9. Бурлака О.С. Атестаційні провадження : дисертація. Київ : Київський національний університет внутрішніх справ. 2007. 220 с.

10. Шопіна І.М. Правові та організаційні засади підвищення ефективності професійної діяльності слідчих органів внутрішніх справ України : дисертація. Харків : Національний університет внутрішніх справ. 2004. 192 с.

11. Бортник С.М. Професійна підготовка поліцейського в Україні: зміст та завдання. Харків : Особистість, суспільство, закон. 2021. С. 192–195.

12. Швець Д.В. Поняття, зміст та функції професійної підготовки поліцейського в Україні. *Форум права.* 2017. № 5. С. 441–446.

УДК 342.9
DOI https://doi.org/10.32844/2618-1258.2023.4.20

КАБИШ О.О.

СУЧАСНИЙ СТАН АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

THE CURRENT STATE OF ADMINISTRATIVE AND LEGAL REGULATION OF THE INTERACTION OF CYBERCRIME COUNTERMEASURES SUBJECTS

Актуальність статті полягає в тому, що широке впровадження нових технічних рішень, які використовуються для реалізації процесу інформатизації у всьому світі, призводить до формування нових геополітичних концепцій в контексті глобальних соціально-технічних систем. Міжнародна інформаційна область стає не лише важливим аспектом співпраці, але і сферою конкуренції між окремими особами, країнами та міжнародними політичними та економічними об'єднаннями. Електронно-комунікаційна інфраструктура, разом із іншими інформаційними ресурсами, стає об'єктом міжнародних змагань за глобальне лідерство або предметом недобросовісної конкуренції у сфері підприємництва й інших суспільних інформаційних відносин. Критичним моментом у забезпеченні безпеки інформації є правомірне використання комп'ютерних систем, що спрямоване на запобігання їх незаконному використанню та порушенням існуючих соціальних і політичних норм. Саме тому, важливим завданням законодавця є забезпечення ефективної співпраці суб'єктів протидії кіберзлочинності, реалізація якої вимагає створення належного нормативно-правового підґрунтя. У статті здійснено комплексний аналіз нормативно-правових актів різної юридичної сили, норми яких спрямовані на регулювання взаємодії суб'єктів протидії кіберзлочинності. Доведено, що в системі правових засад відповідного регулювання ключове місце відводиться нормам адміністративної галузі права, адже саме за їх допомогою розкриваються: організаційно-управлінські аспекти взаємодії; порядок реалізації спільної діяльності уповноважених суб'єктів в секторі кібербезпеки та їх ієрархічне підпорядкування; правовий статус суб'єктів взаємодії, ключові цілі, завдання та функції співпраці; тощо. Зроблено висновок, що юридичне підґрунтя взаємодії суб'єктів протидії кіберзлочинності складає велика група нормативно-правових актів. Вона включає в себе Конституцію України, а також міжнародні документи (ратифіковані у встановленому законом порядку) та прийняті закони і підзаконні нормативно-правові акти, серед яких переважають адміністративно-правові норми. Така галузева приналежність пов'язана із характером суспільно-правових відносин, що виникають

© КАБИШ О.О. – аспірант (Науково-дослідний інститут публічного права)

в процесі взаємодії суб'єктів протидії суспільно-небезпечним діянням вчиненим із використанням інформаційних технологій. Саме в правових актах адміністративного характеру розкриваються: організаційно-управлінські аспекти взаємодії; порядок реалізації спільної діяльності уповноважених суб'єктів в секторі кібербезпеки та їх ієрархічне підпорядкування; правовий статус суб'єктів взаємодії, ключові цілі, завдання та функції співпраці; тощо. Також, на сьогоднішній день стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності можна оцінити неоднозначно. Так, з одного боку, наявною є широка нормативна база, спрямована на регулювання суспільних відносин у відповідній сфері, а з іншої сторони чинне законодавство має низку прогалин та недоліків, до яких слід віднести: невизначеність механізмів взаємодії спеціально уповноважених суб'єктів у відповідній сфері; відсутність законодавчого закріплення.

