НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

КАБИШ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ

УДК 342.9 (477)

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело_____ **О.О. Кабиш**

Науковий керівник **Червяков Олександр Іванович**, кандидат юридичних наук

Київ – 2024

АНОТАЦІЯ

Кабиш О.О. Адміністративно-правові засади взаємодії суб'єктів протидії кіберзлочинності. − *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут публічного права, Науково-дослідний інститут публічного права, Київ, 2024.

Дисертаційну роботу присвячено з'ясуванню сутності та особливостей адміністративно-правових засад взаємодії суб'єктів протидії кіберзлочинності, а також розробленню пропозицій та рекомендацій, спрямованих на вдосконалення адміністративного законодавства у відповідній сфері.

Акцентовано увагу на тому, що відсутність єдиного сформульованого комплексного бачення природи, змісту, особливостей організації, напрямів здійснення та інших аспектів правового регулювання взаємодії суб'єктів протидії кіберзлочинності, ускладнює вироблення її нової концепції та визначення шляхів удосконалення. При цьому підкреслено, що вирішувати відповідні проблеми найбільш доцільно в розрізі адміністративної галузі права, адже саме нормами цієї галузі регулюється діяльність відповідних суб'єктів, їх правовий статус, мета та завдання діяльності, а відтак і визначаються засади взаємодії між суб'єктами протидії кіберзлочинності.

Встановлено, що протидія кіберзлочинності – це комплексна діяльність, яка здійснюється спеціально уповноваженими суб'єктами, та спрямована на реалізацію заходів та процедур із попередження, виявлення та припинення дій окремих осіб та груп, що містять ознаки злочинів у інформаційній сфері, а також факторів, які сприяють їх вчиненню. Протидія кіберзлочинності передбачає об'єднання зусиль різних органів

державної влади та їх можливостей із реалізації вказаного комплексу заходів та процедур.

Узагальнено, що взаємодія суб'єктів протидії кіберзлочинності – це регламентована нормами адміністративного права модель суспільних відносин, яка передбачає тісну інформаційно-організаційну співпрацю, об'єднання ресурсів, реалізацію спільних заходів, а також поділ відповідальності у процесі здійснення державно-значущої діяльності у напрямку протидії та запобігання суспільно-небезпечним діянням, які складають структуру кіберзлочинності.

Доведено, 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: фактичну відсутність ефективних та злагоджених механізмів взаємодії спеціально уповноважених суб'єктів у відповідній сфері; невизначеність форм та методів здійснення досліджуваної спільної діяльності; тощо.

З'ясовано, що механізм адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, найбільш доцільно тлумачити, як формалізовану систему спеціальних, взаємодіючих та взаємозалежних між собою юридичних елементів, за рахунок яких встановлюються матеріальні та процедурні засади впливу права на суспільно-правові відносини, що виникають в сфері спільної діяльності суб'єктів, які уповноважені на виявлення, припинення та профілактику кіберзлочинів. Виокремлено та надано характеристику наступним ключовим елементам даного механізму: принципи права; норми адміністративного права; нормативно-правові акти; адміністративні правовідносини.

Встановлено, що принципи являють собою сукупність вихідних засад, основоположних, розчинених у адміністративно-правових нормативних актах, стабільних, загальнообов'язкових ідей, які визначають призначення, вектори, цілі та особливості правового регулювання суспільно-правових відносин, що виникають в контексті взаємодії уповноважених суб'єктів протидії кіберзлочинності. До вказаних принципів віднесено такі принципи: принцип законності, принцип поєднання цілей, принцип визначеності суб'єктного складу, принцип координації та контролю, принцип плановості, принцип науковості та принцип достатності.

Відзначено, що адміністративно-правовий статус суб'єктів протидії кіберзлочинності в Україні – це сукупність визначених нормами адміністративного права елементів, які в своїй єдності визначають положення та роль суб'єктів протидії кіберзлочинності у суспільно-правових відносинах, що виникають в процесі здійснення ними спільної діяльності за відповідним напрямом. До елементів адміністративно-правового статусу відповідних суб'єктів віднесено: компетенцію, повноваження, гарантії діяльності та юридичну відповідальність. Надано змістовну характеристику кожному із окреслених елементів.

Під формами взаємодії суб'єктів протидії кіберзлочинності запропоновано розуміти зовнішній вираз спільної, взаємоузгодженої практичної діяльності спеціально уповноважених органів державної влади та їх посадових осіб, яка спрямована на досягнення єдиної мети – протидія та запобігання правопорушенням та злочинним діям, які відбуваються в кіберпросторі або з використанням комп'ютерних технологій і мереж. Зауважено, що в науковій літературі не сформовано єдиного підходу щодо переліку відповідних форм, а відтак, останні запропоновано поділити на дві групи: 1) нормативно-правові форми: нормотворчість; адміністративний договір; правозастосування; 2) організаційно-управлінські форми: підготовка і реалізація спільних заходів; створення

спільних робочих груп; адміністративний нагляд; просвітницька робота з громадськістю.

Констатовано, що переконання та примус – два нерозривно пов'язані між собою методи взаємодії суб'єктів протидії кіберзлочинності. Так, якщо переконання спрямовано на те, щоб забезпечити свідоме ставлення учасників взаємодії до виконуваних ними обов'язків шляхом позитивної мотивації та створення відповідного внутрішнього переконання, то примус передбачає застосування правового або адміністративного тиску для досягнення конкретних цілей в галузі кібербезпеки та протидії кіберзлочинності.

Узагальнено, що на сьогоднішній день у Світі сформувались досить дієві підходи для протидії кіберзлочинності, втім і вони не стали панацеєю для того, щоб повністю мінімізувати ризики виникнення цього негативного явища. Запропоновано авторське бачення щодо того, який саме позитивний досвід провідних країн слід використовувати вітчизняному законодавцю в процесі вдосконалення взаємодії суб'єктів протидії кіберзлочинності.

Акцентовано увагу на тому, що прийняття «Стратегія кібербезпеки України» 2021 року мало вагомий внесок на розвиток сфери протидії та запобігання кіберзлочинності. Втім, вона, переважно, була орієнтована на подолання проблем, які існували ще до початку повномасштабного вторгнення. Разом із тим, з початком війни система протидії кіберзлочинності в нашій країні виявилась не спроможною повною мірою реагувати на існуючі виклики та загрози. А відтак, незважаючи на відносну новизну, даний нормативно-правовий акт є досить застарілим.

З метою вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності запропоновано: 1) розширити коло суб'єктів, які реалізують діяльність у сфері протидії кіберзлочинності, у зв'язку з чим необхідно внести доповнення до пункту 4 статті 5 Закону України «Про основні засади забезпечення кібербезпеки

України», а також змістовно закріпити адміністративно-правовий статус відповідних органів; 2) доповнити статтю 2 Закону України «Про основні засади забезпечення кібербезпеки України» принципом взаємодії суб'єктів протидії кіберзлочинності, адже вирішити існуючі проблеми у відповідній сфері жоден орган державної влади не може самостійно; 3) в Законі України «Про основні засади забезпечення кібербезпеки України» визначити види кіберзлочинів, що в свою чергу створить основу для опрацювання напрямів взаємодії суб'єктів протидії кіберзлочинності; 4) розробити та прийняти окремий законодавчий акт «Про основи взаємодії суб'єкті протидії та запобігання кіберзлочинності».

Доведено, що вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності є фактично неможливим без покращення організаційних засад здійснення відповідної діяльності. В даному контексті запропоновано: 1) покращити систему кадрового забезпечення суб'єктів протидії кіберзлочинності; 2) вдосконалити систему інформаційного забезпечення суб'єктів взаємодії; 3) переглянути підхід до фінансового та матеріально-технічного забезпечення взаємодії суб'єктів протидії кіберзлочинності.

Констатовано, що від професійності кадрів напряму залежить те, як кожен орган державної влади буде виконувати покладені на нього функції у сфері протидії кіберзлочинності, а відтак і ефективність їх спільної діяльності. Підкреслено, що покращення кадрового забезпечення в розрізі представленої проблематики має включати: по-перше, створення системи професійної підготовки фахівців у галузі кібербезпеки; по-друге, постійне підвищення кваліфікації працівників, обмін практичним досвідом між фахівцями різних відомств; по-третє, залучення досвідчених фахівців у галузі кібербезпеки для розв'язання конкретних завдань та передачі знань та практичного досвіду; по-четверте, формування культури безпеки в організаціях та здійснення навчання, тренінгів персоналу щодо правил та процедур безпеки в кіберпросторі; по-п'яте, здійснення постійного

моніторингу і аналізу потреб у кадровому забезпеченні та розробка стратегій покращення кадрової політики для ефективної протидії кіберзлочинності.

Ключові слова: взаємодія, протидія, кіберзлочинність, суб'єкт, механізм, адміністративно-правове регулювання, принципи, адміністративно-правовий статус, форми, методи, міжнародний досвід, вдосконалення, адміністративне законодавство.

SUMMARY

Kabysh O. O. Administrative and legal principles of interaction of subjects of cybercrime counteraction. − *Qualification scientific work on the rights of the manuscript.*

Thesis for obtaining a scientific degree of Candidate of Juridical Science, specialty 12.00.07 «Administrative Law and Procedure; Financial Law; Information Law». – Scientific Institute of Public Law, Scientific Institute of Public Law, Kyiv, 2024.

The thesis is devoted to clarifying the essence and peculiarities of the administrative and legal framework for interaction of cybercrime counteraction entities, as well as the development of proposals and recommendations aimed at improving administrative legislation in the relevant field.

Attention is focused on the fact that the lack of a single formulated comprehensive vision of the nature, content, features of the organization, directions of implementation and other aspects of legal regulation of the interaction of subjects in the fight against cybercrime complicates the development of its new concept and the determination of ways of improvement. At the same time, it is emphasized that it is most appropriate to solve the relevant problems in the context of the administrative field of law, because it is the norms of this field that regulate the activities of the relevant subjects, their legal status, the purpose and tasks of the activity, and thus the principles of interaction between the subjects of countering cybercrime are determined.

It is established that countering cybercrime is a complex activity that is carried out by specially authorized entities and is aimed at the implementation of measures and procedures for the prevention, detection and termination of the actions of individuals and groups that contain signs of crimes in the information sphere, as well as factors that contribute to their commission. Combating cybercrime involves combining the efforts of various state authorities and their capabilities to implement the specified set of measures and procedures.

It is summarized that the interaction of actors in the fight against cybercrime is a model of social relations regulated by the norms of administrative law, which provides for close informational and organizational cooperation, pooling of resources, implementation of joint measures, as well as the division of responsibility in the process of carrying out state-significant activities in the direction of counteraction and prevention of socially dangerous acts that make up the structure of cybercrime.

It is proven that today the state of administrative and legal regulation of the interaction of actors in combating cybercrime can be assessed ambiguously. Thus, on the one hand, there is a broad regulatory framework aimed at regulating social relations in the relevant sphere, and on the other hand, the current legislation has a number of gaps and shortcomings, which should include: the actual lack of effective and coordinated mechanisms for the interaction of specially authorized subjects in the relevant field; uncertainty of the forms and methods of implementation of the researched joint activity; etc.

It is found that the mechanism of administrative and legal regulation of interaction of subjects of counteraction to cybercrime is best interpreted as a formalized system of special, interacting and interdependent legal elements which establish the material and procedural principles of law's influence on social and legal relations arising in the field of joint activities of subjects authorized to detect, suppress and prevent cybercrime. The following key elements of this mechanism are singled out and characterized: principles of law; norms of administrative law; normative legal acts; administrative legal relations.

It is established that the principles represent a set of initial principles, fundamental, dissolved in administrative and legal normative acts, stable, universally binding ideas that determine the purpose, vectors, goals and features of the legal regulation of social and legal relations that arise in the context of the interaction of authorized sub objects of combating cybercrime. These principles include the following principles: the principle of legality, the principle of combination of goals, the principle of certainty of the subject

composition, the principle of coordination and control, the principle of planning, the principle of scientificity and the principle of sufficiency.

It is noted that the administrative and legal status of cybercrime counteraction entities in Ukraine is a set of elements defined by administrative law provisions which, in their unity, determine the position and role of cybercrime counteraction entities in the public and legal relations arising in the course of their joint activities in the relevant area. The elements of the administrative and legal status of the relevant entities include: competence, authority, guarantees of activity and legal responsibility. A meaningful description is provided for each of the outlined elements.

It is proposed that the forms of interaction of cybercrime counteraction actors should be understood as an external expression of joint, mutually coordinated practical activities of specially authorized public authorities and their officials aimed at achieving a single goal - counteraction and prevention of offenses and criminal acts which occur in cyberspace or with the use of computer technologies and networks. It is noted that the scientific literature has not formed a unified approach to the list of relevant forms, and therefore, the latter are proposed to be divided into two groups 1) regulatory and legal forms: rulemaking; administrative contract; law enforcement; 2) organizational and managerial forms: preparation and implementation of joint activities; creation of joint working groups; administrative supervision; public education.

It is stated that persuasion and coercion are two inextricably linked methods of interaction between the subjects of countering cybercrime. Thus, while persuasion is aimed at ensuring that the participants in the interaction have a conscious attitude to their duties through positive motivation and the creation of appropriate internal conviction, coercion involves the use of legal or administrative pressure to achieve specific goals in the field of cybersecurity and countering cybercrime.

It is summarized that today the world has developed quite effective approaches to countering cybercrime, however, they have not become a panacea

in order to completely minimize the risks of this negative phenomenon. The author's vision is offered as to which positive experience of the leading countries should be used by the domestic legislator in the process of improving the interaction of actors in the fight against cybercrime.

Attention is focused on the fact that the adoption of the "Cyber Security Strategy of Ukraine" in 2021 made a significant contribution to the development of the field of combating and preventing cybercrime. However, it was mainly aimed at overcoming problems that existed even before the start of a full-scale invasion. At the same time, with the beginning of the war, the cybercrime prevention system in our country was unable to fully respond to existing challenges and threats. Therefore, despite its relative novelty, this legal act is quite outdated.

In order to improve the administrative and legal regulation of the interaction of cybercrime combating entities, it is proposed: 1) to expand the range of entities that implement activities in the field of cybercrime combating, in connection with which it is necessary to make additions to paragraph 4 of Article 5 of the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine", as well as meaningfully consolidate the administrative and legal status of the relevant bodies; 2) to supplement Article 2 of the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" with the principle of cooperation between actors in the fight against cybercrime, because no state authority can solve existing problems in the relevant field on its own; 3) in the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" to define the types of cybercrimes, which in turn will create a basis for working out the directions of interaction of subjects to combat cybercrime; 4) to develop and adopt a separate legislative act "On the Basis of Interaction Between Subjects of Counteraction and Prevention of Cybercrime".

It is proven that the improvement of the administrative and legal regulation of the interaction of cybercrime countermeasures is practically impossible without improving the organizational foundations of the relevant

activities. In this context, it is proposed to: 1) improve the staffing system of cybercrime countermeasures; 2) improve the system of information provision of interaction subjects; 3) review the approach to financial and logistical support of the cooperation of actors in the fight against cybercrime.

It is established that the professionalism of the staff directly depends on how each state authority will perform the functions assigned to it in the field of combating cybercrime, and therefore the effectiveness of their joint activities. It is emphasized that the improvement of human resources in terms of the presented problems should include: firstly, the creation of a system of professional training of specialists in the field of cyber security; secondly, constant improvement of the qualifications of employees, exchange of practical experience between specialists of different departments; thirdly, involving experienced specialists in the field of cyber security to solve specific tasks and transfer knowledge and practical experience; fourthly, the formation of a security culture in organizations and the implementation of education and training of personnel regarding the rules and procedures of security in cyberspace; fifth, the implementation of constant monitoring and analysis of human resources needs and the development of strategies for improving the human resources policy for effective countermeasures against cybercrime.

Keywords: interaction, counteraction, cybercrime, subject, mechanism, administrative and legal regulation, principles, administrative and legal status, forms, methods, international experience, improvement, administrative legislation.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Кабиш О.О. Стан дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Держава та регіони. Серія Право.* 2021. № 4(74). С. 205–209.

2. Кабиш О.О. Сутність та зміст механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Юридична наука.* 2020. № 8. С. 185–189.

3. Кабиш О. Особливості взаємодії суб'єктів протидії кіберзлочинності. *KELM*. 2022. № 7(51). С. 250–254.

4. Кабиш О.О. Сучасний стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Науковий вісник публічного та приватного права.* 2023. Вип. 4. С. 113–118.

5. Kabysh, O.O. Administrative and legal status of the subjects of interaction in the field of combating cybercrime. *Entrepreneurship, Economy and Law.* 2023. № 9. pp. 101–106.

які засвідчують апробацію матеріалів дисертації:

6. Кабиш О.О. До характеристики принципів адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Виклики сучасності та наукові підходи до їх вирішення:* матеріали міжнародної науково-практичної конференції (Київ, 12–13 серпня 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 42–45.

7. Кабиш О.О. До проблеми визначення поняття протидії кіберзлочинності. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення:* матеріали міжнародної науково-практичної конференції (Київ, 22–23 вересня 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 37–39.

8. Кабиш О.О. Сутність та зміст координації та контролю, як принципів взаємодії суб’єктів протидії кіберзлочинності. *Проблемні питання юридичної науки в контексті реформування правової системи України:* матеріали міжнародної науково-практичної конференції (Київ, 19–20 жовтня 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 21–23.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Вже протягом багатьох століть науково-технічний прогрес є однією із ключових ідей та, водночас, цілей розвитку цивілізованого суспільства. Разом із тим, покращення інформаційних систем та технологій, яке неупинно продовжується в останні декілька десятиліть, не тільки позитивно впливає на державу та суспільство. На сьогоднішній день інформаційні технології також активно використовуються як інструмент скоєння злочинів, які вчиняються за допомогою комп'ютерів, планшетів, платіжних терміналів та інших подібних засобів, а також пов'язані із протиправним створенням, зберіганням, обробкою даних, що належать органам державної влади, а також іншим юридичним та/або фізичним особам, з метою отримання неправомірної вигоди. Особливо гостро ця проблема стоїть сьогодні, адже окрім кіберзлочинності, Україна кожного дня зіштовхується з великою кількістю кібератак від російської федерації, а відтак стала своєрідним плацдармом для тестування та використання кіберзброї.

Не можна не відмітити, що протидія кіберзлочинності є складним та багатоаспектним явищем, яке вимагає здійснення професійної діяльності цілого ряду спеціально уповноважених суб'єктів. При цьому справедливим буде говорити й про те, що жодна державна інституція не може самостійно вирішувати всі проблемні питання, пов'язані із протидією кіберзлочинності, а відтак, необхідним та важливим є створення належних умов для ефективної та результативної взаємодії органів державної влади та їх посадових осіб у відповідній сфері.

Зв'язок теми дисертації із сучасними дослідженнями. Варто відзначити, що окремі проблемні питання пов'язані із протидією кіберзлочинності у своїх наукових працях розглядали: Д.С. Азаров, С.А. Буяджи, І.І. Васильковський, А.В. Войциховський, В.Б. Дзюндзюк, Б.В. Дзюндзюк, В.П. Дулепа, О.М. Жеребець, О.О. Загуменний,

О.Ю. Іванченко, О.О. Йона, Н.Ф. Казакова, Є.В. Котух, М.О. Кравцова, П.Є. Лавренко, В.В. Марков, Є.В. Петров, І.В. Сажнев, І.Б. Тацишин, В.О. Тімашов, Г.В. Форос, Г.М. Чернишов, М.Ю. Якимчук, М.Ю. Яцишин та багато інших. Втім, незважаючи на суттєвий теоретичний доробок вказаних вище науковців, справедливим буде зауважити, що на сьогоднішній день в юридичній літературі недостатньо опрацьованим є дослідження питання адміністративно-правових засад взаємодії суб'єктів протидії кіберзлочинності, що, як вбачається, є суттєвою прогалиною як на теоретичному, так і на практичному рівнях.

Отже наявність низки теоретичних та практичних проблем, пов'язаних із взаємодією суб'єктів протидії кіберзлочинності, а також відсутність комплексних теоретичних досліджень, присвячених даній проблематиці, обумовлюють актуальність та своєчасність представленої дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження узгоджується з основними положеннями: «Стратегії кібербезпеки України», що була введена в дію Указом Президента України від 26 серпня 2021 р. № 447/2021; «Стратегії забезпечення державної безпеки», затвердженої Указом Президента України від 16 лютого 2022 р. №56/2022; Стратегії інформаційної безпеки на період до 2025 року», затвердженої розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. Дисертацію виконано відповідно до плану науково-дослідної роботи Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0120U105390).

Мета і завдання дослідження. *Мета* дисертаційної роботи полягає у тому, щоб на основі аналізу наукових поглядів вчених, норм чинного законодавства України та практики його реалізації, з'ясувати сутність та особливості адміністративно-правових засад взаємодії суб'єктів протидії

кіберзлочинності, а також, спираючись на позитивний вітчизняний та зарубіжний досвід, встановити напрями вдосконалення чинного законодавства у відповідній сфері.

Для досягнення зазначеної мети в дисертаційному дослідженні необхідно було вирішити такі основні *завдання*:

– оцінити стан дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності;

– визначити поняття та розкрити особливості взаємодії суб'єктів протидії кіберзлочинності;

– схарактеризувати сучасний стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності;

– з'ясувати сутність поняття та окреслити структуру механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності;

– встановити коло принципів адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності;

– надати характеристику адміністративно-правового статусу суб'єктів взаємодії у сфері протидії кіберзлочинності;

– виокремити форми та методи взаємодії суб'єктів протидії кіберзлочинності;

– узагальнити міжнародний досвід адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності та опрацювати можливості його використання в Україні;

– запропонувати напрямки вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Об'єктом дослідження є суспільні відносини, що виникають під час взаємодії суб'єктів протидії кіберзлочинності.

Предметом дослідження є адміністративно-правові засади взаємодії суб'єктів протидії кіберзлочинності.

Методи дослідження. В основу дисертаційної роботи покладено загальні та спеціальні методи наукового пізнання. Так, використання *аналітичного* методу дозволило надати оцінку стану дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності (підрозділ 1.1). Для того, щоб: визначити поняття та розкрити особливості взаємодії суб'єктів протидії кіберзлочинності (підрозділ 1.2); а також з'ясувати сутність поняття та розкрити структуру механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності (підрозділ 2.1) було використано *структурно-логічний* метод. Метод *документального аналізу* використовувався з метою характеристики сучасного стану адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності (підрозділ 1.3); а також характеристики адміністративно-правового статусу суб'єктів взаємодії у сфері протидії кіберзлочинності (підрозділ 2.3). *Структурно-логічний* та *системно-функціональний* методи були використані для того, щоб: встановити коло принципів адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності (підрозділ 2.2) та виокремити форми та методи взаємодії суб'єктів протидії кіберзлочинності (підрозділ 2.4). З метою узагальнення міжнародного досвіду адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності та опрацювання можливостей його використання в Україні (підрозділ 3.1) було використано *порівняльно-правовий* метод. Для того, щоб запропонувати напрямки вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності (підрозділ 3.2) було застосовано методи *моделювання* та *прогнозування*.

Науково-теоретичне підґрунтя дослідження становлять праці фахівців із галузей адміністративного та інформаційного права. Окрім того, в процесі підготовки дисертації було використано напрацювання

фахівців з інших галузевих дисциплін, як то: теорії держави і права, теорії управління, соціології, психології, філософії тощо.

Нормативною основою дослідження є Конституція України, міжнародні акти (ратифіковані у встановленому законом порядку), а також низка законодавчих та підзаконних актів, в яких закріплюється нормативно-правова основа взаємодії суб'єктів протидії кіберзлочинності в Україні.

Інформаційну та емпіричну основу дослідження становлять узагальнення практики діяльності суб'єктів протидії кіберзлочинності, періодичні видання, аналітичні статті, довідкові видання, статистичні матеріали.

Наукова новизна отриманих результатів визначається тим, що підготовлене дисертаційне дослідження є однією із перших спроб після повномасштабного вторгнення росії в Україну, комплексно, на монографічному рівні, з'ясувати сутність та особливості адміністративно-правових засад взаємодії суб'єктів протидії кіберзлочинності, на основі чого розробити пропозиції та рекомендації спрямовані на вдосконалення норм чинного законодавства у відповідній сфері. У результаті проведеного дослідження сформульовано низку нових наукових положень та висновків, запропонованих особисто здобувачем. Основні з них такі:

вперше:

– виділено форми взаємодії суб'єктів протидії кіберзлочинності, які в свою чергу запропоновано поділити на дві групи: 1) нормативно-правові форми: нормотворчість; адміністративний договір; правозастосування; та 2) організаційно-управлінські форми: підготовка і реалізація спільних заходів; створення спільних робочих груп; адміністративний нагляд; просвітницька робота з громадськістю;

– доведено, що в Україні на прикладі провідних країн Європи та світу, вбачається необхідним розширити співробітництво між державою (в особі її уповноважених органів) та приватним сектором у сфері протидії та

запобігання кіберзлочинності, що в свою чергу дозволить: по-перше, більш оперативно виявляти правопорушення, пов'язані із використанням інформаційних систем; по-друге, залучати фахівців, здатних більш якісно та оперативно реалізовувати діяльність у напрямку протидії та запобігання кіберзлочинності;

– акцентовано увагу на необхідності розробки та прийняття нової «Стратегії кібербезпеки України», яка повинна враховувати не тільки наявний практичний досвід та існуючі загрози у кіберпросторі, а й: по-перше, окреслити чинники, які обумовлюють виникнення та розвиток кіберзлочинності; по-друге, виокремити шляхи вдосконалення діяльності спеціально уповноважених суб'єктів у напрямку протидії кіберзлочинам; по-третє, закріпити коло суб'єктів, що здійснюють діяльність у сфері протидії кіберзлочинності, а також перспективні напрямки, рівні, форми та методи їх взаємодії;

удосконалено:

– обґрунтування наукової думки про те, що незважаючи на суттєву зацікавленість з боку фахівців різних галузей права, на сьогоднішній день проблема правового регулювання взаємодії суб'єктів протидії кіберзлочинності є недостатньо опрацьованою, зокрема з точки зору науки адміністративного права. З огляду на це наголошено, що вирішувати проблеми у відповідній сфері найбільш доцільно шляхом проведення комплексних теоретичних досліджень, присвячених покращенню саме адміністративного законодавства у цій сфері;

– науковий підхід щодо визначення поняття «механізм адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності», на основі чого виділено ключові ознаки даної наукової категорії: 1) є динамічним явищем, яка показує реальне функціонування права; 2) є складним системним утворенням, адже складається зі спеціальних юридичних елементів, що взаємодіють одне з одним в процесі правового регулювання та виражається крізь систему форм, що мають

адміністративний характер; 3) процес реалізації даного механізму носить формалізований характер, оскільки порядок та особливості його дії нормативно визначені;

– теоретичний підхід щодо визначення поняття «адміністративно-правового статусу суб'єктів взаємодії у сфері протидії кіберзлочинності», до елементів якого віднесено: компетенцію, повноваження, гарантії діяльності та юридичну відповідальність;

дістали подальшого розвитку:

– твердження про те, що протидія кіберзлочинності передбачає об'єднання зусиль різних органів державної влади та являє собою регламентовану нормами адміністративного права модель суспільних відносин, яка передбачає тісну інформаційно-організаційну співпрацю, об'єднання ресурсів, реалізацію спільних заходів, а також поділ відповідальності у процесі здійснення державно-значущої діяльності у напрямку протидії та запобігання суспільно-небезпечним діянням, які складають структуру кіберзлочинності;

– твердження, що ключове місце в системі правових засад взаємодії суб'єктів протидії кіберзлочинності відводиться саме нормам адміністративного права, адже саме за їх допомогою визначаються: організаційно-управлінські аспекти взаємодії; порядок реалізації спільної діяльності уповноважених суб'єктів, а також їх ієрархічне підпорядкування; правовий статус суб'єктів відповідних правовідносин; цілі; завдання та функції співпраці; форми та методи взаємодії тощо;

– узагальнення переліку принципів взаємодії суб'єктів протидії кіберзлочинності, до яких запропоновано віднести таки: принцип законності, принцип поєднання цілей, принцип визначеності суб'єктного складу, принцип координації та контролю, принцип плановості, принцип науковості та принцип достатності.

Практичне значення отриманих результатів полягає в тому, що викладені в дисертації висновки і пропозиції можуть бути використані у:

– *науково-дослідній сфері* – для подальшого розроблення теоретичних та практичних проблем, пов'язаних із взаємодією суб'єктів протидії кіберзлочинності (акт впровадження Науково-дослідного інституту публічного права);

– *правотворчості* – як основа для вдосконалення діючих та для розробки нових нормативно-правових актів різної юридичної сили, норми яких спрямовані на регулювання взаємодії суб'єктів протидії кіберзлочинності;

– *правозастосовній діяльності* – з метою вдосконалення практичної складової використання адміністративно-правових форм та методів взаємодії суб'єктів протидії кіберзлочинності;

– *освітньому процесі* – під час підготовки підручників, навчальних посібників, лекційних та науково-методичних матеріалів з дисциплін «Адміністративне право»; «Інформаційне право» та «Правоохоронна діяльність» (акт впровадження Науково-дослідного інституту публічного права).

Апробація матеріалів дисертації. Підсумки розроблення проблеми в цілому, окремих її аспектів, одержані узагальнення і висновки було оприлюднено на міжнародних науково-практичних конференціях, семінарах, круглих столах, зокрема: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 12–13 серпня 2020 р.); «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 22–23 вересня 2021 р.); «Проблемні питання юридичної науки в контексті реформування правової системи України» (м. Київ, 19–20 жовтня 2022 р.)

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації становить 207 сторінок. Список використаних джерел включає 230 найменувань та розміщений на 24 сторінках.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

1.1. Стан дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Якщо у XX столітті цифрові технології лише почали своє зародження та поширення на всі сфери життєдіяльності людства, то у XXI кожен з нас не може уявити свій день без використання електронного гаджету підключеного до всесвітньої мережі Інтернет. Дана ситуація має дві сторони. З одного боку, технології суттєво полегшують життя суспільства, адже надають більш широкі можливості у процесі віддаленої комунікації різноманітних суб'єктів, соціального управління, автоматизації певних функціональних процесів виробничого характеру тощо. Разом із тим, на тлі розвитку комп'ютерів та цифрової революції в цілому, з'являються окремі особи та групи, що намагаються за допомогою новітніх технічних інструментів порушити права та свободи інших людей шляхом: незаконного заволодіння їх особистими даними; викрадення грошових коштів, які знаходяться на електронних рахунках; втягнення людей у різноманітні шахрайські схеми, наприклад, пов'язані із продажом неіснуючих товарів і таке інше. Все перелічене в сукупності сформувало серйозну проблему кіберзлочинності, яка постійно перебуває у полі зору правоохоронних органів та міжнародної спільноти.

