УДК 342.9
DOI https://doi.org/10.24144/2307-3322.2024.83.2.40

СИСТЕМА СУБ'ЄКТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Крупнова А.О.,
аспірант Міжнародного економіко-гуманітарного університету імені Степана Дем'янчука,
адвокат
ORCID: 0009-0007-7819-9813

Крупнова А. Система суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні.

У статті, на основі аналізу чинного законодавства, наявних наукових, публіцистичних та методичних джерел, з'ясовано зміст системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні. Запропоновано під системою суб'єктів адміністративно-правового забезпечення інформаційної безпеки розуміти сукупність органів законодавчої, виконавчої та судової влад, державних, громадських та інших організацій і об'єднань, громадян, які можуть брати участь в адміністративно-правовому забезпеченні інформаційної безпеки відповідно до законодавства, що регламентує відносини у сфері інформаційної безпеки.

Встановлено, що система суб'єктів адміністративно-правового забезпечення інформаційної безпеки містить у собі широке коло структур як державної, так і недержавної приналежності. Перша група (державні суб'єкти) – представлена державою в особі Президента України, законодавчих, виконавчих і судових органів, які маючі різну компетенцію в сфері адміністративно-правового забезпечення інформаційної безпеки виконують в ній ключові завдання та функції. Другу групу (недержавні суб'єкти) можна поділити на дві підгрупи. До першої віднесено суспільство в особі юридичних осіб, а саме: комерційні компанії та недержавні організації (освітні заклади, дослідницькі інститути, науково-аналітичні центри тощо). До другої – фізичних осіб (громадян), які можуть безпосередньо брати участь у забезпеченні інформаційної безпеки, в особі фахівців, експертів, консультантів з інформаційної безпеки тощо.

Запропоновано: включити всіх недержавних суб'єктів до механізму реалізації мети та завдань Стратегії інформаційної безпеки; якомога ширше використовувати можливості недержавних суб'єктів у розглянутій сфері, а тому активізувати залучення громадян, громадських об'єднань, організацій тощо до вирішення проблеми забезпечення інформаційної безпеки; у структурі Ради національної безпеки і оборони України створити Міжвідомчу комісію із забезпечення інформаційної безпеки.

Ключові слова: система, суб'єкти, адміністративно-правове забезпечення, інформаційна безпека, національна безпека, захист інформації, інформаційні відносини.

Krupnova A. The system of subjects of administrative and legal support of information security in Ukraine.

Based on the analysis of current legislation, available scientific, journalistic and methodological sources, the article clarifies the content of the system of subjects of administrative and legal support of information security in Ukraine. It is proposed that the system of subjects of administrative and legal support of information security should be understood as a set of legislative, executive and judicial authorities, state, public and other organizations and associations, and citizens who may participate in administrative and legal support of information security in accordance with the legislation regulating relations in the field of information security.

It is established that the system of subjects of administrative and legal support of information security includes a wide range of structures of both state and non-state affiliation. The first group (state entities) is represented by the State represented by the President of Ukraine, legislative, executive and

judicial bodies, which, having different competencies in the field of administrative and legal support of information security, perform key tasks and functions in it. The second group (non-state actors) can be divided into two subgroups. The first one includes society represented by legal entities, namely, commercial companies and non-governmental organizations (educational institutions, research institutes, research and analytical centers, etc.) The second group includes individuals (citizens) who may be directly involved in ensuring information security, represented by specialists, experts, information security consultants, etc.

It is proposed to: include all non-state actors in the mechanism for implementing the goals and objectives of the Information Security Strategy; make the widest possible use of the capabilities of non-state actors in this area, and therefore intensify the involvement of citizens, public associations, organizations, etc. in solving the problem of information security; create an Interagency Commission on Information Security within the structure of the National Security and Defense Council of Ukraine.

Key words: system, subjects, administrative and legal support, information security, national security, information protection, information relations.

Постановка проблеми. Складність адміністративно-правового регулювання інформаційної безпеки визначається її багатоаспектністю, що зумовлює необхідність участі в цьому процесі безлічі різноманітних суб'єктів, які входять до єдиної системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки. Під системою суб'єктів адміністративно-правового забезпечення інформаційної безпеки слід розуміти сукупність органів законодавчої, виконавчої та судової влад, державних, громадських та інших організацій і об'єднань, громадян, які можуть брати участь в адміністративно-правовому забезпеченні інформаційної безпеки відповідно до законодавства, що регламентує відносини у сфері інформаційної безпеки. Суб'єкти, задіяні в процесі забезпечення інформаційної безпеки, діють у чітко окреслених рамках і суто в межах своєї компетенції. Станом на сьогодні, де інформаційна безпека стає ключовим елементом успіху державної політики та виживання держави загалом, активна участь у її забезпеченні різних суб'єктів стає неминучою та виправданою.

Стан опрацювання проблематики. Різні аспекти проблематики адміністративно-правового забезпечення інформаційної безпеки в Україні розкривали в своїх працях: І. Арістова, О. Баранов, В. Брижко, О. Довгань, О. Золотар, І. Корж, Р. Калюжний, Б. Кормич, В. Ліпкан, А. Марущак, В. Пилипчук, В. Рубан, Г. Сащук, Я. Собків, С. Феденько, Л. Харченко, В. Шамрай та ін. Визнаючи всю важливість виконаної вченими роботи, водночас необхідно відзначити, що попередні наукові праці, у тому числі на рівні дисертаційних досліджень, головним чином, були присвячені проблемам правового регулювання сфери забезпечення інформаційної безпеки в Україні.

