DOI https://doi.org/10.51647/kelm.2023.7.24

SPECYFIKA STATUSU PRAWNEGO PODMIOTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI

Ivan Nedokhliebov
laureat katedry Prawa Konstytucyjnego i Administracyjnego
Zaporoski Uniwersytet Narodowy (Zaporoże, Ukraina)
ORCID ID: 0009-0006-9450-2379
nedokhliebov_i@ukr.net

Adnotacja. W artykule dokonano kompleksowej analizy prawnej systemu podmiotów zapewniających bezpieczeństwo informacji na Ukrainie. Proponuje się podzielenie wszystkich podmiotów bezpieczeństwa informacji, w zależności od ich statusu prawnego, na trzy grupy: podmioty strategiczne (określają koncepcyjne zagadnienia zapewnienia bezpieczeństwa informacji); jednostki administracyjne (bezpośrednio odpowiedzialne za realizację strategii bezpieczeństwa informacji państwa); podmioty kontrolujące (zapewniają zgodność z przepisami dotyczącymi bezpieczeństwa informacji). Udowodniono, że różnorodność poszczególnych rodzajów działalności informacyjnej wyklucza praktyczną możliwość łączenia wszystkich uprawnień w ramach konkretnej władzy odpowiedzialnej za bezpieczeństwo informacyjne państwa. Autor zauważa, że obiecującym kierunkiem we współczesnych warunkach jest koordynacja interakcji państwowych i niepaństwowych podmiotów bezpieczeństwa informacji w ramach jednego mechanizmu zarządzania informacją. Zakłada się, że mechanizm ten przewiduje przyznanie społeczeństwu maksymalnej liczby praw i włączenie go do współpracy na wszystkich poziomach bezpieczeństwa informacji (państwo, społeczeństwo, jednostka).

Słowa kluczowe: działalność wykonawcza i administracyjna, instytucje rządowe, społeczeństwo obywatelskie, bezpieczeństwo informacji, kompetencje i władza, stan prawny, system podmiotów.

PECULIARITIES OF THE LEGAL STATUS OF INFORMATION SECURITY SUBJECTS

Ivan Nedokhliebov
Postgraduate Student at the Department ofConstitutional and Administrative Law
Zaporizhzhia National University (Zaporizhzhia, Ukraine)
ORCID ID: 0009-0006-9450-2379
nedokhliebov_i@ukr.net

Abstract. In the article, a comprehensive legal analysis of the system of entities providing information security in Ukraine is carried out. It is proposed to divide all subjects of information security, depending on their legal status, into three groups: strategic subjects (determine conceptual issues of ensuring information security); administrative entities (directly responsible for the implementation of state information security strategies); controlling entities (ensure compliance with information security legislation). It has been proven that the diversity of individual types of information activity excludes the practical possibility of combining all powers within the framework of a specific authority responsible for the information security of the state. The author notes that a promising direction in modern conditions is the coordination of the interaction of state and non-state subjects of information security within the framework of a single mechanism of information governance. It is assumed that this mechanism provides for granting the public the maximum amount of rights and involving it in cooperation at all levels of information security (state, society, individual).

Key words: executive and administrative activity, government institutions, civil society, information security, competence and authority, legal status, system of subjects.

ОСОБЛИВОСТІ ПРАВОВОГО СТАТУСУ СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Іван Недохлєбов
здобувач кафедри конституційного та адміністративного права
Запорізького національного університету (Запоріжжя, Україна)
ORCID ID: 0009-0006-9450-2379
nedokhliebov_i@ukr.net

Анотація. У статті здійснено комплексний правовий аналіз системи суб'єктів забезпечення інформаційної безпеки в Україні. Запропоновано розділити усіх суб'єктів інформаційної безпеки в залежності від їхнього правового статусу на три групи: стратегічні суб'єкти (визначають концептуальні питання забезпечення інформаційної безпеки); розпорядчі суб'єкти (безпосередньо відповідають за реалізацію державних стратегій інформаційної безпеки); контролюючі суб'єкти (забезпечують додержання законодавства у сфері інформаційної безпеки). Доведено, що різноплановість окремих видів інформаційної діяльності виключає практичну можливість об'єднати усі повноваження в рамках конкретного органу влади, який би відповідав за інформаційну безпеку

держави. Автор зазначає, що перспективним напрямом в сучасних умовах є координація взаємодії державних та недержавних суб'єктів інформаційної безпеки в рамках єдиного механізму інформаційного врядування. Зроблене припущення, що цей механізм передбачає наділення громадськості максимальним обсягом прав та залучення її до співпраці на усіх рівнях інформаційної безпеки (держава, суспільство, особистість).