Кіберзлочинність як самостійна сфера суспільних відносин та деструктивний соціальний інститут, неодноразово ставали предметом комплексних вчених робіт. Наприклад, В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко, М.Я. Швець, Р.А. Калюжний та П.В. Мельник розглянули проблему кіберзлочинів через призму інформаційного права та механізмів забезпечення безпеки інформації. В роботі науковців наголошується, що

масове впровадження нових технічних засобів, на основі яких здійснюється інформатизація у всьому світі, робить прозорими державні кордони і формує нові геополітичні парадигми у розумінні глобальних соці-технічних систем. Міжнародна інформаційна сфера стає не тільки однією з важливих сфер співробітництва, а й середовищем конкуренції між окремими особами, державами, міждержавними політичними та економічними угрупованнями. Електронно-комунікаційна інфраструктура, як і інші інформаційні ресурси, стає об'єктом міждержавної боротьби за світове лідерство або об'єктом недобросовісної конкуренції у підприємницькій діяльності чи інших суспільних інформаційних відносин. На думку вчених, ключове значення у механізмі організації безпеки інформації становить організація законного використання комп’ютерних систем, що попередить користування ними не за цільовим призначенням та порушення за допомогою них існуючих соціальних та політичних засад. Враховуючи викладене вчені пишуть: «Загальний аналіз проблем організовування захисту інформації в автоматизованих комп'ютерних системах дає можливість визначити три агреговані організаційні моделі заходів: 1) організація запобіжних заходів; 2) організація блокування (протидії) реальним загрозам, що реалізуються; 3) організація подолання наслідків загроз, які не вдалося блокувати або запобігти їм». Крім того науковці доводять, що в основі організації захисту інформації та протидії порушенням, знаходиться тісна модель співпраці одночасно представників як публічної влади, так і приватного сектору і, навіть, окремих громадян» [150].

Про глобальний характер кіберзлочинності наголосили у своїй роботі А.В. Боровик та І.М. Копотун. Вчені відзначили, що «сьогодні важливу роль в соціальному й економічному розвитку багатьох країн світу відіграють кібернетичний та інформаційний простори, а також інформаційне суспільство, яке сформувалося внаслідок стрімкого розвитку науково-технічного прогресу та комп'ютеризації. Проте існування

глобального інформаційного простору призвело до появи інформаційних загроз. Отже, тема кібербезпеки надзвичайно актуальна і відкрита, особливо для України, враховуючи сучасний стан держави. Кібербезпекою є стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також вчасне виявлення, запобігання та нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним або національним інтересам» - пишуть вчені. Далі в роботі автори запропонували до основних напрямів забезпечення кібербезпеки України віднести: 1) розвиток інформаційної інфраструктури держави, гарантування безпечного функціонування об'єктів критичної інформаційної інфраструктури; 2) розвиток міжнародного співробітництва у сфері кібербезпеки; зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з проявами кіберзлочинності та кібертероризму; 3) забезпечення ефективного застосування Збройних сил України для адекватної відповіді реальним та потенційним кіберзагрозам національному сегменту кіберпростору; 4) розвиток пріоритетних напрямів науки й техніки як основи створення високих інформаційних технологій; підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників; 5) адаптацію законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення стійкості до кібератак, спроможності держави ефективніше захищати національні інтереси в кіберпросторі; 6) забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту

інформації, захисту персональних даних; підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі [31, с.9].

Різноманітні аспекти змісту кіберзлочинності, а також взаємодії суб'єктів протидії цьому негативному явищу розкривались в рамках монографій та дисертацій у царині різних юридичний галузей. Так, Д.С. Азаров присвятив своє кримінально-правове дослідження встановленню сутності злочинів у сфері комп'ютерної інформації. У його монографії досліджуються проблеми кримінальної відповідальності за злочини у сфері комп'ютерної інформації, пов'язані зі ступенем і характером суспільної небезпеки цих посягань та їх міжнародним характером, ознаками складів цих злочинів, а також санкціями, передбаченими за їх вчинення. Узагальнюється зарубіжний та міжнародний досвід кримінально-правової протидії «комп'ютерним» злочинам. Вченим розроблено доктринальна модель системи норм про кримінальну відповідальність за аналізовані злочини, для втілення якої пропонується проект Закону України «Про внесення змін і доповнень до Кримінального кодексу України щодо відповідальності за злочини у сфері комп'ютерної інформації» [6].

В тій же юридичній галузі проводила своє дослідження І.М. Леган, яка розглянула теоретико-правові засади міжнародного співробітництва щодо запобігання та протидії транснаціональній злочинності. В дисертації вчена наголосила, що транснаціональна злочинність є найбільш скоординованою, раціональною та професійною частиною сучасного кримінального середовища, характерними ознаками якої є прагнення мінімізувати потенційні ризики та максимізувати при цьому прибутки, вдаючись за допомогою до висококваліфікованих фахівців і використовуючи найсучасніші технології. У зв'язку з підвищеною суспільною небезпекою транснаціональної злочинності й особливої складності протидії та запобігання їй, пріоритетного значення для України набуває розробка системного й оптимального механізму реалізації заходів

на шляху сприяння міжнародному співробітництву щодо запобігання та протидії транснаціональній злочинності. Науковець відмітила, що даний різновид злочинності реалізується за допомогою широкого кола інструментів, серед яких цифрові та інформаційні технології і, таким чином, включає в себе, як органічну частину, кіберзлочини. Метою дисертаційного дослідження вчена визначила здійснення наукового аналізу та обґрунтування шляхів вирішення комплексної наукової проблеми теоретико-правових засад міжнародного співробітництва щодо запобігання та протидії транснаціональній злочинності шляхом формування цілісної наукової концепції та розроблення комплексу практичних рекомендацій та пропозицій, спрямованих на удосконалення правозастосовної практики та чинного законодавства [127, с.3-4]. Для досягнення поставленої мети вирішувались такі наукові та практичні задачі: 1) оцінити історико-правові передумови становлення та розвитку міжнародного співробітництва щодо запобігання та протидії транснаціональній злочинності; 2) обґрунтувати теоретико-методологічні основи та кримінологічні підходи до визначення поняття «транснаціональна злочинність», її різновиди, прояви та детермінанти; 3) формалізувати і систематизувати основні напрями, форми та види міжнародного співробітництва щодо запобігання та протидії транснаціональній злочинності; 4) надати кримінологічну характеристику організованих злочинних груп як суб'єктів вчинення транснаціональних злочинів; 5) здійснити оцінку сучасного стану та тенденції кримінологічних показників транснаціональної злочинності в Україні та світі; 6) розглянути діяльність ООН та організації взаємодії міжнародних правоохоронних організацій щодо запобігання і протидії транснаціональній злочинності; 7) розкрити роль і значення Інтерполу як центру міжнародного співробітництва держав щодо запобігання та протидії транснаціональним злочинам; 8) визначити роль Європолу в міжнародному співробітництві держав щодо запобігання та протидії транснаціональній злочинності; 9) оцінити особливості міжнародного

співробітництва та кримінологічні засади запобігання і протидії кіберзлочинності та кібертероризму; 10) виокремити принципи міжнародного співробітництва щодо запобігання та протидії транснаціональній злочинності; 11) провести аналіз національного законодавства й участі України у формуванні міжнародно-правового механізму протидії транснаціональній злочинності; 12) розробити дієвий та ефективний правовий механізм удосконалення міжнародного співробітництва щодо запобігання та протидії транснаціональній злочинності [127, с.3-4].

З точки зору кримінального процесу та криміналістики протидію кіберзлочинності та взаємодію в рамках даного питання дослідила Л.В. Борисова у дисертації: «Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження». Мета дослідження полягала в тому, щоб на основі сучасних концепцій науки криміналістики розробити тактичні й процесуальні основи криміналістичного дослідження транснаціональних комп'ютерних злочинів. Для досягнення поставленої мети було сформульовано такі взаємопов'язані між собою завдання: 1) розкрити поняття комп'ютерної інформації як предмета правового захисту та визначити криміналістично значущі вихідні дані про транснаціональні комп'ютерні злочини; 2) визначити зміст поняття «транснаціональний комп'ютерний злочин»; 3) розкрити сутність основних елементів криміналістичної характеристики транснаціональних комп'ютерних злочинів та взаємозв'язків між ними; 4) типізувати слідчі ситуації початкового етапу розслідування транснаціональних комп'ютерних злочинів; 5) розкрити особливості виявлення і закріплення слідів транснаціональних комп'ютерних злочинів; 6) охарактеризувати місце та особливості застосування спеціальних знань у ході розслідування транснаціональних комп'ютерних злочинів; 7) розробити систему рекомендацій, спрямованих на запобігання, протидії та розслідування транснаціональних комп'ютерних злочинів [30, с.9].

В тій же галузі наукових знань, але у більш специфічному напряму протидію кіберзлочинності розглянув Б.Б. Теплицький. В своїй дисертації присвяченій техніко-криміналістичному забезпеченню розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку автор вказав, що аналіз криміногенної ситуації в Україні та практики органів досудового розслідування підтверджує тенденцію до збільшення кількості випадків кримінальних правопорушень, пов'язаних з обігом комп'ютерної інформації, а також діянь, у яких комп'ютерні інформаційні системи є засобами та знаряддями їх учинення або ж використовуються для приховування факту і слідів злочинної діяльності, а також спрямування зусиль правоохоронців на хибні об'єкти. Процеси глобальної інформатизації безпосередньо впливають на криміногенну ситуацію, обумовлюють нові способи і технології злочинних посягань в інформаційному простості й середовищі комп'ютерних мереж. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, а також мереж електрозв'язку здебільшого високолатентні. Поряд з відсутністю очевидної слідової картини й традиційного «місця події» доволі ускладненим є збирання доказів, що зумовлено як застосуванням засобів віддаленого доступу, так і специфічним, нематеріальним, елементом обстановки – кібернетичним простором. Злочинній діяльності відповідного спрямування притаманні переважно системний, професійний і груповий характер, наявність у правопорушників спеціальних знань, умінь і навичок у різних галузях науки і техніки (електроніка, електротехніка, програмування, телекомунікації, зв'язок тощо). Зважаючи на викладене метою дисертації вчений визначив розроблення теоретичних положень та науково обґрунтованих рекомендацій щодо техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем

та комп'ютерних мереж і мереж електрозв'язку. Для реалізації визначеної мети науковець виділив такі обов'язкові завдання, як: а) розкрити особливості техніко-криміналістичного забезпечення проведення окремих слідчих (розшукових) дій у кримінальних проваджень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; б) визначити специфіку та запропонувати рекомендації з удосконалення техніко-криміналістичного забезпечення проведення окремих негласних слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; в) розкрити особливості призначення найбільш типових видів судових експертиз при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; г) проаналізувати та розкрити особливості взаємодії суб'єктів техніко-криміналістичного забезпечення при розслідуванні вказаної категорії злочинів тощо [208, с.9].

Міжнародно-правову характеристику взаємодії у сфері протидії кіберзлочинності надала М.Ю. Яцишин. Вчена довела, що повноцінне функціонування суспільства в сучасних умовах значною мірою залежить від інформаційно-комунікаційних технологій (далі – ІКТ). Автор констатувала: «Незважаючи на позитивні досягнення, пов'язані із впровадженням ІКТ, необхідно констатувати, що кіберпростір значним чином криміналізовано. Статистичні дані щодо кількості кіберзлочинів у світі постійно зростають, їх наслідки стають дедалі масштабнішими, що вказує на необхідність удосконалення існуючої системи протидії кіберзлочинності. Враховуючи особливу транскордонну природу цього виду злочинів, дієвість національних механізмів боротьби з кіберзлочинністю залежить, насамперед, від ефективності міжнародно-правового співробітництва держав у визначеній сфері». Через це, метою її дисертації став комплексний аналіз міжнародно-правового співробітництва

у сфері боротьби з кіберзлочинністю, узагальнення основних засад універсальної концепції кіберзлочинності, а також визначення шляхів її розвитку [228, с.2]. Досягнення поставленої мети здійснювалось шляхом вирішення таких основних завдань: 1) розкрити сутність і дати визначення поняття «кіберзлочин» через аналіз джерел міжнародного права, виділити його характерні ознаки; 2) дослідити та узагальнити сучасні підходи до класифікації кіберзлочинів; 3) проаналізувати генезис та розвиток інституту міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю; 4) розкрити зміст міжнародно-правової заборони використання сили у кіберпросторі; 5) дослідити напрями удосконалення матеріальних норм інституту міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю; 6) проаналізувати міжнародно-правові норми виявлення та розслідування кіберзлочинів; 7) здійснити аналіз правових та інституційних основ протидії кіберзлочинності в Україні; 8) дати правову оцінку кібератакам на території України під час агресії Російської Федерації [228, с.2].

Цікавою є праця С.А. Буяджи, який розглянув правове регулювання боротьби з кіберзлочинністю у теоретико-правовому аспекті. Його робота націлювалась на розробку концептуального розуміння специфіки генезису та тенденцій розвитку і механізму правового регулювання боротьби із кіберзлочинністю. Для досягнення зазначеної мети вчений поставив такі задачі: 1) визначити правову природу боротьби із кіберзлочинністю; 2) дослідити генезис правового регулювання боротьби із кіберзлочинністю; 3) охарактеризувати структуру механізму правового регулювання боротьби з кіберзлочинністю; 4) розкрити та конкретизувати досвід міжнародно-правового регулювання боротьби з кіберзлочинністю; 5) з’ясувати специфіку національного правового регулювання боротьби з кіберзлочинністю; 6) виокремити тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні; 7) виділити особливості правового регулювання боротьби з кіберзлочинністю у

зарубіжних країнах. Окрім цього, в дисертації науковець детально проаналізував особливості міжнародного співробітництва в сфері боротьби з кіберзлочинністю, визначивши, що остання здійснюється в наступних напрямках: 1) прийняття міжнародно-правових механізмів регулювання та взаємодії правоохоронних органів у питаннях боротьби із кіберзлочинністю; 2) гармонізація національних законодавств із міжнародним законодавством; 3) безпосередня співпраця, як офіційна, так і неофіційна; 4) узгодження повноважень при здійсненні боротьби із кіберзлочинністю [34].

Варто наголосити, що переважна більшість наукових опрацювань питання взаємодії суб'єктів протидії кіберзлочинності та правового регулювання даної проблеми, проводились у форматі наукових статей. Багато подібних робіт написано теоретиками міжнародного права. Так, А.В. Войціховський відмічає: широке використання сучасних інформаційних технологій у державних і недержавних структурах, а також у суспільстві в цілому висуває вирішення проблем інформаційної безпеки в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Актуальність даної теми статті обумовлена саме тим, що зростання інформаційних технологій зумовлює не тільки прогресивні зміни в економіці, але й негативні тенденції розвитку злочинного світу, появу нових форм і видів злочинних посягань. Це виявляється в тім, що зловмисники активно використовують у своїй злочинній діяльності новітні комп'ютерні засоби і нові інформаційні технології. Розповсюдження комп'ютерних вірусів і дитячої порнографії, шахрайство з пластиковими платіжними картками, розкрадання грошових коштів з банківських рахунків, комп'ютерний тероризм – це далеко не повний перелік злочинів, сукупність яких отримала широковживану назву «кіберзлочинність». Метою його статті стало комплексне вивчення

проблем, пов'язаних із міжнародною співпрацею правоохоронних органів у боротьбі з кіберзлочинністю і на базі цього розроблення пропозицій щодо підвищення ефективності протистояння даним злочинам [41, с.107].

В.В. Марковим досліджено особливості злочинів у сфері інформаційно-телекомунікаційних технологій, звертається увага на основні проблеми щодо їх виявлення, розкриття та розслідування. Висвітлено напрямки міжнародної взаємодії у сфері протидії кіберзлочинності, що базуються на міжнародних нормативно-правових актах. Наголошено на необхідності вивчення досвіду зарубіжних країн щодо організації діяльності підрозділів боротьби з кіберзлочинністю. Вченим цілком слушно та змістовно було здійснено аналіз досвіду діяльності поліції Канади в цьому напрямку. Виділено рівні взаємодії оперативних нашої держави з метою оперативного документування злочинів у сфері інформаційно-телекомунікаційних технологій та види їх співробітництва з правоохоронними органами інших держав. В статті науковця зауважено, що удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні має відбуватися з урахуванням національних особливостей на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн [134]. Втім, ряд пропозицій автора носять суто теоретичний характер.

У статті М.Ю. Якимчук розглянуто основні аспекти правового регулювання кіберзлочинності в національному праві через призму міжнародного. Наголошено, що у сучасному світі країни розробляють нові методи боротьби з такими злочинами. Зазначено: «США сформувала так звані «NIST Cyber security Framework» – стандарти з безпеки, які дозволяють виявляти, реагувати і навіть запобігати кіберзлочинам, а також Акт про повідомлення щодо порушення правил безпеки «Notice of Security Breach Act», згідно з яким компанії мають право вільно вибрати для себе спосіб забезпечення приватності своїх систем; Європейський Союз прийняв Директиву щодо мережевої та інформаційної безпеки «NIS

Directive on security of network and information systems», що визначив важливе значення надійності й безпеки мережевих та інформаційних систем для економічної та суспільної діяльності; Україна створила підрозділ «CERT-UA», який у межах своїх повноважень проводить аналіз та накопичення даних про кіберінциденти, веде державний їх реєстр» [227].

У розрізі кримінального права та кримінології написано статтю А.В. Микитчика, яка була присвячена запобігання кіберзлочинності в Україні. В ній вчений довів, що запобігання кіберзлочинності є однією з найбільш актуальних і складних кримінологічних проблем. Висока латентність, зростання числа кіберзлочинів, вдосконалення інформаційних технологій, що створюють нові можливості вчинення злочинів, вимагають кардинально інших підходів запобігання злочинів що вчиняються у віртуальному просторі та створюють загрози для глобальних інформаційних мереж і суспільства в цілому. Проведений вченим аналіз стану і криміногенного комплексу кіберзлочинності дозволив сформулювати висновок про те, що запобігання їй повинно ґрунтуватися на декількох основних підходах, серед яких: а) правовий підхід – пов’язаний з удосконаленням правових механізмів національного та міжнародного законодавства, що передбачає відповідальність за кіберзлочини. Вказаний вище науковець відмічає, що оскільки на сьогоднішній день жодна держава не може захистити себе від кіберпосягань приймаючи правові заходи тільки на національному рівні, вбачається необхідним організація і реалізація комплексної програми запобіганні кіберзлочинності, що включає: гармонізацію кримінального законодавства про кіберзлочини; розробку на міжнародному рівні і імплементацію в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах; міжнародне співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні; дієвий механізм

вирішення юрисдикційних питань в кіберпросторі; б) організаційний підхід – має на меті розробку і запровадження в практику, удосконалених організаційно профілактичних заходів. Перш за все слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій, і перейти до активної розробки інформаційної безпеки на випередження. Необхідно об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян [116, с.138].

Безпосередньо внутрішній сутності проблеми правового регулювання протидії кіберзлочинності присвятив увагу Г.В. Форос. Науковець відмітив, що кіберзлочинність – це реальна глобальна загроза, яка може походити з будь-якої країни світу і виходити за межі конкретної юрисдикції на відміну від багатьох інших традиційних злочинів. Особливу занепокоєність викликає можливість розробки, застосування та розповсюдження інформаційної зброї, виникнення у зв'язку з цим інформаційних війн та кібертероризму, чиї негативні наслідки майже не передбачувані. Організація протидії цьому виду злочинності в Україні складалася тривалий час не досить ефективно що, в першу чергу, пов'язувалось з відсутністю необхідної законодавчої бази. Тому можна констатувати той факт, що раніше зазвичай не приділялося достатньої уваги цьому виду суспільно небезпечних злочинних діянь. І лише після того, коли, матеріальні збитки від вищевказаних діянь досягли таких розмірів, що стали різко виділятися на загальному рівні збитків від загально кримінальної злочинності, прийшов час, коли на цьому новому злочинному явищі зосереджено увагу, зроблено акцент. З огляду на визначене вчений відмітив необхідність комплексного аналізу в правовому та організаційному аспектах найбільш актуальних і важливих питань протидії кіберзлочинам та визначення шляхів удосконалення цієї діяльності [217, с.164].

Отже, спираючись на проведений у даному підрозділі аналіз можемо констатовано, що незважаючи на чималу кількість наукових робіт, чітко сформульованого підходу до розкриття сутності та оцінки правового регулювання взаємодії суб'єктів протидії кіберзлочинності на сьогодні в юридичній літературі досі не сформовано. Поверхнево вказане питання розглядалось в межах багатьох галузевих наук та в рамках більш широких проблематик, присвячених кібербезпеці держави взагалі. Так, представники кримінального права та кримінології акцентують увагу лише на тому, що взаємодія є необхідним організаційним заходом подолання негативного явища кіберзлочинності. В свою чергу представники кримінального процесуального права та криміналістики обмежують свої дослідження виключно рамками існуючих процесуальних механізмів та порядком здійснення відповідних слідчих дій та заходів, вважаючи взаємодію виключно моделлю розвитку процесуальних відносин. Міжнародники переймаються лише світовою співпрацею у сфері боротьби з кіберзлочинами та її юридичним оформленням. Теоретики права розглядають взаємодію у контексті дослідження і розкриття особливостей змісту кіберзлочинності загалом і таке інше. Безумовно, фахівці вказаних вище галузей права зробили вагомий внесок у розвиток даного інституту. Проте, відсутність єдиного сформульованого комплексного бачення природи, змісту, особливостей організації, напрямів здійснення та інших аспектів правового регулювання взаємодії суб'єктів протидії кіберзлочинності, ускладнює вироблення її нової концепції та визначення шляхів удосконалення. При цьому необхідно підкреслити, що вирішувати відповідні проблеми найбільш доцільно в розрізі адміністративної галузі права, адже саме її нормами регулюється діяльність відповідних суб'єктів, їх правовий статус, мета та завдання діяльності, а відтак і визначаються засади взаємодії спеціально уповноважених органів державної влади у галузі протидії кіберзлочинності [78].

1.2. Поняття та особливості взаємодії суб’єктів протидії кіберзлочинності.

Використання сучасних інформаційних технологій у державних і недержавних структурах, а також у суспільстві в цілому, стає однією з ключових складових боротьби з проблемами інформаційної безпеки. Окрім очевидного збитку, завданого можливими випадками незаконного доступу до інформації, її зміною або знищенням, процес інформатизації може стати джерелом загрози для державної безпеки та прав людини. Так, злочинці активно користуються сучасними комп'ютерними засобами та інформаційними технологіями у своїх злочинних діях, зокрема розповсюдження комп'ютерних вірусів, порнографії, шахрайство з використанням пластикових платіжних карток, крадіжки коштів з банківських рахунків та комп'ютерний тероризм. Це лише декілька прикладів кіберзлочинності, яка поширюється і вдосконалюється завдяки новим інструментам і технологіям. А відтак, важливим напрямком діяльності держави є здійснення протидії цьому негативному явищу, що передбачає взаємодію спеціально уповноважених суб’єктів.

З точки зору етимології взаємодія – це взаємний зв’язок між предметами у дії, а також погоджена дія між ким-, чим-небудь. Часто дане слово співвідносять із поняттям «координація», яке походить від лат. «со» – спільно, «ordinatio» – погодження, узгодження, взаємопов’язування, упорядкування [197; 37, с.85; 221, с.161; 17, с.101]. У філософії взаємодія – це відносини, які породжують єдність речей та процесів відчуття. Її також розглядають, як категорію, що відображає вплив одного об’єкта на інший, їх взаємну обумовленість та породження одним об’єктом іншого. Психологія тлумачить взаємодію як взаємне злиття душі та тіла, психічного та фізичного, у військовій науці – узгодження бойових дій військ для досягнення загальної мети [128, с.60]. У соціологічних науках взаємодія – це діяльність людини разом із іншими представниками

соціуму, наприклад: навчається, працює тощо [209, с.450]. Логіка надає наступне розуміння зазначеної категорії: загальна форма зв'язку предметів, явищ, об'єктивної дійсності, а також зв'язків думок, що є відображенням предметів, явищ та їх зв'язків і відносин у свідомості людини [96].

Багато науковців формулювали власні підходи до тлумачення змісту взаємодії. Наприклад, В.М. Дрьомін пише: «Взаємодія – це такий вид зв'язку між явищами, що віддзеркалює їх взаємний вплив один на одного, їхню взаємну детермінацію. Кожна зі взаємодіючих сторін виступає як детермінанта і одночасно як наслідок впливу іншої сторони» [61, с.74]. О.О. Кравченко доводить, що взаємодія – це активна поведінка учасників суспільних відносин, спрямована на певні зміни у сфері інтересів цих учасників чи третьої сторони або на недопущення таких змін. Під взаємозв'язком необхідно розуміти обопільно усвідомлений суб'єктами фактичний стан відносин між ними, за якого вони можуть вчинювати певні дії, що стосуються їх інтересів чи інтересів третьої сторони або утримуватися від певних дій [111, с.28-29]. Згідно із тлумаченням Ю.В. Гаруста, взаємодія проявляється в процесі взаємовпливу і використанні можливостей один одного для досягнення власних цілей. Взаємодія виникає там і тоді, де взаємозв'язок між суб'єктами об'єднаний спільною метою. По-друге, взаємодія полягає не тільки в безперервному впливі один на одного, а також і під час використання взаємодіючими сторонами можливостей один одного для досягнення власних цілей [43, с.138]. На думку В.М. Круглого, взаємодія – це сукупність усіх взаємозв'язків між соціальними суб'єктами; наявність найрізноманітніших стійких, об'єктивно обумовлених та необхідних функціонально залежних, кількісно та якісно в зовнішньому виразі не обмежених форм взаємозв'язку між ними; процес та результат взаємовпливів взаємодіючих сторін [117, с.134; 96, с.17]. Вкрай цікавим є погляд І.М. Мінаєва, який розкрив особливості взаємодії крізь призму структурних зв'язків, що

виникають між її суб'єктами: координаційні структурні зв'язки (горизонтальні) і субординаційні структурні зв'язки (вертикальні). Так, вертикальні зв'язки – в яких один з учасників підпорядкований іншому, тобто даний вид відносин складається між супідрядними суб'єктами, коли один з них наділений повноваженнями впливати на інший, незалежно від волі останнього. Горизонтальні зв'язки складаються між учасниками, які не підпорядковані один одному (між не супідрядними суб'єктами) [17, с.102]. В.В. Чумак, провівши аналіз різних наукових підходів, констатував, що, як правило, під час розкриття змісту поняття «взаємодія» науковці зазначають наступне: 1) взаємодія полягає в узгодженні дій її суб'єктів за цілями, часом, місцем проведення, виконавцями і програмою; 2) для взаємодії необхідна наявність не менше двох суб'єктів; 3) під час взаємодії кожен із взаємодіючих суб'єктів (систем) діє в межах наданої йому законодавцем компетенції; 4) суб'єктів взаємодії об'єднує єдина мета щодо виконання спільних завдань [221, с.162; 17, с.101]. Г.А. Туманов, К.Н. Єрмаков та В.В. Ковальська розглядають взаємодію, як важливу умову співіснування певних елементів єдиної системи. Звідси вчені виділяють основні ознаки взаємодії: 1) узгодженість діяльності – передбачає ряд відповідних дій та використання загальних або доповнюючих одна одну форм і методів реалізації цих дій; 2) певна кількість суб'єктів – допускається участь як мінімум двох сторін, причому кожну з цих сторін можуть представляти декілька учасників; 3) поєднання зусиль суб'єктів, що визначає відносини співпраці між ними та передбачає наявність спільних цілей та інтересів для взаємодіючих сторін; 4) партнерський характер відносин у рамках співпраці, при цьому сторони рівні й незалежні одна від одної; 5) законність, відповідно до якої реалізуються дії й використовуються форми, методи, сили і засоби [97, с.151-152].

З вищенаведеного виходить, що взаємодія – це особлива форма взаємовідносин між певними суб'єктами, яка передбачає загальну

цілеспрямованість, узгодженість, координованість їх діяльності задля виконання спільних поточних завдань та досягнення єдиної кінцевої мети. Взаємодія має цілком добровільний характер, адже в її основі лежить співпраця, однакове прагнення та заінтересованість кожного суб'єкта досягти поставлених цілей. Однак, це найбільш базове розуміння досліджуваної категорії, яке може отримати певну специфіку в залежності від зовнішнього контексту. Так, унікальні властивості взаємодія отримує, коли її учасниками є суб'єкти протидії кіберзлочинності.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2161-VIII, кіберзлочинність – це сукупність кіберзлочинів – суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за які передбачена законом України про кримінальну відповідальність та/або які визнано злочином міжнародними договорами України [174]. Натомість, І.І. Васильковський, розбираючись із сутністю досліджуваної категорії більш глибоко наголосив, що термін «кіберзлочин» утворений сполученням двох слів: кіберпростір і злочин. Термін «кіберпростір» (у вітчизняній літературі частіше зустрічаються терміни «віртуальний простір» або «віртуальний світ») позначає інформаційний простір, що моделюється за допомогою комп'ютера, в якому існують визначені об'єкти або символьне уявлення інформації – місце, де діють комп'ютерні програми і переміщуються дані. Використання цього терміну поширене у світовій науковій літературі та вживається не як юридична категорія, а як визначення соціального та технічного феномену. Визначення кіберзлочинності головним чином залежать від того, в яких цілях цей термін буде використовуватися. Основу кіберзлочинності становлять обмежене число діянь, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних даних або систем, що передбачають використання комп'ютера в цілях отримання особистого або фінансового прибутку або заподіяння особистої або фінансової шкоди, включаючи

форми злочинів, пов'язаних з використанням персональних даних. Автор робить висновок, що кіберзлочин (або злочин з використанням комп'ютерних технологій) – це економічний злочин, скоєний з використанням обчислювальної техніки та мережі Інтернет [36, с.277-278].

Схожий підхід пропонує В.В. Марков, наголошуючи: кіберзлочинність – це злочинність у так званому «віртуальному просторі». Віртуальний простір (або кіберпростір) можна визначити як модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, наведені в математичному, символьному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі. Науковець відмічає: «Кіберпростір стає ареною конфліктів між державами, організаціями та приватними особами. За сучасних умов активізації міжнародних терористичних, екстремістських організацій та злочинних структур, які використовують інформаційні технології для реалізації своїх злочинних намірів, забезпечення інформаційної безпеки є однією з найважливіших складових системи забезпечення національної і міжнародної безпеки» [136, с.120]. О.Ю. Іванченко розуміє кіберзлочинність як сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем, шляхом використання комп'ютерних мереж чи інших засобів віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [72, с.173; 71, с.68].

В свою чергу, В.Б. Дзюндзюк, В. Болгов та О. Гладун наголосили, що кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних, суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і

використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію. Вчені виділяють наступні ознаки кіберзлочинності: 1) такий тип злочинів вчиняється у віртуальному просторі або в межах комп'ютерних мереж; 2) вчинення кіберзлочинів, на відміну від інших, є більш доступним для людей із невисокими соціальними і віковими можливостями; 3) вчинення злочину у віртуальному просторі вимагає застосування певного комплексу знань, крім того, в суспільстві активно пропагується ідея «інтелектуальності» хакерів, роблячи цю субкультуру ще більш популярною; 4) кіберзлочини є анонімними та неперсоніфікованими; 5) цьому виду злочинності властивий високий рівень латентності [27; 54].