Метою статті є з'ясування на основі аналізу чинного законодавства, наявних наукових, публіцистичних та методичних джерел, сутності та змісту системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні.

Виклад основного матеріалу. У системі суб'єктів адміністративно-правового забезпечення інформаційної безпеки основна відповідальність за запобігання та усунення загроз, що знижують рівень інформаційної безпеки, покладається на державні органи, які зайняті державним управлінням у сфері національної безпеки. Однак, виходячи з цілей і завдань, закріплених у Законі України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII [1] та Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28.12.2021 р. № 685/2021 [2], не останню роль у забезпеченні інформаційної безпеки мають відігравати й недержавні структури. Це передбачає наявність комплексної інтеграції зусиль усіх учасників процесу, включно з представниками, як державного, так і приватного секторів, для створення багаторівневої та мультидисциплінарної системи захисту інформації.

У контексті сучасних викликів та загроз національній безпеці України в інформаційній сфері, особливо важливим стає розробка теоретично обґрунтованої класифікації суб'єктів, що входять до системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки. Хоча класифікація за своєю природою не може бути абсолютно вичерпною через різноманіття інформаційної сфери та постійно мінливі умови, вона має залишатися практичною та функціональною для правозастосування. Вважаємо, що система суб'єктів адміністративно-правового забезпечення інформаційної безпеки містить у собі кілька основних груп суб'єктів, кожна з яких відіграє свою роль у запобіганні загрозам національній безпеці України в інформаційній сфері. Перша

група (державні суб'єкти) – представлена державою в особі Президента України, законодавчих, виконавчих і судових органів, які маючі різну компетенцію в сфері адміністративно-правового забезпечення інформаційної безпеки виконують в ній ключові завдання та функції. Другу групу (недержавні суб'єкти) можна поділити на дві підгрупи. До першої ми віднесли суспільство в особі юридичних осіб, а саме: комерційні компанії та недержавні організації (освітні заклади, дослідницькі інститути, науково-аналітичні центри тощо). До другої – фізичних осіб (громадян), які можуть безпосередньо брати участь у забезпеченні інформаційної безпеки, в особі фахівців, експертів, консультантів з інформаційної безпеки тощо. Окремо звернемо увагу, що громадяни можуть розглядатися як суб'єкти аналізованої нами системи лише умовно. Адже найчастіше вони беруть участь у забезпеченні інформаційної безпеки опосередковано.

Окреслені групи формують багаторівневу структуру адміністративно-правового забезпечення інформаційної безпеки, де кожен рівень робить свій внесок у загальну систему захисту. Держава, в особі своїх органів, відіграє ключову роль в адміністративно-правовому забезпеченні інформаційної безпеки. Володіючи значними ресурсами, вони виконують широкий спектр завдань та функцій, починаючи з розроблення та впровадження правових актів, що стосуються інформаційної сфери, і закінчуючи регулюванням і контролем виконання цих актів. На додачу до цього, держава фінансує освітні програми для підготовки фахівців, співпрацює на міжнародному рівні для захисту від транскордонних інформаційних загроз, стимулює розвиток технологій у сфері інформаційної безпеки тощо. Ефективна державна участь і координація між різними органами та секторами є критично важливою для створення надійної системи із захисту національної безпеки України в інформаційній сфері. Державна участь є невід'ємною та критично важливою у забезпеченні комплексного захисту інформації на всіх рівнях. Державні ініціативи та дії спрямовані на створення надійної та стійкої системи інформаційної безпеки, здатної протистояти сучасним загрозам і викликам. Щодо суспільства та громадян, то вони доповнюють роботу, яку здійснюють державні органи, вносячи інновації та спеціалізовані знання, що допомагають у розв'язанні специфічних завдань і створенні нових технологічних рішень, які сприяють забезпеченню інформаційної безпеки. Отже, важливість кожної з цих груп не може бути недооцінена, оскільки тільки спільні зусилля всіх суб'єктів, які входять до єдиної системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки дають змогу створити ефективну та стійку систему захисту інформаційного простору. У цьому разі розвиток міжсекторальної взаємодії та посилення співробітництва між усіма зацікавленими сторонами, а також залучення громадськості до процесів ухвалення рішень та контролю за дотриманням інформаційної безпеки, стають ключовими елементами у зміцненні національної безпеки України в інформаційній сфері. Розглядаючи можливі напрями організації спільної діяльності суб'єктів адміністративно-правового забезпечення інформаційної безпеки, необхідно мати на увазі, що взаємодію в широкому плані можна здійснювати у формах взаємного обміну інформацією, спільного планування та проведення заходів, взаємного використання сил і засобів в інтересах вирішення спільних завдань, організації спеціального моніторингу тощо.

Надана класифікація дає змогу визначити чіткі рамки для правового регулювання та управління в цій сфері, враховуючи різні рівні відповідальності та можливості позначених нами груп. Вона сприяє розробленню цілеспрямованих нормативно-правових актів, які стосуються як окремих суб'єктів, так і їх групи, або всієї системи загалом. Такий підхід дає змогу створити стійку й адаптивну систему адміністративно-правового забезпечення інформаційної безпеки, яка здатна ефективно реагувати на внутрішнє та зовнішнє середовище, що динамічно змінюється.

До системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні відносяться: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; Міністерство культури та інформаційної політики України; Міністерство з питань реінтеграції тимчасово окупованих територій України; Національна поліція України; Служба безпеки України; Служба зовнішньої розвідки України, Державна прикордонна служба України; Державна спеціальна служба транспорту; Державна служба України з надзвичайних ситуацій; Державна служба спеціального зв'язку та захисту інформації України; Збройні Сили України та інші органи виконавчої влади та військові формування, які входять до сектору інформаційної безпеки; органи місцевого самоврядування; судові органи; комерційні компанії; недержавні організації та громадяни.

Розглядаючи державу як суб'єкт адміністративно-правового забезпечення інформаційної безпеки, наділену відповідними повноваженнями в особі державних органів і посадових осіб, не-

обхідно зазначити, що діяльність, пов'язана з адміністративно-правовим забезпеченням інформаційної безпеки, має будуватися на основі розмежування повноважень органів законодавчої, виконавчої та судової влади. Так, Президент України як глава держави, гарант державного суверенітету і територіальної цілісності України, визначає основні напрями політики щодо забезпечення інформаційної безпеки, здійснює керівництво органами забезпечення інформаційної безпеки, контроль за їхньою діяльністю. Президент України здійснює контроль за сектором інформаційної безпеки як безпосередньо, так і через очолювану ним Раду національної безпеки і оборони України та створювані ним у разі необхідності консультативні, дорадчі та інші допоміжні органи і служби.

Рада національної безпеки і оборони України відповідно до Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України. Згідно ст. 3 Закону України «Про Раду національної безпеки і оборони України» від 05.03.1998 р. № 183/98-ВР [3] до її функцій пов'язаних з адміністративно-правовим забезпеченням інформаційної безпеки можна віднести наступні: внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері інформаційної безпеки; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері інформаційної безпеки у мирний час; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері інформаційної безпеки в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України. В структурі Ради національної безпеки і оборони України є Центр протидії дезінформації, утворений її Рішенням «Про створення Центру протидії дезінформації» від 11.03.2021 р. № 106 [4]. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [5]. У своїй діяльності Центр висвітлює тенденції з інформування стану військової справи, ОПК, боротьби зі злочинністю та корупцією, зовнішньої та внутрішньої політики, економіки, об'єктів критичної інфраструктури, екології, охорони здоров'я, соціальної сфери, формування суспільної свідомості, науково-технологічного напряму тощо [6]. Центр протидії дезінформації, діючи в структурі Ради національної безпеки і оборони України, ефективно стримує поширення дезінформації та інформаційного тероризму, сприяючи стабільності та безпеці держави. Особлива увага приділяється протидії іноземним інформаційним впливам, особливо в умовах поточного воєнного конфлікту, що дає змогу Україні захищати свої національні інтереси, зміцнювати державний суверенітет і підтримувати суспільну довіру. Загалом Рада національної безпеки і оборони України створює прийнятні умови для реалізації Президентом України його конституційних повноважень пов'язаних із забезпеченням інформаційної безпеки, виявляє інформаційні загрози та розробляє відповідні програми протидії, визначає стратегію інформаційної безпеки.

Верховна Рада України та Кабінет Міністрів України як суб'єкти системи визначають пріоритети в захисті життєво важливих інтересів об'єктів інформаційної безпеки, розробляють загальні засади правового регулювання відносин в інформаційній сфері, встановлюють порядок організації та діяльності органів забезпечення інформаційної безпеки. Так, Верховна Рада України в межах повноважень, визначених Конституцією України, формує державну політику і законодавчу базу в інформаційній сфері та здійснює контроль за практикою застосування законодавчих актів у діяльності суб'єктів забезпечення інформаційної безпеки та їх посадових осіб; здійснює парламентський контроль та приймає закони України, які визначають і регулюють діяльність органів сектору інформаційної безпеки та їхні повноваження, а також затверджує відповідні бюджетні асигнування та приймає рішення щодо звіту про їх використання; створює комітети, до повноважень яких належить, зокрема, забезпечення контрольних функцій Верховної Ради України за діяльністю органів сектору інформаційної безпеки; для вивчення, підготовки і попереднього розгляду окремих питань у сфері інформаційної безпеки створює тимчасові спеціальні комісії, а для проведення розслідування з питань, що становлять суспільний інтерес, – тимчасові слідчі комісії; проводить парламентські слухання з питань інформаційної безпеки, що становлять суспільний інтерес і потребують законодавчого врегулювання. Кабінет Міністрів України забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет, фінансування програм, пов'язаних з інформаційною безпекою, розробляє та затверджує план за-

ходів з реалізації Стратегії інформаційної безпеки, на основі якого відповідні органи виконавчої влади реалізують заходи щодо забезпечення інформаційної безпеки [2], звітує з цих питань перед Президентом України і Верховною Радою України. Кабінет Міністрів України здійснює керівництво підвідомчими йому органами виконавчої влади, що входять до системи забезпечення інформаційної безпеки, організовує розроблення та реалізацію заходів щодо забезпечення інформаційної безпеки зазначеними органами.

Верховна Рада України та Кабінет Міністрів України виконують найважливіші функції в системі забезпечення інформаційної безпеки країни. Правове регулювання, управління та контроль з боку цих органів дають змогу формувати ефективну та адаптивну політику в секторі інформаційної безпеки, що є ключовим для підтримання національної безпеки України загалом. Комплексний контроль за діяльністю суб'єктів адміністративно-правового забезпечення інформаційної безпеки зміцнює довіру суспільства та підвищують захищеність інформаційного простору країни, що створює надійне підґрунтя для її існування в існуючих сьогодні умовах геополітичного виклику.