Ключові слова: виконавчо-розпорядча діяльність, владні інституції, громадянське суспільство, інформаційна безпека, компетенція та повноваження, правовий статус, система суб'єктів.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В умовах нових загроз та викликів, пов'язаних з інформаційною війною держави-агресора проти України, першочерговим завданням є перегляд системи суб'єктів забезпечення інформаційної безпеки. На даному етапі вона не розглядається як єдине ціле, що негативно позначається на ефективності заходів захисту інтересів держави, суспільства та особистості в інформаційній сфері. Тому, обрана тема наукового пошуку є достатньо актуальною та дозволяє удосконалити теоретичні уявлення про систему суб'єктів забезпечення інформаційної безпеки.

Аналіз останніх досліджень і публікацій з даної теми, виділення невирішених раніше частин загальної проблеми, яким присвячується дана стаття. Правовий статус окремих суб'єктів забезпечення інформаційної безпеки України в різні часи досліджували: А. А. Головка, З. А. Добош, В. В. Дулгер, М. В. Ковалів, О. Є. Каглинський, І. І. Килимник, Б. В. Паш, Т. Ю. Ткачук, З. Д. Чуйко, Н. П. Христинченко, О. І. Яременко та інші вчені. Однак, з урахуванням появи нових загроз та викликів, а також необхідності залучити громадянське суспільство до забезпечення інформаційної безпеки, їхні наукові праці частково втратили актуальність.

Формування цілей статті. Метою статті є комплексний правовий аналіз системи суб'єктів забезпечення інформаційної безпеки в Україні.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Для визначення переліку суб'єктів забезпечення інформаційної безпеки, слід звернутися до норм законодавства у сфері національної безпеки. Відповідно до норм Закону України від 21 червня 2018 року № 2469-VIII «Про національну безпеку», сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки (Закон № 2469-VIII, 2018). На нашу думку, наведене визначення адаптоване до умов збройного конфлікту, однак воно не зовсім прийнятне для інформаційної безпеки, в забезпеченні якої приймають участь різні за статусом інституції.

У наукових колах питання системи суб'єктів інформаційної безпеки є достатньо обговорюваним, про що свідчать численні наукові праці вчених-правників. Зокрема, Т. Ю. Ткачук зазначає, що усіх суб'єктів забезпечення інформаційної безпеки можна поділити на три підсистеми: 1) підсистема інформаційного захисту (захист суспільної моралі та інформаційно-психологічний захист; 2) підсистема інформаційної розвідки (виявлення та попередження загроз національним інтересам); підсистема інформаційного впливу (реалізація державної інформаційної політики). Науковець наголошує, що ці три підсистеми включають в себе кібернетичний аспект забезпечення інформаційної безпеки (Ткачук, 2017: 54). Вважаємо, що подібний розподіл є не зовсім коректним, оскільки він здійснений без урахування багаторівневості інформаційної безпеки.

Б. В. Паш вважає, що суб'єктами інформаційної безпеки є: 1) громадяни України та громадські об'єднання; 2) Президент України, Верховна Рада України, Кабінет Міністрів України та інші органи виконавчої влади; 3) ЗМІ та суб'єкти господарювання; 4) наукові установи, освітні і навчальні заклади України, які здійснюють дослідження та підготовку фахівців в галузі інформаційної безпеки (Паш, 2017: 511). Слід лише частково погодитися з таким переліком, адже ЗМІ, суб'єкти господарювання та наукові установи не можуть вважатися самостійними суб'єктами інформаційної безпеки, оскільки вони представляють рівень інформаційної безпеки суспільства. На нашу думку, подібний розподіл здійснено науковцем з урахуванням тих загроз, які можуть походити від кожного суб'єкта.

