Список використаних джерел:

1. Letellier P. Ethical eye: Euthanasia. Volume I, ethical and human aspects. Strasbourg : Council of Europe Publishing, 2003. 200 p.
2. The Belgian Act on Euthanasia. URL: http://www.ethical-perspectives.be/viewpic.php?TABLE=EP&ID=59
3. The Dutch Termination of Life on Request and Assisted Suicide (Review Procedures) Act. URL: https://wetten.overheid.nl/BWBR0012410/2002-04-01#HoofdstukII_Artikel2
4. The Luxemburg Law on Euthanasia and Assisted Suicide. URL: http://legilux.public.lu/eli/etat/leg/loi/2009/03/16/n2/jo
5. Emanuel E.J. Onwuteaka-Philipsen B.D., Urwin J.W., Cohen J. Attitudes and Practices of Euthanasia and Physician-Assisted Suicide in the United States, Canada, and Europe. *JAMA*. 2016. № 316(1). P. 79–90.
6. 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
7. Белей К.В. Евтаназія − право на гідну смерть чи вбивство? *Актуальні проблеми держави і права* : збірник наук. праць. Одеса : Юрид. л-ра, 2005. № 25. С. 43−45.
8. Закон України «Основи законодавства України про охорону здоров'я». URL: https://zakon.rada.gov.ua/laws/show/2801-12
9. Цомко-Пестєрєва О.О. Проблеми евтаназії в контексті біоетики. Мультиверсум. *Філософський альманах.* 2005. № 51. URL: https://www.filosof.com.ua/Jornel/M_51/Comko.htm

ВЕСЕЛОВА Л. Ю.,
кандидат юридичних наук,
доцент кафедри адміністративної
діяльності поліції
(Одеський державний
університет внутрішніх справ)

УДК 342.9.07:007(477)
DOI https://doi.org/10.32842/2078-3736-2019-5-2-3

КОМПЕТЕНЦІЯ СУБ'ЄКТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В КІБЕРНЕТИЧНІЙ СФЕРІ

Під час дослідження визначаються проблемні питання щодо компетенції суб'єктів адміністративно-правового забезпечення національної безпеки України в кібернетичній сфері в умовах гібридної війни. У статті охарактеризовано компетенцію суб'єктів адміністративно-правового забезпечення кібернетичної безпеки в Україні. Констатовано, що компетенція суб'єктів забезпечення кібернетичної безпеки України відображена в низці нормативно-правових актів, чільне місце серед яких посідає Стратегія кібернетичної безпеки України, в якій вперше на законодавчому рівні сформовано національну систему кібернетичної безпеки та визначено основних суб'єктів її забезпечення. Встановлено, що до суб'єктів забезпечення кібернетичної безпеки належать: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Констатовано, що Стратегія кібернетичної безпеки України не в повному обсязі відображає систему суб'єктів забезпечення кібернетичної безпеки України, яка має

включати, поряд з основними, ще й спеціальних суб'єктів забезпечення кібернетичної безпеки, наділених специфічними функціями та повноваженнями в цьому напрямі. Після вивчення та аналізу наукових досліджень та останніх джерел з означеної тематики у статті звернуто увагу, що кібернетична агресія має цілком конкретні суспільно небезпечні протиправні наслідки, які виражаються у вигляді виникнення техногенних надзвичайних ситуацій, створенні перешкод у роботі комп'ютерних мереж та електронної техніки, збоях у процесі реалізації механізму надання адміністративних та банківських послуг, а також здійснення бюджетних виплат. Також під час вивчення проблематики зроблено наголос на прогалинах, які, безперечно, не сприяють формуванню цілісної, а головне – ефективної організаційної побудови системи суб'єктів забезпечення безпеки в кібернетичній сфері. Так, попри те, що Стратегія кібернетичної безпеки України в ієрархії законодавчих актів є підзаконним нормативно-правовим актом, видається, що перелік органів у сфері забезпечення кібернетичної безпеки України, визначений у цьому документі, сформульований більш виважено та логічно, аніж у Законі України «Про основні засади забезпечення кібернетичної безпеки України».