Міністерство культури та інформаційної політики України (МКІП), основним задаванням якого є забезпечення формування та реалізація державної політики у сферах інформаційного суверенітету (у частині повноважень з управління цілісними майновими комплексами державного підприємства «Мультимедійна платформа іномовлення України» та Українського національного інформаційного агентства «Укрінформ»), інформаційної безпеки України [7]. В сфері інформаційної безпеки МКІП реалізує наступні заходи: розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи; розробляє плани заходів щодо сприяння незалежності засобів масової інформації, захисту прав журналістів та споживачів інформаційної продукції; організовує проведення досліджень впливу результатів діяльності засобів масової інформації на суспільну свідомість; сприяє дотриманню в Україні свободи слова; розробляє та вносить на розгляд Кабінету Міністрів України програмні документи у сфері захисту інформаційного простору України від зовнішнього інформаційного впливу; забезпечує моніторинг інформації у вітчизняних та іноземних засобах масової інформації; забезпечує організацію та проведення мистецьких конкурсів з метою реалізації культурно-мистецьких проектів, спрямованих на здійснення заходів у сфері захисту національного інформаційного простору; вживає заходів до захисту прав громадян на вільний збір, зберігання, використання і поширення інформації, зокрема на тимчасово окупованих територіях, відповідно до покладених на МКІП завдань; вживає разом з іншими органами державної влади заходів до захисту неповнолітніх від негативного впливу інформаційної продукції, зокрема аудіо- і відеопродукції, яка становить загрозу суспільній моралі або може зашкодити фізичному, психічному чи моральному розвитку неповнолітніх; надає методичну та практичну допомогу засобам масової інформації у сфері інформаційного суверенітету України (у частині повноважень з управління цілісним майновим комплексом Українського національного інформаційного агентства «Укрінформ») та інформаційної безпеки [8]. Отже, Міністерство культури та інформаційної політики України відіграє критичну роль у захисті та розвитку інформаційного суверенітету країни. Через свої різноманітні ініціативи та програми, МКІП зміцнює інформаційну безпеку, підтримує незалежність ЗМІ, захищає права журналістів і споживачів інформаційної продукції, та сприяє дотриманню свободи слова. Заходи, що вживаються Міністерством, спрямовані на формування в межах країни стійкого національного інформаційного простору.

Міністерство з питань реінтеграції тимчасово окупованих територій України, що забезпечує формування та реалізує державну політику з питань тимчасово окупованої Російською Федерацією території України, а також прилеглих до неї територій, дотримання норм міжнародного гуманітарного права на всій території України, інформаційного суверенітету України у сфері захисту прав примусово переміщених (депортованих) осіб, зокрема захисту прав осіб, депортованих за національною ознакою [9]. Міністерство виконує безліч функцій, спрямованих на підтримку і захист прав людини. Основний акцент робиться на інформаційній підтримці населення, яке проживає на окупованих територіях і прилеглих до них районах, що охоплює збір та аналіз інформації щодо дотримання міжнародного гуманітарного права, а також щодо порушень прав людини, включно з фактами незаконного позбавлення волі. В умовах триваючого військового конфлікту та інформаційної війни, роль Міністерства стає стратегічно значущою. Воно займається узагальненням даних щодо порушень міжнародного гуманітарного права і прав людини, систематиза-

цією фактів незаконних дій збройних формувань та окупаційних адміністрацій. Ця інформація використовується для формування обґрунтованих звернень і звітів до міжнародних органів та інституцій, що сприяє формуванню міжнародного тиску на агресора та захисту прав українських громадян. До того ж Міністерство веде активну інформаційну кампанію, спрямовану на зменшення соціального, економічного та екологічного впливу вибухонебезпечних предметів та протимінної діяльності, що також сприяє захисту та інформуванню населення на окупованих та прилеглих територіях. У сукупності, ці дії Міністерства сприяють зміцненню інформаційного суверенітету України та формуванню сталого державного інформаційного поля, що має стратегічне значення для національної безпеки та захисту державних інтересів в умовах воєнного конфлікту.

Державна служба спеціального зв'язку та захисту інформації України, яка є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону [10]. Служба відіграє ключову роль в адміністративно-правовому забезпеченні інформаційної безпеки, забезпечуючи захист від зовнішніх і внутрішніх інформаційних загроз. Як інтегральна частина сектору безпеки і оборони України, Служба сприяє зміцненню стабільності та безпеки держави шляхом захисту інформаційних ресурсів, забезпечення безпеки зв'язку та контролю за обігом секретної інформації. Її діяльність спрямована на запобігання кіберзагрозам, шпигунству та іншим формам інформаційного впливу, що робить її незамінним елементом у забезпеченні національної безпеки України загалом.

Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку. Національна комісія здійснює: державне регулювання, а також державний нагляд (контроль) щодо виявлення та запобігання порушенням вимог законодавства суб'єктами господарювання та забезпечення інтересів суспільства у сферах: електронних комунікацій; радіочастотного спектра; надання послуг поштового зв'язку; заходи щодо сприяння адаптації (гармонізації) законодавства України у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку до законодавства Європейського Союзу [11]. Національна комісія відіграє суттєву роль у забезпеченні відповідності та дотримання законодавства в ключових галузях інформаційної безпеки: комунікації та зв'язку. Здійснюючи державне регулювання та нагляд, комісія не лише запобігає порушенням, а й активно працює над інтеграцією українського законодавства з нормами ЄС.