Вбачається доцільним розподілити усіх суб'єктів інформаційної безпеки в залежності від їхнього правового статусу на наступні групи: 1) стратегічні суб'єкти (вони визначають концептуальні питання забезпечення інформаційної безпеки, тобто ідеологічні засади політики держави у сфері інформаційної безпеки, окреслюючи при цьому інтереси держави та систематизуючи наявні і потенційні загрози); 2) розпорядчі суб'єкти (частково приймають участь у формуванні та безпосередньо відповідають за реалізацію державних стратегій інформаційної безпеки); 3) контролюючі суб'єкти (забезпечують додержання законодавства у сфері інформаційної безпеки та сприяють усуненню протиправних дій, що загрожують стану захищеності інформаційних інтересів держави, суспільства та особистості). Пропонуємо окремо дослідити кожну групу, звертаючи увагу на особливості правового статусу та форм участі окремих суб'єктів, що належать до групи, в забезпеченні інформаційної безпеки.

1. Стратегічні суб'єкти. До цієї групи суб'єктів забезпечення інформаційної безпеки доцільно віднести Президента України, РНБО та Верховну Раду України. Означені суб'єкти наділені повноваженнями формувати концептуальні засади захисту інтересів держави, суспільства та особистості в інформаційній сфері. Мова йде про: 1) визначення реальних та потенційних проблем функціонування національної інформаційної системи; 2) окреслення пріоритетних цілей та очікуваних результатів політики інформаційної безпеки; 3) регламентацію правових режимів доступу до окремих видів інформації; 4) наділення повноваженнями суб'єктів сектору безпеки та оборони; 5) формування моделі міжнародного співробітництва у сфері захисту

інформації в інформаційно-телекомунікаційних системах. Коротко схарактеризуємо правовий статус окремих суб'єктів цієї групи.

Президент України як глава держави, гарант державного суверенітету, територіальної цілісності України, додержання Конституції, прав та свобод людини і громадянина виконує такі повноваження у сфері інформаційної безпеки: здійснює загальне керівництво з питань забезпечення інформаційної безпеки; визначає напрями й заходи забезпечення реалізації внутрішньої і зовнішньої державної політики інформаційної безпеки; утворює організаційно-функціональну систему суб'єктів забезпечення інформаційної безпеки; санкціонує застосування спеціальних заходів і засобів щодо попередження й нейтралізації широкомасштабних внутрішніх і зовнішніх загроз інформаційній безпеці України (Закон № 254к/96-ВР, 1996).

Важливим суб'єктом цієї групи є РНБО, яка згідно Закону України від 05 березня 1998 року № 183/98-ВР «Про Раду національної безпеки та оборони України», забезпечує визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки і оборони в інформаційній, а також є відповідальною за реалізацію заходів інформаційного характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України (Закон № 183/98-ВР, 1998). Без сумніву цей суб'єкт забезпечує ухвалення стратегічних рішень, які безпосередньо впливають на розвиток національної інформаційної системи, особливо коли мова йде про її розвиток в умовах воєнного стану.

Невід'ємним стратегічним суб'єктом забезпечення інформаційної безпеки Верховна Рада України. З. Д. Чуйко зазначає, що її повноваження у сфері інформаційної безпеки спрямовані на законодавче забезпечення цієї сфери, на реалізацію контролю, виділення через Державний бюджет необхідних коштів для інформаційної безпеки. Одним із пріоритетних напрямів її діяльності є структурне і організаційно-правове вдосконалення механізму забезпечення інформаційної безпеки України, маючи на меті підвищення його ефективності, особливо під час виникнення кризових ситуацій (Чуйко, 2005: 164]. Вбачається, що Український парламент поєднує стратегічні та контрольні повноваження, однак ми відносимо його саме до цієї групи суб'єктів, оскільки законодавча діяльність дозволяє сформувати систему правового регулювання різних видів інформаційної діяльності.