Ключові слова: *компетенція, суб'єкти забезпечення кібернетичної безпеки, національна безпека, Стратегія кібербезпеки України, державні органи, кіберполіція, Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.*

The research identifies problematic issues regarding the competence of subjects of administrative and legal support of national security of Ukraine in the cyber sphere in the conditions of hybrid war. The article describes the competence of the subjects of administrative and legal support of cyber security in Ukraine. It was stated that the competence of the subjects of providing cyber security of Ukraine is reflected in a number of normative legal acts, the main place of which is the Strategy of cyber security of Ukraine, which for the first time at the legislative level formed the national system of cyber security and identified the main subjects of its provision. It was established that the subjects of providing cyber security are: Ministry of Defense of Ukraine, State Service for Special Communications and Information Protection of Ukraine, Security Service of Ukraine, National Police of Ukraine, National Bank of Ukraine, intelligence agencies. It is stated that the Cyber security Strategy of Ukraine does not fully reflect the system of subjects of providing cyber security of Ukraine, which should include, along with the main, also special entities providing cyber security, endowed with specific functions and powers in this direction. After studying and analyzing the research and recent sources on the topic, the article points out that cyber aggression has quite specific socially dangerous unlawful consequences, which are expressed in the form of technogenic emergencies, interference in the work of computer networks and electronic equipment, failures in the process of implementing the mechanism of administrative and banking services, as well as making budgetary payments. Also, in the study of the problems, the emphasis was placed on the gaps, which undoubtedly do not contribute to the formation of a holistic, and most importantly − effective organizational building of the system of subjects of security in the cybernetic sphere. Thus, despite the fact that the Cyber Security Strategy of Ukraine in the hierarchy of legislative acts is a by-law, it seems that the list of authorities in the field of cyber security in Ukraine, defined in this document, is formulated more carefully and logically than in the Law of Ukraine." On the basic principles of ensuring cyber security in Ukraine.

Key words: *competence, subjects of providing cyber security, national security, cyber security strategy of Ukraine, state bodies, cyber police, Ministry of Defense of Ukraine, State Service for Special Communications and Information Protection of Ukraine, Security Service of Ukraine, National Police of Ukraine, National Bank of Ukraine , intelligence agencies.*

Вступ. Правові відносини виступають як головний елемент у механізмі правового регулювання суспільних відносин. За допомогою правовідносин відбувається приведення в дію механізму правового регулювання та реалізація правових норм. Водночас окремі властивості правових норм, пов'язані із встановленням загальних правил поведінки, визначенням кола суб'єктів їх реалізації, їх правового положення, взаємних прав та обов'язків, заходів відповідальності за вчинення протиправних дій, ще не призводять до утворення правовідносин.

Виникнення правових відносин, передусім, пов'язане із появою обставин, передбачених у диспозиціях відповідних норм права. Тому одне з першочергових завдань теоретичного обґрунтування моделі забезпечення кібербезпеки України полягає у спроможності суб'єктів права набувати статусу учасників правовідносин у сфері забезпечення кібербезпеки, з наділенням їх відповідною компетенцією.

У науковій літературі питання адміністративно-правового статусу суб'єктів правовідносин та їх співвідношення із правовими категоріями «учасник правовідносин», «суб'єкт права» досліджені доволі докладно. Наукову розвідку у вказаному напрямі здійснювали як вітчизняні, так і зарубіжні вчені: В.Б. Авер'янов, Л.В. Авраменко, С.С. Алексеєв, О.В. Артеменко, Д.М. Бахрах, Р.В. Бідонько, М.Г. Глобінець, І.С. Гриценко, І.В. Діордіца, С.В. Ківалов, В.А. Ліпкан, І. Литвин, Р.С. Мельник, О.В. Петришин, А.А. Пухтецька, Б.В. Россинський, Л.О. Самілик, Т.О. Санжарук, Ю.М. Старилов, Ю.М. Фролов, М.В. Цвік, В. Шаповал та деякі інші. Разом із цим варто зазначити, що напрям державного управління, пов'язаний із забезпеченням кібербезпеки України, порівняно новий та такий, що динамічно розвивається. Тому питання, пов'язані із характеристикою компетенції суб'єктів забезпечення кібербезпеки України, набувають особливої актуальності.

Постановка завдання. Мета дослідження полягає в тому, щоб на основі вітчизняних та зарубіжних наукових джерел та сучасного адміністративного законодавства в галузі національної безпеки України охарактеризувати компетенцію суб'єктів адміністративно-правового забезпечення кібернетичної безпеки в Україні.

Результати дослідження. Адміністративно-правовий статус суб'єктів забезпечення кібербезпеки України відображений у низці нормативно-правових актів, чільне місце серед яких посідає Стратегія кібербезпеки України. Вперше на законодавчому рівні сформовано національну систему кібербезпеки України та визначено основних суб'єктів її забезпечення. Так, у частині 1 розділу 3 коментованого нормативно-правового акта сформульовано необхідність забезпечення взаємодії органів державної влади, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, з питань забезпечення кібербезпеки [1]. Водночас частина 3 розділу 3 коментованого документа виокремлює низку державних органів, які становлять основу національної системи кібербезпеки. До таких суб'єктів забезпечення кібербезпеки належать: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи [1].