Ключові слова: *нормативно-правові акти, адміністративно-правове регулювання, правове регулювання, взаємодія, суб'єкти, протидія кіберзлочинність.*

The relevance of the article lies in the fact that the wide implementation of new technical solutions, which are used to implement the process of informatization throughout the world, leads to the formation of new geopolitical concepts in the context of global socio-technical systems. The international information field is becoming not only an important aspect of cooperation, but also a field of competition between individuals, countries, and international political and economic associations. Electronic communication infrastructure, together with other information resources, becomes the object of international competitions for global leadership or the subject of unfair competition in the field of entrepreneurship and other social information relations. A critical point in ensuring information security is the lawful use of computer systems aimed at preventing their illegal use and violations of existing social and political norms. That is why an important task of the legislator is to ensure the effective cooperation of the actors in the fight against cybercrime, the implementation of which requires the creation of an appropriate regulatory and legal basis. In the article, a comprehensive analysis of normative legal acts of different legal force, the norms of which are aimed at regulating the interaction of actors in the fight against cybercrime, is carried out. It is proved that in the system of legal foundations of the relevant regulation, the key place is assigned to the norms of the administrative branch of law, because it is with their help that the following are revealed: organizational and management aspects of interaction; the procedure for implementing joint activities of authorized entities in the cyber security sector and their hierarchical subordination; legal status of subjects of interaction, key goals, tasks and functions of cooperation; etc. It was concluded that the legal basis for the interaction of actors in the fight against cybercrime is a large group of normative and legal acts. It includes the Constitution of Ukraine, as well as international documents (ratified in accordance with the procedure established by law) and adopted laws and bylaws, among which administrative and legal norms prevail. Such branch affiliation is related to the nature of social and legal relations that arise in the process of interaction of subjects against socially dangerous acts committed with the use of information technologies. It is in legal acts of an administrative nature that the following are disclosed: organizational and management aspects of interaction; the procedure for implementing joint activities of authorized entities in the cyber security sector and their hierarchical subordination; legal status of subjects of interaction, key goals, tasks and functions of cooperation; etc. Also, to date, the state of administrative and legal regulation of the interaction of cybercrime countermeasures can be assessed ambiguously. So, on the one hand, there is a broad regulatory framework aimed at regulating social relations in the relevant field, and on the other hand, the current legislation has a number of gaps and shortcomings, which should include: the uncertainty of the mechanisms of interaction of specially authorized subjects in the relevant field; lack of legal confirmation.

Key words: *regulatory and legal acts, administrative and legal regulation, legal regulation, interaction of subjects, combating cybercrime.*

Постановка проблеми. Широке впровадження нових технічних рішень, які використовуються для реалізації процесу інформатизації у всьому світі, призводить до формування нових геополітичних концепцій в контексті глобальних соціально-технічних систем. Міжнародна інформаційна область стає не лише важливим аспектом співпраці, але і сферою конкуренції між окремими особами, країнами та міжнародними політичними та економічними об'єднаннями. Електронно-комунікаційна інфраструктура, разом із іншими інформаційними ресурсами, стає об'єктом міжнародних змагань за глобальне лідерство або предметом недобросовісної конкуренції у сфері підприємництва й інших суспільних інформаційних відносин. Критичним моментом у забезпеченні безпеки інформації є правомірне використання комп'ютерних систем, що спрямоване на запобігання їх незаконному використанню та порушенням існуючих соціальних і політичних норм. Саме тому, важливим завданням законодавця є забезпечення ефективної співпраці суб'єктів протидії кіберзлочинності, реалізація якої вимагає створення належного нормативно-правового підґрунтя.

Стан дослідження проблеми. Окремі проблемні питання, пов'язані із регулюванням протидії кіберзлочинності, у своїх наукових працях розглядали: П.П. Андрушко, В.О. Голубєва, І.В. Кобзев, Н.С. Козак, С.Й. Кравчук, С.А. Кузьмін, А.М. Кулик, М.С. Кучеренко, Н.І. Мазниченко, М.С. Мазуренко, В.В. Марков та багато інших. Втім, незважаючи на суттєві теоретичні здобутки, вчені у своїх працях досить поверхневу увагу приділяли саме питанню адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Саме тому **метою статті** є: оцінити сучасний стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Постановка проблеми. Розкриття стану адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності варто починати із опрацювання центрального документу національної правової системи –Конституції України від 28.06.1996 № 254к/96-вр. Так, в Конституції знаходять своє закріплення засади суспільно-політичного та державного устрою, як то специфіка поділу державної влади, політико-територіальний поділ країни, повноваження вищих інституцій державної влади (Президент України, Кабінет Міністрів України, Верховна Рада України), основоположні права та свободи людини і громадянина тощо. Конституційними положеннями питання взаємодії суб'єктів протидії кіберзлочинності прямо не регламентовано, але норми Основного закону становлять базу адміністративно-правового регулювання їх діяльності в цілому. В статті 17 документу зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України. Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом» [1].

Відмітити варто статтю 9 Основного Закону, яка фактично наділяє юридичною силою іншу групу правових засада взаємодії суб'єктів протидії кіберзлочинності – міжнародні нормативно-правові акти. Відповідно до вказаного конституційного положення чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України. Укладення міжнародних договорів, які суперечать Конституції України, можливе лише після внесення відповідних змін до Конституції України [1].