2. Розпорядчі суб'єкти. До цієї групи суб'єктів забезпечення інформаційної безпеки входить Кабінет Міністрів України, органи виконавчої влади, правоохоронні органи, військові адміністрації. На відміну від першої групи, ці суб'єкти наділені виконавчо-розпорядчими повноваженнями та забезпечують реалізацію політики у сфері інформаційної безпеки. Мова йде як про загальнодержавний, так і про регіональний аспекти захисту національних інтересів в інформаційній сфері. Отже, ці суб'єкти шляхом нормотворчості та організаційно-розпорядчої і установчої діяльності забезпечують захист означених інтересів та законність в різних сферах інформаційної діяльності. Як і суб'єкти першої групи, вони здійснюють свої функції на усіх рівнях інформаційної безпеки (держава, суспільство, особистість). Також вказані суб'єкти безпосередньо взаємодіють з громадянами та громадськими об'єднаннями в питаннях забезпечення інформаційної безпеки. Схарактеризуємо статус та форми діяльності окремих суб'єктів цієї групи.

Перш за все, слід звернути увагу на правовий статус Кабінету Міністрів України, який відповідає за реалізацію політики у сфері національної безпеки, а, отже, забезпечує її інформаційну складову. О. І. Яременко вважає, що Кабінет Міністрів України в інформаційній сфері реалізує дві основні групи повноважень – установчі та правотворчі. На виконання установчих повноважень урядом створюються спеціальні інституції, які забезпечує інформаційний суверенітет України та беруть участь у формуванні державної інформаційної політики. Правотворчі повноваження уряду полягають у розробці проектів законодавчих актів у інформаційній сфері, а також виданні власних актів – постанов та розпоряджень, які. спрямовані на розбудову окремих аспектів інформаційного суспільства (Яременко, 2015: 18).

Окремо слід зупинитися на статусі правоохоронних органів України, які належать до системи суб'єктів інформаційної безпеки. Пропонуємо зосередити увагу на Службі безпеки України, яка має значні повноваження у сфері національної безпеки. О. Є. Каглинський наголошує, що Служба безпеки України є одним із суб'єктів забезпечення інформаційної безпеки держави, а її правовий статус являє собою визначене нормами права становище у системі інших правоохоронних органів як суб'єктів захисту національної безпеки держави. До числа завдань цього органу науковець відносить: 1) виявлення та усунення причин та умов, що можуть призвести до проявів інформаційного тероризму; 2) захист людини і громадянина, суспільства та держави від інформаційного тероризму; 3) попередження, своєчасне виявлення та запобігання зовнішнім і внутрішнім загрозам інформаційній безпеці України; 4) мінімізація суспільно небезпечних наслідків дезінформації (Каглинський, 2022: 73). Вбачається, що ключові завдання цього правоохоронного органу зі спеціальним статусом пов'язані із захистом національних інтересів в інформаційній сфері, шляхом проведення контррозвідувальних, антитерористичних та інших заходів з метою виявлення та припинення протиправної діяльності різних за статусом суб'єктів.

На регіональному рівні розпорядчими суб'єктами забезпечення інформаційної безпеки є військові адміністрації, які наділені певними повноваження в інформаційній сфері. В. В. Дулгер вказує, що військові адміністрації є складовою частиною системи органів державної влади, а їхня діяльність полягає у цілеспрямованому впливі на організацію діяльності на певній території в інтересах успішного й ефективного вирішення поставлених перед ними завдань. За своїм правовим статусом ці тимчасові органи є органами розпорядницько-виконавчими. Водночас органи військової адміністрації наділені відповідно до принципу централізації керівництва правами встановлювати нові правила, видавати на основі законодавства та в межах

певних повноважень обов'язкові для виконання підлеглими органами та посадовими особами акти управління як нормативні, так і індивідуальні, які спрямовані на запровадження і здійснення заходів правового режиму воєнного стану (Дулгер, 2018: 37].

