи : дис. ... канд. юрид. наук. Харків, 2003. 191 с.

62. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.

63. Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

64. Кондратенко В. М. Основні чинники розвитку адміністративно-правових засобів забезпечення прав і свобод осіб з інвалідністю в умовах європейської інтеграції. URL: http://nvppp.in.ua/vip/2018/5/tom_2/21.pdf.

65. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

66. Резнікова О. О., Цюкало В. Ю., Паливода В. О., Дрьомов С. В., Сьомін С. В. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналітична доповідь. Київ : НІСД, 2015. 58 с.

67. Корж І. Безпека: методологічні підходи до поняття. Национальный юридический журнал: теория и практика. 2019. URL: http://www.jurnaluljuridic.in.ua/archive/2019/4/part_1/14.pdf.

68. Корж І. Ф. Адміністративно-правове регулювання відносин у сфері державної безпеки України : монографія. Київ : Нілан-ЛТД, 2013. 384 с.

69. Кошиков Д. О. Гарантії прав учасників адміністративно-правових відносин у сфері реалізації державної політики у сфері забезпечення економічної безпеки держави. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/abba30eb-924c-44d5-a874-0226d636fe77/content.

70. Кременовська І. В. Правові та організаційні засади діяльності суб'єктів виконавчої влади у сфері забезпечення національної безпеки України : дис. ... канд. юрид. наук : 12.00.07. Ірпінь, 2010. 210 с.

71. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

72. Крисань Т. Є. Правова природа юридичних гарантій цивільних прав. Університетські наукові записки. 2013. № 1. С. 519–523.

73. Криштанович М. Ф. Механізми державної політики України щодо забезпечення національної безпеки. Публічне управління та митне адміністрування. 2019. № 3 (22). С. 248–253.

74. Крук С. І. Інституційний розвиток державного управління у сфері забезпечення національної безпеки України : дис. … д-ра наук з держ. упр. : 25.00.05. Харків, 2019. 449 с.

75. Куций О. А. Адміністративно-правові засоби забезпечення прав фізичних осіб у податкових правовідносинах : дис. ... канд. юрид. наук. Одеса.

76. Лазур Я. В. Забезпечення прав і свобод громадян в сфері публічного управління : автореф. дис. ... д-ра юрид. наук : 12.00.07. Київ, 2011. 40 с.

77. Ліпкан В. А. Адміністративно-правові основи забезпечення національної безпеки України : автореф. дис. … д-ра юрид. наук : 12.00.07. Київ, 2008. 34 с.

78. Ліпкан В. А. Національна безпека України : навч. посіб. 2-ге вид. Київ : КНТ, 2009. 576 с.

79. Лук'янова Г. Ю. Механізм адміністративно-правового забезпечення координації суб'єктів протидії корупції: змістовне наповнення поняття. Юридична наука. 2020. № 5(107), т. 2. С. 31–39. URL: https://journal-nam.com.ua/index.php/journal/article/view/298/287.

80. Мазурик Р. В. Адміністративно-правові засоби як універсальні інструменти регулювання публічно-правових відносин у сфері організації

прокурорської діяльності. Держава та регіони. Серія: Право. 2020. № 4 (79), т. 2. С. 75–82. DOI: https://doi.org/10.32840/1813-338X-2020.4-2.14.

81. Макарчук В. В. Генеза поняття «національна безпека» в адміністративному праві. Економіка. Фінанси. Право. 2021. № 4(1). С. 5–8.

82. Мартинюк С. О. Адміністративно-правове регулювання забезпечення функціонування OSINT у сфері національної безпеки. Аналітично-порівняльне правознавство. 2023. Вип. 5. С. 355–358. URL: http://journal-app.uzhnu.edu.ua/article/view/290720/284349.

83. Мартинюк С. О. Характеристика принципів функціонування OSINT у сфері національної безпеки. Юридичний науковий електронний журнал. 2021. № 9. С. 332–334.

84. Мартинюк С. О. Щодо змісту поняття адміністративно-правового забезпечення OSINT у сфері національної безпеки України. Актуальні завдання та напрями розвитку юридичної науки у XXI столітті : матеріали міжнар. наук.-практ. конф. (м. Львів, 15–16 жовтня 2021 р.). Львів : Західноукраїнська організація «Центр правничих ініціатив», 2021.

85. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. Системи управління, навігації та зв'язку. 2016. Вип. 4. С. 81–84.

86. Митрицька Г. Правові засоби в механізмі правового регулювання суспільних відносин у сфері нацманої праці. URL: http://pgp-journal.kiev.ua/archive/2021/3/21.pdf.

87. Міжнародний пакт про громадянські і політичні права від 19.10.1973 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text.

88. Мурашко А. М. Реалізація державної політики у сферах національної безпеки і оборони на регіональному рівні : автореф. дис. ... канд. наук з держ. упр. Чернігів, 2021. 21 с.

89. Навроцький О. Поняття адміністративно-правових гарантій забезпечення прав дитини в україні. URL: https://eppd13.cz/wp-content/uploads/2017/2017-4-1/30.pdf.

90. Наконечна І. В. Адміністративно-правовий механізм забезпечення національної безпеки в умовах євроінтеграції: питання теорії і практики : дис. ... д-ра юрид. наук. Київ, 2023. 412 с.

91. Наконечна І. В. Сутність явища «безпека»: теоретико-правовий аналіз. KELM. 2022. № 6(50). С. 249–253.

92. Наливайко О. І. Правовий захист людини як предмет дослідження загальної теорії права. Держава і право : зб. наук. праць. Юридичні і політичні науки. Київ : Інститут держави і права ім. В. М. Корецького НАН України, 2001. Вип. 12. С. 18–24.

93. Нашинець-Наумова А. Концептуальні підходи щодо забезпечення національної безпеки: інформаційно-правові та інституційні засади. Підприємництво, господарство і право. 2017. № 1. С. 34–39.

94. Новий тлумачний словник української мови : у 4 т. / уклад.: В. Яременко, О. Сліпушко. Київ : Аконіт, 2000. Т. 2. 912 с.

95. Олефіренко Е. Адміністративно-правові гарантії реалізації прав і свобод громадян : автореф. дис. … канд. юрид. наук : 12.00.07. Ірпінь, 2006. 20 с.

96. Оніщенко Ю. М. Використання методу OSINT під час підготовки фахівців з кібербезпеки. URL: https://univd.edu.ua/science-issue/issue/6904.

97. Онуфрієнко О. В. Правові засоби у контексті інструментальної теорії права : автореф. дис. ... канд. юрид. наук : 12.00.01. Харків, 2004. 18 с.

98. Остапенко О. Наукові уявлення про механізм адміністративно-правового регулювання. Науковий вісник Львівського державного університету внутрішніх справ. Серія : Юридична. 2010. Вип. 2. С. 142–149.

99. Павлюков І. І. Правові засоби: поняття, види, функції та взаємодія в процесі регулювання суспільних відносин. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/03/8.pdf.

100. Панченко І. В. Цифрові технології в роботі з джерелами інформації. Одеса : Університет Ушинського, 2023. 27 с.

101. Парламентський контроль за воєнною розвідкою / Женевський центр з питань урядування в секторі безпеки. URL: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Parliamentary-Oversight-of-Military-Intelligence_UKR_Final.pdf.

102. Пащенко Т. П. Гібридна війна та соціальні мережі. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 62–65.

103. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук: 12.00.07. Львів, 2019. 268 с.

104. Пилипчук В. Г., Дзьобань О. П., Настюк В. Я. Система і компетенція державних органів зі спеціальним статусом у сфері національної безпеки України: монографія. Харків: Право, 2009. 200 с.

105. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14.01.2015 р. № 2. URL: https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF.

106. Положення про Апарат Ради національної безпеки і оборони України: затв. Указом Президента України від 14.10.2005 р. № 1446/2005. URL: https://www.rnbo.gov.ua/ua/Aparat-Rady-natsionalnoi-bezpeky-i-oborony-Ukrainy.html.

107. Положення про Центр протидії дезінформації: затв. Указом Президента України від 07.05.2021 р. № 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021.

108. Пономаренко Г. О. Управління у сфері забезпечення внутрішньої безпеки держави: адміністративно-правові засади: монографія. Харків: Видавець Вапнярчук Н. М., 2007. 448 с.