На сьогоднішній день Україною ратифіковано низку документів в сфері протидії кіберзлочинності. Відмітити, як приклад, варто Конвенцію Ради Європи про кіберзлочинність від 23.11.2001. В преамбулі документу наголошено, що він є необхідним для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [2]. Так, Конвенція містить чіткий перелік дій, які визнаються кіберзлочинами на території держав-учасниць документу, зокрема: незаконний доступ, нелегальне перехоплення, втручання у данні, втручання у систему, зловживання пристроями, шахрайство, пов'язане з комп'ютерами і таке інше [2].

Суттєву увагу в Конвенції приділено питанню співпраці у протидії кіберзлочинності, як на внутрішньо-національному, так і міжнародному рівні. Наприклад, в статті 21 говориться про те, що компетентні органи сторін-учасниць документу зобов'язані співробітничати у зборі або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, яка здійснюється за допомогою комп'ютерних систем. В свою чергу, у статті 23 наголошено, що сторони співробітничають між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень [2].

В рамках національної системи права окрім Конституції, до правових засад взаємодії в сфері протидії кіберзлочинності варто віднести Кримінальний кодекс України (далі – ККУ) та Кримінальний процесуальний кодекс України (далі – КПК). Важливість першого документу полягає в тому, що його ключовим завданням є правове забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України від кримінально-протиправних посягань, забезпечення миру і безпеки людства, а також запобігання кримінальним правопорушенням. Закон визначає, які саме діяння слід вважати кібезлочинами та які міри кримінально-правового впливу застосовуються до осіб, які їх вчиняють [3].

В свою чергу, Кримінальний процесуальний кодекс України визначає процедурний порядок протидії передбаченим ККУ кіберзлочинам шляхом здійснення кримінального провадження. Стаття 2 КПК закріплює, що завданнями останнього є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура. Кримінальне провадження щодо відповідних кіберзлочинів передбачає здійснення відповідних слідчих (розшукових) та негласних (слідчих) розшукових дій з метою збору доказів для подальшого судового розгляду факту вчинення суспільно-небезпечного діяння та притягнення у разі доведення вини особи до кримінальної відповідальності [4].

Серед законодавчих актів, що входять до системи правових засад взаємодії суб'єктів протидії злочинності, варто виділити Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII. Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Згідно до статті 1 документу, кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [5].

Національна система кібербезпеки реалізується сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків [5].

До нормативно-правових актів в сфері регулювання протидії кіберзлочинності також варто віднести Закон України «Про розвідку» від 17.09.2020 №912-IX в рамках якого питанню кібербезпеки присвячено значну увагу. Вказаний Закон декларує, що розвідка – це організаційно-функціональне поєднання визначених законодавством розвідувальних органів та діяльності, яку вони здійснюють самостійно або у взаємодії між собою та з іншими суб'єктами розвідувального співтовариства з метою забезпечення національної безпеки і оборони України. Основними завданнями розвідки є: 1) своєчасне забезпечення споживачів розвідувальною інформацією; 2) сприяння реалізації національних інтересів України; 3) протидія зовнішнім загрозам національній безпеці України у визначених законом сферах. Відповідно до них, однією з ключових функцій діяльності розвідувальних органів визначено: виявляти та визначати ступінь зовнішніх загроз національній безпеці України, у тому числі у кіберпросторі, життю, здоров'ю її громадян та об'єктам державної власності за межами України, організовувати і проводити спеціальні (активні) заходи щодо таких загроз та з протидії іншій діяльності, що становить зовнішню загрозу національній безпеці України [6].

Регулювання суспільних відносин в сфері протидії кіберзлочинності та взаємодії суб'єктів цієї діяльності відбувається за рахунок не тільки законодавчих, але й цілого ряду підзаконних документів, які неможливо оминути увагою. До числа останніх, зокрема, відносяться акти Президента України. Так, Указом Голови держави від 26.08.2021 № 447/2021 уведено в дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Стратегія визначає, що для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є: посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування); набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість); забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами – членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія) [7].

Висновки. Отже, юридичне підґрунтя взаємодії суб'єктів протидії кіберзлочинності складає велика група нормативно-правових актів. Вона включає в себе Конституцію України, а також міжнародні документи (ратифіковані у встановленому законом порядку) та прийняті закони і підзаконні нормативно-правові акти, серед яких переважають адміністративно-правові норми. Така галузева приналежність пов'язана із характером суспільно-правових відносин, що виникають в процесі взаємодії суб'єктів протидії суспільно-небезпечним діянням вчиненим із використанням інформаційних технологій. Саме в правових актах адміністративного характеру розкриваються: організаційно-управлінські аспекти взаємодії; порядок реалізації спільної діяльності уповноважених суб'єктів в секторі кібербезпеки та їх ієрархічне підпорядкування; правовий статус суб'єктів взаємодії, ключові цілі, завдання та функції співпраці; тощо.