Відповідно до норм Закону України 12 травня 2015 року № 389-VIII «Про правовий режим воєнного стану», військові адміністрації наділені наступними повноваженнями, які стосуються питань інформаційної безпеки: 1) запровадження та здійснення заходів правового режиму воєнного стану; 2) сприяння діяльності суду, органів прокуратури, юстиції, служби безпеки, органів Національної поліції, адвокатури і Державної кримінально-виконавчої служби України; 3) скасування актів виконавчих органів відповідної ради, які не відповідають Конституції України та чинному законодавству; 4) забезпечення в умовах воєнного стану реалізації державних гарантій, визначених законами України (Закон № 389-VIII, 2015). В умовах сьогодення, військові адміністрації виступають своєрідними гарантами суспільної безпеки на регіональному рівні.

3. Контролюючі суб'єкти. Наявність цієї групи суб'єктів забезпечення інформаційної безпеки обумовлена об'єктивними потребами контролю у сфері національної безпеки. Зокрема, згідно законодавства, основним принципом її забезпечення є демократичний цивільний контроль за функціонуванням сектору безпеки та оборони. На цьому етапі пропонуємо зосередитися на судовому та громадському контролі в системі інформаційної безпеки, оскільки ці види контролю є доволі перспективними, хоча і не розвинені належним чином в сучасній Україні. З. А. Добош зазначає, що судовий контроль у сфері інформаційної безпеки є особливим видом діяльності судів різних юрисдикцій, що полягає у прямій (безпосередній) та непрямій (опосередкованій) перевірці законності та правомірності прийнятих рішень, дій або бездіяльності як певного суб'єкта владних повноважень, так і органів влади. Наслідком судового контролю може бути відновлення порушеного режиму законності, забезпечення охорони суспільних відносин й поновлення порушених прав, через спеціальні органи виконання судових рішень або у добровільному порядку (Добош, 2021: 151).

Вбачається, що контроль судів в системі інформаційної безпеки відбувається через право на інформацію, захист якого є ключовою функцією судової влади. Слід враховувати, що метою судового контролю є: забезпечення цивільної пріоритетності при розробленні та реалізації державної політики у сфері інформаційної безпеки; контроль додержання вимог законодавства у діяльності суб'єктів сектора безпеки і оборони, запобігання їх використанню для протиправних цілей; сприяння розробленню та реалізації стратегій, доктрин, концепцій і програм у сфері інформаційної безпеки; участь у забезпеченні реформування і розвитку суб'єктів сектора безпеки (Христинченко, Ковалів, 2023: 44).

Останнім часом пріоритетності набуває громадський контроль у сфері забезпечення національної безпеки та її окремих складових. З цього приводу І. І. Килимник зазначає, що однією з найважливіших тенденцій сьогодення в контексті забезпечення інформаційної безпеки, є активне залучення до усіх процесів недержавних суб'єктів, насамперед членів громадянського суспільства. Натомість, залучення громадянського суспільства справляє позитивний вплив за умов наявності ключового стратегічного документа, який спрямовує діяльність усіх суб'єктів забезпечення інформаційної безпеки, визначає ключові напрямки зазначеної діяльності та завдання, поставлені перед суб'єктами (Килимник, 2023: 57). На сьогодні, таким документом є Стратегія інформаційної безпеки, яка, на жаль, не має досконалих механізмів взаємодії влади та громадськості у сфері інформаційної безпеки.

А. А. Головка систематизує три механізми взаємодії держави та громадськості в сфері інформаційної безпеки: 1) інституційний вимір (комунікативні зв'язки між владою і суспільством через систему консультативно-дорадчих органів); 2) нормативно-правовий вимір (залучення громадськості до нормотворчості та прийняття управлінських рішень); 3) практичний вимір (реалізація спільних проектів та ініціатив, активна діяльність в суспільно-політичній практиці) (Головка, 2015: 16). З цього випливає, що громадськість залучена на усіх рівня забезпечення інформаційної безпеки, а її потенціал застосовується для вирішення широкого спектру завдань (ідеологічні, організаційні, правові).