Перелік суб'єктів забезпечення кібербезпеки визначено й іншим законодавчим актом, законом України від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України» (скорочено – Закон). Порівняльно-правовий аналіз ст.ст. 5, 8 Закону дав змогу дійти висновку про наявність деяких дискусійних положень у частині визначення переліку суб'єктів забезпечення кібербезпеки. Зокрема, у ст. 5 Закону визначено немовби вичерпний перелік зазначених суб'єктів державного управління, до яких зараховано: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації зараховані до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єд-

нання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [2].

Навіть побіжний аналіз переліку суб'єктів, зазначених у ст.ст. 5, 8 Закону, свідчить про їх дублювання. Наприклад, серед суб'єктів, визначених у ст. 5 Закону, вказуються правоохоронні органи, до числа яких, безперечно, входить Національна поліція України, яка також визначена як основний суб'єкт у ст. 8 Закону. Також незрозумілим є одночасне внесення до ст.ст. 5, 8 Закону, Національного банку України та Збройних сил України як суб'єктів забезпечення кібербезпеки. Крім того, логіка побудови ст. 8 коментованого законодавчого акта передбачає наявність, окрім основних суб'єктів забезпечення кібербезпеки, ще й додаткових, перелік яких законодавцем, на жаль, не визначено.

Таким чином, вказані прогалини, безперечно, не сприяють формуванню цілісної, а головне – ефективної організаційної побудови системи суб'єктів забезпечення безпеки у кібернетичній сфері. Попри те, що Стратегія кібербезпеки України в ієрархії законодавчих актів є підзаконним нормативно-правовим актом, видається, що перелік органів у сфері забезпечення кібербезпеки України, визначений у цьому документі, сформульований більш виважено та логічно, аніж у Законі України «Про основні засади забезпечення кібербезпеки України».

У Стратегії забезпечення кібербезпеки України та Законі України «Про основні засади забезпечення кібербезпеки України» закріплена низка специфічних повноважень основних суб'єктів національної системи кібербезпеки, до числа яких, відповідно до ч. 2 ст. 8 Закону, належать: Державна служба спеціального зв'язку та захисту інформації України; Національна поліція України; Служба безпеки України; Міністерство оборони України та Генеральний штаб Збройних сил України; розвідувальні органи; Національний банк України.

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» визначає загальні напрями діяльності та повноваження Служби спецзв'язку у сфері забезпечення кібербезпеки України. Разом із тим безпосередня реалізація державної політики у вказаному напрямі покладена на спеціальний орган, який функціонує у складі Служби спецзв'язку, – Державний центр кіберзахисту та протидії кіберзагрозам, положення про який затверджено наказом Державної служби спеціального зв'язку та захисту інформації України від 11 листопада 2016 р. № 704 (скорочено – Центр) [3].

Функції Центру мають переважно координаційну спрямованість та полягають у забезпеченні ефективної взаємодії органів державної влади з питань запобігання та усунення наслідків кіберінцидентів, координації діяльності операторів та провайдерів щодо збору інформації про кіберінциденти, міжнародної координації з питань кіберзахисту.

Серед суб'єктів забезпечення кібербезпеки України органи охорони правопорядку представлені Національною поліцією та Службою безпеки України. Головна відмінність реалізації ними повноважень у кіберсфері полягає в наявності в їхньому арсеналі яскраво вираженої правоохоронної функції, реалізація якої здійснюється за допомогою застосування примусових та попереджувальних заходів, а також заходів юридичної відповідальності.

Так, Стратегією кібербезпеки України на Національну поліцію України покладені завдання із забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі, запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі [1].

Реалізація вищевказаних завдань здійснюється Національною поліцією України відповідно до законодавчих та підзаконних нормативно-правових актів. Так, відповідно до ст. 23 Закону України «Про Національну поліцію», поліція запобігає вчиненню адміністративних та кримінальних правопорушень шляхом здійснення превентивної та профілактичної діяльності [4].

На відміну від Служби безпеки України, у структурі Національної поліції функціонує спеціальний підрозділ, діяльність якого безпосередньо пов'язана з організацією протидії

правопорушенням у кібернетичній сфері. Так, відповідно до Постанови Кабінету Міністрів України № 831 від 13 жовтня 2015 р. «Про утворення територіального органу Національної поліції» [5] утворено структурний підрозділ Національної поліції – кіберполіцію.