На завершення хотілося б відзначити, що на сьогоднішній день стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності можна оцінити неоднозначно. Так, з одного боку, наявною є широка нормативна база, спрямована на регулювання суспільних відносин у відповідній сфері, а з іншої сторони чинне законодавство має низку прогалин та недоліків, до яких слід віднести: невизначеність механізмів взаємодії спеціально уповноважених суб'єктів у відповідній сфері; відсутність законодавчого закріплення форм та методів здійснення даної спільної діяльності; тощо.

Список використаних джерел:

1. Конституція України: закон від 28.06.1996 № 254к/96-ВР. *Офіційний вісник України*. 2010. № 72/1. Ст. 2598.

2. Конвенція про кіберзлочинність: конвенція про кіберзлочинність: конвенція, міжнародний документ від 23.11.2001. *Офіційний вісник України.* 2007. № 65. Ст. 107.

3. Кримінальний кодекс України : кодекс від 05.04.2001 № 2341-III. *Відомості Верховної Ради України.* 2001. № 25. Ст. 131.

4. Кримінальний процесуальний кодекс України : Закон від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України.* 2013. № 9–10. Ст. 474.

5. Про основні засади забезпечення кібербезпеки України : Закон від 05.10.2017 № 2163-VIII. *Офіційний вісник України.* 2017. № 91. Ст. 31.

6. Про розвідку: закон від 17.09.2020 № 912-IX. *Офіційний вісник України.* 2020. № 86. Ст. 2761.

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: указ, стратегія від 26.08.2021 № 447/2021. *Офіційний вісник України.* 2021. № 70. Ст. 4417.

УДК 342.951 + 351.74
DOI https://doi.org/10.32844/2618-1258.2023.4.21

КАМИШАНСЬКИЙ О.Ю.

СЛУЖБА В ПОЛІЦІЇ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ: ОСОБЛИВОСТІ ТА ПРОБЛЕМИ ЇХНЬОЇ КЛАСИФІКАЦІЇ

POLICE SERVICE DURING MARTIAL LAW IN UKRAINE: FEATURES AND PROBLEMS OF THEIR CLASSIFICATION

Актуальність статті полягає в тому, що служба в поліції завжди вирізнялася внутрішньою спрямованістю, адже головні завдання цього органу пов'язані із забезпеченням публічної безпеки та порядку у суспільстві. Водночас, після повномасштабного вторгнення російської федерації на територію України, виникла необхідність адаптації системи Національної поліції до функціонування в особливих умовах воєнного стану. В зв'язку із цим були переглянуті окремі пріоритети поліцейської діяльності, розширені повноваження та оптимізовані завдання. Мета статті полягає у розкритті основних підходів до класифікації особливостей служби в поліції під час дії воєнного стану в Україні та пов'язаних із цим проблем. У статті розкрито основні підходи до класифікації особливостей служби в поліції під час дії воєнного стану в Україні та пов'язані із цим проблеми. Наголошено на необхідності адаптації системи Національної поліції до функціонування в особливих умовах воєнного стану, зокрема, перегляді окремих пріоритетів поліцейської діяльності, розширенні повноважень та оптимізації завдань. Особливості служби в поліції під час дії воєнного стану в Україні розглянуто в межах трьох рівнів: законодавчого, організаційного та суб'єктивного – на яких поліцейська служба набуває рис і ознак, що позначаються на системі поліції, повноваженнях, порядку проходження служби, грошовому і медичному забезпеченні, а також відповідальності поліцейських під час дії особливого правового режиму. Так на законодавчому рівні зроблено акцент на змінах і доповненнях до нормативно-правових актів, якими врегульовано діяльність Національної поліції. Вказано на можливість участі поліції особливого призначення безпосередньо у бойових діях, а також на розширення закріплених Законом України «Про Національну поліцію» повноважень. На організаційному рівні звернуто увагу на формування у системі поліції нового міжрегіонального територіального органу – Департаменту поліції особливого призначення «Об'єднана штурмова бригада Національної поліції України «Лють». Також, враховано зміни у взаємодії поліції та суспільства в особливий період. На суб'єктивному рівні від-

© КАМИШАНСЬКИЙ О.Ю. – кандидат юридичних наук, https://orcid.org/0000-0001-8460-0035