Висновки з дослідження і перспективи подальших розвідок у даному науковому напрямку. Дивлячись на проаналізовану систему суб'єктів інформаційної безпеки, можна зазначити про декілька принципових аспектів. На сьогодні в Україні дійсно відсутній єдиний суб'єкт, який би відповідав за її забезпечення. Однак, чи є об'єктивною необхідність такого суб'єкта? На нашу думку ні, оскільки різноплановість окремих видів інформаційної діяльності виключає практичну можливість об'єднати усі повноваження в рамках конкретного органу влади. Інакше кажучи, набагато ефективнішим вбачається індивідуалізація означених сфер з урахуванням наявних та потенційних загроз. Перспективним напрямом сьогодні є координація взаємодії державних та недержавних суб'єктів інформаційної безпеки в рамках єдиного механізму інформаційного врядування. Кожен з проаналізованих суб'єктів, має свій законодавчий статус та коло повноважень, однак, в умовах «гібридної» інформаційної війни необхідно шукати альтернативні способи захисту інтересів в інформаційній сфері. На нашу думку, таким способом і є механізм інформаційного врядування, в рамках якого влада та громадськість розглядаються у якості повноцінних партнерів. Цей механізм передбачає наділення громадськості максимальним обсягом прав та залучення її до співпраці на усіх рівнях інформаційної безпеки. Перспективним напрямком подальшого пошуку є обгрунтування означеного механізму, зокрема деталізація його основоположних категорій розбудови.

Список використаних джерел:

1. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. *Голос України*. 2018. № 122.
2. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Інформація і право*. 2017. № 4. С. 42–46.
3. Паш Б. В. Складові інформаційної безпеки держави: постановка питання. Закарпатські правові читання: матеріали Міжнародної науково-практичної конференції (м. Ужгород, 20–22 квітня 2017 року). Ужгород: УжНУ. 2017. С. 510–513.
4. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. *Голос України*. 1996. № 128.
5. Про Раду національної безпеки та оборони України: Закон України від 05 березня 1998 р. № 183/98-ВР. *Голос України*. 1998.
6. Чуйко З. Д. Верховна Рада України в механізмі забезпечення національної безпеки. *Державне будівництво та місцеве самоврядування.* 2005. № 10. С. 155–167.
7. Яременко О. І. Правовий статус Кабінету Міністрів України як суб'єкта державного управління інформаційною сферою. Інформація і право. 2015. № 2 (14). С. 13–19.
8. Каглинський О. Є. Правові засади діяльності Служби безпеки України як суб'єкта сфери безпеки і оборони. *Нове українське право*. 2022. № 3. С. 68–74.
9. Дулгер В. В. Військові адміністрації як тимчасові державні органи з елементами військової організації управління у складі сектору безпеки й оборони України. *Південноукраїнський правничий часопис*. 2018. № 4. С. 33– 37.
10. Про правовий режим воєнного стану: Закон України 12 травня 2015 р. № 389-VIII. *Голос України*. 2015. № 101.
11. Добош З. А. Особливості застосування судового контролю у діяльності публічної адміністрації. *Науковий вісник Ужгородського нац. ун-ту.* 2021. № 68. С. 148–152.
12. Христинченко Н. П., Ковалів М. В. Демократичний цивільний контроль сектору безпеки і оборони: поняття, зміст, форми реалізації в реаліях сьогодення. *Проблеми сучасної трансформації*. 2023. № 8. С. 37–45.
13. Килимник І. І. Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. *Науковий вісник Ужгородського нац. ун-ту*. 2023. № 76. С. 53–57.
14. Головка А. А. Інститути громадянського суспільства в системі Інформаційної безпеки України. *Вісник НТУУ «КПІ».* 2015. № 3. С. 13–16.