Національна рада України з питань телебачення і радіомовлення, що здійснює державне регулювання, нагляд і контроль у сфері медіа. Національна рада відіграє ключову роль у сфері медіа. Вона відповідає за розвиток суспільного мовлення, що важливо для зміцнення демократичних інститутів і забезпечення доступу громадян до об'єктивної та неупередженої інформації. Ініціатива щодо переходу на цифрове ефірне телебачення також заслуговує на увагу, оскільки це покращує контроль над інформацією, що, безсумнівно, сприяє забезпеченню інформаційної безпеки. У цьому напрямі Національна рада ставить на чільне місце посилення національних пріоритетів у медіапросторі, що сприяє збереженню культурної спадщини та підтримці національної ідентичності української нації. Регулярний аналіз та огляд дезінформації, здійснюваний Національною радою, є важливими елементами боротьби з пропагандою та захистом громадської думки від впливу шкідливих інформаційних атак. Зазначені дії у своїй сукупності сприяють створенню більш здорового інформаційного середовища в країні.

Збройні Сили України – військове формування, на яке покладаються оборона України, захист її суверенітету, територіальної цілісності і недоторканності [12]. Інформаційну безпеку у сфері оборони держави забезпечує належним чином урегульована та дієва інформаційна діяльність Збройних Сил України, яка спрямована на: створення нормальних умов функціонування з'єднань, військових частин і підрозділів, чим підкреслюється подвійний взаємозв'язок і залежність між діяльністю Збройних Сил України та інформаційною безпекою; недопущення витоку державної таємниці, розповсюдження службової інформації, персональних даних, а також неправдивої інформації у сфері оборони країни; недопущення деструктивного інформаційного впливу на особовий склад підрозділів і населення України у сфері функціонування Збройних Сил України; недопущення кібератак на інформаційні системи відомчого та міжвідомчого характеру [13, с. 240]. Загалом інформаційна безпека, що здійснюється Збройними Силами України, цілеспрямовано

фокусується на запобіганні як поточним, так і потенційним загрозам, що спрямовані проти Збройних Сил. Ефективність цих заходів залежить від ретельного і стратегічного планування інформаційних операцій, які призначені для запобігання реалізації загроз у реальні дії, а також від суворого дотримання встановленого законодавства в процесі виконання різних аспектів інформаційної діяльності Збройними Силами України. Усе це передбачає використання комплексного підходу до управління інформаційною безпекою, який має охоплювати як оперативні, так і превентивні заходи для захисту критично важливої інформації та підтримання загальної готовності Збройних Сил України до відсічі зовнішніх і внутрішніх загроз. Ефективне управління інформаційною безпекою допомагає запобігти можливим загрозам та забезпечує стабільне функціонування Збройних Сил України, що є ключовим для забезпечення виживання країни.

Служба безпеки України, яка є органом спеціального призначення, що забезпечує державну безпеку України. Служба здійснює державне управління в галузі забезпечення безпеки, і окремо перед нею поставлено таке завдання, як забезпечення інформаційної безпеки України. Служба безпеки України у межах компетенції здійснює: моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері; протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [2]. В структурі Служба безпеки України функціонує Департамент кібербезпеки СБУ, який займається комплексним контррозвідувальним захистом інформаційної та кібернетичної безпеки держави. Пріоритетними завданнями на цьому напрямі діяльності Служби є: боротьба з кібертероризмом і кібершпигунством; розслідування кіберінцидентів і кібератак на державні електронні інформаційні ресурси; протидія проведенню ворожих спеціальних інформаційних операцій [14]. До того ж Служба безпеки України здійснює організацію забезпечення криптографічної та інженерно-технічної безпеки інформаційно-телекомунікаційних систем, а також систем шифрованого, засекреченого та інших видів спеціального зв'язку.

Національній поліції України, яка служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку у сучасних умовах прогресивного інформаційно-комунікаційного розвитку притаманні наступні напрями адміністративно-правового забезпечення інформаційної безпеки: організація протидії не бажаному для інтересів суспільства й держави впливу за допомогою технічних засобів захисту, причому засоби захисту мають бути адекватними засобам впливу, що означає необхідність застосування належних за кількістю та якістю технічних засобів захисту інформаційних систем (наприклад, створення системи просторового зашумлення для приховування інформації в обмеженому середовищі чи екранування технічних засобів у приміщенні); організація протидії негативному впливу на учасників інформаційних відносин, зокрема протидія кіберзлочинам як таким, що несуть безпосередню суспільну небезпеку; визначення майнових і моральних утрат та їхня мінімізація в разі порушення функціонування інформаційної системи, важливої для належного забезпечення інтересів суспільства та держави, включаючи взаємодію з іншими правоохоронними та судовими органами як України, так і зарубіжних держав для притягнення до відповідальності й відшкодування заподіяних протиправними діями (бездіяльністю) збитків [15, с. 187]. Що стосується повноважень поліції щодо забезпечення інформаційної безпеки держави, то до них насамперед слід віднести: здійснення превентивної та профілактичної діяльності, спрямованої на запобігання вчиненню правопорушень у сфері інформації; виявлення причин та умов, які сприяють вчиненню кримінальних та адміністративних правопорушень у сфері інформації, вжиття в межах своєї компетенції заходів для їх усунення; вжиття заходів з метою виявлення кримінальних, адміністративних правопорушень у сфері інформаційної безпеки; вжиття заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, які виникли внаслідок вчинення кримінального, адміністративного правопорушення у сфері інформаційної безпеки; здійснення досудового розслідування кримінальних правопорушень у сфері інформації та інформаційної безпеки в межах визначеної підслідності; розшук осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, які вчинили зазначені вище правопорушення; у випадках, визначених законом, здійснення проваджень у справах про адміністративні правопорушення у сфері інформації, прийняття рішень про застосування адміністративних стягнень, забезпечення їх виконання [16, с. 170-171] та ін.