Подібний підхід, але у більш лаконічному вигляді підтримує В.А. Голубєв, який вказує, що кіберзлочинність – це протиправна поведінка, яка спрямована на порушення відносин у суспільстві та приватної чи корпоративної безпеки під час того, як особи обмінюються інформацією за допомогою електронних пристроїв [227]. Є. Скулиш наводить визначення кіберзлочинності у двох аспектах: 1) у вузькому – це будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є безпека комп'ютерних систем і оброблюваних ними даних; 2) у широкому (як злочин, пов'язаний з комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж [227, с.183-184].

Окремо варто виділити підхід В.М. Дрьоміна. Науковець, досліджуючи місце мережі Інтернет у механізмі інституціоналізації

злочинності, звертає увагу на глобалізацію кіберзлочинності та її транснаціональний характер. Він зазначає: «Комп'ютерні злочини небезпечні не тільки самі по собі, але й тим, що створюють умови для вчинення нових злочинів, розширюють сферу кримінальної дійсності та сприяють відтворенню злочинності, глобалізуючи її. Електронна комунікація може бути використана злочинцями для планування або координації практично усіх незаконних дій у будь-якій точці світу. Інтернет сприяє інституціоналізації неформальних соціальних практик, адже неформальні стандарти спілкування набувають глобальний та фактично неконтрольований характер» [60, с.370-371; 219].

Таким чином, кіберзлочинність є складною категорією, що обумовлено наступним: *по-перше*, це суспільно небезпечне явище, яке детерміновано негативними тенденціями державного розвитку (недосконалість законодавства, низький рівень соціального забезпечення та добробуту населення, нестабільна економіка, «негромадянська» політична система, неефективність роботи правоохоронних органів, недостатність освіти і таке інше) та проявляється в активній діяльності окремих осіб та груп; *по-друге*, це комплексне явище, яке включає в себе цілу систему різноманітних суспільно-небезпечних діянь, юридична відповідальність за які передбачена законодавством України; *по-третє*, вчинення кіберзлочинів зумовлює настання найсуворішого виду юридичної відповідальності – кримінальної, яка обумовлює застосування до особи найбільш суворих заходів державного примусу; по-четверте, кіберзлочинність є ненасильницьким різновидом кримінальних діянь, які вчиняються із протиправним, таким що порушує права та свободи людей, використання комп'ютерних технологій.

Тож, взаємодія у сфері кіберзлочинності передбачає те, що її суб'єкти мають справу із комплексним, негативним соціальним явищем, яке складається із великого масиву суспільно-небезпечних діянь за які передбачено кримінальне покарання згідно до законодавства України. З

цього ж виходить інша особливість цієї категорії. Учасники взаємодії провадять спеціальний різновид діяльності – протидію кіберзлочинам.

Слово «протидія» у словниках розкривається як дія, спрямована проти іншої дії, перешкоджає їй [24]. Відносно тлумачення категорії «протидія злочинності» серед науковців існує дискусія. Так, В.М. Куц тлумачить її, як складне соціально-правове явище та поняття про нього, в якому відображається теорія і практика специфічної соціально-управлінської діяльності та суспільних і приватних ініціатив, а також кримінально-юстиційних зусиль, спрямованих на перешкоджання вчиненню кримінальних правопорушень та реагування на їх вчинення [123; 124, с. 153]. С.Г. Міщенко зазначає, що протидія злочинності за своїм характером є правоохоронною діяльністю, яка розглядається, як багатофункціональне і різноаспектне поняття, що охоплює практично усі сфери державної діяльності. Вона здійснюється на загально-соціальному та спеціальному рівнях. Загально-соціальна протидія злочинності є основою спеціальної протидії. Спеціальна протидія здійснюється шляхом правового реагування на вчинення злочину та спеціально-кримінологічного запобігання новим злочинам [141, с.10; 159].

Розглядаючи зміст поняття протидії злочинності, О.М. Бандурка, Л.М. Давиденко та О.М. Литвинов зазначили, що вона охоплює як боротьбу зі злочинністю, так і боротьбу в аспекті запобігання їй. Боротьба зі злочинністю в усіх її виявах, напрямах та формах є в основі кримінально-правової політики. Спираючись на це, вчені визначають протидію злочинності, як особливо інтегрований, багаторівневий об’єкт соціального управління, який складається з різноманітної за формами діяльності відповідних суб’єктів (державних, недержавних органів та установ, громадських формувань та окремих громадян), які взаємодіють у вигляді системи різнорідних заходів, спрямованих на пошук шляхів, засобів та інших можливостей ефективного впливу на злочинність з метою зниження інтенсивності процесів детермінації злочинності на усіх рівнях,

нейтралізації дії її причин та умов для обмеження кількості злочинних виявів до соціально толерантного рівня [13, с.86; 14, с.45]. О.І. Пономарьов протидію злочинності визначає як історично складену систему заходів політичного, соціально-економічного, інформаційно-пропагандистського, організаційного, правового та іншого характеру, направлену на виявлення, попередження і усунення об'єктивних та суб'єктивних причин і умов, що породжують і сприяють злочинності, припинення злочинної діяльності, а також мінімізація наслідків її діяльності, що здійснюються шляхом цілеспрямованої діяльності всіх інститутів суспільства. Така протидія, на думку автора, повинна відповідати наступним ознакам: 1) заходи політичного, соціально-економічного, інформаційно-пропагандистського, організаційного, правового та іншого характеру повинні мати системний характер, що проявляється в постійності їх виконання і взаємозв'язку між собою; 2) протидія злочинності повинна бути направлена на виявлення, попередження і усунення об'єктивних та суб'єктивних причин і умов, що породжують і сприяють злочинності, припинення злочинної діяльності, а також мінімізацію наслідків її діяльності; 3) в реалізації зазначених заходів повинні бути задіяні всі інститути суспільства [225, с.148].

Тож, протидія кіберзлочинності – це комплексна діяльність, яка здійснюється спеціально уповноваженими суб'єктами, та спрямована на реалізацію заходів та процедур із попередження, виявлення та припинення дій окремих осіб та груп, що містять ознаки злочинів у інформаційній сфері, а також факторів, які сприяють їх вчиненню. Протидія кіберзлочинності передбачає консолідацію зусиль різних органів державної влади та їх можливостей із реалізації вказаного комплексу заходів та процедур [**Error! Reference source not found.**].

Рухаючись за логікою дослідження можемо виділити третю особливість взаємодії в сфері протидії кіберзлочинності – обмеженість переліку суб'єктів які вступають у подібний формат відносин. Зокрема, їх учасниками є суб'єкти, що уповноважені на реалізацію правоохоронної

функції держави. Зауважимо: слово «функція» походить від латинського терміну «functio», яким позначалося кілька понять: виконання, службовий обов'язок, сплата податків. У сучасній мові цей термін є ще більше багатозначним. Зокрема, функція розкривається як: 1) явище, яке залежить від іншого явища, є формою його виявлення і змінюється відповідно до його змін; 2) робота кого-небудь, чого-небудь, обов'язок, коло діяльності, когось, чогось; повинність, місія; 3) специфічна діяльність організму людини, тварин, рослин, їхніх органів, тканин і клітин; 4) величина, яка змінюється зі зміною незалежної змінної величини (аргументу).[146, с.707; 214, с.1443–1444; 47, с.272; 90, с.124].

Надаючи характеристику безпосередньо правоохоронній функції Г.Н. Манов доводить, що вона висвітлює діяльність держави, спрямовану на охорону правопорядку, власності, прав і законних інтересів громадян. На його думку, цю функцію здійснюють усі органи держави, але поряд з цим існують спеціальні органи, на які безпосередньо покладається здійснення правоохоронної діяльності, наприклад, суд, прокуратура [62]. О. Кулик наголошує на збірному змісті правоохоронної функції та вважає, що вона складається із: функції охорони державної безпеки, громадського порядку, майна фізичних та юридичних осіб, контролю за станом дотримання нормативних актів в окремих сферах суспільного життя, виявлення фактів скоєння злочинів і адміністративних правопорушень; їх припинення; розгляду адміністративних справ та накладення адміністративних стягнень [119, с.828; 62, с.275]. Й.І. Горінецький пропонує наступне визначення: правоохоронна функція сучасної держави – це самостійний і пріоритетний напрям державної політики, котрий за допомогою юридичних засобів здійснюється для досягнення такого соціального ефекту, як захист права загалом, основ конституційного ладу, в тому числі прав, свобод і законних інтересів людини і громадянина та інших об'єктів, зміцнення законності і правопорядку, і одночасно виступає правовою формою досягнення інших цілей суспільства і держави [45, с.7].

Поділяє таку позицію І.В. Сажнєв: правоохоронна функція – це напрямок діяльності держави, що виражає її сутність на даному історичному етапі, спрямований на вирішення основних завдань по забезпеченню охорони конституційного ладу, прав та свобод громадян, законності та правопорядку, усіх врегульованих правом суспільних відносин, і здійснюється у відповідних формах та особливими методами [186, с.68; 67, с.97-98].

Тож, правоохоронна функція держави – це напрям діяльності спеціально уповноважених державою суб'єктів із забезпечення прав та свобод людини та громадянина на території України, а також формування та підтримки суспільного ладу, в якому панує тотальний правопорядок – дотримання всіма та кожним вимог Конституції та чинного законодавства України. Протидія злочинності, зокрема, вчинюваній за допомогою комп'ютерних технологій – це невід'ємний атрибут процесу реалізації правоохоронної функції, адже виявлення та припинення суспільно-небезпечних діянь дозволяє попередити порушення прав та свобод окремих осіб та соціальних груп в майбутньому.

Звідси виходить, що взаємодія в сфері протидії кіберзлочинності відбувається між обмеженим колом учасників, а саме суб'єктами, які володіють спеціальними повноваженнями та обов'язком реалізовувати правоохоронну функцію держави. Державно-правовий характер взаємодії суб'єктів протидії кіберзлочинності зумовлює останню особливість – адміністративно-правову урегульованість. В класичному розумінні, правове регулювання – це процес упорядкування певного виду суспільних правовідносин, що здійснюється за допомогою різних правових засобів, серед яких центральне місце належить правовим актам та нормам [216, с.89]. В свою чергу, адміністративно-правове регулювання – це більш складне, комплексне й багатогранне явище і водночас процес. З ним пов'язано з'ясування суті, змісту та форми держави (форми державного правління і форми державного устрою), розкриття функціональних,

організаційно-структурних і політико-правових параметрів виконавчої влади як окремої гілки державної влади. Особливість виконавчої влади серед інших гілок державної влади полягає в тому, що саме у процесі її реалізації відбувається реальне втілення в життя законів та інших нормативних актів держави, практичне застосування всіх важелів державного регулювання та управління важливими процесами суспільного розвитку [215, с.40-41]. Розкриваючи зміст даної категорії вчений влучно зауважив, що адміністративно-правове регулювання – це цілеспрямований, організуючий і регулюючий вплив держави через систему органів та посадових осіб на процеси, які відбуваються в суспільстві. До ознак адміністративно-правового регулювання відносять: забезпечення реалізації цілей, завдань і функцій держави; реалізація спеціально уповноваженими суб'єктами, які наділені адміністративними повноваженнями; систематичність; цілеспрямованість; ієрархічність; систематичність; процесуальний характер; цілеспрямованість та інше. Адміністративно-правові відносини – це суспільні відносини в сфері державного управління, учасники яких виступають носіями прав і обов'язків, урегульованих нормами адміністративного права [5, с.50; 204, с.39].

Як ми бачимо, адміністративно-правове регулювання – це вплив права на суспільно-правові відносини, виникнення яких пов'язано із виконанням функції держави спеціально уповноваженими суб'єктами. Саме такими є суспільні зв'язки у сфері протидії кіберзлочинності, адже виникають з факту виконання суб'єктами із особливими, офіційно визначними правами та обов'язками державної правоохоронної функції та використання імперативного, владного інструментарію впливу [77].

Проведене дослідження показує, що взаємодія суб'єктів протидії кіберзлочинності, відрізняється від звичайного формату співпраці наступними чинниками: 1) головною ціллю є комплексне суспільно-небезпечне явище, яке наносить шкоду правам, свободам та інтересам громадян України, а також включає негативні дії, за які законодавством

передбачено найсуворіший різновид покарання – кримінальний; 2) відбувається в рамках протидії кіберзлочинності – спеціальної комплексної діяльності, спрямованої на реалізацію заходів та процедур із попередження, виявлення та припинення дій окремих осіб та груп, що містять ознаки кіберзлочинів, а також факторів, які сприяють їх вчиненню; 3) вступати у дану взаємодію можуть виключно спеціально-уповноважені суб'єкти, які мають права та обов'язки реалізовувати правоохоронну функцію держави; 4) взаємодія суб'єктів протидії кіберзлочинності є об'єктом адміністративно-правового регулювання [77].

Таким чином, проведене наукове дослідження да змогу узагальнити, що взаємодія суб'єктів протидії кіберзлочинності – це регламентована нормами адміністративної галузі права модель суспільних відносин, яка передбачає тісну інформаційно-організаційну співпрацю, консолідацію ресурсів, реалізацію спільних заходів, а також поділ відповідальності у процесі здійснення державно-значущої діяльності у напрямку протидії та запобігання суспільно-небезпечним діянням, які складають структуру кіберзлочинності [77].

1.3. Сучасний стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

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 і 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.

В зазначеній сфері сконцентровано велику кількість правових норм різного рівня та значення. Найпершим документом, який варто виділити, є Конституція України, котра, як і належить Основному Закону, посідає найвище місце в національній правовій системі. Її положення є первинними і основоположними. Якщо уявити правові акти, які діють у державі у вигляді певного організованого і взаємопов'язаного цілого, системи, єдиного комплексу, то Конституція – це основа, стрижень і одночасно вершина всього права, фундамент його розвитку. Однією з ознак конституції є особливе, відмінне від інших джерел конституційного права, найменування. Термін «конституція» в сучасних державах використовується для позначення особливого нормативного акту. Крім того, на відміну від законів та інших нормативно-правових актів, предмет конституційного регулювання в найменуваннях конституції не розшифровується. Для неї характерні особливий порядок розробки, прийняття і введення в дію, особливий порядок внесення змін, особливий предмет правового регулювання, найвища юридична сила. Конституція виконує правоутворюючу роль, вона є своєрідним центром правової системи, вона більше ніж просто закон [149, с.95-97].

Так, в Конституції знаходять своє закріплення засади спільно-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» [106]. 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 [106].

На сьогоднішній день Україною ратифіковано низку документів в сфері протидії кіберзлочинності. Відмітити, як приклад, варто Конвенцію Організації Об'єднаних Націй (далі – ООН) проти транснаціональної організованої злочинності від 15.11.2000 метою якої визначено сприяння співробітництву в справі більш ефективного попередження транснаціональної організованої злочинності та боротьби з нею. Документ визначає, що визнання злочину транснаціональним, у тому числі в сфері кібербезпеки, можливо за умови того, що він: a) вчинений у більш ніж одній державі; b) вчинений в одній державі, але істотна частина його підготовки, планування, керівництва або контролю має місце в іншій державі; c) вчинений в одній державі, але за участю організованої злочинної групи, яка здійснює злочинну діяльність у більш ніж одній

державі; або d) вчинений в одній державі, але його істотні наслідки мають місце в іншій державі [103]. У Конвенції наголошено, що кожна держава-учасниці документу прагне забезпечити використання будь-яких передбачених у її внутрішньому законодавстві дискреційних юридичних повноважень, що відносяться до кримінального переслідування осіб за злочини, що охоплюються Конвенцією, для досягнення максимальної ефективності правоохоронних заходів щодо цих злочинів та з належним урахуванням необхідності перешкодити вчиненню таких злочинів [103].

У 2005 році Україною ратифіковано 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 [104]. Так, Конвенція містить чіткий перелік дій, які визнаються кіберзлочинами на території держав-учасниць документу, зокрема: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями, шахрайство, пов’язане з комп’ютерами і таке інше [104].

Глибоку 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 [104].

Важливе значення для формування дієвої системи взаємодії із протидії кіберзлочинності на території України та Європейського Союзу (далі – ЄС) має Угода про асоціацію між Україною та ЄС. Зокрема, необхідно відмітити статтю 22 документу де прямо вказано, що сторони-підписання співробітничають у боротьбі з кримінальною та незаконною організованою чи іншою діяльністю, а також з метою її попередження. Таке співробітництво спрямовується на вирішення, «inter alia», таких проблем: a) незаконне переправлення через державний кордон нелегальних мігрантів, торгівля людьми і вогнепальною зброєю та незаконний обіг наркотиків; b) контрабанда товарів; c) економічні злочини, зокрема злочини у сфері оподаткування; d) корупція як у приватному, так і в державному секторі; e) підробка документів; f) кіберзлочинність. Сторони посилюють двостороннє, регіональне та міжнародне співробітництво у цій сфері, зокрема співробітництво із залученням Європолу. Сторони і надалі розвивають співробітництво, «inter alia», стосовно: a) обміну найкращими практиками, в тому числі щодо методик розслідування та криміналістичних досліджень, b) обміну інформацією відповідно до існуючих правил, c) посилення потенціалу, зокрема навчання та, у разі необхідності, обмін персоналом, d) питань, пов’язаних із захистом свідків та жертв [212].

Дослідження положень міжнародних документів в сфері протидії кіберзлочинності показує, що вони, як і Конституція України декларують в більшій мірі головні, міжнародно обґрунтовані стандарти боротьби із зазначеним негативним явищем, а також механізми міжнародної співпраці на рівні держав.

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 він має ключовим завданням 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 [114].

Цьому питанню присвячено Розділ XVI ККУ «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку». Згідно до статті 361-1 даного розділу створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років [114]. Згідно до статті 361-2 ККУ несанкціоновані збут або розповсюдження інформації з обмеженим

доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років [114].

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 [115].

Серед законодавчих актів, що входять до системи правових засад взаємодії суб’єктів протидії злочинності, варто виділити Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 №2135-XII. Документ наголошує, що оперативно-розшукова діяльність – це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів. Завданням оперативно-розшукової діяльності є пошук і фіксація

фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [172].

Реалізовувати оперативно-розшукову діяльність згідно із законом мають право обмежене коло суб'єктів, а саме виключно оперативні підрозділи: Національної поліції України, Державного бюро розслідувань, Служби безпеки України, Служби зовнішньої розвідки України, Державної прикордонної служби України, Управління державної охорони, органів і установ виконання покарань та слідчих ізоляторів Державної кримінально-виконавчої служби України, розвідувального органу Міністерства оборони України, Національного антикорупційного бюро України, Бюро економічної безпеки України [172].

Підставами проведення оперативно-розшукової діяльності Закон визначає: «1) наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів, про: а) кримінальні правопорушення, що готуються; б) осіб, які готують вчинення кримінального правопорушення; в) осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання; г) осіб безвісно відсутніх; ґ) розвідувально-підривну діяльність спецслужб іноземних держав, організацій та окремих осіб проти України; д) реальну загрозу життю, здоров'ю, житлу, майну працівників суду і правоохоронних органів у зв'язку з їх службовою діяльністю, а також осіб, які беруть участь у кримінальному судочинстві, членів їх сімей та близьких родичів, з метою створення необхідних умов для належного відправлення правосуддя; співробітників розвідувальних органів України у зв'язку із службовою діяльністю цих осіб, їх близьких родичів, а також осіб, які

конфіденційно співробітничають або співробітничали з розвідувальними органами України, та членів їх сімей з метою належного здійснення розвідувальної діяльності; 2) запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках, а також осіб, яким надається дозвіл на перебування без супроводу в контрольованих та стерильних зонах, зонах обмеженого доступу, що охороняються, та критичних частинах таких зон аеропортів; 2-1) необхідність перевірки осіб у зв'язку з призначенням на посади в розвідувальних органах України або залученням до конфіденційного співробітництва з такими органами, доступом осіб до розвідувальної таємниці; 3) випадки, передбачені законодавством України в сфері розвідувальної діяльності; 4) наявність узагальнених матеріалів центрального органу виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, отриманих в установленому законом порядку» [172].

Одним з головних обов'язків органів, уповноважених реалізовувати оперативно-розшукову діяльність визначено здійснювати взаємодію між собою та іншими правоохоронними органами, в тому числі відповідними органами іноземних держав та міжнародними антитерористичними організаціями, з метою швидкого і повного попередження, виявлення та припинення кримінальних правопорушень [172].

Важливе значення має Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» від 30.06.1993 №3341-XII, який визначає головні напрями загальнодержавної політики та організаційно-правові основи боротьби з організованою злочинністю. Під організованою злочинністю в Законі розуміється сукупність кримінальних правопорушень, у тому числі кіберзлочинів, що вчиняються у зв'язку з створенням та діяльністю організованих злочинних угруповань.

Основними напрямами боротьби з організованою злочинністю відповідно до Закону є: «1) створення правової основи, організаційних, матеріально-технічних та інших умов для ефективної боротьби з організованою злочинністю, організація міжнародного співробітництва у цій сфері; 2) виявлення та усунення або нейтралізація негативних соціальних процесів і явищ, що породжують організовану злочинність та сприяють їй; 3) запобігання нанесенню шкоди людині, суспільству, державі; 4) запобігання виникненню організованих злочинних угруповань; 5) виявлення, розслідування, припинення і запобігання правопорушенням, вчинюваним учасниками організованих злочинних угруповань, притягнення винних до відповідальності; 6) забезпечення відшкодування шкоди фізичним та юридичним особам, державі; 7) запобігання встановленню корумпованих зв'язків з державними службовцями та посадовими особами, втягненню їх у злочинну діяльність; 8) протидія використанню учасниками організованих злочинних угруповань у своїх інтересах об'єднань громадян і медіа; 9) запобігання легалізації коштів, здобутих злочинним шляхом, використанню суб'єктів підприємницької діяльності для реалізації злочинних намірів» [173].

Цільовим документом в сфері протидії кіберзлочинності виступає 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 [174].

Національна система кібербезпеки є 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. Зазначається, що 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 [174].

До засадничих правових актів в сфері регулювання протидії кіберзлочинності також відноситься Закон України «Про розвідку» від 17.09.2020 №912-IX в рамках якому питанню кібербезпеки присвячено значну увагу. Вказаний акт 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 [180].

Регламент 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) [177].

Акцентувати увагу також треба на Постанові Кабінету Міністрів України від 29.12.2021 №1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту». Відповідно до положень останнього, організаційно-технічна модель кіберзахисту є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем. Організаційно-технічна модель кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки. При цьому, визначено, що організаційно-керуюча інфраструктура кіберзахисту складається з таких секторів: 1) загальнодержавний, до складу якого входять основні суб'єкти національної системи кібербезпеки, сили безпеки і оборони та Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України; 2) галузевий, до складу якого входять центральні органи виконавчої влади, інші державні органи, які забезпечують формування та/або реалізацію державної політики в одній чи кількох сферах, або безпосередньо проводять відповідно до компетенції заходи із забезпечення кібербезпеки, об'єкти критичної інфраструктури незалежно від форми власності; 3) регіональний (місцевий), до складу якого входять місцеві органи виконавчої влади, органи місцевого самоврядування, підприємства, установи та організації незалежно від форми власності, що провадять діяльність у сфері захисту інформації та кіберзахисту; 4) освіти та науки, до складу якого входять науково-дослідні установи, заклади вищої освіти у сфері захисту інформації та кібербезпеки, що беруть участь у підготовці, підвищенні кваліфікації та перепідготовці професійних кадрів; 5) приватний, до складу якого входять підприємства

недержавної форми власності, організації та установи, що провадять діяльність у сфері захисту інформації та кіберзахисту (крім об'єктів критичної інфраструктури); 6) громадський, до складу якого входять громадські організації, об'єднання, асоціації, спілки та фахівці у сфері кібербезпеки, а також міжнародні та міжурядові організації, що провадять свою діяльність у сфері кібербезпеки [167].

В Постанові Кабінету Міністрів України від 04.04.2023 №299 затверджено деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. У документі вказано, що реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки шляхом вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту. Суб'єкти забезпечення кібербезпеки вживають заходів відповідно до методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Держспецзв'язку. Реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки послідовно такими етапами, як підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти/кібератаки. Реагування суб'єктами забезпечення кібербезпеки на кіберінциденти/кібератаки розпочинається з етапу підготовки, під час якого здійснюються заходи з вивчення та дослідження сучасних видів кіберінцидентів/кібератак, розроблення методів і механізмів запобігання та протидії можливим кіберінцидентам/кібератакам [53].

Отже, юридичне підґрунтя взаємодії суб'єктів протидії кіберзлочинності складає велика група нормативно-правових актів. Вона включає в себе Конституцію України, міжнародні документи (ратифіковані у встановленому законом порядку), а також закони і підзаконні акти. В системі відповідних правових засад ключове місце відводиться нормам адміністративної галузі права. Зазначене, перш за все, пов'язано із характером суспільно-правових відносин, які виникають в процесі взаємодії суб'єктів протидії суспільно-небезпечним діянням, вчиненим із використанням інформаційних технологій. Саме в актах адміністративного характеру розкриваються: організаційно-управлінські аспекти взаємодії; порядок реалізації спільної діяльності уповноважених суб'єктів в секторі забезпечення кібербезпеки та їх ієрархічне підпорядкування; правовий статус суб'єктів відповідних правовідносин, ключові цілі, завдання та функції співпраці; тощо [81].

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: фактична відсутність ефективних та злагоджених механізмів взаємодії спеціально уповноважених суб'єктів у відповідній сфері; невизначеність форм та методів здійснення досліджуваної спільної діяльності; тощо [81].

Висновки до Розділу 1

Акцентовано увагу на тому, що у XXI кожен з нас не може уявити свій день без використання електронного гаджету підключеного до всесвітньої мережі Інтернет. Дана ситуація має дві сторони. З одного боку,

технології суттєво полегшують життя суспільства, адже надають більш широкі можливості у процесі віддаленої комунікації різноманітних суб'єктів, соціального управління, автоматизації певних функціональних процесів виробничого характеру тощо. Разом із тим, відзначено, що на тлі розвитку комп'ютерів та цифрової революції в цілому, з'являються окремі особи та групи, що намагаються за допомогою новітніх технічних інструментів порушити права та свободи інших людей шляхом: незаконного заволодіння їх особистими даними; викрадення грошових коштів, які знаходяться на електронних рахунках; втягнення людей у різноманітні шахрайські схеми, наприклад, пов'язані із продажом неіснуючих товарів і таке інше. Все перелічене в сукупності сформувало серйозну проблему кіберзлочинності, яка постійно перебуває у полі зору правоохоронних органів та міжнародної спільноти.

Констатовано, що незважаючи на чималу кількість наукових робіт, чітко сформульованого підходу до розкриття сутності та оцінки правового регулювання взаємодії суб'єктів протидії кіберзлочинності на сьогодні в юридичній літературі досі не сформовано. Поверхнево вказане питання розглядалось в межах багатьох галузевих наук та в рамках більш широких проблематик, присвячених кібербезпеці держави взагалі. Так, представники кримінального права та кримінології акцентують увагу лише на тому, що взаємодія є необхідним організаційним заходом подолання негативного явища кіберзлочинності. В свою чергу представники кримінального процесуального права та криміналістики обмежують свої дослідження виключно рамками існуючих процесуальних механізмів та порядком здійснення відповідних слідчих дій та заходів, вважаючи взаємодію виключно моделлю розвитку процесуальних відносин. Міжнародники переймаються лише світовою співпрацею у сфері боротьби з кіберзлочинами та її юридичним оформленням. Теоретики права розглядають взаємодію у контексті дослідження і розкриття особливостей змісту кіберзлочинності загалом і таке інше. Безумовно, фахівці вказаних

вище галузей права зробили вагомий внесок у розвиток даного інституту. Проте, відсутність єдиного сформульованого комплексного бачення природи, змісту, особливостей організації, напрямів здійснення та інших аспектів правового регулювання взаємодії суб'єктів протидії кіберзлочинності, ускладнює вироблення її нової концепції та визначення шляхів удосконалення. При цьому необхідно підкреслити, що вирішувати відповідні проблеми найбільш доцільно в розрізі адміністративної галузі права, адже саме її нормами регулюється діяльність відповідних суб'єктів, їх правовий статус, мета та завдання діяльності, а відтак і визначаються засади взаємодії спеціально уповноважених органів державної влади у галузі протидії кіберзлочинності.

З'ясовано, що взагалі, взаємодія – це особлива форма взаємовідносин між певними суб'єктами, яка передбачає загальну цілеспрямованість, узгодженість, координованість їх діяльності задля виконання спільних поточних завдань та досягнення єдиної кінцевої мети. Взаємодія має цілком добровільний характер, адже в її основі лежить співпраця, однакове прагнення та заінтересованість кожного суб'єкта досягти поставлених цілей.

Аргументовано, що кіберзлочинність є складною категорією, що обумовлено наступним: по-перше, це суспільно небезпечне явище, яке детерміновано негативними тенденціями державного розвитку (недосконалість законодавства, низький рівень соціального забезпечення та добробуту населення, нестабільна економіка, «негромадянська» політична система, неефективність роботи правоохоронних органів, недостатність освіти і таке інше) та проявляється в активній діяльності окремих осіб та груп; по-друге, це комплексне явище, яке включає в себе цілу систему різноманітних суспільно-небезпечних діянь, юридична відповідальність за які передбачена законодавством України; по-третє, вчинення кіберзлочинів зумовлює настання найсуворішого виду юридичної відповідальності – кримінальної, яка обумовлює застосування

до особи найбільш суворих заходів державного примусу; по-четверте, кіберзлочинність є ненасильницьким різновидом кримінальних діянь, які вчиняються із протиправним, таким що порушує права та свободи людей, використання комп'ютерних технологій.

Встановлено, що протидія кіберзлочинності – це комплексна діяльність, яка здійснюється спеціально уповноваженими суб'єктами, та спрямована на реалізацію заходів та процедур із попередження, виявлення та припинення дій окремих осіб та груп, що містять ознаки злочинів у інформаційній сфері, а також факторів, які сприяють їх вчиненню. Протидія кіберзлочинності передбачає консолідацію зусиль різних органів державної влади та їх можливостей із реалізації вказаного комплексу заходів та процедур.

Наголошено, що правоохоронна функція держави – це напрям діяльності спеціально уповноважених державою суб'єктів із забезпечення прав та свобод людини та громадянина на території України, а також формування та підтримки суспільного ладу, в якому панує тотальний правопорядок – дотримання всіма та кожним вимог Конституції та чинного законодавства України. Протидія злочинності, зокрема, вчинюваній за допомогою комп'ютерних технологій, – це невід'ємний атрибут процесу реалізації правоохоронної функції, адже виявлення та припинення суспільно-небезпечних діянь дозволяє попередити порушення прав та свобод окремих осіб та соціальних груп в майбутньому.