109. Пономарьов С. П. Адміністративно-правове забезпечення діяльності сектору безпеки і оборони України: дис. ... д-ра юрид. наук: 12.00.07 / Харк. нац. ун-т внутр. справ. Харків, 2018. 513 с.

110. Популярна юридична енциклопедія / В. К. Гіжевський, В. В. Головченко, В. С. Ковальський (кер.). Київ: Юрінком Інтер, 2003. 528 с.

111. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15.

112. Про внесення змін до Положення про Міністерство цифрової трансформації України: Постанова Кабінету Міністрів України від 29.04.2022 р. № 501. URL: https://zakon.rada.gov.ua/laws/show/501-2022-%D0%BF.

113. Про Державну прикордонну службу України: Закон України від 03.04.2003 р. № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15.

114. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. Відомості Верховної Ради України. 2006. № 30. Ст. 258. URL: https://zakon.rada.gov.ua/laws/show/3475-15.

115. Про затвердження Положення про Міністерство оборони України: Постанова Кабінету Міністрів України від 26.11.2014 р. № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF.

116. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF.

117. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

118. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

119. Про Кабінет Міністрів України: Закон України від 27.02.2014 р. № 794-VII. URL: https://zakon.rada.gov.ua/laws/show/794-18.

120. Про контррозвідувальну діяльність: Закон України від 26.12.2002 р. № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374-15.

121. Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16.01.1997 р. № 3/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80.

122. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016.

123. Про Національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

124. Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19.

125. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12.

126. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

127. Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України: Указ Президента України від 14.04.1999 р. № 379/99. URL: https://zakon.rada.gov.ua/laws/show/379/99.

128. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80.

129. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021.

130. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021.

131. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ

Президента України від 26.05.2015 р. № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015.

132. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України»: Указ Президента України від 08.06.2012 р. № 389/2012. URL: https://web.archive.org/web/20200616202321/https://zakon.rada.gov.ua/laws/show/389/2012.

133. Про розвідку: Закон України від 17.09.2020 р. № 912-IX. Відомості Верховної Ради України. 2020. № 912-20. URL: https://zakon.rada.gov.ua/laws/show/912-20.

134. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12.

135. Про створення Центру протидії дезінформації: Указ Президента України від 19.03.2021 р. № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21.

136. Прощаєв В. В. Принципи розвідувальної діяльності за законодавством країн пострадянського простору: порівняльний аналіз. Науковий вісник публічного та приватного права. 2019. Випуск 1, том 1. С. 96-101.

137. Рабінович П. М. Основи загальної теорії права та держави: навч. посіб. 5-те вид., зі змінами. Київ: Атіка, 2001. 176 с.

138. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Відомості Європейського Союзу. 2016. № 984_008-16. URL: https://zakon.rada.gov.ua/laws/show/984_008-16.

139. Резолюція 1373 (2001), прийнята Радою Безпеки ООН на 4385 засіданні 28.10.2001 р. URL: https://documents.un.org/doc/undoc/gen/n01/557/45/pdf/n0155745.pdf.

140. Ржевська Н. Ф., Кожушко О. О. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE). Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців: матеріали Всеукр. наук. конф. Львів, 2011. С. 257–261.

141. Рубан А. В. Державне управління у сфері національної безпеки України: дис. … канд. наук держ. упр.: 25.00.05 / Нац. ун-т цивільного захисту України. Харків, 2019. 253 с.

142. Сектор безпеки і оборони України: теорія, стратегія, практика: монографія / Ф. В. Саганюк, В. С. Фролов, О. В. Устименко, М. М. Лобко та ін. Київ: Академпрес, 2017. 180 с.

143. Семенченко А. І. Стратегічне планування у сфері державного управління національною безпекою: автореф. дис. ... д-ра наук: 25.00.02. Київ, 2008. 32 с.

144. Серватовський А. В., Онищенко Ю. М., Макаренко П. В. Міжнародний досвід використання OSINT. URL: https://univd.edu.ua/science-issue/issue/3329.

145. Ситник Г. П. Державне управління національною безпекою України: монографія. Київ: Вид-во НАДУ, 2004. 408 с.

146. Ситник Г. П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади): підручник. Київ: НАДУ, 2012. 730 с.