Не можна не погодитися з тим, що основний тягар реалізації державної політики в галузі інформаційної безпеки лягає на органи виконавчої влади, які здійснюють на основі законодавства адміністративно-державне управління. Важливою особливістю участі державних органів, зокрема й органів виконавчої влади, у реалізації заходів із забезпечення інформаційної безпеки є те, що кожен із цих органів здійснює свою діяльність на базі використання складових інформаційної інфраструктури суспільства, виробляє і споживає певні інформаційні ресурси, вступає у відносини з громадянами і, як представник власника державних інформаційних ресурсів і частини компонентів інформаційної інфраструктури, повинен вживати заходів щодо забезпечення їхньої безпеки [17, с. 270]. Загалом у своїй сукупності органи виконавчої влади: забезпечують виконання законодавства України, указів Президента України та постанов Кабінету Міністрів України в галузі адміністративно-правового забезпечення інформаційної безпеки; у межах своєї компетенції вносять пропозиції щодо вдосконалення системи забезпечення інформаційної безпеки та розробляють правові акти у зазначеній сфері, подають їх у встановленому порядку на розгляд Президенту України, Кабінету Міністрів України та ін. вищим за рівнем органам; взаємодіють між собою з питань виконання законодавства у зазначеній сфері.

Щодо міжвідомчих і державних комісій, які створюються Президентом України та Кабінетом Міністрів України, то вони відповідно до наданих їм повноважень розв'язують локальні завдання в рамках адміністративно-правового забезпечення інформаційної безпеки. Предмети їхнього відання, як і предмети відання органів виконавчої влади, визначаються положеннями про них, а владні повноваження, як правило, обмежуються ухваленням рішень, що мають рекомендаційний характер.

Судовим органам у системі суб'єктів адміністративно-правового забезпечення інформаційної безпеки також належить не остання роль. Вони здійснюють правосуддя у справах, пов'язаних із посяганнями на законні інтереси людини і громадянина, суспільства і держави в інформаційній сфері, та забезпечують судовий захист фізичних і юридичних осіб, чиї права було порушено у зв'язку з діяльністю із забезпечення інформаційної безпеки України. Предметом відання органів судової влади є соціальні конфлікти, пов'язані з дійсним або передбачуваним порушенням правових норм, що регулюють суспільні відносини в інформаційній сфері. Їхні владні повноваження полягають у можливості ухвалення рішень у справах, обов'язкових для виконання всіма учасниками конфлікту. Судові органи, виконуючи свої функції, не тільки застосовують чинне законодавство, а й формують правозастосовчу практику, важливу для розвитку всієї системи інформаційної безпеки. Судові рішення в цих справах допомагають в інтерпретації правових норм, забезпечуючи тим самим передбачуваність і стабільність правозастосування, що критично важливо для захисту законних інтересів людини і громадянина, суспільства і держави. Ба більше, судові органи сприяють зміцненню законності та правопорядку в інформаційній сфері, що є суттєвим елементом загальнодержавної стратегії у сфері інформаційної безпеки. Виконуючи превентивну функцію, суди сприяють недопущенню нових порушень у цій царині, що зі свого боку підвищує довіру суспільства до механізмів захисту прав і свобод людини в умовах цифровізації.

Продовжуючи наше дослідження, акцентуємо увагу на тому, що розв'язання проблем інформаційної безпеки не може бути успішним, якщо в її адміністративно-правовому забезпеченні не братимуть участі різноманітні недержавні, громадські та ін. організації, а також громадяни, основна роль яких полягає у сприянні державним органам у частині виконання ними функцій та завдань у сфері інформаційної безпеки.

Значний вплив недержавних суб'єктів на процеси формування та збереження інформаційної безпеки як складової національної безпеки пояснюється вимогами сучасних міжнародних подій та результатами практичної діяльності недержавних суб'єктів, їх високої активності в політичному та соціальному житті країни, високого професійного та наукового потенціалу активістів, глибоких знань соціальних, політичних, економічних проблем сучасної України, досвіду міжнародного спілкування, знайомства зі шляхами вирішення проблем у демократичних країнах світу. Розглядаючи діяльність недержавних суб'єктів по адміністративно-правовому забезпеченню інформаційної безпеки, необхідно зазначити, що на них обов'язки з безпосереднього забезпечення безпеки не покладаються; вони покликані виконувати інші функції. Недержавні суб'єкти: беруть участь у роботі консультативно-дорадчих органів при органах державного управління у сфері контролю та регулювання інформаційних ресурсів країни; беруть участь у публічних громадських обговореннях, що проводяться державними суб'єктами адміністративно-правового забезпечення

інформаційної безпеки; займаються підготовкою інформаційних запитів та скарг про інформаційні правопорушення у процесі громадського контролю за дотриманням законності впроваджених заходів у сфері забезпечення інформаційної безпеки держави; вивчають громадську думку та доводять основні кризові явища у суспільстві до державних суб'єктів адміністративно-правового забезпечення інформаційної безпеки [18, с. 297]. Отже, недержавні суб'єкти беруть активну участь і надають дієву підтримку державним суб'єктам адміністративно-правового забезпечення інформаційної безпеки в реалізації їхніх завдань та функції.