Обґрунтовано, що взаємодія суб'єктів протидії кіберзлочинності, відрізняється від звичайного формату співпраці наступними чинниками: 1) головною ціллю є комплексне суспільно-небезпечне явище, яке наносить шкоду правам, свободам та інтересам громадян України, а також включає негативні дії, за які законодавством передбачено найсуворіший різновид покарання – кримінальний; 2) відбувається в рамках протидії кіберзлочинності – спеціальної комплексної діяльності, спрямованої на реалізацію заходів та процедур із попередження, виявлення та припинення

дій окремих осіб та груп, що містять ознаки кіберзлочинів, а також факторів, які сприяють їх вчиненню; 3) вступати у дану взаємодію можуть виключно спеціально-уповноважені суб'єкти, які мають права та обов'язки реалізовувати правоохоронну функцію держави; 4) взаємодія суб'єктів протидії кіберзлочинності є об'єктом адміністративно-правового регулювання.

Узагальнено, що взаємодія суб'єктів протидії кіберзлочинності – це регламентована нормами адміністративної галузі права модель суспільних відносин, яка передбачає тісну інформаційно-організаційну співпрацю, консолідацію ресурсів, реалізацію спільних заходів, а також поділ відповідальності у процесі здійснення державно-значущої діяльності у напрямку протидії та запобігання суспільно-небезпечним діянням, які складають структуру кіберзлочинності.

Акцентовано увагу на тому, що юридичне підґрунтя взаємодії суб'єктів протидії кіберзлочинності складає велика група нормативно-правових актів. Вона включає в себе Конституцію України, міжнародні документи (ратифіковані у встановленому законом порядку), а також закони і підзаконні акти. В системі відповідних правових засад ключове місце відводиться нормам адміністративної галузі права. Зазначене, перш за все, пов'язано із характером суспільно-правових відносин, які виникають в процесі взаємодії суб'єктів протидії суспільно-небезпечним діянням, вчиненим із використанням інформаційних технологій. Саме в актах адміністративного характеру розкриваються: організаційно-управлінські аспекти взаємодії; порядок реалізації спільної діяльності уповноважених суб'єктів в секторі забезпечення кібербезпеки та їх ієрархічне підпорядкування; правовий статус суб'єктів відповідних правовідносин, ключові цілі, завдання та функції співпраці; тощо.

Доведено, 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: фактична відсутність ефективних та злагоджених механізмів взаємодії спеціально уповноважених суб'єктів у відповідній сфері; невизначеність форм та методів здійснення досліджуваної спільної діяльності; тощо.

РОЗДІЛ 2.
МЕХАНІЗМ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

2.1. Поняття та структура механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Взаємодія суб'єктів протидії кіберзлочинності, в силу своєї правової природи, має багато спільних рис із співпрацею учасників багатьох відносин, які виникають з приводу боротьби із іншими суспільно-негативними та небезпечними явищами. Разом із цим, досліджуваній в дисертації категорії притаманний ряд специфічних рис, пов'язаних із особливістю механізму її адміністративно-правового регулювання.

Слово «механізм» походить від грецького «μηχαυη», що значить знаряддя або пристрій [23, с.81]. В сучасних тлумачних словниках даний термін розкривається, як: внутрішній устрій (система ланок) машини, пристрою, апарата, що приводить їх в дію; система, устрій, що визначає порядок якого-небудь виду діяльності; послідовність станів, процесів, які визначають собою яку-небудь дію, явище [131, с.71]. В техніці поняття «механізм» трактується як сукупність динамічно з'єднаних частин, що виконують під впливом прикладених сил заданий рух. Неважко помітити, що при такому розумінні слово «механізм» асоціюється з певним функціонуючим пристроєм, між елементами якого існують конструктивні і функціональні зв'язки з жорстко заданими параметрами [130, с.93]. В науці управління під механізмом розуміється: 1) сукупність і логічний взаємозв'язок соціальних елементів, процесів і закономірностей, через які суб'єкт державного управління (його компоненти) «схоплює» потреби, інтереси і цілі суспільства в управляючих впливах, закріплює їх у своїх управлінських рішеннях і діях і практично втілює їх в життя, спираючись

на державну владу; 2) взаємодія різних елементів управління, що мають характер стійких взаємозалежностей і причинно-наслідкових зв'язків; 3) сукупність цілей, функцій, принципів та методів, взаємодія яких забезпечує ефективне функціонування соціальної системи; 4) сукупність матеріально-юридичних та процедурно-юридичних установлень, за допомогою яких забезпечується розробка змісту, зовнішнього вигляду, послідовності прийняття рішень в органах внутрішніх справ для вирішення юридичних справ у межах їх компетенції; 5) організація практичного здійснення державного управління, елементами якого є загальна система державного управління, включаючи статут і функції спеціальних органів і інших органів, що діють у тій чи іншій сфері, галузі; 6) набір адміністративно-правових регуляторів, характерних для певної сфери, галузі, комплект, стандарт необхідних правових актів та інших регулюючих документів, механізм державного контролю і нагляд, інформаційне забезпечення; ступінь участі громадян та їх об'єднань в управлінні і таке інше [105, с.134-135].

Враховуючи викладене, механізм є міждисциплінарним та міжгалузевим поняттям, яке узагальнено характеризує комплексний, системний об'єкт, елементи котрого забезпечують його активну роботу.

Схожим чином зміст механізму розвинуто у правовій науці, але з великою долею галузевої специфіки. На сьогоднішній день існують різні підходи до тлумачення механізму правового регулювання тих чи інших суспільних відносин, зокрема, в сфері взаємодії суб'єктів протидії кіберзлочинності. Наприклад, А.М. Подоляка розглядає дану категорію, як систему всіх державно-правових (юридичних) засобів, за допомогою яких держава здійснює владно-розпорядчий вплив на суспільні відносини в сфері охорони громадського порядку [160, с.32]. Аналогічну позицію займає О.Ф. Скакун у розумінні якої механізм правового регулювання – це узята в єдності система правових засобів, способів і форм, за допомого яких нормативність права переводиться в упорядкованість суспільних

відносин, задовольняються інтереси суб'єктів права, встановлюється і забезпечується правопорядок («належне» у праві стає «сущим») [192]. На думку В.О. Рибакова, під механізмом правового регулювання слід розуміти взяті в єдності та взаємодії всі правові засоби (елементи), за допомогою яких здійснюється правове регулювання [188, с.214].

М.С. Кельман та О.Г. Мурашин визначають механізм правового регулювання як єдину систему правових засобів, за допомогою яких здійснюється результативне правове впорядкування суспільних відносин та подолання перепон, які стоять на шляху задоволення інтересів суб'єктів права [85, с.372; 9, с.126]. В той же час, С.О. Погрібний зауважує, що механізм правового регулювання – це сполучна ланка між діяльністю суб'єкта правового регулювання та результатами такої діяльності. Саме через цей механізм матеріалізується ідеальна модель суспільних відносин, яка закладена в нормі, що його регулює [158; 58, с.140].

Варто виділити позицію М.І. Матузова та О.В. Малько, які у своїх працях пишуть, що правове регулювання в процесі свого здійснення складається з певних етапів і відповідних елементів, що забезпечують рух інтересів суб'єктів до цінності. Кожен з етапів і юридичних елементів правового регулювання викликається до «життя» в силу конкретних обставин, які відображають логіку правової упорядкованості громадських відносин, особливості впливу правової форми на соціальний зміст. Поняття, що позначає дану стадійність юридичного управління і одночасно участь в ньому сукупності юридичних засобів, зазначають правники, отримало в літературі найменування «механізм правового регулювання». Таким чином, механізм правового регулювання, на їх думку, – це система юридичних засобів, організованих найбільш послідовним чином з метою упорядкування суспільних відносин, сприяння задоволенню інтересів суб'єктів права [162, с.113-114].

За А. Андрєевим механізм правового регулювання є системою у технічному розумінні цього поняття. Усі його складові елементи існують

самі по собі, проте лише у сукупності вони органічно поєднуються між собою і доповнюють один іншого [9]. В свою чергу, С.С. Лукаш розглядає механізм правового регулювання через систему притаманних йому ознак. «Він являє собою систему юридичних засобів; зазначена система покликана найоптимальнішим чином впорядковувати ті чи інші питання суспільного життя; він має інструментальний характер. Вищенаведені ознаки дійсно є одними з найбільш істотних, за допомогою яких може бути охарактеризований механізм правового регулювання в загальнотеоретичному значенні. При цьому, говорячи про механізм правового регулювання якихось конкретних юридичних інститутів, варто зазначити, що він буде мати й власні специфічні ознаки, серед яких варто відзначити те, що його сутність та особливості структурних елементів будуть полягати й знаходити свій прояв в одночасній дії та співвідношенні. Саме дія цих норм права буде переважати над іншими нормами», - наголошує вчений [58, с.139-140].

В сфері адміністративного права механізм правового регулювання набуває галузевої трансформації та окремого змісту. Наприклад, Н.О. Бедрак бачить в даній категорії систему адміністративно-правових засобів, які спрямовані на урегулювання відносин, що виникають у процесі задоволення публічно-правових інтересів публічними органами управління. «Механізм адміністративно-правового регулювання як спосіб реалізації відповідного адміністративно-правового режиму можна розглядати у двох аспектах: по-перше, механізм адміністративно-правового регулювання є структурним елементом правового режиму; по-друге, є рушійною силою щодо забезпечення відповідного режиму», - вказує Н.О. Бедрак [18, с.10]. Як вважає В.Я. Малиновський, механізм адміністративно-правового регулювання слушно розуміти як саму організацію, процес практичної реалізації адміністративно-правового регулювання. Ця організація є складною функціонуючою системою і включає три найважливіших елементи: суб’єкти адміністративно-

правового регулювання, об’єкти адміністративно-правового регулювання, взаємодію суб’єктів і об’єктів адміністративно-правового регулювання [133, с.558].

Досить цікавою є думка А.С. Васильєва, який механізм адміністративно-правового регулювання у сфері охорони прав громадян визначив, як сукупність адміністративно-правових засобів впливу на суспільні відносини щодо забезпечення особистої та суспільної безпеки, що складаються у процесі виконавчо-розпорядницької діяльності держави, у результаті якої створюється правоохоронний юридичний режим [35, с.249; 93, с.56]. Т.С. Гончарук, вважає, що механізм адміністративно-правового регулювання – це система адміністративно-правових засобів (елементів), за допомогою яких здійснюється правове регулювання (упорядкування) суспільних відносин у сфері державного управління [44, с.23; 190, с.64].

В свою чергу М.В. Макарєйко обґрунтовує позицію відповідно до якої механізм адміністративно-правового регулювання – це сукупність адміністративно-правових засобів, які, впливаючи на управлінські відносини, організовують їх відповідно до завдань суспільства і держави. Загальна характеристика механізму адміністративно-правового регулювання за думкою автора виглядає у наступному: сам механізм є сукупністю юридичних засобів; засоби носять адміністративно-правовий характер; об'єктом дії виступають управлінські відносини; направлене на рішення задач суспільства і держави; активізує суб'єктів управлінських відносин, підвищує рівень їх правосвідомості, правової культури; забезпечується примусовою силою держави [32, с.269-270].

На думку В.В. Галунька під механізмом адміністративно-правового регулювання слід розуміти засоби функціонування єдиної системи адміністративно-правового регулювання з метою забезпечення прав, свобод і публічних законних інтересів фізичних та юридичних осіб, функціонування громадянського суспільства і держави. Механізм

адміністративно-правового регулювання дозволяє охопити весь процес правового регулювання, представити його в системно-динамічному вигляді, розкрити його структуру, взаємозв'язок і взаємодію всіх елементів [66, с.68]. «Механізм адміністративно-правового регулювання – це засоби функціонування єдиної системи адміністративно-правового регулювання з метою забезпечення прав, свобод і публічних законних інтересів фізичних та юридичних осіб, функціонування громадянського суспільства і держави. Найважливішими засобами механізму адміністративно-правового регулювання є нормативні та індивідуальні акти. Ці акти відповідають двом рівням адміністративно-правового регулювання: по-перше, складають загальні правила поведінки людей, по-друге – утворюють індивідуальні акти, що визначають на основі адміністративно-правової норми права й обов'язки конкретних учасників у правовідносинах. Акт застосування норми адміністративного права», - доводить О.М. Бабійчук [12, с.132].

Отже, відповідно до вищевикладеного, механізм адміністративно-правового регулювання являє собою складну систему юридичних елементів, інструментів та засобів, за рахунок яких визначаються матеріальні та процедурні засади дії/впливу права на суспільно-правові відносини. До ключових властивостей такого механізму доцільно віднести: 1) є динамічною категорією, яка показує реальне функціонування права; 2) являє собою складне системне утворення, так як складається із спеціальних юридичних елементів, що взаємодіють одне з одним в процесі правового регулювання та виражається крізь систему форм, що носять адміністративний характер; 3) процес реалізації даного механізму носить формалізований характер, адже порядок і особливості його дії нормативно визначені.

Тож, механізм адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, найбільш доцільно тлумачити, як формалізовану систему спеціальних, взаємодіючих та взаємозалежних між

собою юридичних елементів, за рахунок яких встановлюються матеріальні та процедурні засади впливу права на суспільно-правові відносини, що виникають в сфері спільної діяльності суб’єктів, які уповноважені на виявлення, припинення та профілактику кіберзлочинів.

Далі, задля з’ясування структури досліджуваного механізму, проаналізуємо позиції науковців з аналогічних та суміжних питань. Наприклад, С.С. Алексєєв структурними елементами механізму правового регулювання називає: а) юридичні норми; б) правовідносини, а саме: суб'єктивні права та юридичні обов'язки учасників таких відносин; в) акти реалізації прав та обов'язків; г) індивідуальні приписи та акти застосування права [140, с.100]. З точки зору М.В. Цвіка, В.Д. Ткаченка, О.В. Петришина структурними елементами категорії є: правова свідомість; принципи права; правові норми; акти тлумачення і застосування норм права; юридичні факти; правові відносини; суб’єктивні юридичні права і обов’язки; акти реалізації юридичних норм; правова культура; законність та інші [70, с.413; 162, с.123].

Досліджуючи механізм правового регулювання відносин у сфері соціального страхування, С.О. Сільченко виділяє такі його елементи, як: норми права, юридичні факти (фактичні склади), правовідносини, акти реалізації (застосування, виконання) прав і обов'язків, охоронні правозастосовні факти, заходи захисту, інші юридичні прийоми і конструкції [191, с.295; 140, с.100]. Натомість О.М. Куракін обстоює позицію про те, що до структури механізму правового регулювання входить: 1) норма права, безпосередній регулятор поведінки суб’єктів права, що наділяє їх визначеним обсягом взаємних суб’єктивних прав та юридичних обов’язків; 2) нормативно-правовий акт. Форма існування попереднього елемента, трансформація в яку надає правовій нормі формально-визначеність, офіційність та загальнообов’язковість; 3) юридичний факт. Як правило, його значення недооцінюється і юридичний факт визнається підпорядкованою правовою категорією; 4) правові

відносини. Це не є абстрактна модель поведінки суб'єктів права, а реалізація її зразка, викладеного в нормі права; 5) тлумачення права. Діяльність із визначення змісту норми права у разі її незрозумілості чи невідповідності вимогам юридичної техніки; 6) реалізація права. У науковій літературі висловлюється думка, що нерідко реалізація норм здійснюється поза допомогою правовідносин; 7) законність, реалізація правових приписів через дотримання нормативно-правових вимог суб'єктами права; 8) правосвідомість, усвідомлення суб'єктами правових приписів; 9) правова культура. Проявляється в спілкуванні та поведінці суб'єктів взаємодії і формується під впливом системи культурного та правового виховання і навчання; 10) правомірна поведінка. Діяльність суб'єктів, що відповідає вимогам норм права та соціально корисним цілям і знаходиться в установлених законодавством межах; 11) протиправна поведінка. Антипод попереднього елемента; 12) юридична відповідальність. Міра державного примусу, що застосовується до правопорушника [121].

Дещо іншу структуру виділяють представники адміністративної науки, аналізуючи галузевий приклад механізму правового регулювання. Наприклад, В. Олефір та М. Пихтін вважають, що складовими останнього є: 1) норми адміністративного права та їх зовнішнє вираження – джерела права; 2) публічна адміністрація; 3) принципи діяльності публічної адміністрації; 4) індивідуальні акти публічної адміністрації; 5) адміністративно-правові відносини; 6) форми адміністративного права; 7) тлумачення норм адміністративного права; 8) методи адміністративного права; 9) процедури реалізації адміністративно-правових норм; 10) принципи законності [108, с.116].

На думку С.В. Ківалова та Л.Р. Білої, структура механізму адміністративно-правового регулювання складається з: а) адміністративно-правових норм; б) адміністративно-правових відносин, до яких належать: об'єкт (дія, поведінка людей, матеріальні предмети, речі), суб'єкт

(громадяни, особи, державні органи, підприємства установи, організації та інші), зміст (сукупність прав й обов'язків сторін) [89, с.14–17; 20, с.32]. А.Л. Правдюк доводить: «До структури цього механізму насамперед входять норми адміністративного права, акти тлумачення таких норм та акти їх реалізації, а також адміністративно-правові відносини. Крім названих елементів до структури механізму адміністративно-правового регулювання нерідко включають також правову культуру та правову свідомість» [165, с.127].

Наведені позиції науковців показують, що на сьогоднішній день існують різні думки з приводу системного складу механізму правового та адміністративно-правового регулювання зокрема. Умовно, всі наукові концепції можна поділити на дві групи. В першу входять ті підходи в рамках яких до структури механізму правового або адміністративно-правового регулювання відносяться не тільки суто юридичні засоби та інструменти, але й інші явища правової дійсності, котрі займають відповідне місце у правовому регулюванні суспільних відносин: правова культура, правосвідомість, поведінка суб'єктів суспільних зв'язків і таке інше. Другу групу складають більш вузькі підходи в аспекті яких до структури механізму правового регулювання включають тільки спеціально-юридичні засоби та інструменти, крізь які відбувається безпосередня регуляторна дія права на суспільні відносини.

На нашу думку, обрання тієї чи іншої наукової позиції залежить від галузі та об'єкту правового регулювання, що в багатьох моментах визначають той кінцевий результат до якого правовий вплив має привести. Тож, враховуючи викладене, до структури механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності відносяться:

1) принципи права. Найчастіше, дослідники при висвітленні елементів механізму правового або адміністративно-правового регулювання нехтують принципами, що є суттєвим недоліком, адже

останні складають ідейне підґрунтя даного механізму. В силу своєї вищої імперативності та загальнообов'язковості принципи мають першочергове значення у правовому регулюванні, визначаючи його соціально- та політико-правові орієнтири та спрямовуючи дію інших юридичних засобів впливу;

2) норми адміністративного права. В сучасній правовій системі України норми є ключовими цеглинами дії права. Як пише Ю.Ф. Кравченко, норми права – це офіційне, формальне, певне, загальнообов'язкове правило поведінки, що встановлюється або санкціонується державою, охороняється нею від порушень, спрямоване на регулювання найважливіших суспільних відносин і охорону соціальних цінностей шляхом встановлення юридичних прав і обов'язків суб'єктів права [112, с.157-158]. Схожим чином категорію тлумачить С.В. Городянко, наголошуючи: «Норма права – це правило поведінки, встановлене або санкціоноване державою, елементарна частина права, яка відноситься до нього як частина до цілого. Норма права – це загальнообов'язкове, встановлене або санкціоноване й охоронюване державою правило поведінки, що виражає обумовлену матеріальними умовами життя суспільну волю та інтереси народу, активно впливає на суспільні відносини з метою їх впорядкування. Ці норми утворюють єдину систему національного права України, яка складається з галузей та інститутів. Їх ефективна дія неможлива без зв'язку одне з одним. Реалізація правових норм гарантується державою і в необхідних випадках підтримується примусовою силою» [46, с.89].

Влучним є висловлення С.В. Венедіктова: «Норма права – це модель правових відносин. Але сама вона не породжує правовідносин, оскільки будь-яка юридична норма є правилом загального характеру про належну поведінку. Прямого зв'язку з конкретним суб'єктом правових відносин норма не має. Для виникнення правовідносин необхідна подія або дія, що

передбачається нормою і має характер юридичного факту, з появою якого законодавець пов'язує виникнення правових відносин» [38, с.80].

Безпосередньо з приводу змісту норм адміністративного права висловлювався Ю.Н. Старілов, який наголосив, що це встановлені, санкціоновані або ратифіковані державою, формально визначені і забезпечені можливістю державного примусу правила поведінки суб'єктів, що діють у галузі державного управління та сфері забезпечення публічного правопорядку, призначенням і безпосередньою метою яких є організація й регулювання суспільних відносин (а також сприяння цій меті), що забезпечує виникнення та функціонування адміністративно-правових відносин, а також умови реалізації учасниками цих відносин своїх прав та виконання покладених на них обов'язків [73, с.78]. В.М. Манохін вважає, що норми адміністративного права – це встановлені компетентними органами, суворо визначені, забезпечені заходами державного примусу правила поведінки учасників державного управління [4, с.109].

С.В. Пєтков пише: адміністративно-правова норма – це загальнообов'язкове правило поведінки, встановлене державою з метою регулювання суспільних відносин, що входять до предмета адміністративного права, і забезпечене засобами державного примусу. При цьому, науковець уточнює, що норми адміністративного права мають особливу сферу свого застосування – сферу державного управління [157, с.57; 222, с.212]. В.В. Богуцький доводить: адміністративно-правова норма – правило поведінки, яке встановлене державою (Верховною Радою України, органом виконавчої влади) з метою врегулювання суспільних відносин у сфері державного управління. Норми адміністративного права визначають межі належної, допустимої або рекомендованої поведінки людей, діяльності органів виконавчої влади та їх посадових осіб, а також підприємств, установ, організацій і трудових колективів у сфері виконавчої влади [27; 4, с.110].

Отже, норми адміністративного права – це елементарні цеглини правової матерії, крізь які відбувається упорядкування та регулювання суспільно-правових відносин. Значення даних норм у механізмі адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності проявляється в тому, що саме за їх допомогою встановлюються: правила виникнення, функціонування та припинення такої взаємодії, а також повноваження та цілі діяльності її учасників. Тобто, адміністративні норми визначають режим реалізації співпраці між уповноваженими суб'єктами у напрямку протидії кіберзлочинності;

3) нормативно-правові акти. Як зауважує В.С. Нерсесянц, поняття «нормативно-правові акти» охоплює широкий комплекс актів правотворчості, прийнятих органами законодавчої, виконавчої, а іноді й судової влади. Нормативно-правовими актами, продовжує вчений, вони називаються тому, що містять норми права. По суті дане поняття є синонімом поняття «законодавство» в широкому значенні. Це основне джерело права в країнах романо-германського правового сімейства [164]. В.В. Лазарев під нормативними правовими актами розуміє акти, які встановлюють норми права, що вводять їх в дію, змінюють або відміняють правила загального характеру [164, с.70].

О.Г. Дергільова вказує: правовий акт – це передусім акт-волевиявлення (рішення) уповноваженого суб'єкта права. Саме завдяки волевиявленню ми отримуємо результат у вигляді певного акту, що регулює суспільні відносини. Фактично, таке регулювання здійснюється за допомогою встановлення (зміни, скасування) правових норм, а також визначення (зміни, припинення) на основі цих норм прав і обов'язків учасників конкретних правовідносин, міри їх відповідальності. Зазначене волевиявлення здебільшого оформляється у вигляді письмового документа (акту-документа). Враховуючи зазначені характеристики, можна виділити певні ознаки правового акту: він виражає волю (волевиявлення) уповноваженого суб'єкта права, його владні веління; зазначене

волевиявлення має офіційний характер, воно обов'язкове для виконання; його соціальне призначення – регулювання суспільних відносин; завдяки такому волевиявленню встановлюються правові норми, а також виникають конкретні правовідносини; може бути актом-документом, зміст якого фіксується у документальній формі, і актом-дією, за допомогою якого виникає юридичний результат (усний наказ командира або жест представника поліції); і, безумовно, таке волевиявлення становить юридичний факт, що спричиняє певні правові наслідки [52, с.4].

Широку та обґрунтовану характеристику надає М.І. Смокович, який вказує: «Нормативно-правовий акт – це акт правотворчої діяльності компетентних державних органів, що встановлює, змінює чи скасовує норми права. Іншими словами, нормативно-правовий акт – це документ, прийнятий у визначеному порядку компетентним державним органом, у якому містяться норми права. Нормативні акти діють у часі, просторі та щодо кола осіб. Характеризуючи дію нормативно-правових актів у часі, важливо визначити момент набрання та припинення ними чинності, а також можливість зворотної дії у часі. За загальним правилом, закони набирають чинності через 10 днів із моменту опублікування, а інші акти – із моменту опублікування. Проте можливі й інші варіанти набрання чинності нормативно-правовими актами. Так, термін може встановлюватися у самому нормативному акті. Якщо нормативний акт не публікується, він набирає чинності з моменту його одержання виконавцем. Нормативно-правовий акт втрачає чинність внаслідок закінчення терміну, протягом якого передбачалась його дія, прямого скасування або фактичного скасування іншим актом» [199, с.36].

Отже, роль нормативно-правових актів у механізмі адміністративно-правового регулювання взаємодії суб’єктів протидії кіберзлочинності полягає у тому, що вони є формою зовнішнього вираження адміністративних норм. Це офіційні документи, прийняті та затверджені уповноваженими державними органами у відповідному порядку, завдяки

чому закріплені в них норми набувають загальнообов'язковості та формальної визначеності. Окрім того, нормативні акти визначають ієрархію адміністративних норм, що регулюють відносини в сфері взаємодії суб'єктів протидії кіберзлочинності, визначаючи їх приналежність до конкретного рівня правової системи та встановлюючи таким чином їх юридичну силу.

4) адміністративні правовідносини. Особливий різновид суспільних зв'язків, які, окрім урегульованості нормами адміністративного права, володіють додатковими та унікальними ознаками. Зокрема, адміністративні правовідносини побудовані на засадах «влада-підпорядкування», де відсутня юридична рівність сторін та виникають в зв'язку з реалізацією органами державної влади та місцевого самоврядування своєї публічної компетенції [196, с.120]. Як елемент механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, правовідносини є середовищем реалізації останніми своїх прав та обов'язків. Тобто, правовідносини зумовлюють законність та нормативну відповідність досліджуваної взаємодії, перетворюючи її із безособового, теоретично можливого типу діяльності на реальну сукупність суспільних зв'язків між уповноваженими суб'єктами дії яких мають юридичні наслідки [80].

Таким чином, саме так, на нашу думку, виглядає механізм адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, адже саме у представлених чотирьох елементах найбільш яскраво висвітлено призначення та закономірність правового впливу. Необхідно наголосити, що кожна наведена складова є цілком самостійною категорією із власним набором специфікацій, але у єдності та взаємодії вони формують цілісне механічне утворення, яке показує юридичну складову виявлення, припинення та профілактики злочинності в кіберпросторі [80].

2.2. Принципи адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Адміністративно-правове регулювання взаємодії суб'єктів протидії кіберзлочинності є складним явищем в основі якого лежить система відправних начал, вихідних ідей, які в науковій літературі прийнято називати принципами. В перекладі з латинського слово «principium» означає основу, першоджерело. В сучасній українській мові під принципом розуміють: 1) основне вихідне положення якої-небудь системи; 2) основні, найзагальніші, вихідні положення, засоби, правила, що визначають природу і соціальну сутність явища, його спрямованість і найсуттєвіші властивості; 3) внутрішнє переконання людини, яке визначає її відношення до дійсності, її норми поведінки та діяльності [147; 122].

Виходячи тільки із лексичної сутності категорії принцип, можна зробити висновок, що в ній уособлено зміст головного, будівного аспекту, певну ідею або закономірність, котра виступає відправною засадою якоїсь діяльності або основною створення чогось, змісту певного об'єкту, теорії і таке інше. Визначене підкреслює полігалузевий характер принципів, внаслідок чого вони зустрічаються практично в кожній науковій галузі. Наприклад, відповідно до філософської точки зору термін «принцип» трактується як особлива форма наукового пізнання, яка забезпечує цілісний зв'язок між фактами, поняттями, законами та теоріями, спрямовуючи процес пізнання та практичного перетворення дійсності. Згідно до логіки принцип означає – основне положення, передумову будь-якої теорії, концепції. У загальній психології під принципом розуміють теорію психології, яка відбиває її закономірність, враховує минулий досвід та стає вихідною вимогою для подальших досліджень і побудов її наступних теорій [143, с.72].

А.Є. Конверський вивчаючи теоретичні та методологічні принципи науки зазначив: принцип – це головне вихідне положення наукової теорії,

що виступає як перше й найабстрактніше визначення ідеї як початкової форми систематизації знань. Автор відмічає, що принцип не вичерпує всього змісту ідеї. Якщо в основі теорії лежить завжди одна ідея, то принципів може бути декілька. Ідеї та принципи створюють закони науки, що відбивають суттєві, стійкі та постійно повторювані об'єктивні внутрішні зв'язки між явищами, предметами, елементами, якостями. Принцип і категорії, що його розкривають, становлять сутність наукової теорії, а перші здогадки, формулювання гіпотези, попередні висновки висловлюються як тлумачення [152].

Ґрунтовного дослідження принципи знайшли в науці управління. За визначенням Ц.А. Ямпольської вони являють собою об'єктивно зумовлені начала, у відповідності з якими відбувається управління, на основі яких воно функціонує [48, с.66]. О.М. Бандурка переконаний, що принципи управління – це вихідні, основні правила, керівні настанови, норми діяльності для впровадження системи, управління загальними процесами. Принципи управління забезпечують інтеграцію окремих видів управлінської діяльності в різних підрозділах системи управління, взаємну їх погодженість та загальну направленість на реалізацію вироблених цілей. На основі принципів організовано процес управління, тобто науково обґрунтоване впровадження дій для здійснення управлінських функцій, вибору методів та прийомів управлінського впливу [15, с.32]. О.В. Жадан охарактеризував принципи управління як систему базових положень, ідей, правил, згідно з якими здійснюється діяльність працівників у тій чи іншій сфері суспільного життя. Вони (принципи управління) відображають закономірності функціонування соціальних спільнот [64, с.576]. Принципи управління за Ю.Ф. Кравченком, – це основні положення, які відображають пізнані та засвоєні людиною об'єктивні закони та закономірності, котрими керуються органи управління в процесі створення й функціонування систем управління. Вони виявляють вимоги до системи, структури, механізму процесу управління. Принципи управління являють

собою результат узагальнення людьми об'єктивно діючих законів та закономірностей, притаманних їм загальних рис, характерних фактів та ознак, що стають загальним началом їхньої діяльності [207, с.109; 42, с.69].

В свою чергу, принципи державного управління на думку О.Ф. Дегтярьова, – це керівні теоретичні ідеї, які покладені в основу формування і функціонування органів державної виконавчої влади. Вони поділяються на соціально-політичні та організаційні. Соціально політичні принципи державного управління: законність, позапартійність, демократизм, науковість, гласність та врахування громадської думки. Організаційні принципи: принцип диференціації та фіксації функцій і повноважень, який передбачає визначення компетенції кожного органу і посадової особи; принцип відповідальності в рамках компетенції; принцип поєднання галузевих, міжгалузевих і територіальних засобів управління, принцип поєднання лінійних і функціональних засад в управлінні [51, с.18]

В площині юридичної науки характеристика категорії принципів відбувається за власним вектором. В найбільш узагальненому вигляді їх визначено як основні засади, вихідні ідеї, що відображають суттєві положення теорії, вчення, науки, системи внутрішнього і міжнародного права [226, с.110–111]. Це енциклопедичне визначення, яке досить часто не підтримується юристами-дослідниками взагалі, або береться за основу в процесі побудови власних доктринальних визначень.