147. Ситник Г. П., Олуйко В. М., Вавринчук М. П. Національна безпека України: теорія і практика. Хмельницький – Київ: Кондор, 2007. 669 с.

148. Сокуренко В. В. Публічне адміністрування сферою оборони в Україні: автореф. дис. ... д-ра юрид. наук: 12.00.07 / Нац. акад. внутр. справ, Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2016. 40 с.

149. Сорока Л. В. Державний нагляд і контроль як основа адміністративно-правового забезпечення та реалізації державних гарантій. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2020. Том 31. № 4. С. 173–177.

150. Соціально-економічна безпека: навч. посіб. / Бережницька У. Б., Савко О. Я., Данилюк М. О., Бережницька У. Б. Івано-Франківськ: Симфонія, 2016. 264 с. URL: http://chitalnya.nung.edu.ua/node/3587.

151. Столбовий В. Нормативно-правове забезпечення службових правовідносин у сфері національної безпеки України. Підприємство, господарство і право: науково-практичний юридичний журнал. 2019. № 2. С. 120–124.

152. Про Стратегію національної безпеки України «Україна у світі, що змінюється» : Указ Президента України від 12 лютого 2007 р. № 105. URL: https://zakon.rada.gov.ua/laws/show/105/2007#Text.

153. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text.

154. Стрельченко А. Г. Доктринальна характеристика забезпечення діяльності органів Державної виконавчої служби Україні. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/02/11-1.pdf.

155. Стрюк М. П. Формування системи управління сектором безпеки і оборони України: адміністративно-правовий аспект : дис. ... канд. юрид. наук. Дніпро, 2022. 199 с.

156. Стукалін Т. А. Система державного управління у сфері оборони держави та основні напрями її розвитку в контексті реформування сектора безпеки і оборони. Теорія та практика державного управління. 2016. Вип. 2. С. 213–220.

157. Тихий В. П. Безпека людини: поняття, правове забезпечення, значення, види. Вісник Національної академії правових наук України. 2016. № 2. С. 31–46.

158. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 411 с.

159. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Міжнародна угода від 27.06.2014 р. № 984_011. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.

160. Управління та реформування сектора безпеки (УРСБ). Рекомендації для співробітників ОБСЄ. Відень : ОБСЄ, 2016. 132 с. URL: https://www.osce.org/files/f/documents/a/e/253156.pdf.

161. Феденко О. О. Військово-політичні аспекти становлення системи національної безпеки України : автореф. дис. ... канд. політ. наук : 23.00.02. Львів, 2002. 16 с.

162. Федеральна розвідувальна служба (Bundesnachrichtendienst, BND) : веб-сайт. URL: https://www.bnd.bund.de/EN/Home/home_node.html.

163. Федеральне відомство захисту конституції (BfV) : веб-сайт. URL: https://www.verfassungsschutz.de/DE/Home/home_node.html.

164. Федеральне управління кримінальної поліції (Bundeskriminalamt, BKA) : веб-сайт. URL: https://www.bka.de/EN/Home/home_node.html.

165. Цивільний демократичний контроль сектору розвідки : матеріали "круглого столу" Україна — НАТО (Київ, 19 грудня 2005 р.) / Женевський центр демократичного контролю над збройними силами, Комітет Верховної Ради України з питань національної безпеки і оборони, Рада національної безпеки і оборони України, Організація Північноатлантичного договору — НАТО ; за заг. ред. О. С. Бодрука. Київ : НІПМБ, DCAF, 2005. 152 с.

166. Чемодурова А. Правове регулювання та його ефективність у сучасному світі. Підприємництво, господарство і право. 2020. № 4. С. 262–267.

167. Чистоклетов Л., Хитра О. Поняття адміністративно-правового забезпечення та його механізму. Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки". 2020. № 3(27). С. 173–180.

168. Чорнописька В. З. Адміністративно-правові гарантії діяльності релігійних організацій в Україні : дис. ... д-ра юрид. наук : 12.00.07. Львів, 2021. 500 с.

169. Чуйко З. Д. Конституційні основи національної безпеки України : дис. ... канд. юрид. наук : 12.00.02. Харків, 2008. 209 с.

170. Шевчук О. Сектор безпеки України як об’єкт публічного адміністрування. Підприємництво, господарство і право. 2021. № 2. С. 138–143.