Характерною особливістю всіх недержавних суб'єктів адміністративно-правового забезпечення інформаційної безпеки є те, що їхнє коло і статус залишається невизначеним. Вбачається, що ситуація, яка склалася, є суттєвим упущенням, оскільки вона не сприяє консолідації суспільства в запобіганні головних загроз інформаційній безпеці держави. Вважаємо, що дана прогалина в законодавстві потребує негайного усунення, шляхом включення всіх недержавних суб'єктів до механізму реалізації мети та завдань Стратегії інформаційної безпеки, а не лише наукових та науково-дослідних установ, які повинні забезпечувати науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики [2]. Іншою характерною особливістю статусу недержавних суб'єктів є те, що більшість нормативно-правових актів, які визначають порядок діяльності комерційних компаній, освітніх установ, дослідницьких інститутів, науково-аналітичних центрів тощо, є тимчасовими, а також значно застарілими, такими, що не відповідають вимогам часу. Обидві ці обставини перешкоджають їх становленню як повноцінних суб'єктів адміністративно-правового забезпечення інформаційної безпеки. Вбачається, що необхідно якомога ширше використовувати можливості недержавних суб'єктів у розглянутій сфері, а тому активізувати залучення громадян, громадських об'єднань, організацій тощо до вирішення проблеми забезпечення інформаційної безпеки.

Проведений аналіз підтверджує чільну роль державних органів влади в рамках адміністративно-правового забезпечення інформаційної безпеки. Ці органи виступають основними суб'єктами, що мають двоїсте становище в адміністративних правовідносинах. По-перше, державні органи несуть адміністративну відповідальність за свої дії у сфері інформаційної безпеки. По-друге, вони наділені повноваженнями для здійснення правозастосовчої діяльності, включно з притягненням до адміністративної відповідальності інших суб'єктів за порушення законодавства у сфері інформаційної безпеки. Таке становище передбачає використання різних заходів впливу на порушників у зазначеній сфері, які не просто є реактивними, а такими, що створюють систему обмежень, які можуть стосуватися різних аспектів їхнього життя. Важливість такого підходу полягає у формуванні умов, за яких порушення інформаційної безпеки фізичними та юридичними особами сприйматиметься як діяння, пов'язане з реальними, відчутними негативними наслідками. Варто зазначити, що ефективність заходів впливу, а внаслідок чого й ефективність усієї системи адміністративно-правового забезпечення інформаційної безпеки, безпосередньо залежить від якості законодавчої бази та механізмів її виконання, що вимагає постійного аналізу й адаптації правових норм відповідно до мінливих умов інформаційного простору. Цьому питанню більш детальну увагу буде приділено в наступних розділах нашого дисертаційного дослідження.

У рамках адміністративно-правової регуляції, державні органи, що володіють повноваженнями у сфері забезпечення інформаційної безпеки, несуть посилену відповідальність за дотримання правових норм. Це позиціонує їх як ключових акторів у забезпеченні законності та порядку в інформаційному просторі, де порушення можуть мати серйозні наслідки для національної безпеки України загалом. Коли державні органи стикаються з ознаками адміністративних правопорушень, вони зобов'язані діяти в суворій відповідності до закону. Порядок дій охоплює не тільки ідентифікацію та документування самого факту правопорушення та його обставин, а й установлення осіб, відповідальних за його скоєння. Держава вимагає від органів влади застосування всіх необхідних заходів для покарання винних, накладення на винних різноманітних адміністративні стягнень, передбачених Кодексом України про адміністративні правопорушення. Зазначений обов'язок вимагає від державних органів високого ступеня професіоналізму і точності в застосуванні правових актів, оскільки будь-які помилки можуть призвести до негативних наслідків, включаючи неправомірне обмеження прав і свобод людини і громадянина. Також не варто забувати про випадки зловживання владою у сфері інформаційної безпеки. У зв'язку з цим, державні органи перебувають під суворим перехресним контролем під час виконання ними своїх завдань та функцій, і адміністративна відповідальність тут виступає як механізм забезпечення сумлінності дій

посадових осіб органів державної влади. У профільній літературі неодноразово наголошувалося на тому, що така система не тільки сприяє підтримці порядку в інформаційній сфері, а й стимулює державні структури до постійного вдосконалення своїх процедур і практик, що в підсумку сприяє зміцненню адміністративно-правового забезпечення інформаційної безпеки в Україні.