Систематизоване визначення принципів права здійснила Н.М. Крестовська, на думу якої: «принципи права – це закріплені в різних його джерелах або виражені в стійкій юридичній практиці загальновизнані основоположні ідеї, що адекватно відображають рівень пізнання загальносоціальних і специфічних закономірностей права і служать для створення внутрішньо узгодженої та ефективної системи юридичних норм, а також для безпосереднього регулювання суспільних відносин за її прогальності та суперечності» [113, с.219].

Широку та обґрунтовану позицію щодо принципів права навів в своїх роботах М.І. Козюбра: «Принципи права, як і саме право – явище багатогранне, багаторівневе і багатовимірне. Принципи права не можуть бути зведені до зовнішньо виражених знакових форм, що існують незалежно від суб'єкта – людини, як і саме право – до замкнутої, логічно несуперечливої системи норм, сформульованих у законах та інших державних нормативних актах. Принципи права, як і право, мають недержавне походження. Держава долучилася до їхнього формування лише на певних історичних етапах правового розвитку, коли суто емпіричний процес правотворення та усна форма передачі правової інформації виявилися неспроможними забезпечити надійне нормативно-правове регулювання в умовах ускладнення суспільних відносин та їх зростаючого динамізму. У зв'язку з цим виникла потреба в письмовому вираженні правових норм і принципів у формі державних нормативних актів, які не обмежуються фіксацією існуючих типізованих відносин (правовідносин) і судових рішень, а намагаються, з одного боку, регулювати їх наперед, випереджаючи динамізм суспільного життя, що призвело до підвищення рівня абстрактності, загальності нормативних формулювань, а з другого – надати нормам і принципам права більшої визначеності, яка б усувала елементи суб'єктивізму при їх застосуванні» [100, с.144-145].

А.М. Кучук та С.М. Перепьолкін обґрунтували, що принципи права – це правила поведінки, які закріплюють основні (відправні) начала, відображають ідеї справедливості, рівності, свободи й вирізняються імперативністю, об'єктивністю, стабільністю, комплексністю і рівнозначністю [125]. На дуалістичному характері принципів наголошує в своїх роботах П.Ф. карпечкін. З одного боку, - зазначає науковець, принципи права відображають його об'єктивні властивості, зумовлені закономірностями розвитку цього суспільства усією гамою історично притаманних йому інтересів, потреб, суперечностей компромісів класів,

груп і верств населення. З іншого боку, в принципах права втілюється суб'єктивне сприйняття його членами суспільства, їх моральні ті правові погляди, почуття, вимоги, що дістають вираження у різних ученнях, то теоріях, напрямах праворозуміння [82].

В.В. Колесніченко доводить, що принципи права – це основні засади формування, розвитку і функціонування права, що відбивають сутність і призначення права; концентровано виражають важливі риси, властиві даній правовій системі, які втілюють у собі найважливіші ціннісні орієнтири суспільства і визначають конкретний зміст і загальну концептуальну спрямованість правового регулювання суспільних відносин. Вченим висловлюється думка про те, що правильним є погляд, відповідно до якого принципи права не обов'язково повинні бути сформульовані у правових нормах, тому що далеко не завжди і не всі принципи права прямо закріплюються у правових нормах [101, с.7].

Дослідження наукових концепцій дозволило виокремити наступні особливості принципів права в цілому та принципів адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності зокрема. По-перше, в принципах уособлюються загально-соціальні ідеї, уявлення та цінності про дух права та його зв'язок із політичними, економічними, суспільними та іншими процесами життя української нації. Говорячи іншими словами, принципи виражають ідею про право та зміст і призначення його регулюючого впливу на суспільні відносини в тій чи іншій сфері. По-друге, принципи, на відміну від інших юридичних положень, характеризуються найвищим рівнем абстрактності, адже проявляються не в конкретних нормах, а сукупних положеннях нормативно-правових актів, які регулюють відповідний спектр суспільних відносин. Поряд із цим, принципи є найбільш імперативними юридичними положеннями, дія яких розповсюджується на всіх суб'єктів права без виключення. По-третє, принципи визначають зміст і закономірності побудови системи національного права, а також вектори його еволюції та

розвитку. Вони виступають фундаментом або ж ядром права навколо та відповідно до якого вибудовуються складні структури юридичних норм, як то інститути або галузі. По-четверте, принципи забезпечують стабільність та незмінюваність правового регулювання, адже залежать не від писаних положень, а суспільної ідеї про право, якій вони відповідають та яку виражають в собі. Тому їх зміна можлива виключно за рахунок появи нових суспільних цінностей, які змінюють бачення населення стосовно права і правового регулювання, а також зумовлюють бажання змінити існуючи юридичні основи.

Спираючись на викладене, принципи представляють собою сукупність вихідних засад, основоположних, розчинених у адміністративно-правових нормативних актах, стабільних, загальнообов'язкових ідей, які визначають призначення, вектори, цілі та особливості правового регулювання суспільно-правових відносин, що виникають в контексті взаємодії уповноважених суб'єктів протидії кіберзлочинності.

На сторінках юридичної літератури до принципів взаємодії в сфері діяльності суб'єктів публічної влади найчастіше відносять: планування, оперативності та безперервності, чіткого розмежування повноважень, добровільності, індивідуальності та колективності, науковості, конфіденційності, доцільності, наявності єдиної інформаційної бази, раціональності та ефективності, самоврядування, територіальності, забезпечення взаємного зацікавлення суб'єктів взаємодії, відповідальності суб'єктів взаємодії за організацію і виконання спільних заходів і таке інше [99; 224, с.145; 213; 68].

В свою чергу, сектор забезпечення кібербезпеки України, згідно до положень Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII ґрунтується на принципах: 1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом; 2)

забезпечення національних інтересів України; 3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі; 4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері; 5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі; 6) пріоритетності запобіжних заходів; 7) невідворотності покарання за вчинення кіберзлочинів; 8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; 9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях; 10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки [174].

Ми вважаємо, що до ключових принципів, які мають знаходитись в основі адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності слід віднести:

1) принцип законності взаємодії. Категорія законності має складний зміст, внаслідок чого у навчальній та науковій літературі характеризується як: принцип діяльності держави; принцип державного управління; метод державного управління; режим суспільних відносин; мета та функція державного управління тощо. З цього можна стверджувати, що узагальнено законність – це режим (стан) відповідності

суспільних відносин законам і підзаконним нормативно-правовим актам держави, який утворюється в результаті їх неухильного виконання всіма суб'єктами права. До основних ознак (властивостей) законності у правовій державі соціально-демократичної орієнтації відносяться: 1) неухильне дотримання і виконання нормативно- правових актів всіма суб'єктами права; 2) верховенство закону щодо всіх інших правових актів; 3) послідовна боротьба з правопорушеннями і невідворотність юридичної відповідальності за їх вчинення [40].

З викладеного виходить, що законність, як вихідна засада адміністративно-правового регулювання взаємодії суб’єктів протидії кіберзлочинності – це принципова вимога провадження такої спільної діяльності у порядку, який чітко відповідає конституційним положенням та інших Законів України. Це своєрідне легальне «обмеження» взаємодії установленими правовими нормами, яке, в свою чергу, забезпечує її правомірність та юридичну обґрунтованість;

2) принцип поєднання цілей. Дана вихідна засада корелюється із принципом законності. Так, кожен суб’єкт протидії кіберзлочинності взаємодії із іншими виходячи із власних, суб’єктивних функціональних цілей, що визначено на законодавчому рівні. Наприклад, в нормах Закону України «Про Національну поліцію» від 02.07.2015 №580-VIII відмічається, що поліція у процесі своєї діяльності взаємодіє з органами правопорядку та іншими органами державної влади, а також органами місцевого самоврядування відповідно до закону та інших нормативно-правових актів [171]. В Законі України «Про Службу безпеки України» визначено: «Служба безпеки України взаємодіє з державними органами, підприємствами, установами, організаціями та посадовими особами, які сприяють виконанню покладених на неї завдань. Громадяни України та їх об'єднання, інші особи сприяють законній діяльності Служби безпеки України на добровільних засадах» [181]. Тобто, вступаючи у взаємовідносини із іншими органами державної влади, органами місцевого

самоврядування або безпосередньо громадськістю, кожен суб'єктів протидії кіберзлочинності має на меті реалізувати власні інтереси та цілі. Тому, взаємодія в секторі кібербезпеки повинна органічно відповідати запитам всіх учасників, надаючи можливість кожному із них досягти бажаних результатів діяльності;

3) принцип визначеності суб'єктного складу. Згідно із цією основоположною ідеєю взаємодія із протидії кіберзлочинності основується на чітко визначеному колі суб'єктів, які не просто вступають у взаємні відносини, а мають на це повноваження згідно до свого адміністративно-правового статусу. Зазначений принцип втілюється у статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII де вказано: «Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України). Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи

місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; 8) суб'єкти господарювання, громадяни України та об'єднання 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» [174];

4) принцип координації та контролю. Особливий зміст та важливість діяльності із протидії кіберзлочинності зумовлює необхідність забезпечення чіткої, послідовної взаємодії із дотриманням і виконанням кожним суб'єктом своїх обов'язків, що відповідає його адміністративно-правовому статусу в даних відносинах. Досягається це за рахунок існування відповідного порядку контролю та координації процесів співпраці.

Ключове значення в даному питанні відведено Національному координаційному центру кібербезпеки, що є складовим елементом Ради національної безпеки і оборони України. Відповідно до Указу Президента України «Про Національний координаційний центр кібербезпеки» від 07.06.2016 №242/2016 головними завданнями Центру є: 1) здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; 2) здійснення аналізу: стану кібербезпеки; стану кіберзахисту критично важливих об'єктів інфраструктури; результатів проведення огляду національної системи кібербезпеки, огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань

протидії кіберзагрозам, здійснення превентивних заходів у боротьбі з кіберзлочинністю і таке інше; 3) участь у розробленні галузевих індикаторів стану кібербезпеки; 4) прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України; 5) розроблення концептуальних засад і пропозицій щодо: підвищення ефективності заходів стосовно виявлення та усунення чинників, які формують потенційні і реальні загрози у сфері кібербезпеки, підготовки проектів відповідних програм та планів щодо їх попередження і нейтралізації тощо; 6) узагальнення міжнародного досвіду у сфері забезпечення кібербезпеки та кіберзахисту критично важливих об’єктів інфраструктури; 7) участь у забезпеченні розроблення і впровадження суб'єктами забезпечення кібербезпеки механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків; 8) оперативне, інформаційно-аналітичне забезпечення Ради національної безпеки і оборони України з питань кібербезпеки та кіберзахисту критично важливих об’єктів інфраструктури тощо [170].

В даному випадку відмітити також варто органи прокуратури, які володіють повноваженнями координувати діяльність правоохоронних та інших органів в сфері боротьби зі злочинністю, у тому числі кіберзлочинності. Згідно зі статтею 25 Закон України «Про прокуратуру» від 14.10.2014 №1697-VII Генеральний прокурор, керівники відповідних прокуратур, їх перші заступники та заступники відповідно до розподілу обов’язків координують діяльність правоохоронних органів відповідного рівня у сфері протидії злочинності [175].

Детальне окреслення змісту координаційної діяльності прокуратури наведено у Наказі Офісу Генерального прокурора «Про затвердження Порядку координації діяльності правоохоронних органів у сфері протидії злочинності» від 08.02.2021 №28. Згідно до його положень, основними засадами координації є: верховенство права; законність; незалежність і

рівність суб'єктів координаційної діяльності у визначенні проблем у сфері протидії кримінальним правопорушенням, ініціюванні, розробці, узгодженні та реалізації заходів, спрямованих на їх вирішення; обов'язковість виконання узгоджених заходів та контроль за їх реалізацією; системність і повнота використання різних форм координації; публічність, гласність і відкритість координаційних заходів, оприлюднення їх результатів у встановленому законодавством порядку в межах, які не суперечать вимогам законодавства про захист прав і свобод людини та громадянина, державної таємниці та іншої інформації з обмеженим доступом. Основною формою координації є проведення координаційних нарад із керівниками правоохоронних органів. Координація може здійснюватися також в інших формах: а) проведення спільних нарад з керівництвом правоохоронних та інших державних органів; б) створення міжвідомчих робочих груп; в) здійснення спільних виїздів у регіони для проведення узгоджених дій, перевірок і надання допомоги правоохоронним органам у протидії злочинності; г) обмін аналітичною інформацією з питань протидії злочинності, проведення спільних аналітичних досліджень; ґ) розробка спільних наказів, а також підготовка листів інформаційного характеру і документів організаційного та методичного спрямування; д) розробка і забезпечення виконання спільних планів із запобігання, виявлення та припинення кримінальних правопорушень, усунення причин та умов, які сприяли їх вчиненню тощо [168].

Таким чином, дотримання принципу взаємодії та координації має важливе значення з точки зору забезпечення успішної та ефективної протидії кіберзлочинності, оскільки ця сфера вимагає спільних зусиль та постійного оновлення стратегій і заходів для виявлення та подолання загроз. А відтак, координація та контроль допомагають підтримувати високий рівень інформаційної безпеки та ефективно реагувати на нові виклики у сфері кіберзахисту.

Ключове значення в даному питанні відведено Національному координаційному центру кібербезпеки, що є складовим елементом Ради національної безпеки і оборони України. Відповідно до Указу Президента України «Про Національний координаційний центр кібербезпеки» від 07.06.2016 №242/2016 головними завданнями Центру є: «1) здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; 2) здійснення аналізу: стану кібербезпеки; стану кіберзахисту критично важливих об'єктів інфраструктури; результатів проведення огляду національної системи кібербезпеки, огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення превентивних заходів у боротьбі з кіберзлочинністю і таке інше; 3) участь у розробленні галузевих індикаторів стану кібербезпеки; 4) прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України; 5) розроблення концептуальних засад і пропозицій щодо: підвищення ефективності заходів стосовно виявлення та усунення чинників, які формують потенційні і реальні загрози у сфері кібербезпеки, підготовки проектів відповідних програм та планів щодо їх попередження і нейтралізації тощо; 6) узагальнення міжнародного досвіду у сфері забезпечення кібербезпеки та кіберзахисту критично важливих об'єктів інфраструктури; 7) участь у забезпеченні розроблення і впровадження суб'єктами забезпечення кібербезпеки механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків; 8) оперативне, інформаційно-аналітичне забезпечення Ради національної безпеки і оборони України з питань кібербезпеки та кіберзахисту критично важливих об'єктів інфраструктури» тощо [170].

В даному випадку відмітити також варто органи прокуратури, які володіють повноваженнями координувати діяльність правоохоронних та інших органів в сфері боротьби зі злочинністю, у тому числі кіберзлочинності. Згідно зі статтею 25 Закон України «Про прокуратуру» від 14.10.2014 №1697-VII Генеральний прокурор, керівники відповідних прокуратур, їх перші заступники та заступники відповідно до розподілу обов'язків координують діяльність правоохоронних органів відповідного рівня у сфері протидії злочинності [175].

Детальне окреслення змісту координаційної діяльності прокуратури наведено у Наказі Офісу Генерального прокурора «Про затвердження Порядку координації діяльності правоохоронних органів у сфері протидії злочинності» від 08.02.2021 №28. Згідно до його положень, основними засадами координації є: «верховенство права; законність; незалежність і рівність суб'єктів координаційної діяльності у визначенні проблем у сфері протидії кримінальним правопорушенням, ініціюванні, розробці, узгодженні та реалізації заходів, спрямованих на їх вирішення; обов'язковість виконання узгоджених заходів та контроль за їх реалізацією; системність і повнота використання різних форм координації; публічність, гласність і відкритість координаційних заходів, оприлюднення їх результатів у встановленому законодавством порядку в межах, які не суперечать вимогам законодавства про захист прав і свобод людини та громадянина, державної таємниці та іншої інформації з обмеженим доступом». Основною формою координації є проведення координаційних нарад із керівниками правоохоронних органів. Координація може здійснюватися також в інших формах: «а) проведення спільних нарад з керівництвом правоохоронних та інших державних органів; б) створення міжвідомчих робочих груп; в) здійснення спільних виїздів у регіони для проведення узгоджених дій, перевірок і надання допомоги правоохоронним органам у протидії злочинності; г) обмін аналітичною інформацією з питань протидії злочинності, проведення

спільних аналітичних досліджень; ґ) розробка спільних наказів, а також підготовка листів інформаційного характеру і документів організаційного та методичного спрямування; д) розробка і забезпечення виконання спільних планів із запобігання, виявлення та припинення кримінальних правопорушень, усунення причин та умов, які сприяли їх вчиненню тощо» [168];

5) принцип плановості. В науці управління планування являє собою діяльність по виробленню і ухваленню управлінського рішення – воно визначає перспективу розвитку і майбутній стан системи як об'єкта, так і суб'єкта управління, разом узяте. Тобто, це процес прийняття управлінського рішення, який базується на опрацюванні вихідної інформації і передбачає вибір та наукову постановку мети, вибір засобів і шляхів її досягнення за допомогою порівняльної оцінки альтернативних варіантів і вибору найбільш прийнятного з них в очікуваних умовах розвитку [163, с.85-86].Отже, взаємодія суб’єктів протидії кіберзлочинності передбачає проведення цілої низки спільних заходів, кожен з яких має власні особливості реалізації, а також кінцеві цілі. Окрім того, вкрай важливою є доцільність тих чи інших заходів у відповідний проміжок часу та з врахуванням об’єктивної ситуації, наприклад, стадії вчинення злочину, кількості залучених осіб і таке інше. За даних умов планування дозволяє визначити: як саме має відбуватись взаємодія суб’єктів протидії злочинності, які заходи повинна включати, тощо [76];

6) принцип науковості. Ця вихідна засада вимагає, щоб взаємодія суб’єктів протидії кіберзлочинності обґрунтовувалась не тільки юридично, але й науково, тобто спиралась на теоретико-правову базу, а також визначні наукові дослідження, що стане запорукою ефективності, якості, дієвості співпраці, гарантованості виконання державних функції та захисту прав і законних інтересів людини і громадянина у сфері кібербезпеки [76];

7) принцип достатності. Відповідно до цієї вихідної засади взаємодія суб’єктів протидії злочинності повинна включати в себе таку

кількість заходів і процедур, а також консолідацію спільних ресурсів, які забезпечуватимуть повне виконання мети і завдань протидії суспільно-небезпечним діянням в сфері кібербезпеки [76].

Таким чином, саме виділені принципи адміністративно-правового регулювання обумовлюють глобальне призначення, напрям руху та характер взаємодії суб'єктів протидії кіберзлочинності. Вони несуть в собі ґрунтовні, вихідні вимоги щодо механізму провадження такої співпраці та фактично визначають її правову конструкцію. Тому виділення, дотримання та врахування цих принципів є обов'язковим в контексті побудови ефективної та якісної системи взаємодії суб'єктів протидії кіберзлочинності [76].

2.3. Адміністративно-правовий статус суб'єктів взаємодії у сфері протидії кіберзлочинності.

Взаємодія неможлива без сторін, які приймають в ній участь та забезпечують виконання цілей. Кожен із зазначених суб'єктів володіє своїм, особливим адміністративно-правовим статусом. У тлумачних словниках його трактують як стан чого-небудь, або становище [25]. Філософи розглядають статус, як позицію індивіда або групи в системі, що визначається за рядом ознак, характерних даній системі [129, с.663]. Вищевикладене свідчить, що оцінювати статус, як синонім категорії «стан» є помилкою. Адже етимологічно стан – це сукупність величин, що характеризують фізичні ознаки тіла [25]. Тобто, в даному разі йдеться про набір певних внутрішніх ознак якогось об'єкту, в той час як статус – це характеристика останнього у системі зовнішніх координат, що підтверджується філософськими трактуваннями.

Значного розвитку та вивчення концепція статусу отримала у соціологічній науці. Зокрема, категорія «соціальний статус» є важливим

елементом понятійного апарату вказаної галузі знань. В широкий науковий обіг це поняття введене М. Вебером. Терміном «соціальний статус» вчений позначає реальні претензії на позитивні чи негативні привілеї щодо соціального престижу, якщо він ґрунтується на одному або більшій кількості наступних критеріїв: 1) спосіб життя; 2) формальна освіта, яка полягає в практичному або теоретичному навчанні та засвоєнні відповідного способу життя; 3) престиж народження чи професії. Також необхідно зазначити, що стратифікаційний статус може бути пов'язаний із класовим статусом різними способами. На думку М. Вебера, гроші та підприємницькі позиції не є умовами, які визначають статус, хоча можуть спонукати їх. Відсутність власності також не є самостійним приводом для виключення з певного статусу, хоча теж може сприяти цьому. Навпаки, соціальний статус частково або повністю може визначати класовий статус, хоча і не ідентичний йому. Класовий статус, скажімо, військового офіцера, цивільного службовця чи студента, оскільки вони залежать від одержуваних доходів, може сильно відрізнятися, хоча в усіх прикладах їх спосіб життя визначається загальною умовою – освітою [218, с.111].

В сучасній соціології розуміння статусу набуло подальшого розвитку та вивчення. Наприклад, В.В. Вербець, О.А. Субота та Т.А. Христюк доводять: соціальний статус – це положення соціального суб'єкта в суспільстві, що передбачає для нього певні специфічні права і обов'язки, правила поведінки. Соціальний статус визначає становище індивіда або соціальної групи стосовно інших індивідів і груп, яке визначається за соціально значущими для даної соціальної системи критеріями (економічними, політичними, соціально-правовими, професійно-кваліфікаційними тощо). Соціальний статус не є поняттям статичним, оскільки виступає як елемент співвідношення з іншими соціальними суб'єктами. Конкретний статус охоплює визначену систему відносин і відноситься лише до неї. Він у будь-якому випадку, передбачає для

соціального суб'єкта певні права й обов'язки, правила розпорядку або правила поведінки [39].

М.В. Сидоров наголошує на тому, що соціальний статус є однією із найголовніших характеристик індивіда, що детермінує його цінності, поведінку, можливості, обов’язки та права, стиль життя тощо. Соціальний статус, здебільшого, корелюється майже з усіма позиціями індивіда, його реакціями на соціо-культурні та економічні зміни, світові процеси тощо. Через статус відбувається аналіз його поглядів, реакцій на події. Без належної системи визначення соціального статусу неможлива адекватна оцінка реального положення індивіда, яке він займає у соціальній системі суспільства [189].

За концепцією М.В. Примуша, соціальний статус – це становище індивіда (або групи людей) у системі соціальних зв'язків і відносин, що обумовлюється її приналежністю до певної соціальної спільноти та визначає сукупність її прав та обов'язків. Статус людини формується різноманітними ознаками, серед яких є ті, які успадковуються – стать, етнічна приналежність, соціальне походження, а також ті, які людина здобуває завдяки власним зусиллям – освіта, професія, доходи тощо. Відповідно до цього розрізняють статус аскриптивний (приписаний) і статус здобутий. Будь-яку людину можна охарактеризувати за допомогою певного статусного набору – це сукупність усіх статусів, що має дана людина. Але її положення у суспільстві визначає, так званий, головний статус. Якщо соціальний статус визначає місце індивіда в суспільстві, то – особистий його позицію в середовищі безпосередньо до оточуючих його людей. Особистий статус – це становище людини в малій (первинній) групі, що обумовлюється тим, як ставляться до нього оточуючі [166].

Таким чином, соціальний статус – це набір характеристик людини, які визначають її місце та роль у суспільстві в цілому та відповідних соціальних групах, зокрема, сім’ї, трудовому чи навчальному колективі тощо. Подібна концептуальна модель лягла в основу категорії «правовий

статус» із певними відмінностями. Так, І.І. Литвин пише, що правовий статус – це юридично закріплене становище суб’єкта в суспільстві, тобто сукупність прав та обов'язків, які визначені та гарантовані Конституцією та законами України, іншими нормативно-правовими актами, міжнародними договорами, згода на обов'язковість. яких надана Верховною Радою України [129, с.21].

На думку О.В. Зайчука, правовий статус як юридична категорія не лише визначає стандарти можливої та необхідної поведінки, що забезпечують нормальну життєдіяльність соціального середовища, а й характеризують реальну взаємодію держави та особи [201, с.48]. Ю.С. Новікова визначає правовий статус або стан як обумовлений соціально-культурними умовами життєдіяльності суспільства різновид соціального стану, який представляє собою спосіб юридичного буття суб'єктів, об'єктів або суспільних відносин у визначений проміжок часу у визначеному просторі, як правило, закріплений у встановленому законом порядку. Автор розглядає правовий стан як самостійну правову категорію, наділену певними характерними ознаками: 1) є загальним поняттям правознавства, зміст якого ширше аналогічних понять галузевих юридичних наук; 2) виступає у формі фундаментального теоретичного поняття теорії права та грає методологічну роль по відношенню до галузевих юридичних наук; 3) дає можливість відтворити реальну картину правової дійсності, роз- крити її суттєві властивості, виявити особливості права у порівнянні з іншими суспільними явищами; відображає не лише теоретичні, але і практичні потреби; 4) сприяє поєднанню правових знань, розроблених в галузевих юридичних науках, і тим самим сприяє цілісності пізнавальної діяльності в усіх областях юридичної науки; 5) може бути переміщена на інші області знань [29, с.17]. Р.М. Савчук скомпонував в своєму науковому дослідженні різні підходи до розуміння правового статусу вказавши, що категорію можна розглядати у таких значеннях: 1) визначене нормативно-правовими актами правове становище фізичної або

юридичної особи, що характеризується сукупністю її прав, обов'язків, гарантій та відповідальності; 2) юридична міра соціальної свободи суб'єкта права, що визначає межі, в яких можуть відбуватися кількісні зміни його правового становища; 3) сукупність юридичних прав, свобод і обов'язків особи, які закріплені в діючому законодавстві і складають соціально допустимі і необхідні потенційні можливості особи мати суб'єктивні права і обов'язки і реалізувати їх в системі суспільних відносин; 4) встановлене правовими нормами положення його суб'єктів, сукупність їх прав та обов'язків, що у концентрованому вигляді відображається у законах, положеннях, статутах та інших нормативно-правових актах про відповідні органи, установи [185]. За позицією Н.М. Оніщенко правовий статус – це система законодавчо встановлених та гарантованих державою прав, свобод, законних інтересів та обов'язків суб'єкта суспільних відносин. Характерними ознаками правового статусу науковець вважає: 1) універсальність (він поширюється на всіх суб'єктів); 2) індивідуальність (він відображає індивідуальні особливості людини та її реальне становище у суспільних відносинах); 3) взаємозв'язок із іншими компонентами; 4) системність [205, с.366; 50].

Адміністративно-правовий статус є відмежуванням правового та показує відповідну галузеву належність. У словнику термінів з адміністративного права дана категорія визначена, як закріплене нормами адміністративного права положення суб'єкта, яке характеризується суб'єктивними правами, юридичними обов'язками та відповідальністю суб'єкта у сфері публічного адміністрування, а його ознаками є: 1) урегульованість адміністративно-правовими нормами; 2) структурність (права, обов'язки, відповідальність); 3) визначення меж діяльності суб'єкта щодо інших осіб; 4) визначення сфери його реалізації у межах наступних блоків правовідносин: публічного управління, відносин адміністративних послуг, відносин відповідальності публічної адміністрації за неправомірні дії або бездіяльність, відносин відповідальності суб'єктів суспільства

(індивідальних і колективних) за порушення встановленого публічною адміністрацією порядку і правил [2, с.405; 132, с.195]

На думку Т.О. Коломоєць, адміністративно-правовий статус – це сукупність суб'єктивних прав і обов'язків закріплених нормами адміністративного права за певним органом. Водночас обов'язковою ознакою набуття суб'єктом адміністративно-правового статусу є наявність у нього конкретних суб'єктивних прав і обов'язків, що реалізуються у рамках як адміністративних правовідносин, так і поза ними [102, с.64]. С.Г. Стеценко наголошує: адміністративно-правовий статус – це сукупність прав, обов’язків та гарантій їх реалізації, закріплених у нормах адміністративного права. В основі адміністративно-правового статусу лежить адміністративна правосуб’єктність. Вчений відмічає, що кожний суб’єкт адміністративного права має свій варіант притаманного йому адміністративно-правового статусу. Важлива обставина, на яку слід звернути увагу,– модифікація з часом проявів адміністративної правосуб’єктності та, як наслідок, адміністративно-правового статусу [202, с.92-93; 210, с.68].

Б.М. Лазарєв, пов’язує зміст адміністративно-правового статусу виключно із суб’єктами владних повноважень, а саме органами державної влади. Розкриваючи зміст категорії вчений наголосив, що вона передбачає відповіді на питання: а) органом якого рівня є даний орган: центральний, місцевий або міжтериторіальний; б) до якого виду органів належить за змістом своєї діяльності: орган влади, орган управління, правосуддя, яке офіційне найменування даного органу; в) хто його утворює, формує особовий склад; г) кому він підпорядкований, підзвітний, підконтрольний і перед ким, хто може відміняти, призупиняти, змінювати і опротестовувати його акти; д) яка компетенція органу; є) хто йому підпорядкований, підзвітний, підконтрольний, чиї акти він може відміняти, призупиняти, змінювати і опротестовувати та інше; ж) яка юридична сила актів даного органу; з) які джерела фінансування; і) чи володіє правами юридичної

особи [19, с.5]. У схожих наукових координатах адміністративно-правовий статус досліджував Ю.А. Дмітрієв, вказуючи, що це характеристика цілей, функцій та повноважень органів державної влади та публічного управління у певній сфері [200, с.229].

Таким чином, категоріями правового та адміністративно-правового статусу описується місце суб'єкта у межах суспільно-правових відносин, а також набуття ним у зв'язку із цим визначених законодавством України додаткових суб'єктивних характеристик, як то права та обов'язки. Спираючись на це, адміністративно-правовий статус суб'єктів протидії кіберзлочинності в Україні – це сукупність визначених нормами адміністративної галузі права елементів, які в своїй єдності визначають положення та роль суб'єктів протидії кіберзлочинності у суспільно-правових відносинах, що виникають в процесі здійснення ними спільної діяльності за відповідним напрямом.

При цьому, складові адміністративно-правового статусу – це не абстрактне поняття, а цілком реальний перелік структурних елементів. Наукові підходи щодо виділення останніх різняться на сьогоднішній день. Наприклад, за Д.М. Бахрахом, адміністративно-правовий статус складається з трьох блоків: 1) цільового, який визначає норми про цілі (мету), завдання та функції діяльності; 2) організаційно-структурного, який утворюють правові приписи, що регламентують порядок утворення, реорганізації, ліквідації суб'єкту адміністративно-правових відносин, його структуру, лінійну і функціональну підпорядкованість; 3) компетенції як сукупності владних повноважень і підвідомчості [7, с.90]. А.М. Подоляка пропонує такі структурні елементи адміністративно-правового статусу: права, обов'язки, особливості юридичної відповідальності, які обумовлюються специфікою повноважень [161, с.10; 87, с.44].