171. Шевчук О. Ю. Основні принципи запобігання та протидії корупції. Реалізація державної антикорупційної політики в міжнародному вимірі : матеріали Міжнар. наук.-практ. конф. (Київ, 2016 р.). Київ : НАВС, 2016. С. 441–444.

172. Шматова Ю. О. Механізм адміністративно-правового забезпечення прав людини в умовах надзвичайних ситуацій : дис. ... канд. юрид. наук. Київ, 2012. 233 с.

173. Шовкун Ю. І. Поняття та система адміністративно-правового забезпечення дотримання обмежень під час проходження публічної служби. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/b1f8bdd2-50ae-4b4a-b34c-5f69eb3ae32f/content.

174. Шопіна І. М. Адміністративно-правове регулювання управління органами внутрішніх справ України : дис. ... д-ра юрид. наук : 12.00.07. Київ, 2012. 514 с.

175. Шопіна І. М. Феномен адміністративно-правового забезпечення в адміністративному праві України. Наука і правоохорона. 2018. № 4. С. 141–145.

176. Щербань В. Д. Концепція адміністративно-правового забезпечення функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах України : дис. ... д-ра юрид. наук. Київ, 2020. 443 с.

177. Юридична енциклопедія : в 6 т. / за ред. Ю. С. Шемшученка. Київ : Укр. енциклопедія. Т. 1 : А-Г. 627 с.

178. Яровий Т. С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. URL: https://journals.maup.com.ua/index.php/expert/article/view/1622/2563.

179. Bundesdatenschutzgesetz (BDSG) : Закон про захист даних : від 30.06.2017 р. URL: https://www.gesetze-im-internet.de/bdsg_2018/.

180. Bundesverfassungsschutzgesetz (BVerfSchG). URL: https://www.gesetze-im-internet.de/bverfschg/.

181. Central Intelligence Agency. CIA's Role in National Security. URL: https://www.usa.gov/agencies/central-intelligence-agency#:~:text=The%20Central%20Intelligence%20Agency%20(CIA,abroad%20to%20safeguard%20national%20security.

182. Conference on Security and Co-operation in Europe. Helsinki, 1975. URL: https://www.osce.org/files/f/documents/5/c/39501.pdf.

183. Data Protection Act 2018 : Act of Parliament : від 23.05.2018 р. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents.

184. Federal Bureau of Investigation. FBI's Mission and Responsibilities. URL: https://www.justice.gov/archive/mps/2006omf/manual/fbi.htm#:~:text=The%20mission%20of%20the%20FBI,agencies%20and%20partners%3B%20and%20to.

185. Freedom of Information Act (FOIA). URL: https://www.foia.gov/.

186. Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, PKGrG. URL: https://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html.

187. Grundgesetz für die Bundesrepublik Deutschland. URL: https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz#:~:text=Das%20Grundgesetz%20(GG)%20ist%20die,und%20von%20den%20Alliierten%20genehmigt.

188. Williams H. J., Blum I. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Library of Congress Control Number: 2018943942, 2018.

189. Information Commissioner's Office. Data Protection Act 2018. URL: https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%2

0UK’s%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently.

190. Intelligence and Security Committee of Parliament. URL: https://isc.independent.gov.uk/how-the-committee-works/.

191. Intelligence Reform and Terrorism Prevention Act of 2004. URL: https://en.wikipedia.org/wiki/Intelligence_Reform_and_Terrorism_Prevention_Act#:~:text=The%20Intelligence%20Reform%20and%20Terrorism,titles%20with%20varying%20subject%20issues.

192. Investigatory Powers Act 2016. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents.

193. Investigatory Powers Commissioner. URL: https://www.ipco.org.uk/investigatory-powers/.

194. Justice and Security Act 2013. URL: https://www.legislation.gov.uk/ukpga/2013/18/contents/enacted.

195. MI5. Annual Report. URL: https://www.mi5.gov.uk/faq.

196. MI6. Intelligence and Security Committee Report. URL: https://isc.independent.gov.uk/publications/.

197. National Crime Agency Main Estimate 2024–25. URL: https://assets.publishing.service.gov.uk/media/669e15530808eaf43b50d36b/NCA_Main_Estimates_memorandum_2024-25.pdf.