References:

1. Pro natsionalnu bezpeku Ukrainy [About the national security of Ukraine]: Zakon Ukrainy vid 21 chervnia 2018 r. № 2469-VIII. *Holos Ukrainy*. 2018. № 122 [in Ukrainian].
2. Tkachuk T. Y. (2017) Sub'iekty zabezpechennia informatsiinoi bezpeky derzhavy: funktsionalnyi analiz [Subjects of state information security: functional analysis]. *Informatsiia i pravo*. 2017. № 4. pp. 42–46 [in Ukrainian].
3. Pash B. V. (2017) Skladovi informatsiinoi bezpeky derzhavy: postanovka pytannia [Components of information security of the state: posing the question]. Zakarpatski pravovi chytannia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii (m. Uzhhorod, 20–22 kvitnia). Uzhhorod: UzhNU. pp. 510–513 [in Ukrainian].
4. Konstytutsiia Ukrainy [Constitution of Ukraine]: Zakon Ukrainy vid 28 chervnia 1996 r. № 254k/96-VR. *Holos Ukrainy*. 1996. № 128 [in Ukrainian].
5. Pro Radu natsionalnoi bezpeky ta oborony Ukrainy [About the National Security and Defense Council of Ukraine]: Zakon Ukrainy vid 05 bereznia 1998 r. № 183/98-VR. *Holos Ukrainy*. 1998 [in Ukrainian].
6. Chuiko Z. D. (2005) Verkhovna Rada Ukrainy v mekhanizmi zabezpechennia natsionalnoi bezpeky [Verkhovna Rada of Ukraine in the mechanism of ensuring national security]. *Derzhavne budivnytstvo ta mistseve samovriaduvannia*. № 10. pp. 155–167 [in Ukrainian].
7. Yaremenko O. I. (2015) Pravovyi status Kabinetu Ministriv Ukrainy yak sub'iekta derzhavnoho upravlinnia informatsiinoiu sferoiu [Legal status of the Cabinet of Ministers of Ukraine as a subject of state management of the information sphere]. *Informatsiia i pravo*. № 2 (14). pp. 13–19 [in Ukrainian].
8. Kahlynskyi O. Y. (2022) Pravovi zasady diialnosti Sluzhby bezpeky Ukrainy yak sub'iekta sfery bezpeky i oborony [Legal principles of the activity of the Security Service of Ukraine as a subject of the sphere of security and defense]. *Nove ukrainske pravo*. № 3. pp. 68–74 [in Ukrainian].
9. Dulher V. V. (2018) Viiskovi administratsii yak tymchasovi derzhavni orhany z elementamy viiskovoi orhanizatsii upravlinnia u skladi sektoru bezpeky y oborony Ukrainy [Military administrations as temporary state bodies with elements of a military management organization as part of the security and defense sector of Ukraine]. *Pivdennoukrainskyi pravnychyi chasopys*. № 4. pp. 33–37 [in Ukrainian].
10. Pro pravovyi rezhym voiennoho stanu [About the legal regime of martial law]: Zakon Ukrainy 12 travnia 2015 r. № 389-VIII. *Holos Ukrainy*. 2015. № 101 [in Ukrainian].
11. Dobosh Z. A. (2021) Osoblyvosti zastosuvannia sudovoho kontroliu u diialnosti publichnoi administratsii [Peculiarities of the application of judicial control in the activity of public administration]. Naukovyi visnyk Uzhhorodskoho nats. un-tu. № 68. pp. 148–152 [in Ukrainian].
12. Khrystynchenko N. P., Kovaliv M. V. (2023) Demokratychnyi tsyvilnyi kontrol sektoru bezpeky i oborony: poniattia, zmist, formy realizatsii v realiiakh sohodennia [Democratic civilian control of the security and defense sector: concept, content, forms of implementation in today's realities]. *Problemy suchasnoi transformatsii*. № 8. pp. 37–45 [in Ukrainian].
13. Kylymnyk I. I. Informatsiine suspilstvo ta informatsiina bezpeka. Novi vyklyky ta shliakhy podolannia informatsiinykh zahroz [Information society and information security. New challenges and ways to overcome information threats]. *Naukovyi visnyk Uzhhorodskoho nats. un-tu*. № 76. pp. 53–57 [in Ukrainian].
14. Holovka A. A. (2015) Instytuty hromadianskoho suspilstva v systemi Informatsiinoi bezpeky Ukrainy [Institutes of civil society in the Information Security system of Ukraine]. *Visnyk NTUU «KPI»*. № 3. pp. 13–16 [in Ukrainian].