М.Г. Ісаков наголосив, що елементами адміністративно-правового статусу є: 1) мета, завдання та функції; 2) компетенція; 3) гарантії діяльності; 4) відповідальність [74, с.93]. До елементів адміністративно-

правового статусу, на думку О.В. Мещерякової, слід відносити: адміністративну правосуб'єктність, права, обов'язки, заборони і відповідальність за їх порушення [139, с.610; 49, с.87; 216, с.118-119]. М.М. Добкін, висловив думку відповідної до якої адміністративно-правовий статус є комплексним явищем, яке складається з прав, обов'язків, гарантій і відповідальності суб'єктів права. Вчений наголошує, що передумовою виникнення адміністративно-правового статусу є наявність адміністративної правосуб'єктності, яка свідчить про те, що орган влади є суб'єктом адміністративного права. Адміністративна правосуб'єктність розуміється ним як здатність мати й здійснювати суб'єктивні права й обов'язки [56, с.13; 95, с.93]

В роботах окремих науковців структура адміністративно-правового статусу виділяється у відношенні до конкретних суб'єктів правовідносин. Наприклад, елементами адміністративно-правового статусу органів місцевого самоврядування І.Я. Рущак вважає сукупність предметів відання, завдань, функцій, територіальних меж діяльності кожного окремого органу, повноважень щодо управління справами місцевого значення під свою відповідальність в інтересах та від імені відповідних територіальних громад в межах Конституції та законів України [184]. О.М. Рєзнік пропонує у структурі адміністративно-правового статусу правоохоронних органів як суб'єктів забезпечення фінансово-економічної безпеки держави виділяти такі елементи як: 1) мету, завдання та функції правоохоронних органів, що забезпечують фінансово-економічну безпеку України; 2) компетенцію і повноваження правоохоронних органів, що забезпечують фінансово-економічну безпеку України; 3) організаційно-штатну структуру правоохоронних органів, що забезпечують фінансово-економічну безпеку України; 4) юридичні гарантії та юридичну відповідальність правоохоронних органів. При цьому науковець відмічає, що компетенція становить сферу діяльності певного правоохоронного органу, тоді як повноваження – сукупність прав і обов'язків

правоохоронного органу, наданих йому законодавством для виконання покладених на нього функцій у межах компетенції [183, с.141; 132, с.196].

Досліджені підходи щодо елементів категорії «адміністративно-правовий статус» показують відсутність спільної концептуальної позиції з приводу даної проблеми. При цьому, найчастіше вчені надають не загальну характеристику складових структури, а розглядають їх крізь особливості відповідного суб'єкта правовідносин. Через це, фактично відсутня на сьогодні класична модель структури адміністративно-правового статусу, яка б містила в собі загально-обов'язковий перелік елементів.

Спираючись на вказаний негативний момент, на нашу думку, до елементів адміністративно-правового статусу суб'єктів взаємодії у сфері протидії кіберзлочинності, слід віднести:

1) компетенцію. В адміністративному праві компетенцію прийнято розглядати, як певний обсяг діяльності, покладений на конкретний суб'єкта, або коло питань, передбачених законодавством, іншими нормативно-правовими актами, які він має право вирішувати в процесі практичної діяльності (коло питань, що вирішуються міністерством, визначається у положенні про відповідне міністерство; відомством – у положенні про відповідне відомство) [8, с.39]. Кожен суб'єкт протидії кіберзлочинності володіє власною компетенцією, яка закладена в його установчих документах (законах та положеннях). Наприклад, КМУ згідно із законом України «Про Кабінет Міністрів України» від 27.02.2014 №794-VII здійснює виконавчу владу безпосередньо та через міністерства, інші центральні органи виконавчої влади, Раду міністрів Автономної Республіки Крим та місцеві державні адміністрації, спрямовує, координує та контролює діяльність цих органів. До основних завдань Кабінету Міністрів України належать: «1) забезпечення державного суверенітету та економічної самостійності України, здійснення внутрішньої та зовнішньої політики держави, виконання Конституції та законів України, актів

Президента України; 2) вжиття заходів щодо забезпечення прав і свобод людини та громадянина, створення сприятливих умов для вільного і всебічного розвитку особистості; 3) забезпечення проведення бюджетної, фінансової, цінової, інвестиційної, у тому числі амортизаційної, податкової, структурно-галузевої політики; політики у сферах праці та зайнятості населення, соціального захисту, охорони здоров'я, освіти, науки і культури, охорони природи, екологічної безпеки і природокористування; 4) розроблення і виконання загальнодержавних програм економічного, науково-технічного, соціального, культурного розвитку, охорони довкілля, а також розроблення, затвердження і виконання інших державних цільових програм; 5) забезпечення розвитку і державної підтримки науково-технічного та інноваційного потенціалу держави; 6) забезпечення рівних умов для розвитку всіх форм власності; здійснення управління об'єктами державної власності відповідно до закону; 7) здійснення заходів щодо забезпечення обороноздатності та національної безпеки України, громадського порядку, боротьби із злочинністю, ліквідації наслідків надзвичайних ситуацій; 8) організація і забезпечення провадження зовнішньоекономічної діяльності, митної справи; 9) спрямування та координація роботи міністерств, інших органів виконавчої влади, здійснення контролю за їх діяльністю» [169].

Однак, вступаючи у відносини із протидії кіберзлочинності та взаємодії з іншими суб'єктами цій сфері, компетенція КМУ розширюється за рахунок спеціального законодавства, що регулює основи забезпечення кібербезпеки. Положеннями Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII, на наш погляд, досить вірно та повно визначено компетенцію всіх учасників досліджуваних суспільно-правових відносин. Так, відповідно до частини 5 статті 5 Закону суб'єкти забезпечення кібербезпеки у межах своєї компетенції: 1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та

інших протиправних і злочинних цілях; 2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; 3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; 4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; 5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; 6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору [174];

2) повноваження. Це складова компетенції, яка включає в себе права, обов'язки та завдання діяльності кожного суб'єкта. Повноваження також поділяються на загальні та цільові. Перші притаманні суб'єктам взаємодії у сфері протидії кіберзлочинності згідно до їх відомчих документів за напрямами діяльності, в той час як другі вони набувають в контексті співпраці та протидії кіберзлочинам. Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII зазначене питання досить ґрунтовно розкрито. В положеннях акту вказано: основними суб'єктами національної системи кібербезпеки є 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, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання: «1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки

щодо кіберзахисту тощо; 2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі; 3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; 4) Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану; 5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки; 6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких

здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг» і таке інше [174];

3) гарантії. Зазначений елемент адміністративно-правового статусу включає в себе зовнішні та внутрішні, юридично визначені умови, які забезпечують повну та ефективну реалізацію вказаними суб'єктами своїх повноважень. Сюди можна віднести: 1) діяльність Національного координаційного центру кібербезпеки, який стимулює роботу уповноважених учасників протидії кіберзлочинності, а також слідкує за її правильністю, корегуючи за необхідності; 2) обов'язок сприяння суб'єктам забезпечення кібербезпеки з боку всіх органів державної влади, місцевого самоврядування та громадян; 3) функціонування урядової команди реагування на комп'ютерні надзвичайні події України «CERT-UA», завданнями якої є: «а) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; б) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; в) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; г) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; г) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; д) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки із сплатою щорічних членських внесків; е) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; є) опрацювання отриманої від громадян інформації про

кіберінциденти щодо об’єктів кіберзахисту; ж) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам» [174].

4) юридична відповідальність суб’єктів взаємодії у сфері протидії кіберзлочинності. В загальному значенні відповідальність – це необхідність відповідати за свої дії, бути відповідальним за них. Філософія вивчає відповідальність як поняття, що відображає об’єктивний, історично конкретний характер взаємин між особою, колективом, суспільством з погляду свідомого здійснення взаємних вимог. З точки зору соціології, відповідальність – це підзвітність кожного члена суспільства, положеність до відповіді, обов’язок дати звіт про свою суспільну поведінку. Відповідальність взагалі – значить обов’язок дати відповідь за свою суспільну поведінку і прийняти осуд, його негативні суспільні наслідки. Відповідальним є той, хто зобов’язаний; хто не зобов’язаний, той не відповідає [107, с.59; 142; 187, с.358]. Юридична відповідальність – це передбачені законом вид і міра державно-владного (примусового) зазнання особою втрат благ особистого, організаційного і майнового характеру за вчинене правопорушення [91, с.224].

Таким чином, саме така структура найбільш повно та повно розкриває всі особливості адміністративно-правового статусу суб’єктів взаємодії у сфері протидії кіберзлочинності. Виділені елементи в своїй сукупності дозволяють побачити: як саме трансформується юридичне положення учасників у відносинах взаємодії та якими новими характеристиками доповнюється.

2.4. Форми та методи взаємодії суб'єктів протидії кіберзлочинності.

Спільна діяльність суб'єктів протидії кіберзлочинності знаходить своє об'єктивне відображення у низці форм, які в свою чергу реалізуються за допомогою використання спеціальних інструментів та засобів, які прийнято називати методами. Термін «форма», на переконання О.Б. Німко, означає вид, будь-який зовнішній прояв певного змісту. Це шлях здійснення цілеспрямованого впливу, що вказує як практично здійснюється управлінська діяльність [145]. Ю.П. Битяк та В.В. Зуй визначили форми управління як зовнішнє вираження конкретних дій державного органу, його структурних підрозділів та посадових осіб (службовців), що використовуються в процесі державної виконавчої діяльності і спрямовані на реалізацію функцій управління [21, с.91].

Форми, пише О.Ф. Андрійко, представляють собою зовнішні, постійно використовувані вирази (вияви) практичної діяльності державних органів у процесі формування та виконання управлінських завдань і функцій, а також в забезпеченні їх власного функціонування. Форму, продовжує автор, можна описати як видиму дію, яку виконавчий орган (або його посадова особа) здійснює в рамках своєї компетенції, і яка призводить до конкретних наслідків. Якщо ці наслідки мають юридичний характер або важливі юридичні наслідки, то такі форми узагальнено класифікуються як адміністративно-правові [10, с. 43]. Н.М. Пахоменко вказує, що форма у праві представляє собою комплексну наукову категорію, яка служить для відображення різних соціальних явищ, що потребують нормативного регулювання. Крім того, вона виступає основною структурною основою в самому праві, де вона організовує і об'єднує всі юридичні явища та надає їм логічну послідовність. Коли ми говоримо про правові форми, ми маємо на увазі саме право як певне соціальне явище, відокремлене від інших явищ, таких як політика, релігія,

чи мораль, і спільно з ними обумовлене матеріальними та економічними умовами суспільства. Іншими словами, термін «правова форма» є загальним способом відображення об'єктивних зв'язків між правом і тими явищами, на які воно впливає, та визначає його позицію серед інших форм в суспільстві [153].

Таким чином, під формами взаємодії суб’єктів протидії кіберзлочинності найбільш доцільно розуміти зовнішній вираз спільної, взаємоузгодженої практичної діяльності спеціально уповноважених органів державної влади та їх посадових осіб, яка спрямована на досягнення єдиної мети – протидія та запобігання правопорушенням та злочинним діям, які відбуваються в кіберпросторі або з використанням комп'ютерних технологій і мереж. Варто зауважити, що в науковій літературі не сформовано єдиного підходу щодо переліку відповідних форм, а відтак, останні, на нашу думку, найбільш доцільно поділити на дві групи: 1) нормативно-правові: нормотворчість; адміністративний договір; правозастосування; 2) організаційно-управлінські форми: підготовка і реалізація спільних заходів; створення спільних робочих груп; адміністративний нагляд; просвітницька робота з громадськістю. Надамо характеристику кожній із окреслених форм.

В юридичній науці нормотворчість – це ключовий елемент правотворення, який представляє собою специфічний юридичний процес, який виконується уповноваженими суб'єктами і призводить до перетворення волі політичних сил, які мають владні повноваження (наприклад, народу, класу або соціальної групи), в норми права, що виражаються у вигляді юридичних норм в певних джерелах права. Основні характеристики нормотворчості, на переконання І.О. Пасічної, включають: 1) виконання уповноваженими суб'єктами, такими як державні органи (парламент, уряд, міністерства, місцеві адміністрації) або цивільне суспільство (народ, його організації); 2) владна вольова діяльність уповноважених суб'єктів, яка включає аналіз, узагальнення та

систематизацію типових конкретних юридичних відносин, що виникають у суспільстві. Ця діяльність не є диктатом волі уповноважених суб'єктів, а процесом формулювання норм, які відповідають соціальним відносинам і стали типовими діями їх учасників; 3) санкціонування існуючих норм або встановлення нових, зміну або припинення дії чинних правових норм відповідно до закону; 4) завершення виражається у створенні письмового акта-документа, який називається нормативно-правовим актом, наприклад, законом. Результат нормотворчої діяльності може набувати інших юридичних форм вираження, таких як нормативний договір, судовий прецедент або правовий звичай; 5) виконання з дотриманням правового регулювання, включаючи процедури підготовки і прийняття нормативного акта [154].

На переконання О.В. Петришина, нормотворчість означає діяльність, яку проводять уповноважені суб'єкти з розроблення, розгляду, прийняття та офіційного оприлюднення нормативно-правових актів, і ця діяльність виконується відповідно до встановленої процедури. Також вчений виділив такі характеристики нормотворчості: 1) нормотворчість є етапом процесу створення правових норм. Під час нормотворчості в нормативно-правових актах закріплюються правові норми, які виникають на основі узагальнення найбільш важливих і повторюваних суспільних відносин і служать для витіснення шкідливої практики; 2) нормотворчість є однією з форм діяльності публічної влади, яка існує поруч з правозастосуванням, тлумаченням права, контролем та установчою діяльністю; 3) результатом нормотворчості є нормативно-правові акти, які офіційно закріплюють правові норми; 4) нормотворчість виконується уповноваженими суб'єктами, такими як органи державної влади, органи місцевого самоврядування, їх посадові особи, народ та територіальні громади; 5) нормотворчість проводиться відповідно до певної процедури, яка регулюється законодавством [206].

О.Ф. Скакун досить розгорнуто підійшла до визначення сутності та змісту нормотворчості. Так, вчена вказала, що нормотворчість представляє собою офіційну діяльність суб'єктів, уповноважених державою та громадянським суспільством, спрямовану на встановлення, зміну, призупинення і скасування правових норм, а також на їх систематизацію. Основною метою нормотворчості є формулювання нових правових норм, які відповідають сучасним соціальним відносинам, тобто створення моделі суспільних відносин, які з погляду держави або громадянського суспільства (народу) є прийнятними або необхідними. Зміни в чинних нормах та скасування застарілих правових положень сприяють укріпленню нових норм і, таким чином, вони включаються в сферу нормотворчості як її важливий аспект [193]. До основних рис нормотворчості, на переконання О.ф. Скакун, слід віднести такі: 1) здійснюється вповноваженими суб'єктами, а саме: а) державою та її органами (парламентом, урядом, міністерствами, місцевими адміністраціями тощо); б) громадянським суспільством (народом) і його організаціями; 2) ця діяльність є формою волевиявлення уповноважених суб'єктів, що включає в себе аналіз, узагальнення та систематизацію типових конкретних правовідносин, що виникають у суспільстві. Важливо підкреслити, що нормотворчість не є простим диктатом волі уповноважених суб'єктів, а складною процедурою формулювання норм, які відповідають соціальним відносинам та стають типовими для їх учасників; 3) результати нормотворчості виражаються у санкціонуванні чинних правових норм, уведенні нових норм, зміні чинних норм або призупиненні їх дії відповідно до вимог законодавства; 4) нормотворчість завершується оформленням у письмовому акті-документі, який називається нормативно-правовим актом, наприклад, законом [193].

Ю.П. Сурмін і В.Д. Бакуменко пишуть, що нормотворчість – це спеціальна організаційно-правова діяльність уповноважених суб’єктів, яка полягає в ініціюванні, підготовці й розгляді проєктів нормативних актів,

ухваленні нормативних актів та введенні їх у дію. Нормотворчість здійснюється за певною процедурою, що складається із низки стадій – самостійних, логічно завершених етапів та організаційно-технічних дій щодо підготовки та ухвалення нормативних актів, якими є: нормотворча ініціатива і підготовка проєкту нормативного акта, внесення проєкту нормативного акта на розгляд суб'єкту нормотворення, розгляд та обговорення проєкту нормативного акта, ухвалення нормативного акта, введення нормативного акта в дію [64]. Тож, нормотворчість є комплексною науковою категорією, яка характеризується тим, що вона є: початковою стадією механізму правового регулювання, елементом правової системи і правової культури суспільства, в процесі якого відбувається перетворення потреб та інтересів у загальнообов'язкові, формально-визначені приписи і правила; засобом організації соціального управління, однак при цьому процес нормотворчості сам врегульований правом й іншими соціальними нормами; цілеспрямованою діяльністю, що триває в певних часових проміжках і містить внутрішні елементи – етапи процесу зародження правової норми і набрання нею чинності, за допомогою якої відбувається зміна суспільного життя [144].

Таким чином, нормотворчість є надважливо формою взаємодії суб'єктів протидії кіберзлочинності, адже саме за її допомогою вбачається можливим створити нормативно-правові основи: по-перше, для забезпечення загального функціонування сфери протидії та запобігання кіберзлочинності, тобто незаконному отриманню, збереженню, обробці, передачі або використанню інформації тощо; по-друге, для належного функціонування спільної діяльності відповідних органів державної влади та їх посадових осіб, що зробить їх роботу більш ефективною та дієвою. Окрім того, саме за допомогою нормотворчості вбачається можливим оновити законодавство у відповідній сфері, зокрема виявити та покращити застарілі та не ефективні норми, які перешкоджають нормальному функціонуванню суспільних відносин у досліджуваній сфері.

Поряд із нормотворчістю також слід вказати таку форму взаємодії, як адміністративний договір. Адміністративний договір, пише С.С. Скворцов, – це нове суперечливе та недостатньо досліджене явище, оскільки природа державного управління полягає в імперативності одностороннього волевиявлення з метою організуючого впливу на суспільство, а природа договорів полягає у рівності сторін та свободі вибору поведінки [182, с. 81]. Зауважимо, що відповідно до п. 16 ч. 1 ст. 4 КАС України: «адміністративний договір – спільний правовий акт суб'єктів владних повноважень або правовий акт за участю суб'єкта владних повноважень та іншої особи, що ґрунтується на їх волеузгодженні, має форму договору, угоди, протоколу, меморандуму тощо, визначає взаємні права та обов'язки його учасників у публічно-правовій сфері і укладається на підставі закону: а) для розмежування компетенції чи визначення порядку взаємодії між суб'єктами владних повноважень; б) для делегування публічно-владних управлінських функцій; в) для перерозподілу або об'єднання бюджетних коштів у випадках, визначених законом; г) замість видання індивідуального акта; ґ) для врегулювання питань надання адміністративних послуг» [98]. Щодо даного визначення Н.В. Добровольська зазначила, що сприйняття цитованої офіційної дефініції потребує урахування двох важливих аспектів: по-перше, вона визначається в контексті вищого юридичного акта та, у сфері адміністративного права (матеріально-процесуального), може розглядатися скоріше як допустима прийнятність (в відсутності "іншого") ніж обрана доцільність; по-друге, ця офіційна інтерпретація адміністративного договору встановлювалася для чіткого визначення тематичних меж юрисдикції адміністративних судів (що підтверджується обмеженою кількістю прямих згадувань адміністративного договору в законодавстві України - лише у чотирьох статтях). Це пояснює і виправдовує деякі критичні оцінки стосовно законної дефініції (в умовах такого контексту важко досягти її абсолютної досконалості, оскільки вона об'єднує

різноманітні теоретичні підходи) та спонукає до подальших обговорень. Необхідно відзначити, що законодавча дефініція стала узагальненням різних дотримуваних теоретичних позицій, і зв'язок між "правом" і "процесом" є безсумнівним. Положення, зокрема спеціалізовані, Конституційного Суду України стають важливою орієнтирною точкою для теоретичних розв'язань у сфері адміністративного права, наприклад, в питаннях тлумачення "публічної служби" або розуміння принципів адміністративних процедур з урахуванням критеріїв, за якими суд оцінює законність рішень, дій або бездіяльності суб'єктів з владними повноваженнями [57].

С.С. Скворцов доводить, що адміністративний договір – це заснована на правових нормах добровільна угода двох чи більше суб’єктів адміністративного права, один із яких завжди є самостійним суб’єктом державної виконавчої влади, наділеним владними повноваженнями у сфері державного управління, за допомогою якого формуються акти державного управління, на основі яких встановлюються, змінюються чи припиняються взаємні права і обов’язки учасників договору, визначається їх відповідальність. За допомогою адміністративного договору, продовжує автор, учасники правовідносин визначають правила власного поводження і встановлюють послідовність своїх дій, досягають необхідного для них правового результату [195, с.12]. Ю.П. Битяк та О. Константий вважають, що «адміністративний договір – це правовий акт управління, що встановлюється на підставі норм права двома (або більше) суб’єктами адміністративного права, один з яких обов’язково є органом виконавчої влади, може містити у собі загальнообов’язкові правила поведінки (нормативний характер) або встановлювати (змінювати, припиняти) конкретні правовідносини між його учасниками (індивідуальний характер)» [22, с. 106]. С.М. Ольховська пише, що адміністративні договори характеризуються низкою особливостей, а саме: при їх укладанні обов’язковою є участь органу виконавчої влади або органу місцевого

самоврядування, що обумовлює наявність інших важливих ознак: правосуб'єктність сторін договору (можливість мати право та використовувати право для укладання та підписання певного договору) може бути спеціальною (правосуб'єктність органів влади) або виключною (правосуб'єктність конкретного органу виконавчої влади або органу місцевого самоврядування); особливе правове регулювання договірних умов (вибір нормативного акта, який регулює порядок та зміст укладеного договору, безпосередньо пов'язаний із рівнем органу влади); порядок розглядання можливих спорів (розглядання таких спорів здійснюється виключно адміністративними судами) [148].

Суттєвими ознаками, що характеризують зміст адміністративного договору, А.Кудін вважає за доцільне виокремити такі [118]: 1) метою адміністративного договору є задоволення публічних потреб. Органи виконавчої влади як суб'єкти таких договорів мають на меті ефективне виконання завдань публічної (державної) служби, створеної для задоволення державних або суспільних потреб. Як приклад можна навести договори у сфері управління державною власністю, договори, що забезпечують державні потреби (державні контракти на поставку продукції для державних потреб) тощо. Як адміністративні договори доцільно розглядати й так звані договори про концесії публічної (державної) служби, за допомогою яких орган виконавчої влади, особливо місцева державна адміністрація, делегують господарським товариствам, а також особам, які займаються підприємницькою діяльністю, частину своїх функцій і повноважень для забезпечення суспільних потреб; 2) адміністративному договору властиві певні обмеження вільного волевиявлення, свободи договору, юридичної рівності (зокрема суб'єкт владних повноважень, як правило, при укладенні адміністративного договору зв'язаний вимогами (процедурами, обмеженнями), визначеними законодавством щодо вибору контрагента, установлення суттєвих умов договору); 3) порядок укладення та виконання адміністративно-правової

угоди, за загальним правилом, регулюється нормами публічного права із субсидіарним застосуванням в окремих випадках норм цивільного права. Мова йде про такі категорії цивільного права, як форма договору, термін виконання договору, забезпечення виконання зобов'язань, визначених у договорі, відповідальність за порушення умов договору, його зміну та розірвання тощо; 4) в адміністративному договорі неможлива (за будь-яких умов) одностороння відмова від виконання договірних умов. Норми про форс-мажор у таких договорах, як правило, не застосовуються; 5) адміністративні договори мають включати в себе контрольно-наглядові повноваження органів виконавчої влади, які полягають у контролі за виконанням адміністративного договору з боку суб'єктів владних повноважень, перевірці діяльності адміністрації та трудового колективу підприємства й організації, що вступили в договірні відносини, а також можливості застосування економічних та інших санкцій за невиконання або неналежне виконання обов'язків за договором [118].

Отже, укладення адміністративного договору є важливою формою взаємодії суб'єктів протидії, адже за його допомогою, у разі виникнення кіберзагроз, спеціально уповноважені суб'єкти мають можливість залучити до реалізації певних заходів не тільки інші державні інституції, а й спеціальні агентства, певних спеціалістів, тощо. Окрім того, саме за допомогою адміністративного договору вбачається можливим: по-перше, забезпечити оперативний обмін інформацією між сторонами взаємодії, що в свою чергу дає їм можливість більш оперативно реагувати на загрози, що виникають у кіберпросторі; по-друге, врегулювати взаємні права та обов'язки сторін взаємодії, а також міру їх відповідальності одне перед одним в процесі реалізації спільних заходів у досліджуваній сфері; по-третє, створити умови для більш оперативного та якісного вирішення спорів, що можуть виникнути в процесі взаємодії; тощо.

І останні нормативно-правова форма – правозастосовна. О.Ф. Скакун зазначає, що правозастосування - це владно-організуюча діяльність

компетентних державних органів і посадових осіб, що здійснюється в процедурно-процесуальному порядку, яка полягає в індивідуалізації юридичних норм стосовно конкретних суб'єктів і конкретних життєвих випадків в акті застосування норм права [194, с. 388–389]. В теорії права домінує точка зору, згідно з якою основні з них такі: здійснюється компетентними, спеціально уповноваженими державою суб'єктами; є опосередкованою формою реалізації права; має владний, організаційно-управлінський, індивідуально-конкретний характер; є складною формою реалізації права, оскільки відбувається у поєднанні з такими її формами, як виконання, дотримання, використання і їх взаємопроникненні одна в одну; здійснюється відповідно до визначеного в законі порядку (саме ця ознака дає можливість виявити зв'язок між правозастосуванням і правозастосовною процедурою, що його регламентує); завершується прийняттям правозастосовних актів, у яких фіксуються індивідуально-конкретні приписи [16]. Ключовими ознаками правозастосування, на переконання О.Ф. Скакун, є наступні: Владний характер: 1) воно є діяльністю компетентного органу або посадової особи, обмеженою їх повноваженнями; 2) індивідуалізований та персоніфікований - це процес вирішення конкретних справ, життєвих ситуацій або правових питань на основі чинного законодавства; Процедурно-процесуальний: він включає офіційний порядок дій, що складається з ряду стадій; 3) творчий та інтелектуальний: правозастосування завжди вимагає інтелектуального зусилля, оскільки враховує норми права і вимагає свідомих дій; 4) здійснюється на основі норм права: воно ґрунтується на чинних правових нормах; 5) має юридично оформлений характер: завершується ухваленням спеціального акта, який називається актом застосування норм права або правозастосовним актом; 6) у своїй результативній частині (правозастосовний акт) завжди відіграє роль юридичного факту, який породжує, змінює або припиняє конкретні правовідносини (наприклад, укладання шлюбу, розлучення подружжя, усиновлення дитини) [16].

Правозастосування – це найбільш гнучка та дієва частина механізму забезпечення правореалізації, яка дозволяє не тільки оперативно вивчати суспільні потреби, а й формувати їх у вигляді, сприйнятному для законодавця. У правозастосуванні не тільки вагомо, а й зримо виявляються соціально-політичні фактори, що дозволяє суб'єктам правозастосування їх відчувати, сприймати, оцінювати та узагальнювати для інших суб'єктів суспільства. Особливість правозастосовної діяльності полягає в тому, що вона є специфічним різновидом соціальної діяльності як явище, яке відбувається в соціумі, окресленому правовими межами і впливає на відносини в суспільстві, регулюючи їх. Фактори, будучи рушійною силою і причиною правозастосовної діяльності, теж є соціальними за своєю природою [86].

Правозастосування, як форма взаємодії суб'єктів протидії кіберзлочинності, представляє собою системний і координований процес, спрямований на забезпечення кібербезпеки та боротьбу з кіберзлочинами. Воно включає в себе наступні ключові аспекти: 1) розслідування кіберзлочинів спеціально уповноваженими суб'єктами, які здійснюють виявлення та ідентифікацію осіб, які скоюють кіберзлочини; 2) компетентні органи реалізують заходи для захисту критичних інформаційних систем, мереж та інших об'єктів від кібератак; 3) у разі доведення вини злочинця відповідні справи передаються до розгляду до суду; 4) крім реактивних заходів, правозастосування включає в себе і проактивні дії для запобігання кіберзлочинам.

Наступну групу форм складаються організаційно-управлінські, які представляють собою сукупність дій, реалізують спеціально-уповноважені суб'єкти для досягнення кінцевої мети досліджуваної взаємодії. До відповідних форм найбільш доцільно віднести наступні:

- підготовка і реалізація спільних заходів. В даному контексті суб'єкти взаємодії: 1) розподіляють ролі та завдання у сфері кіберзахисту, а також рівень відповідальності та компетентності для забезпечення

ефективності здійснення спільних дій; 2) обмін інформацією про потенційні загрози, їх види, що дозволяє бути в курсі сучасних тенденцій; 3) розробляють та впроваджують технічні заходи кібербезпеки, політики безпеки та навчання персоналу; 4) надають взаємну підтримку в випадках кіберкриз та інцидентів. Це може включати в себе обмін експертами, ресурсами та координацію заходів у випадках, коли потрібна негайна реакція; тощо;

- проведення нарад, круглих столів, семінарів, конференцій, тренінгів тощо. Так, наради – це процес реалізації управління, під час якого здійснюється обмін інформацією і досвідом роботи на підґрунті використання колективних знань, а також виробляються, приймаються та доводяться рішення до виконавців [220, с.12]. Нарада дозволяє прискорити доведення завдань до слідчих, погоджувати їх діяльність, заохочувати до вироблення управлінських рішень. Тренінг – це і метод отримання знань, який відрізняється тим, що його учасники навчаються на власному досвіді. Основною характеристикою тренінгу є інтерактивність, яка полягає як в активності самих учасників, так і активній взаємодії між ними, отриманні зворотного зв'язку [223]. Що стосується конференцій, то їх існує декілька видів: 1) науково-теоретична конференція + ця форма заходу призначена для обговорення теоретичних підходів до вирішення наукових проблем, які виникають у процесі проведення досліджень та наукових експериментів. На науково-теоретичних конференціях також вивчаються статистичні дані, обговорюються нові відкриття та розробки; 2) науково-практична конференція - ця форма зустрічі спрямована на обмін досвідом та знаннями з практичних питань; 3) науково-технічна конференція - це захід, на якому здійснюється обмін інформацією та досвідом з різноманітних технологічних та технічних питань.

- адміністративний нагляд. В сучасній юридичній літературі прийнято вважати, що адміністративний нагляд – це систематичне спостереження за точним і неухильним додержанням посадовими особами

та громадянами правил і застосування норм, що охороняють життя, здоров'я, права та свободи громадян, регулюють громадський порядок і громадську безпеку з метою попередження, припинення порушень цих правил, виявлення порушників та притягнення їх до адміністративної чи кримінальної відповідальності, застосування до них заходів громадського впливу [1, с.124].