198. National Crime Agency. Annual Plan. URL: https://www.gov.uk/government/publications/national-crime-agency-annual-report-and-accounts-2023-to-2024/national-crime-agency-annual-report-and-accounts-2023-to-2024-accessible.

199. National Security Act of 1947. URL: https://history.state.gov/milestones/1945-1952/national-security-act#:~:text=The%20National%20Security%20Act%20of,National%20Security%20Council%20(NSC).

200. National Security Agency. NSA’s Intelligence and Security Responsibilities. URL:

https://www.nsa.gov/about/#:~:text=NSA%20provides%20foreign%20signals%20intelligence,U.S.%20goals%20and%20alliances%20globally.

201. Hassan N. A., Hijazi R. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, 2018.

202. Office of the Director of National Intelligence. Annual Report. URL: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023.

203. Open Source Intelligence, U.S. Army Field Manual Interim FMI 2-22.9, December 2006. URL: www.fas.org/irp/doddir/army/fmi2-22-9.pdf.

204. Resolution 2178 (2014) / adopted by the Security Council at its 7272nd meeting, on 24 September 2014. Цифрова бібліотека ООН. URL: https://digitallibrary.un.org/record/780316?v=pdf.

ДОДАТОК

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Мартинюк С. О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал.* 2021. № 9. С. 332–334. DOI: https://doi.org/10.32782/2524-0374/2021-9/82.

2. Мартинюк С. О. Адміністративно-правове регулювання забезпечення функціонування OSINT у сфері національної безпеки. *Аналітично-порівняльне правознавство.* 2023. Випуск 5. С. 355–358. DOI: https://doi.org/10.24144/2788-6018.2023.05.63.

3. Мартинюк С. О. Зарубіжний досвід функціонування OSINT у сфері національної безпеки: адміністративно-правовий аспект. *Наукові перспективи.* 2025. № 3 (57). С. 1061–1071. DOI: https://doi.org/10.52058/2708-7530-2025-3(57)-1061-1071.

4. Мартинюк С. О. Національна безпека, як об'єкт адміністративно-правового забезпечення: поняття та зміст у працях вітчизняних дослідників. 2025. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. № 2(74) (2025). С. 78-83. DOI: https://doi.org/10.32689/2522-4603.2025.2.12

Статті у зарубіжних періодичних наукових виданнях:

5. Lata N., Martyniuk S., Minka T., Ilchyshyn N., Yurakh V. Administrative and legal security of public information services in the activities of bodies of legislative and judicial power: Seguridad administrativa y jurídica de los servicios de información pública en las actividades de los órganos del poder

legislativo y judicial. *Cuestiones Políticas*. 2022. Vol. 40 (72). P. 656–669. DOI: https://doi.org/10.46398/cuestpol.4072.38.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Мартинюк С. О. Щодо змісту поняття адміністративно-правового забезпечення OSINT у сфері національної безпеки України. *Актуальні завдання та* напрями *розвитку юридичної науки у XXI столітті*: матеріали Міжнародної науково-практичної конференції (м. Львів, 15–16 жовтня 2021 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», 2021. С. 77–79.

7. Мартинюк С. О. Забезпечення прав людини при використанні OSINT у сфері національної безпеки. *Права людини: методологічний, гносеологічний та онтологічний аспекти:* матеріали Міжнародної науково-практичної конференції присвяченої 75-річчю проголошення Загальної декларації прав людини (м. Дніпро, 5 грудня 2023 р.). Дніпро, 2023. С. 213–215.

8. Мартинюк С. О. Організаційно-правові засоби адміністративно-правового забезпечення функціонування OSINT у сфері національної безпеки. *Український правовий вимір: пошук відповідей на глобальні міжнародні виклики*: матеріали VI Міжнародної науково-практичної конференції (м. Дніпро, 24 травня 2024 р.) / Університет митної справи та фінансів. Дніпро, 2024. С. 66–69.

9. Мартинюк С. О. Роль OSINT для безпеки бізнесу: організаційно-правовий аспект. *Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності*: матеріали X Міжнародної науково-практичної конференції (м. Київ, 20–22 травня 2025 р.). Київ: Міжрегіональна Академія управління персоналом, 2025. С. 572–574.