За словами Міністра внутрішніх справ А. Авакова, кіберполіція – це новий підрозділ правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзлочини та кіберзагрози, а також відповідно до кращих світових стандартів проводитиме міжнародну співпрацю із знешкодження транснаціональних злочинних угрупувань у цій сфері [6].

За словами О.В. Артеменка та Р.В. Бідонька, кіберполіція оснащена доволі потужною нормативно-правовою базою, що забезпечує функціонування та регламентує її діяльність та свідчить про перспективи подальших наукових досліджень в інформаційній сфері права [7, с. 117].

Аналіз основних напрямів діяльності Департаменту кіберполіції дав змогу сформулювати сфери суспільних відносин, які слугують об'єктом правової охорони підрозділів кіберполіції: а) сфера інформаційної безпеки; б) сфера використання платіжних систем; в) сфера електронної комерції та господарської діяльності; г) сфера інтелектуальної власності.

Загалом, підкреслюючи надзвичайну важливість правоохоронної діяльності кіберполіції у сфері забезпечення кібербезпеки, варто наголосити, що протягом 2018 р. основним напрямом діяльності підрозділів кіберполіції стало розслідування кримінальних правопорушень у сфері високих технологій. Так, протягом року працівники Департаменту кіберполіції були залучені до розслідування понад 11 000 кримінальних проваджень. Крім того, упродовж вказаного періоду поліцейські виявили 6000 злочинів, вчинених у сфері використання високих інформаційних технологій та викрили понад 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій [8].

Служба безпеки України реалізує повноваження щодо забезпечення національної безпеки в кібернетичній сфері через Ситуаційний центр забезпечення кібербезпеки Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки [9].

Нагадаємо, що розпочата у 2014 р. агресія Російської Федерації на території України передбачає, в тому числі, й здійснення кібернетичних атак на державні установи та об'єкти інформаційної критичної інфраструктури з використанням шкідливого програмного забезпечення. Зазначена діяльність має цілком конкретні суспільно небезпечні протиправні наслідки, які виражаються у вигляді виникнення техногенних надзвичайних ситуацій, створенні перешкод у роботі комп'ютерних мереж та електронної техніки, збоях у процесі реалізації механізму надання адміністративних та банківських послуг, а також здійснення бюджетних виплат.

Статистичні дані твердять про виявлення, документування та подальше внесення до санкційного списку уповноваженими працівниками СБУ впродовж 6 місяців 2018 р. 181 інтернет-ресурсу, які належать російським спецслужбам та використовуються з метою дестабілізації політичної та соціально-економічної обстановки в країні [10]. Водночас видається, що заходи, здійснювані працівниками Служби безпеки України у сфері забезпечення кібербезпеки, виглядають недостатньо ефективними з кількох причин. Перш за все, варто наголосити на необхідності подальшої реалізації рішення Ради національної безпеки і оборони України від 28 квітня 2017 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», затвердженого Указом Президента України від 15.05.2017 р. №133 [11], в частині правової регламентації порядку блокування інформаційних ресурсів працівниками СБУ, який у чинному законодавстві взагалі не визначено.

Головне завдання Міністерства оборони України щодо забезпечення національної безпеки у кіберпросторі, відповідно до Положення про Міністерство оборони України, полягає у здійсненні заходів із забезпечення інформаційної безпеки, кібербезпеки та кіберзахисту, а також підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони).

Цим же документом визначено й загальну функцію Міністерства оборони України щодо забезпечення кібербезпеки, яка полягає в реалізації в межах повноважень, передбачених законом, державної політики у сфері охорони державної таємниці, захисті інформації

з обмеженим доступом, інформаційної безпеки та кібербезпеки, а також технічному захисті інформації, контроль за її збереженням в апараті Міноборони, на підприємствах, в установах і організаціях, які належать до сфери його управління [12].

Більш детально повноваження Збройних сил України у кіберсфері визначені у Положенні про Генеральний штаб Збройних сил України, затвердженому указом Президента України від 30.01.2019 р. № 23/2019. Функції Генерального штабу Збройних сил України дають уявлення про доволі широкий спектр напрямів діяльності ЗС України щодо захисту кіберпростору. Водночас слід констатувати, що організаційно-правове забезпечення діяльності Міністерства оборони України у цьому напрямі знаходиться ще на початковому етапі свого розвитку, проходить фазу становлення. Активна діяльність щодо створення правового базису та організаційного забезпечення діяльності Збройних сил України щодо забезпечення кібербезпеки розпочалось тільки з початком збройної агресії РФ на території України.

Серед основних суб'єктів забезпечення кібербезпеки України визначено й Національний банк України, що обґрунтовано його особливим статусом у системі органів державного управління.