Висновки. На підставі вищевикладеного можна дійти висновку, що система суб'єктів адміністративно-правового забезпечення інформаційної безпеки містить у собі широке коло структур як державної, так і недержавної приналежності, що неминуче породжує приватні, відомчі інтереси, взаємне суперництво. Їхня діяльність має чітко вписуватися в річище єдиної, цілеспрямованої державної інформаційної політики, що являє собою сукупність цілей, які відображають національні інтереси України в інформаційній сфері, і тому вона потребує ефективної координації на всіх наявних рівнях. На нашу думку, загальне регулювання діяльності різних суб'єктів забезпечення інформаційної безпеки в умовах воєнного стану повинен узяти на себе орган, що має значний вплив і авторитет. Незважаючи на те, що центральним органом виконавчої влади зі спеціальним статусом у сфері інформаційної безпеки є Національна комісія, що здійснює державне регулювання з питань інформаційної безпеки, вважаємо, що в умовах сьогодення, в цьому питанні, вона має передати всі свої повноваження Раді національної безпеки і оборони України, яка вже займається координацією та здійсненням контролю за діяльністю органів виконавчої влади у сфері інформаційної безпеки в умовах воєнного стану. У структурі Ради слід створити Міжвідомчу комісію із забезпечення інформаційної безпеки. І саме така Комісія, наділена відповідними повноваженнями, через Раду національної безпеки і оборони України підпорядкована безпосередньо Президенту України, має виконувати багатопланову роль розробника політики у сфері забезпечення інформаційної безпеки та координатора її здійснення в непростих умовах, в яких існує країна.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради (ВВР)*, 2018. № 31. Ст. 241.
2. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/ show/685/2021#n5 (дата звернення: 11.06.2024).
3. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР. *Відомості Верховної Ради України (ВВР)*, 1998. № 35. Ст. 237.
4. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021 р. № 106. URL: https://zakon.rada.gov.ua/ laws/show/n0015525-21#Text (дата звернення: 11.06.2024).
5. Положення про Центр протидії дезінформації, затверджено Указом Президента України від 07.05.2021 р. № 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text (дата звернення: 11.06.2024).
6. Про Центр. URL: https://cpd.gov.ua/documents/про-центр/ (дата звернення: 08.06.2024).
7. Положення про Міністерство культури та інформаційної політики України, затверджено Постановою Кабінету Міністрів України від 16.10.2019 р. № 885. URL: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text (дата звернення: 11.06.2024).
8. Інформаційна політика та безпека. Основні напрямки діяльності. URL: https://mcip.gov.ua/informatsiyna-polityka-ta-bezpeka/osnovni-napriamky-diialnosti/ (дата звернення: 08.06.2024).
9. Положення про Міністерство з питань реінтеграції тимчасово окупованих територій України, затверджено Постановою Кабінету Міністрів України від 08.06.2016 р. № 376 (в редакції постанови Кабінету Міністрів України від 06.05.2020 р. № 371). URL: https://zakon.rada.gov.ua/laws/show/376-2016-%D0%BF#Text (дата звернення: 11.06.2024).
10. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. *Відомості Верховної Ради України (ВВР)*, 2006. № 30. Ст. 258.
11. Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку: Закон України від 16.12.2021 р. № 1971-IX. URL: https://zakon.rada.gov.ua/laws/show/1971-20#Text (дата звернення: 11.06.2024).

12. Про Збройні Сили України: Закон України: Закон України від 06.12.1991 р. № 1934-XII. *Відомості Верховної Ради України (ВВР)*, 1992. № 9. Ст. 108.
13. Тична Б.М. Інформаційна безпека як основа інформаційної діяльності Збройних Сил України. *Право і суспільство*, 2020. № 2. Частина 2. С. 236–241.
14. Захист інформаційного та кіберпростору. URL: https://ssu.gov.ua/ zabezpechennia-informatsiinoi-bezpeky (дата звернення: 09.06.2024)
15. Пересада О.М. Роль Національної поліції України в забезпеченні інформаційної безпеки держави: теоретико-методологічні аспекти. *Правовий часопис Донбасу*, 2019. № 4 (69). С. 183–189.
16. Негодченко В.О Інформаційна безпека в органах Національної поліції України: адміністративно-правове забезпечення. *Право і суспільство*, 2020. № 6. С. 167–174.
17. Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной Безопасности России: дис. ... д-ра юрид. наук: 05.13.19. М., 2004. 371 с.
18. Сіпайло Л.Г., Сіпайло Н.А. Діяльність неурядових організацій у системі забезпечення інформаційної безпеки країни. *Глобальні та національні проблеми економіки*, 2017. Випуск 18. С. 296–299.
19. Стрілецька О.В., Габрелян А.Ю. Реалізація принципу змагальності в ході проведення досудового розслідування. *Науковий вісник УжНУ. Серія «Право»*, 2024. Випуск 81(1). С. 168–179.
20. Стрілецька О.В., Габрелян А.Ю. Реалізація принципу змагальності під час судового розгляду. *Аналітично-порівняльне правознавство*, 2024. Випуск 2. С. 719–731.
21. Стрілецька О.В., Габрелян А.Ю. Організаційні проблеми реалізації принципу змагальності у кримінальному процесі. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*, 2024. № 1. С. 328–340.
22. Стрілецька О.В., Габрелян А.Ю. Реалізація принципу змагальності в кримінальному процесі країн романо-германської правової сім'ї. *VI Міжнародна науково-теоретична конференція «Традиційні та інноваційні підходи до наукових досліджень» (08.03.2024; м. Вінниця, Україна)*, 2024. С. 64–70.
23. Чепель О.В., Габрелян А.Ю. Показання свідка в кримінальному процесі: поняття, зміст, вимоги. *Аналітично-порівняльне правознавство*, 2023. № 4. С. 451 – 458.
24. Чепель О.В., Габрелян А.Ю. Система прав свідка в кримінальному процесі: стан, проблеми та шляхи їх подолання. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*, 2023. № 4. С. 168–180.
25. Чепель О.В., Габрелян А.Ю. Адвокат свідка: проблематика правового статусу. *Science of XXI century: development, main theories and achievements: collection of scientific papers «SCIENTIA» with Proceedings of the V International Scientific and Theoretical Conference (January 26, 2024)*. Helsinki, Republic of Finland: International Center of Scientific Research, 2024. С. 131–136.