- просвітницька робота з громадськістю. Дана форма передбачає ведення активної роботи з населенням, яка спрямована на: а) проведення навчальних заходів, семінарів, вебінарів та інших форм освіти, спрямованих на підвищення кіберсвідомості серед громадян, користувачів Інтернету та інших зацікавлених сторін; б) створення та поширення інформаційних матеріалів, які надають поради та рекомендації щодо безпечного користування Інтернетом, виявлення кіберзагроз та захисту від них; в) залученню громадськості до питань кібербезпеки, що може включати в себе організацію обговорень, форумів та інших заходів, де громадяни можуть спільно обговорювати проблеми кібербезпеки та розробляти спільні заходи для їх вирішення; г) попередження кіберзлочинності шляхом пояснення наслідків та наявних загроз, навчання та поширення найкращих практик щодо кібербезпеки.

Реалізація зазначених форм передбачає використання спеціального набору інструментів та засобів, які прийнято називати методами. За тлумачним словником української мови «метод» – це «прийом або система прийомів, що застосовується в якій-небудь галузі», а «спосіб» – це «прийом або система прийомів, яка дає можливість здійснити що-небудь» [198, с.578]. Поняття методу, зазначає В.Л. Петрушенко, як правило, застосовують для пояснення пізнання, наукового пошуку або ж для окреслення таких інтелектуальних та практичних дій, які передбачають високий рівень усвідомлення того, що ми робимо, чому це робимо саме так і чому результат повинен мати саме такі очікувані характеристики. Самий термін «метод» сходить до давньогрецького виразу «мета – одоїс», що

можна перекласти як «через вистежений (або підготовлений) шлях» [156, с. 223].

З точки зору загальної теорії права, правовий метод – це сукупність юридичних засобів, прийомів впливу, які застосовує держава при правовому регулюванні суспільних відносин, то завданням вчених у сфері галузевих наук є виявлення специфіки зазначених засобів [11, с.38]. В свою чергу адміністративно-правовий метод – це відгалуження загального правового методу, відмінність якого полягає в: по-перше, адміністративно-правовій основі його застосування; по-друге, даний метод застосовується в сфері відносин виключно публічно-правового змісту; по-третє, адміністративно-правові методи характеризують сукупність різноманітних засобів, способів та заходів імперативного регулюючого впливу адміністративно-правових норм на відносини в публічно-правовій сфері. Такий метод характеризується чіткістю правових вимог до суб'єктів правовідносин; жорсткими нормативними рамками реалізації та можливістю застосування до суб'єктів правовідносин заходів примусового характеру [55, с.129-130].

Тож, під методами взаємодії суб'єктів протидії кіберзлочинності найбільш доцільно розуміти сукупність визначених нормами чинного законодавства інструментів та засобів, які в своїй діяльності використовують спеціально уповноважені органи державної влади задля здійснення відповідної спільної діяльності.

Виділяючи конкретні методи в першу чергу слід вказати переконання та примус. Метод переконання - це такий спосіб цілеспрямованого впливу на свідомість і поведінку учасників управлінських відносин, який проявляється в комплексі роз'яснювальних, рекомендаційних, виховних та заохочувальних заходів, що застосовуються з метою забезпечення правомірності їхньої поведінки, підвищення їхньої правосвідомості та законослухнянності, зміцненню дисципліни, соціальної організованості, а також із метою профілактики правопорушень [44, с.82]. В свою чергу

примус – це застосування до правозобов’язаних суб’єктів передбачених адміністративно-правовими нормами заходів впливу морального, особистісного, майнового, організаційного чи іншого характеру з метою попередження чи припинення протиправних дій, подолання їх шкідливих наслідків, покарання за вчинення правопорушення, а також забезпечення громадського порядку і громадської безпеки [137, с.5]. Зауважимо, що методи переконання та примусу найширше застосовуються в усіх сферах управлінської діяльності і становлять систему засобів впливу держави (в особі її відповідних органів та посадових осіб) на свідомість і поведінку людей, є необхідною умовою нормального функціонування суспільства, будь-якого державного або громадського об’єднання, всього процесу управління. Застосовуючи ці засоби, держава забезпечує функціонування всієї суспільної системи, організованість, дисциплінованість, охороняє працю та побут людей, нормальну соціальну обстановку в країні [92, с. 101].

Таким чином, переконання та примус – два нерозривно пов’язані між собою методи взаємодії суб'єктів протидії кіберзлочинності. Так, якщо переконання спрямований на те, щоб забезпечити свідоме ставлення учасників взаємодії до виконуваних ними обов’язків шляхом позитивної мотивації та створення відповідного внутрішнього переконання, то примус передбачає застосування правового або адміністративного тиску для досягнення конкретних цілей в галузі кібербезпеки. Окрім зазначених вище, також до методів взаємодії суб'єктів протидії кіберзлочинності вбачається необхідним віднести:

- метод координації. Координація – це метод управління, суттю якого є встановлення між суб’єктами та об’єктами державного управління горизонтальних зв’язків, тобто поєднання двох і більше однорівневих з точки зору визначеного критерію дій, що забезпечують досягнення запланованого результату. Дослідник зазначає, що координаційні

відносини розрізняються за видами: узгодження, предметно-технологічна взаємодія, ієрархічна або складна взаємодія [64, с.346].

Тож, координація - це метод забезпечення взаємодії різних суб'єктів протидії кіберзлочинності, що передбачає об'єднання їхніх зусиль та ресурсів для спільного реагування на кіберзагрози та підвищення рівня безпеки у відповідній сфері. Цей метод ґрунтується на тому, щоб за допомогою спеціального інструментарію створити необхідні умови для забезпечення партнерства та співпраці між державними органами, приватним сектором, громадськими організаціями та іншими зацікавленими сторонами у досліджуваній сфері.

- метод прогнозування. Прогнозування — це наукове передбачення, систематичне дослідження стану, структури, динаміки, та перспектив управлінських явищ та процесів, притаманних суб’єкту та об’єкту управління [3, с. 116]. Д.М. Стеченко зазначає, що під методом прогнозування слід розуміти сукупність операцій і прийомів, які на основі ретроспективних даних, екзогенних (зовнішніх) та ендогенних (внутрішніх) зв'язків об'єкта прогнозування, а також їхніх змін дають можливість передбачати майбутній його розвиток [203, с.175]. Прогнозування в контексті протидії кіберзлочинності, - це метод, який передбачає аналіз та передбачення можливих загроз та ризиків в кіберпросторі. Основною метою прогнозування є ідентифікація потенційних кіберзагроз та вразливостей в інформаційних системах, щоб приймати заходи їх запобігання та мінімізації можливих шкідливих наслідків.

- метод планування. Планування – це вид управлінської діяльності, що визначає перспективу й майбутній стан організації чи діяльності, шляхи й способи його досягнення. В ході планування виробляється план – це деталізована сукупність рішень, які підлягають реалізації, перелік конкретних заходів і їхніх виконавців [151]. Планування, як метод взаємодії суб'єктів протидії кіберзлочинності, представляє собою

систематичний підхід до розробки стратегічних та тактичних планів для забезпечення кібербезпеки. Цей метод включає в себе кілька ключових аспектів. Спочатку визначається мета та конкретні цілі, які потрібно досягти в галузі кібербезпеки. Це може включати захист критичних інфраструктур, забезпечення конфіденційності даних та забезпечення доступності мереж та систем. Планування також передбачає докладний аналіз потенційних кіберзагроз та ідентифікацію можливих ризиків. Це дозволяє краще розуміти, які види атак можуть виникнути та які ризики пов'язані з кіберзлочинністю. Після аналізу розробляються конкретні стратегії та тактики для запобігання, виявлення та реагування на кіберзагрози. Ці стратегії враховують потреби та ресурси суб'єктів протидії кіберзлочинності та спрямовані на досягнення поставлених цілей.

- інформаційний метод. Інформація – це завжди результат, продукт діяльності людини, орієнтований на створення нових відомостей або зняття відомостей з інших об’єктів матеріального або духовного світу, для об’єднання цих відомостей у певний продукт та товар, необхідний для суспільства. Визначальною є теза, що для права слід використовувати якісну теорію інформації, а не кількісну, яка ігнорує зміст інформації [155]. Інформаційний метод взаємодії суб'єктів протидії кіберзлочинності є ключовим компонентом в боротьбі з кіберзагрозами. Цей метод ґрунтується на обміні, аналізі та поширенні інформації для вчасного виявлення, запобігання та відповіді на кіберзлочинність. Першочергово інформаційний метод передбачає збір інформації про потенційні кіберзагрози. Після збору інформації проводиться аналіз, під час якого аналітики визначають потенційні ризики та загрози. Вони досліджують структуру атак, виявляють їхній спосіб дії, можливі наслідки та шляхи захисту. Обмін інформацією між суб'єктами протидії кіберзлочинності є важливою складовою цього методу. Це дозволяє різним організаціям та установам обмінюватися актуальними даними про кіберзагрози, що допомагає підвищити загальний рівень свідомості та готовності до

реагування на можливі атаки. Тож, інформаційний метод сприяє вдосконаленню систем моніторингу та реагування на кіберзагрози, дозволяючи швидко виявляти, аналізувати та реагувати на потенційні атаки. Він також сприяє спільним діям та співпраці між різними суб'єктами протидії кіберзлочинності, що є ключовим для ефективного протистояння кіберзагрозам.

Таким чином, саме наведені вище форми та методи найбільш змістовно характеризують практичний бік спільної діяльності суб’єктів протидії кіберзлочинності в Україні. Разом із тим, варто зауважити, що на сьогоднішній день відповідні методи не віднайшли свого законодавчого закріплення. А відтак, вказана проблема потребує усунення шляхом вдосконалення як правових, так і організаційних засад здійснення відповідної спільної діяльності.

Висновки до Розділу 2

Доведено, що механізм адміністративно-правового регулювання являє собою складну систему юридичних елементів, інструментів та засобів, за рахунок яких визначаються матеріальні та процедурні засади дії/впливу права на суспільно-правові відносини. До ключових властивостей такого механізму віднесено: 1) є динамічною категорією, яка показує реальне функціонування права; 2) являє собою складне системне утворення, так як складається із спеціальних юридичних елементів, що взаємодіють одне з одним в процесі правового регулювання та виражається крізь систему форм, що носять адміністративний характер; 3) процес реалізації даного механізму носить формалізований характер, адже порядок і особливості його дії нормативно визначені.

З'ясовано, що механізм адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, найбільш доцільно тлумачити, як формалізовану систему спеціальних, взаємодіючих та взаємозалежних між собою юридичних елементів, за рахунок яких встановлюються матеріальні та процедурні засади впливу права на суспільно-правові відносини, що виникають в сфері спільної діяльності суб'єктів, які уповноважені на виявлення, припинення та профілактику кіберзлочинів. До елементів даного механізму віднесено: принципи права; норми адміністративного права; нормативно-правові акти; адміністративні правовідносини.

Встановлено, що норми адміністративного права – це елементарні цеглини правової матерії, крізь які відбувається упорядкування та регулювання суспільно-правових відносин. Значення даних норм у механізмі адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності проявляється в тому, що саме за їх допомогою встановлюються: правила виникнення, функціонування та припинення такої взаємодії, а також повноваження та цілі діяльності її учасників.

Тобто, адміністративні норми визначають режим реалізації співпраці між уповноваженими суб'єктами у напрямку протидії кіберзлочинності

Аргументовано, що роль нормативно-правових актів у механізмі адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності полягає у тому, що вони є формою зовнішнього вираження адміністративних норм. Це офіційні документи, прийняті та затверджені уповноваженими державними органами у відповідному порядку, завдяки чому закріплені в них норми набувають загальнообов'язковості та формальної визначеності

Акцентовано увагу на тому, що як елемент механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, правовідносини є середовищем реалізації останніми своїх прав та обов'язків. Тобто, правовідносини зумовлюють законність та нормативну відповідність досліджуваної взаємодії, перетворюючи її із безособового, теоретично можливого типу діяльності на реальну сукупність суспільних зв'язків між уповноваженими суб'єктами дії яких мають юридичні наслідки.

Виокремлено наступні особливості принципів права в цілому та принципів адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності зокрема. По-перше, в принципах уособлюються загально-соціальні ідеї, уявлення та цінності про дух права та його зв'язок із політичними, економічними, суспільними та іншими процесами життя української нації. Говорячи іншими словами, принципи виражають ідею про право та зміст і призначення його регулюючого впливу на суспільні відносини в тій чи іншій сфері. По-друге, принципи, на відміну від інших юридичних положень, характеризуються найвищим рівнем абстрактності, адже проявляються не в конкретних нормах, а сукупних положеннях нормативно-правових актів, які регулюють відповідний спектр суспільних відносин. Поряд із цим, принципи є найбільш імперативними юридичними положеннями, дія яких розповсюджується на всіх суб'єктів права без

виключення. По-третє, принципи визначають зміст і закономірності побудови системи національного права, а також вектори його еволюції та розвитку. Вони виступають фундаментом або ж ядром права навколо та відповідно до якого вибудовуються складні структури юридичних норм, як то інститути або галузі. По-четверте, принципи забезпечують стабільність та незмінюваність правового регулювання, адже залежать не від писаних положень, а суспільної ідеї про право, якій вони відповідають та яку виражають в собі. Тому їх зміна можлива виключно за рахунок появи нових суспільних цінностей, які змінюють бачення населення стосовно права і правового регулювання, а також зумовлюють бажання змінити існуючи юридичні основи.

Встановлено, що принципи представляють собою сукупність вихідних засад, основоположних, розчинених у адміністративно-правових нормативних актах, стабільних, загальнообов'язкових ідей, які визначають призначення, вектори, цілі та особливості правового регулювання суспільно-правових відносин, що виникають в контексті взаємодії уповноважених суб'єктів протидії кіберзлочинності. До вказаних принципів віднесено наступні: законності, поєднання цілей, визначеності суб'єктного складу, координації та контролю, плановості, науковості та достатності.

Узагальнено, що законність, як вихідна засада адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, – це принципова вимога провадження такої спільної діяльності у порядку, який чітко відповідає конституційним положенням та інших Законів України. Це своєрідне легальне «обмеження» взаємодії установленими правовими нормами, яке, в свою чергу, забезпечує її правомірність та юридичну обґрунтованість

Наголошено, що дотримання принципу взаємодії та координації має важливе значення з точки зору забезпечення успішної та ефективної протидії кіберзлочинності, оскільки ця сфера вимагає спільних зусиль та

постійного оновлення стратегій і заходів для виявлення та подолання загроз. А відтак, координація та контроль допомагають підтримувати високий рівень інформаційної безпеки та ефективно реагувати на нові виклики у сфері кіберзахисту.

З'ясовано, що адміністративно-правовий статус суб'єктів протидії кіберзлочинності в Україні – це сукупність визначених нормами адміністративної галузі права елементів, які в своїй єдності визначають положення та роль суб'єктів протидії кіберзлочинності у суспільно-правових відносинах, що виникають в процесі здійснення ними спільної діяльності за відповідним напрямом. До елементів адміністративно-правового статусу вказаних суб'єктів віднесено: компетенцію, повноваження, гарантії діяльності та юридичну відповідальність.

Під формами взаємодії суб'єктів протидії кіберзлочинності запропоновано розуміти зовнішній вираз спільної, взаємоузгодженої практичної діяльності спеціально уповноважених органів державної влади та їх посадових осіб, яка спрямована на досягнення єдиної мети – протидія та запобігання правопорушенням та злочинним діям, які відбуваються в кіберпросторі або з використанням комп'ютерних технологій і мереж. Зауважено, що в науковій літературі не сформовано єдиного підходу щодо переліку відповідних форм, а відтак, останні запропоновано поділити на дві групи: 1) нормативно-правові: нормотворчість; адміністративний договір; правозастосування; 2) організаційно-управлінські форми: підготовка і реалізація спільних заходів; створення спільних робочих груп; адміністративний нагляд; просвітницька робота з громадськістю.

Акцентовано увагу на тому, що нормотворчість як форма взаємодії суб'єктів протидії кіберзлочинності, дозволяє створити нормативно-правові основи: по-перше, для забезпечення загального функціонування сфери протидії та запобігання кіберзлочинності, тобто незаконному отриманню, збереженню, обробці, передачі або використанню інформації, тощо; по-друге, для належного функціонування спільної діяльності

відповідних органів державної влади та їх посадових осіб, що зробить їх роботу більш ефективною та дієвою. Окрім того, саме за допомогою нормотворчості вбачається можливим оновити законодавство у відповідній сфері, зокрема виявити та покращити застарілі та не ефективні норми, які перешкоджають нормальному функціонуванню суспільних відносин.

Наголошено, що укладення адміністративного договору є важливою формою взаємодії суб'єктів протидії, адже за його допомогою, у разі виникнення кіберзагроз, спеціально уповноважені суб'єкти мають можливість залучити до реалізації певних заходів не тільки інші державні інституції, а й спеціальні агентства, певних спеціалістів, тощо. Окрім того, саме за допомогою адміністративного договору вбачається можливим: по-перше, забезпечити оперативний обмін інформацією між сторонами взаємодії, що в свою чергу дає їм можливість більш оперативно реагувати на загрози, що виникають у кіберпросторі; по-друге, врегулювати взаємні права та обов'язки сторін взаємодії, а також міру їх відповідальності одне перед одним в процесі реалізації спільних заходів у досліджуваній сфері; по-третє, створити умови для більш оперативного та якісного вирішення спорів, що можуть виникнути в процесі взаємодії; тощо.

Обґрунтовано, що правозастосування, як форма взаємодії суб'єктів протидії кіберзлочинності, представляє собою системний і координований процес, спрямований на забезпечення кібербезпеки та боротьбу з кіберзлочинами. Воно включає в себе наступні ключові аспекти: 1) розслідування кіберзлочинів спеціально уповноваженими суб'єктами, які здійснюють виявлення та ідентифікацію осіб, які скоюють кіберзлочини; 2) компетентні органи реалізують заходи для захисту критичних інформаційних систем, мереж та інших об'єктів від кібератак; 3) у разі доведення вини злочинця відповідні справи передаються до розгляду до суду; 4) крім реактивних заходів, правозастосування включає в себе і проактивні дії для запобігання кіберзлочинам.

Відзначено, що підготовка і реалізація спільних заходів як форма взаємодії суб'єктів протидії кіберзлочинності полягає у тому, що суб'єкти взаємодії: 1) розподіляють ролі та завдання у сфері кіберзахисту, а також рівень відповідальності та компетентності для забезпечення ефективності здійснення спільних дій; 2) обмін інформацією про потенційні загрози, їх види, що дозволяє бути в курсі сучасних тенденцій; 3) розробляють та впроваджують технічні заходи кібербезпеки, політики безпеки та навчання персоналу; 4) надають взаємну підтримку в випадках кіберкриз та інцидентів. Це може включати в себе обмін експертами, ресурсами та координацію заходів у випадках, коли потрібна негайна реакція; тощо

Аргументовано, що просвітницька робота з громадськістю, як форма взаємодії у сфері протидії кіберзлочинності, передбачає ведення активної роботи з населенням, яка спрямована на: а) проведення навчальних заходів, семінарів, вебінарів та інших форм освіти, спрямованих на підвищення кіберсвідомості серед громадян, користувачів Інтернету та інших зацікавлених сторін; б) створення та поширення інформаційних матеріалів, які надають поради та рекомендації щодо безпечного користування Інтернетом, виявлення кіберзагроз та захисту від них; в) залученню громадськості до питань кібербезпеки, що може включати в себе організацію обговорень, форумів та інших заходів, де громадяни можуть спільно обговорювати проблеми кібербезпеки та розробляти спільні заходи для їх вирішення; г) попередження кіберзлочинності шляхом пояснення наслідків та наявних загроз, навчання та поширення найкращих практик щодо кібербезпеки.

Методи взаємодії суб'єктів протидії кіберзлочинності запропоновано розуміти сукупність визначених нормами чинного законодавства інструментів та засобів, які в своїй діяльності використовують спеціально уповноважені органи державної влади задля здійснення відповідної спільної діяльності. До вказаних методів віднесено наступні: переконання,

примус, координація, планування, прогнозування, роботу з кадрами та інформаційний метод.

Констатовано, що переконання та примус – два нерозривно пов’язані між собою методи взаємодії суб'єктів протидії кіберзлочинності. Так, якщо переконання спрямований на те, щоб забезпечити свідоме ставлення учасників взаємодії до виконуваних ними обов’язків шляхом позитивної мотивації та створення відповідного внутрішнього переконання, то примус передбачає застосування правового або адміністративного тиску для досягнення конкретних цілей в галузі кібербезпеки.

Підкреслено, що прогнозування в контексті протидії кіберзлочинності, - це метод, який передбачає аналіз та передбачення можливих загроз та ризиків в кіберпросторі. Основною метою прогнозування є ідентифікація потенційних кіберзагроз та вразливостей в інформаційних системах, щоб приймати заходи їх запобігання та мінімізації можливих шкідливих наслідків.

РОЗДІЛ 3.
ШЛЯХИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

3.1 Міжнародний досвід адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності та можливості його використання в Україні.

Протидія кіберзлочинності – це одне із найважливіших та водночас складних завдань кожної сучасної та розвинутої держави світу. Разом із тим, варто відзначити, що різні країни по-різному реагують на кіберзагрози та мають відмінні механізми запобігання та протидії цьому явищу. Саме тому для України важливим є вивчення позитивного зарубіжного досвіду адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності, що дасть можливість використати найбільш корисні практики у вітчизняних реаліях. Варто зауважити, що застосування комп'ютерних технологій у різних сферах діяльності держави дедалі більше наближає Україну до міжнародних стандартів і тенденцій, але також ставить перед нею виклики в сфері кібербезпеки. Економіка, логістика та загальна безпека країни все більше залежать від стану технічної інфраструктури та її захищеності від кіберзагроз. З метою підвищення ефективності заходів протидії кіберзлочинності Україна вже тривалий час працює над розробкою власної стратегії кібербезпеки. Міжнародний досвід свідчить про необхідність створення системи глобального обміну інформацією в цій сфері. Результати досліджень та громадських опитувань підтверджують, що проблема кіберзлочинності турбує не лише державу в цілому, але і кожного громадянина окремо. Тому вивчення позитивних практик країн, які вже набули значного досвіду

у боротьбі з кіберзлочинами, стає актуальним завданням, спрямованим на підвищення рівня кібербезпеки в Україні [75].

Розвиток соціальних мереж за останні роки дав кіберзлочинцям ще один шлях для атак. Meta, материнська компанія Facebook, у 2022 році виявила понад 400 шкідливих додатків для iOS та Android, націлених на користувачів мобільних пристроїв, щоб викрасти їхні облікові дані для входу в Facebook. 43% цих додатків були «фоторедакторами», у тому числі й такими, які дозволяли користувачеві перетворити себе на мультфільм. Ще 15% становили «бізнес-утиліти», які стверджували, що можуть надавати приховані функції, яких немає в офіційних програмах від авторитетних платформ. Створюючи фальшиві відгуки, кіберзлочинці можуть штучно завищувати рейтинг своїх програм і маскувати погані відгуки, які висвітлюють проблеми. Потім нічого не підозрюючи користувачі завантажують програму, де їх потім просять увійти за допомогою Facebook. Будь-яку введену інформацію може побачити хакер. Лише у другому кварталі 2022 року Facebook видалив 8,2 мільйона одиниць контенту, який порушував його політику щодо залякування та агресивних дій. У першому кварталі 2022 року було видалено 9,5 мільйона одиниць вмісту, що порушує політику, та є найбільшим показником за всю історію видалення платформою [230].

Переходячи до аналізу досвіду конкретних держав, перш за все, варто звернути увагу на Сполучені Штати Америки (далі - США), яка на сьогоднішній день є лідером у сфері протидії кіберзлочинності. За оцінками експертів, 53,35 мільйона громадян США постраждали від кіберзлочинності в першій половині 2022 року. У період з липня 2020 року по червень 2021 року США були найбільш цільовою країною для кібератак, на них припадало 46% атак у всьому світі. Громадяни США втратили 6,9 мільярда доларів у 2021 році через кіберзлочини, включно з шахрайством у стосунках (956 мільйонів доларів), інвестиційним

шахрайством (1,4 мільярда доларів) і компрометацією ділової електронної пошти (2,39 мільярда доларів).

Для компаній програми-вимагачі становлять серйозну загрозу безпеці: дані 60% організацій США шифруються під час успішних атак програм-вимагачів. Витрати на усунення цих атак коштували в середньому 1,08 мільйона доларів у 2021 році, що на 49% менше, ніж у 2020 році (2,09 мільйона доларів). Лише 50% організацій у США мають кіберстрахування з повним покриттям. Ще 28% мають кіберстрахування з винятками в полісі, тобто вони можуть не покриватися певними атаками або за певних обставин. Найтривожніше те, що це означає, що приблизно 1 з 10 американських організацій (12%) не мають покриття від кібератак, ризикуючи фінансовим крахом, якщо вони зазнають атаки.

У Сполучених Штатах у боротьбі з кіберзлочинністю беруть участь різні органи та відомства на федеральному, штатному та місцевому рівнях. До ключових органів влади та організацій, які беруть участь у боротьбі з кіберзлочинністю в США, слід віднести наступні:

1) Федеральне бюро розслідувань (ФБР). ФБР відіграє вирішальну роль у розслідуванні та запобіганні кіберзлочинам національного значення. ФБР в США створили кібер-відділи – Cyber Division, в результаті чого спеціально навчені кібер-команди тепер працюють в штаб-квартирі ФБР і в кожному з 56 відділень Бюро з розслідування кіберзлочинів, в тому числі й комп’ютерних вторгнень, крадіжок інтелектуальної власності, персональних даних, дитячої порнографії та шахрайства. ФБР стверджує, що місія таких кібер-відділів полягає в тому, щоб: 1) реагувати, координувати, контролювати кіберрозслідування злочинів, пов’язаних з Інтернетом, комп’ютерних мереж і систем, зокрема загроз, пов’язаних з терористичними організаціями, іноземними урядами, і/або організованою злочинністю; 2) створювати і підтримувати державні/приватні об’єднання з використанням спеціальної освіти і професійної підготовки, щоб максимально протидіяти тероризму,

контррозвідки, і з боку правоохоронних органів з кіберзлочинністю; та 3) запроваджувати і використовувати новітні технології у боротьбі із кіберзлочинністю [126].

2) Агентство з кібербезпеки та безпеки інфраструктури (CISA). CISA є частиною Міністерства внутрішньої безпеки, та зосереджується на захисті критичної інфраструктури та реагуванні на кіберінциденти, які можуть вплинути на національну безпеку;

3) Секретна служба США. Хоча Секретна служба відома в першу чергу захистом високопоставлених осіб, вона також розслідує фінансові та кіберзлочини, зокрема крадіжку особистих даних і шахрайство з кредитними картками. Секретна служба США підтримує оперативні групи з боротьби з електронними злочинами, які зосереджуються на виявленні та пошуку міжнародних кіберзлочинців, пов'язаних з кібервторгненнями, банківським шахрайством, витоком даних та іншими комп'ютерними злочинами. Відділ кіберрозвідки Секретної служби безпосередньо сприяв арешту транснаціональних кіберзлочинців, відповідальних за крадіжку сотень мільйонів номерів кредитних карток і втрату приблизно 600 мільйонів доларів фінансовими та роздрібними установами. Секретна служба також керує Національним інститутом комп'ютерної криміналістики, який надає співробітникам правоохоронних органів, прокурорам і суддям кібернавчання та інформацію для боротьби з кіберзлочинністю.

4) Міністерство юстиції (DOJ). Так, відділ комп'ютерних злочинів та інтелектуальної власності Міністерства юстиції (CCIPS) переслідує кіберзлочинців і надає юридичні рекомендації щодо справ, пов'язаних з кіберпростором. Міністерство та його департаменти є головним органом державної влади із реагування на кіберзагрози та несе основну внутрішню відповідальність за виявлення, припинення, судове переслідування та інше стримування кіберзлочинів. Департамент активно співпрацює як з внутрішніми суб'єктами протидії кіберзлочинності, так і за кордоном. У

своїй діяльності відомство частково покладається на звіти приватного сектору, щоб допомогти виявити та зрозуміти поточну діяльність зловмисників, а також ділиться знаннями, отриманими під час розслідувань, із приватним сектором, щоб допомогти захистити свої мережі та клієнтів. Виконуючи цю роботу, Міністерство зберігає довіру громадськості, забезпечуючи дотримання всіх вимог конфіденційності та безпеки.

5) Центр розслідування кіберзлочинів (C3) Імміграційної та митної служби США (ICE) з питань внутрішньої безпеки (HSI), який надає комп'ютерні та інші технічні послуги для підтримки внутрішніх і міжнародних розслідувань транскордонних злочинів. C3 складається з відділу кіберзлочинів, відділу розслідування експлуатації дітей та відділу комп'ютерної криміналістики. Цей сучасний центр пропонує підтримку та навчання кіберзлочинців для федеральних, державних, місцевих і міжнародних правоохоронних органів. C3 також керує повністю обладнаною лабораторією комп'ютерної криміналістики, яка спеціалізується на відновленні цифрових доказів і пропонує навчання навичкам комп'ютерного розслідування та криміналістики;

6) Державні та місцеві правоохоронні органи. Останні мають свої відділи боротьби з кіберзлочинами для розслідування та боротьби з кіберзлочинами в межах своєї юрисдикції;

7) Федеральна торгова комісія (FTC). Ключове призначення даної комісії полягає у тому, щоб захистити споживачів від кібер-шахрайства та порушень конфіденційності;

8) Центр розгляду скарг на злочини в Інтернеті (IC3). IC3, що працює спільно з ФБР і Національним центром боротьби зі злочинністю білих комірців, є платформою для подання та аналізу скарг на кіберзлочини;

9) Міністерство оборони (DoD), яке відповідає за захист військових мереж та інфраструктури від кіберзагроз;

10) Офіси прокурорів США. У кожному федеральному судовому окрузі є офіс прокурора США, який може брати участь у судовому переслідуванні справ про кіберзлочини у межах його юрисдикції.

Окрім зазначених вище, у сфері протидії кіберзлочинності США діють різні регулюючі органи, галузеві асоціації та приватні фірми, з якими активно співпрацюють спеціальні органи державної влади задля підвищення кібербезпеки та протидії кіберзагрозам. Багатогранний підхід до боротьби з кіберзлочинністю в США включає запобігання, розслідування, судове переслідування та підвищення обізнаності з метою захисту критично важливої інфраструктури, підприємств і окремих осіб від зростаючих загроз у кіберпросторі.