Завдання щодо формування вимог у сфері кіберзахисту деталізуються в Положенні про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженому постановою Правління Національного банку України від 28.09.2017 р. № 95 (скорочено – Положення). Відповідно до вказаного документа на комерційні банки, які підпорядковуються НБУ, покладено низку обов'язків, основні з яких пов'язані із розробленням та впровадженням політики інформаційної безпеки, яка має включати: цілі інформаційної безпеки; сферу застосування політики інформаційної безпеки; принципи, правила та вимоги інформаційної безпеки в банку; визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки [13]. З огляду на останнє завдання варто зазначити, що рольова специфіка діяльності Нацбанку України у сфері забезпечення кібербезпеки випливає, перш за все, з його особливого статусу в системі органів державного управління, який проявляється, передусім, у забезпеченні фінансової стабільності в країні.

Висновки. Таким чином, варто констатувати, що компетенція суб'єктів забезпечення кібербезпеки України відображена в низці нормативно-правових актів, чільне місце серед яких посідає Стратегія кібербезпеки України, в якій вперше на законодавчому рівні сформовано національну систему кібербезпеки та визначено основних суб'єктів її забезпечення. Відповідно до положень вказаного документа до суб'єктів забезпечення кібербезпеки належать: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Також слід зазначити, що суб'єкти забезпечення кібербезпеки України наділені як загальними, так і спеціальними повноваженнями у вказаному напрямі державного управління. Водночас видається, що Стратегія кібербезпеки України не в повному обсязі відображає систему суб'єктів забезпечення кібербезпеки України, яка має включати, поряд з основними, ще й спеціальних суб'єктів забезпечення кібербезпеки, наділених специфічними функціями та повноваженнями в цьому напрямі.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

3. У Держспецзв'язку створено Державний центр кіберзахисту та протидії кіберзагрозам. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473&cat_id=119123.

4. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. Ст. 379.

5. Про утворення територіального органу Національної поліції : Постанова Кабінету Міністрів України від 13 жовтня 2015 р. № 831. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF.

6. Кіберполіція – ваш захист у віртуальному просторі і не лише. URL: https://www.facebook.com/arsen.avakov.1/posts/916452195111554.

7. Артеменко О.В., Бідонько Р.В. Кіберполіція України. Оргнанізація діяльності та перспективи розвитку. *Право і суспільство.* № 1. Ч. 2. 2017. С. 116−119.

8. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/.

9. Ситуаційний центр забезпечення кібербезпеки СБУ. URL: https://ssu.gov.ua/ua/pages/330.

10. Удосконалення законодавства щодо протидії загрозам національній безпеці в інформаційній сфері необхідне для блокування російських кібератак. URL: https://ssu.gov.ua/ua/news/1/category/2/view/5025#.fovsCOAZ.dpbshttps://ssu.gov.ua/ua/news/1/category/2/view/5025#.fovsCOAZ.dpbs.

11. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) : Рішення Ради національної безпеки і оборони України від 28 квітня 2017 р. URL: https://zakon.rada.gov.ua/laws/show/ru/133/2017.

12. Про затвердження Положення про Міністерство оборони України : Постанова Кабінету Міністрів України від 26.11.2014 р. № 671. *Офіційний вісник України*. 2014. № 97. Ст. 2796.

13. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Правління Національного банку України від 28.09.2017 р. № 95. *Офіційний вісник України*. 2017. № 84. Ст. 2575.

ГАЛАЙ В. О.,
кандидат юридичних наук, доцент,
доцент кафедри міжнародного
публічного права
(Київський національний торговельно-економічний університет)

УДК 342.98
DOI https://doi.org/10.32842/2078-3736-2019-5-2-4

ЗМІСТОВІ ЕЛЕМЕНТИ ПРИНЦИПУ РІВНОСТІ НА ПУБЛІЧНІЙ СЛУЖБІ

У статті проаналізовано положення як міжнародних, так і вітчизняних нормативно-правових актів та доктринальні підходи щодо змісту принципу рівності на публічній службі.

Автором з'ясовано, що, виходячи із класичних підходів теорії права, рівність включає в себе рівність перед законом та заборону дискримінації і є елементом законності як складника принципу верховенства права. Проте правова категорія рівності є ширшою за наведену теорію і заслуговує окремого розгляду та дослідження.

Прослідковано, що у правовій доктрині зміст принципу рівності не має єдиного тлумачення та залишається предметом наукових дискусій, відповідно, дослідженню змісту принципу рівності на публічній службі присвячено мало уваги.