Процес співпраці органів влади, які працюють разом у боротьбі з кіберзлочинністю в Сполучених Штатах, є багатогранним і заплутаним заходом, який передбачає численні взаємопов'язані кроки та заходи. Він починається зі збору та обміну важливою інформацією, що стосується кіберзагроз, вразливих місць та моделей кібератак. Такі федеральні агентства, як Федеральне бюро розслідувань (ФБР), Агентство з кібербезпеки та безпеки інфраструктури (CISA) і Секретна служба США, постійно збирають дані та заохочують окремих осіб, зокрема компанії та державні установи повідомляти про кіберінциденти через такі платформи, як Центр скарг на злочини в Інтернеті (IC3). Водночас, організації приватного сектору, що займаються критичною інфраструктурою, також збирають та обмінюються інформацією та даними про загрози. Потім зібрана інформація піддається ретельному аналізу консорціумом організацій, включаючи федеральні, державні та місцеві органи влади. Цей аналіз має на меті виявити нові тенденції, оцінити серйозність загроз і потенційні наслідки для національної безпеки та критичної інфраструктури. Цей етап залежить від скоординованих зусиль і тісної співпраці між цими організаціями.

Державно-приватне партнерство є ключовим елементом процесу протидії кіберзлочинності. Урядові установи тісно співпрацюють із галузями приватного сектора, включаючи енергетику, фінанси, охорону здоров'я та технології. Мета полягає у тому, щоб полегшити обмін інформацією про загрози та передовим досвідом. Ці синергетичні відносини забезпечують більш цілісне розуміння нових загроз і вразливостей і сприяють колективній відповіді на кібервиклики. У разі кіберінциденту запускається скоординований механізм реагування та розслідування. Створюються спільні цільові групи, які об'єднують федеральні агентства, правоохоронні органи штату та місцевого рівня, а також галузевих експертів. Ці оперативні групи співпрацюють у розслідуванні, судовому переслідуванні кіберзлочинів. Агентство з кібербезпеки та безпеки інфраструктури (CISA) відіграє центральну роль у координації цих зусиль з реагування на інциденти та діє як зв'язкова ланка між різними залученими організаціями державного та недержавного сектору.

Підводячи підсумок варто відзначити, що взаємодія органів державної влади у галузі протидії кіберзлочинності в Сполучених Штатах Америки – це комплексна та багатогранна діяльність, який охоплює різні етапи, від збору й аналізу інформації, а також вчинення спеціально уповноваженими суб'єктами дій, що передбачають реагування на інциденти (кіберзагрози), до державно-приватного партнерства, що також включає можливість активного залучення приватного сектору для вирішення певних задач. Це підкреслює критичну важливість синергії між різноманітними зацікавленими сторонами для ефективної протидії досліджуваному суспільно небезпечному явищу.

Переходячи до аналізу досвіду країн Європи, першочергово слід звернути увагу Великобританії. Кіберзлочинність обходиться британській економіці в 27 млрд. фунтів щорічно - повідомили в уряді Британії. Подібні дані були представлені вперше, їх збором займалися державне

Управління з кіберзлочинності і компанія Detica, що спеціалізується на системах мережевої безпеки. Цей звіт стане одним з основних документів при розробці урядом програми по боротьбі з кіберзлочинністю, яку влада називає зростаючою загрозою. Відповідно до статистичних даних, найбільше з вини кібершахраїв втрачає британський бізнес - 21 млрд. фунтів; державні структури втрачають 2,2 млрд. фунтів, а приватні особи - 3,1 млрд. Ці оцінки не є остаточними, і реальні масштаби втрат можуть бути набагато більшими. Близько половини з 21 млрд. фунтів припадає на незаконне завантаження з мережі матеріалів, які є інтелектуальною власністю. Істотну проблему представляє також промислове шпигунство [88].

Велика Британія продовжує зіштовхуватись з постійно зростаючим рівнем кіберзлочинності, включно з високотехнологічним програмним забезпеченням-вимагачем і компрометацією бізнес-електронної пошти, вчинюваними досвідченими кіберзлочинцями, що впливає на компанії будь-якого розміру та в усіх секторах. Згідно з дослідженням, проведеним Surfshark, Великобританія є країною з найвищою щільністю (40%) кіберзлочинності, випереджаючи США, якщо виміряти кількість жертв на один мільйон користувачів. Крім того, статистика Національного центру кібербезпеки Великої Британії (NCSC) показує, що 31% підприємств Великобританії зазнають атак принаймні раз на тиждень. У той час як 82% рад директорів або вищого керівництва компаній Великобританії вважають кібербезпеку пріоритетом. Втім, реальність полягає у тому, що лише 23% мають офіційну стратегію кібербезпеки, менше 20% мають офіційний план реагування на інциденти, і лише 6% мають має сертифікат Cyber Essentials. На цьому тлі партнерство між CSIS і CyberCrowd використовуватиме об’єднані можливості двох команд світового класу, причому особливістю та перевагою є те, як консалтингові та керовані послуги CyberCrowd використовуватимуть технології, інструменти та платформи CSIS для всього.

У Сполученому Королівстві декілька державних органів відповідають за боротьбу з кіберзлочинністю та забезпечення кібербезпеки. Ці організації працюють над запобіганням, розслідуванням і реагуванням на кіберзагрози та злочинну діяльність у цифровій сфері. Серед останніх найбільш доцільно виділити наступні:

1) Національне агентство боротьби зі злочинністю (NCA), яке розслідує широкий спектр кіберзлочинів, включаючи онлайн-шахрайство, хакерство, онлайн-експлуатацію дітей і розповсюдження шкідливого програмного забезпечення. Окрім того, дане відомство працює над виявленням та відстеженням кіберзлочинців, часто співпрацюючи з міжнародними правоохоронними органами. NCA проводить операції та спецоперації із затримання кіберзлочинців і конфіскації їхніх активів.

2) Національний центр кібербезпеки (NCSC). Діяльність NCSC, переважно, спрямована на те, щоб надати ресурси, а також пропозиції та рекомендації окремим організаціям та/або фізичним особам для посилення заходів кібербезпеки. Центр аналізує кіберзагрози та надає своєчасні сповіщення та дані про них суб’єктам критичної інфраструктури, державним установам і приватному сектору. NCSC також розробляє програми навчання з кібербезпеки щоб допомогти окремим особам і організаціям покращити свої навички та вміння у відповідній сфері.

3) Поліція Лондона, зокрема відділ боротьби з кіберзлочинністю, який зосереджується на фінансових кіберзлочинах і справах про шахрайство, зокрема йдеться про: інвестиційне шахрайство, шахрайство з онлайн-банкінгом та фінансові злочини, пов’язані з використанням інформаційних систем та технологій. Відповідні відділи поліції тісно співпрацюють з фінансовими установами та галузевими партнерами для розслідування та боротьби з фінансовими кіберзлочинами.

4) Відділи боротьби з кіберзлочинністю регіональної поліції. Ці підрозділи розслідують широкий спектр кіберзлочинів, таких як: переслідування в Інтернеті, викрадення особистих даних і

кіберзалякування на місцевому та регіональному рівнях. Вони надають допомогу та експертизу особам і підприємствам, які постраждали від кіберзлочинів.

5) Королівська прокуратура (CPS), котра розглядає справи, передані правоохоронними органами, і приймає рішення щодо притягнення до відповідальності осіб і організацій, причетних до кіберзлочинів. Вона відіграє вирішальну роль у розробці серйозних судових справ проти кіберзлочинців і висуненні кримінальних звинувачень.

6) Офіс інформаційного комісара (ICO). ICO забезпечує дотримання законів про захист даних, таких як: Загальний регламент захисту даних (GDPR), і розслідує справи про витоки даних і порушення конфіденційності. Вони виписують штрафи для організацій, які не захищають особисті дані працівників.

7) Податкове та митне управління Її Величності (HMRC). HMRC розслідує податкове шахрайство та ухилення від сплати податків, спричинене кіберзлочинами та цифровими фінансовими маніпуляціями.

8) Управління фінансового контролю (FCA). FCA регулює фінансову галузь та працює над захистом споживачів від фінансових кіберзлочинів, зокрема інвестиційного шахрайства та шахрайських фінансових послуг. Вони виносять попередження та вживають регуляторних заходів щодо суб’єктів, причетних до фінансових зловживань.

Окрім того, варто зауважити, що у Великобританії над захистом критичної інфраструктури, національної безпеки та конфіденційної інформації від кіберзагроз, також працюють інші органи державної влади, а також приватні підприємства, установи та організації, які активно залучаються спеціально уповноваженими інституціями. А відтак, взаємодія – це один із ключових аспектів забезпечення ефективної протидії кіберзлочинам у Великій Британії

Взаємодія різних суб’єктів, які беруть участь у боротьбі з кіберзлочинністю у Великій Британії, характеризується скоординованим

підходом до вирішення багатогранних викликів, які створюють кіберзагрози. Суть такої взаємодії полягає в обміні інформацією, координації зусиль і розвитку навичок. Обмін інформацією лежить в основі їхньої співпраці. Ці організації обмінюються критично важливою інформацією про нові кіберзагрози, шаблони атак та вразливі місця. При цьому варто зауважити, що обмін інформацією здійснюється в режимі реального часу, що дозволяє більш оперативно реагувати на потенційні кіберінциденти. Такі організації, як Національне агентство боротьби зі злочинністю (NCA), Національний центр кібербезпеки (NCSC) і регіональні поліцейські сили співпрацюють у розслідуванні та переслідуванні кіберзлочинців. Вони об'єднують ресурси та досвід, щоб забезпечити ретельне розслідування та притягнення винних до відповідальності.

Крім того, важливо відмітити, що розвиток професійних умінь та навичок працівників різних суб'єктів протидії кіберзлочинності здійснюється колективно. Ці організації формують навчальні програми та семінари для підвищення компетенції свого персоналу та обміну передовим досвідом у сфері кібербезпеки. Ці зусилля з розбудови потенціалу поширюються на окремих осіб та організації в державному та приватному секторах, зміцнюючи загальну кібербезпеку нації. Тож, по суті, взаємодія цих суб'єктів у боротьбі з кіберзлочинністю у Великій Британії характеризується єдиною та взаємопов'язаною екосистемою, де досвід, інформація та ресурси безперебійно перетікають, щоб протистояти мінливій природі кіберзагроз і гарантувати безпеку цифрових технологій.

Наступна Європейська країна, досвіду якої ми приділимо увагу – Німеччина. Дослідження 2022 року показало, що 72,6% німецьких організацій зазнали принаймні однієї успішної кібератаки за попередні 12 місяців. Для порівняння, колумбійські організації постраждали найгірше: 93,9% були скомпрометовані принаймні однією успішною атакою. 74,3% німецьких організацій вказали, що подальші кібератаки в

найближчі 12 місяців швидше за все відбудуться. Проте німецькі хакери сприяють глобальній загрозі фішингу. У 2022 році 5,19% спаму надійшло саме з Німеччини.

Боротьбу з кіберзлочинністю в Німеччині веде велика кількість органів влади різних рівнів. Серед останніх слід виділити наступні:

1) Федеральне управління кримінальної поліції (BKA). BKA відіграє центральну роль у боротьбі з кіберзлочинністю на національному рівні. Будучи центральним офісом німецької поліції, Федеральне управління кримінальної поліції також бере на себе координаційні завдання у сфері боротьби з кіберзлочинністю , надає інформацію та інструменти та є центром міжнародного співробітництва. Крім того, BKA проводить розслідування у сфері кіберзлочинності в рамках своїх первинних обов'язків, наприклад, коли постраждали федеральні органи влади чи установи чи важливі для безпеки посади на життєво важливих об'єктах, або Федеральному управлінню кримінальної поліції доручено виконати розслідування (Розділ 4 BKAG).

2) Державні управління кримінальної поліції (LKA).

3) Центральний контактний пункт з питань кіберзлочинності (ZAC). ZAC є спеціалізованим підрозділом BKA, який зосереджується на боротьбі з кіберзлочинністю та підтримці компаній і громадян у повідомленні про кібератаки.

4) Федеральне відомство з інформаційної безпеки (BSI), яке відповідає за інформаційну безпеку в Німеччині. Він працює для запобігання кібератакам і пропонує компаніям і установам підтримку у зміцненні їх IT-безпеки.

5) Генеральна прокуратура та прокурори відповідають за переслідування кіберзлочинців на регіональному рівні та тісно співпрацюють з органами поліції.

6) Державні центри боротьби з кіберзлочинністю (LZC). У деяких федеральних землях є спеціалізовані підрозділи, які займаються виключно

боротьбою з кіберзлочинністю. Ці LZC координують і підтримують розслідування у своїх відповідних федеральних землях.

7) Федеральна розвідувальна служба (BND), яка відповідаэ за моніторинг та боротьбу з кіберзагрозами в сферах національної безпеки та контррозвідки.

Окрему увагу варто приділити Національному центру по боротьбі з кіберзлочинністю (NKC), який відповідає за співпрацю з органами влади та компаніями приватного сектору в цій сфері. Крім того, безпосередньо в Центрі здійснюють службово-трудову діяльність координатор та офіцер зв'язку, якому, окрім Федерального відомства з інформаційної безпеки (BSI), підпорядковуються: Федеральне відомство із захисту конституції (BfV), Федеральне відомство цивільного захисту та допомоги у разі стихійних лих (BBK), Федеральна поліція (BPOL), Бундесвер (BW), Служба військової контррозвідки (MAD) та Митне управління кримінальних розслідувань (ZKA). Департамент також виконує завдання управління в федеральній мережі центральних контактних пунктів з кіберзлочинності (ZAC). Мережа ZAC була створена, щоб дозволити компаніям, які постраждали від кіберзлочинності, мати прямий контакт із відділами боротьби з кіберзлочинністю федеральної поліції та поліції штату. Сили швидкого реагування (QRF) були створені як цілодобовий підрозділ «першої атаки» правоохоронних органів. QRF ініціює перші невідкладні кримінально-процесуальні заходи у разі кібератак на об'єкти критичної інфраструктури (KRITIS) або федеральні об'єкти.

9 квітня 2019 року земля Баварія подала до Федеральної ради законодавчу пропозицію щодо покращення боротьби з кіберзлочинністю. Інтенсивне використання Інтернету впливає на всі сфери держави, економіки та суспільства, та несе з собою не лише свободу, але й високу ступінь уразливості через різноманітні можливості неправомірного використання. Це стало очевидним завдяки добре відомим «витокам даних» останніх років і нещодавньому збільшенню кількості кібератак за

допомогою троянських програм. Кіберзлочинність особливо загрожує основам демократії, державі та економіці та може підірвати довіру до спроможності державних органів діяти. Завданням кримінального права Німеччини є встановлення винних у таких нападах і застосування до них відповідного покарання.

Наразі, у Німеччині бракує кваліфікуючих фактів і прикладів правил з підвищеною загрозою покарання. Ця тривіалізація продовжується в кримінально-процесуальному законодавстві, де слідчі не мають кримінально-процесуальних повноважень для перспективних розслідувань у цифровому світі. Ось чому Комітет з кримінального права Конференції міністрів юстиції та Робоча група II Конференції міністрів внутрішніх справ доручили Спільній робочій групі правосуддя/поліції (GAG) зайнятися темою кіберзлочинності у 2011 році. Під керівництвом Міністерства юстиції та захисту прав споживачів Баварії він займався актуальними правовими питаннями боротьби з кіберзлочинністю та представив остаточний звіт у 2022 році. Міністри юстиції взяли це до відома на осінній конференції 2023 року попросили BMJV визнати рекомендації робочої групи та вжити необхідних законодавчих кроків. Законопроект спрямований на усунення невиправданої тривіалізації комп'ютерних злочинів і злочинів, пов'язаних з даними.

Що ж стосується безпосередньо представленої проблематики, взаємодія між державними органами Німеччини у боротьбі з кіберзлочинністю базується на скоординованій федеративній структурі. Кожна з 16 федеральних земель Німеччини має власні державні кримінальні слід підрозділи (LKA), які відповідають за розслідування та переслідування кіберзлочинів. Державні органи кримінального розслідування зазвичай тісно співпрацюють з іншими органами поліції на державному та місцевому рівнях для розслідування кіберзлочинів. Зазвичай вони спеціалізовані та мають слідчих, навчених цифровій криміналістиці та вистеженню кіберзлочинців.

Координація між управліннями кримінального розшуку штату часто здійснюється через Федеральне управління кримінальної поліції (BKA), яке діє на федеральному рівні. BKA є центральним контактним пунктом для серйозних справ про кіберзлочини, які виходять за межі національних кордонів. Крім того, проводяться регулярні зустрічі, тренінги та обміни інформацією між державними службами кримінального розслідування для обміну передовим досвідом і знаннями та підвищення ефективності боротьби з кіберзлочинністю. Тісна співпраця між державними органами має вирішальне значення, оскільки вона допомагає розробити та реалізувати послідовну національну стратегію боротьби з кіберзлочинністю в Німеччині, дотримуючись при цьому федеральної структури.

І остання країна, досвіду якої ми приділимо увагу – Франція. ця держава одна з перших в Європі, що вжила заходів до посилення ролі держави в регулюванні кіберпростору. Так, сьогодні в даній державі виділено такі форми кіберзлочинності: 1) суспільно небезпечні діяння, пов'язані з незаконним тиражуванням комп'ютерного програмного забезпечення, незаконним втручанням в автоматизовані системи обробки даних, вторгненням на сайти, створенням і розповсюдженням шкідливих програм тощо; 2) поширення сайтів, пов'язаних з дитячою порнографією, збутом наркотиків, расистської, ксенофобської або антисемітської спрямованості, терористичної спрямованості, про замахи на приватне життя, з інструкціями по експлуатації вибухових речовин, реклами в шахрайських цілях і т.д.. Даний досвід є актуальним для втілення в Україні, з огляду на недосконаліть розуміння і формулювання сутності поняття «кіберзлочинність». Крім того, важливо чіткий розподіл проступків за ступенем впливу на суспільні процеси в державі і негативними наслідками. Якщо регулювання першої форми кіберзлочинності за Французькою класифікацією здійснюється в Україні на достатньому рівні Розділом XVI Кримінального кодексу України, то

досвід регулювання другої форми кіберзлочинів доцільне для детального аналізу [33].

У Франції існують декілька організацій та агентств, які відповідають за протидію кіберзлочинності та забезпечення кібербезпеки:

1) Національна поліція (Police Nationale), яка має спеціалізовані підрозділи, що відповідають за протидію кіберзлочинності. Ці підрозділи проводять розслідування та співпрацюють з іншими національними та міжнародними органами з питань кібербезпеки;

2) Генеральна дирекція з кібербезпеки та розвідки (Direction Générale de la Sécurité Intérieure - DGSI). Ця служба відповідає за національну кібербезпеку та веде розслідування кіберзлочинності, що становить загрозу для внутрішньої безпеки Франції.

3) Центр кібербезпеки Франції (Agence nationale de la sécurité des systèmes d'information - ANSSI): ANSSI є ключовим агентством, відповідальним за захист інформаційних систем державних органів та критичних інфраструктур від кіберзагроз.

4) Генеральний інспекторат з кіберзлочинності (L'Inspection Générale de la Police Nationale - IGPN), який займається розслідуванням злочинів, пов’язаних із використанням інформаційних систем.

5) Центр боротьби з кіберзлочинністю та кібербезпекою (Centre de lutte contre les criminalités numériques - C3N). Цей центр входить до складу Національної поліції і спеціалізується на боротьбі з кіберзлочинністю.

Всі окреслені вище органи та їх структурні підрозділи співпрацюють як на національному, так і на міжнародному рівні з метою виявлення, розслідування та протидії кіберзлочинності та забезпечення належного рівня кібербезпеки у Франції.

Один з ключових аспектів взаємодії - це інформаційний обмін. Органи регулярно обмінюються даними про потенційні кіберзагрози, виявлені кіберзлочинів і методи атак. Цей обмін інформацією допомагає розуміти, які загрози існують і як їм протистояти. Іншими словами, це

дозволяє виявити спільні зразки та підходи до кіберзлочинності та надати можливість іншим органам вчасно приймати відповідні заходи. Окрім цього, органи можуть спільно розслідувати складні кіберзлочини, особливо ті, що мають національну чи міжнародну важливість. Спільні розслідування дозволяють об'єднати ресурси та експертні знання різних агентств для виявлення і припинення кіберзлочинності. Також існують спеціалізовані агентства, такі як ANSSI, які спеціалізуються на забезпеченні кібербезпеки критичних інфраструктур та державних систем. Ці агентства надають консультації та підтримку іншим органам у питаннях кібербезпеки.

Тож, підсумовуючи представлений підрозділ дисертаційного дослідження слід узагальнити, що на сьогоднішній день у Світі сформувались досить дієві підходи для протидії кіберзлочинності, втім і вони не стали панацеєю для того, щоб повністю мінімізувати ризики виникнення цього негативного явища. Втім, це не виключає можливості використання наступного позитивного міжнародного досвіду у сфері протидії кіберзлочинності в українських реаліях:

- по-перше, вбачається необхідним розширити коло суб’єктів протидії кіберзлочинності з чітким розподілом їх ролей у відповідній сфері. Окрім того, вбачається необхідним створити єдиний координаційний центр, який буде відповідати за узгодження діяльності у відповідній сфері (на прикладі Франції та Німеччини);
- по-друге, на прикладі США, доцільно створити розгорнутий та змістовний порядок взаємодії суб’єктів протидії кіберзлочинності, в якому чітко слід розкрити повноваження кожного органу державної влади у відповідній сфері;
- по-третє, в переважній більшості країн ефективність взаємодії напряму залежить від швидкості обміну актуальною інформацією про потенційні та/або існуючі загрози у сфері використання інформаційних технологій. Так, до прикладу, у Великобританії створено систему, за якою

суб'єкти протидії постійно отримують актуальну інформацію існуючі та потенційні загрози кібербезпеці в режимі «он-лайн»;

- по-четверте, наявність в державах Європи ефективної системи збору даних про кіберзлочини, що в тому числі й на основі отримання скарг від звичайних користувачів;

- по-п'яте, фактично в кожній розвинутій країні важливим елементом протидії кіберзлочинності є співпраця держави та приватного сектору. Урядові установи тісно співпрацюють із галузями приватного сектора, включаючи енергетику, фінанси, охорону здоров'я та технології.

- по-шосте, суб'єкти взаємодії у США постійно співпрацюють у науковій сфері, зокрема: проводять тренінги, семінари, науково-практичні конференції, тощо. Останнє дозволяє розвивати науковий потенціал у відповідній сфері.

3.2 Напрями вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Проведений у попередніх підрозділах дисертаційного дослідження аналіз дає змогу констатувати, що на сьогоднішній день законодавство, норми якого спрямовані на регулювання протидії кіберзлочинності взагалі, та щодо взаємодії спеціально уповноважених суб'єктів у цій сфері, зокрема, потребує комплексного вдосконалення, що обумовлено наявністю низки та прогалин у ньому. Прогалина в законодавстві виникає, коли певні аспекти суспільних відносин не регулюються відповідно до правових принципів, навіть тоді, коли законодавець повинен був їх врахувати. Прогалини можуть існувати навіть тоді, коли сфера суспільних відносин підпадає під дію закону, але в законодавстві відсутні відповідні норми. Причини прогалин можуть бути різними, включаючи первинні прогалини, які виникають через не врахування різноманітних життєвих ситуацій у

законодавстві, або наступні прогалини, що виникають внаслідок постійного розвитку суспільних відносин та виникнення нових життєвих ситуацій, які не могли бути передбачені заздалегідь законодавцем. Оскільки повністю уникнути прогалин у правовому регулюванні неможливо, важливо шукати способи їх оперативного заповнення, усунення або подолання [69]. Що ж стосується безпосередньо представленої проблематики, то варто зауважити, що наявні на сьогоднішній день прогалини у сфері протидії кіберзлочинності об'єктивно обумовлені тим, що сфері інформаційних технологій постійно розвивається, а злочинці знаходять все більше способів зловживати наявними ресурсами.

Справедливим буде відзначити, що на сьогоднішній день і законодавці, і науковці досить багато уваги приділяють проблемі забезпечення кібербезпеки в нашій країні. Підтвердженням першого є те, що протягом останніх років було розроблено низку Стратегічних та Концептуальних документів у даній галузі. Так, в першу чергу слід приділити увагу «Стратегії національної безпеки України», схваленої Указом Президента України від 14.09.2020 р. № 392/2020. Відповідно до вказаного нормативного документу «пріоритетами національних інтересів України та забезпечення національної безпеки є: відстоювання незалежності і державного суверенітету; відновлення територіальної цілісності у межах міжнародно визнаного державного кордону України; суспільний розвиток, насамперед розвиток людського капіталу; захист прав, свобод і законних інтересів громадян України; європейська і євроатлантична інтеграція» [176]. Одним із способів реалізації вказаних вище пріоритетів законодавець називає необхідність «посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі» [176]. «Сучасна модель глобалізації уможливила поширення міжнародного тероризму та міжнародної злочинності, зокрема у кіберпросторі,

наркоторгівлі, торгівлі людьми, релігійного та ідеологічного фундаменталізму та екстремізму, підживлюваного з-за кордону сепаратизму, нелегальної міграції, легалізації (відмивання) доходів, одержаних злочинним шляхом, розповсюдження зброї масового ураження тощо». Окрім того, у документі йдеться про те, що сьогодні «посилюються загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України» [176]. «Основним завданням у сфері воєнної безпеки є розвиток потенціалу стримування. Безумовним пріоритетом є боєздатні Збройні Сили України, підготовлений і вмотивований військовий резерв та ефективна територіальна оборона, які у поєднанні зі спроможностями інших органів сектору безпеки і оборони здатні завдати таких неприйнятних для противника втрат на землі, у повітрі, на морі та у кіберпросторі, що унеможливить реалізацію його агресивних намірів. Держава врахує уроки гібридної агресії проти України, бойових дій на Близькому Сході у нових доктринальних підходах до забезпечення воєнної безпеки» [176]. «Державний суверенітет, територіальна цілісність, демократичний конституційний лад та інші життєво важливі національні інтереси мають бути захищені також від невоєнних загроз з боку Російської Федерації та інших держав, зокрема спроб спровокувати внутрішні конфлікти. Пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції є: активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді; запобігання, виявлення та припинення проявів сепаратизму, тероризму, екстремізму, припинення діяльності незаконних збройних формувань, політично мотивованого насильства та інших зазіхань на конституційний

лад; отримання повної і достовірної упереджувальної інформації про ситуацію в Україні та світі, протидія зовнішнім загрозам національній безпеці України, сприяння реалізації національних інтересів України [176]. Важливим моментом, який слід відзначити в розрізі представленої проблематики є те, що вказаною вище Стратегією було передбачено необхідність розробки «Стратегії кібербезпеки України», що була введена в дію Указом Президента України від 26.08.2021 р. № 447/2021.

Відповідно до вказаної вище Стратегії «забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі». «Питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів» [177]. «Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі» [177].

Відповідно до «Стратегі кібербезпеки України» загрозами кібербезпеці України є: «кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки

України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо; організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності. Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію; використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності» [177].

Україна посилить спроможності у протидії кіберзлочинності шляхом [177]: «завершення імплементації в законодавство України положень Конвенції про кіберзлочинність; врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав - членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки; розроблення концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей); запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів; розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних вебсайтах;

розроблення методики проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечення проведення таких досліджень; розроблення методики комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створення необхідних умов для її практичної реалізації; запровадження механізмів ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України; врегулювання на законодавчому рівні правового статусу криптовалют; проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози; забезпечення підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів; забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів; залучення приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів» [177].

Таким чином, вказана вище «Стратегія кібербезпеки України» здійснила вагомий внесок у розвиток сфери протидії та запобігання кіберзлочинності. Втім, вона, переважно, була орієнтована на подолання проблем, які існували ще до початку повномасштабного вторгнення. Разом із тим, з початком війни система протидії кіберзлочинності в нашій країні виявилась не спроможною повною мірою реагувати на існуючі виклики та

загрози. А відтак, незважаючи на відносну новизну, даний нормативно-правовий акт, на нашу думку, є досить застарілим.

Наступною, на нашу думку, слід виділити «Стратегію інформаційної безпеки на період до 2025 року», яка була затверджена розпорядженням КМУ від 30.03.2023 р. N 272-р. Стратегія «визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних» [178]. Метою даного нормативно-правового акту «є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина» [178].

Основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання ряду стратегічних цілей та завдань. Такими цілями є: «протидію дезінформації та інформаційним операціям, особливо з боку держави-агресора. Ці операції спрямовані на ліквідацію незалежності України, порушення конституційного ладу, територіальної цілісності, пропаганду війни, насильства та розпалу ворожнечі; забезпечення розвитку української культури та зміцнення громадянської ідентичності; підвищення рівня медіакультури та медіаграмотності суспільства для захисту від дезінформації та маніпуляційної інформації; забезпечення прав особи на інформацію, свободу висловлювання, приватне життя і доступ до достовірної інформації. Також важливо гарантувати захист прав журналістів та їх безпеку; інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях. Це включає відновлення їхнього доступу до інформації та можливість підтримувати зв'язок з Україною; створення ефективної системи стратегічних

комунікацій; розвиток інформаційного суспільства та підвищення рівня культури діалогу» [178].

І останній документ, якому ми приділимо увагу - «Стратегія забезпечення державної безпеки», яка була затверджена Указом Президента України від 16.02.2022 р. №56/2022. Відповідно до вказаного нормативного акту «сучасна модель глобалізації уможливила поширення міжнародного тероризму та нових схем його фінансування, міжнародної злочинності, зокрема в кіберпросторі, наркоторгівлі, торгівлі людьми, релігійного фундаменталізму, політичного та релігійного екстремізму, підживлюваного з-за кордону сепаратизму, нелегальної міграції, легалізації (відмивання) доходів, одержаних злочинним шляхом, розповсюдження зброї масового знищення та засобів її доставки тощо» [179]. Окрім того, «посилюються загрози для критичної інфраструктури, пов’язані з тимчасовою окупацією частини території України, триваючими гібридними впливами з боку суб’єктів розвідувально-підривної діяльності, погіршенням технічного стану такої інфраструктури та намаганнями несанкціонованого втручання в її функціонування, зокрема фізичного і кіберхарактеру» [179]. «Стратегія є основою для розроблення відповідних програмних документів у сфері забезпечення державної безпеки та нормативно-правових актів щодо розвитку складових сил безпеки України, зокрема з питань: контррозвідувальної діяльності; удосконалення механізмів та інституційної спроможності суб’єктів боротьби з тероризмом, транснаціональною та організованою злочинною діяльністю, що використовується іноземними спецслужбами, терористичними організаціями та незаконними збройними формуваннями; захисту об’єктів критичної інфраструктури; охорони державної таємниці та службової інформації; забезпечення кібербезпеки» [179].

Таким чином, аналіз наведених вище Стратегічних документів свідчить про значну зацікавленість законодавця у вирішенні проблем,

пов’язаних із протидією кіберзлочинності. Адже зазначене суспільно небезпечне явище негативним чином впливає но фінансово-економічне становище не тільки кожної окремої людини, а й держави і суспільства в цілому. З огляду на це, на сьогоднішній день важливим кроком законодавця має бути розробка та прийняття нової «Стратегії кібербезпеки України». Вказаний нормативно-правовий акт повинен враховувати не тільки існуючі загрози у кіберпросторі, а й визначати: по-перше, окреслити чинники, які обумовлюють виникнення та розвиток кіберзлочинності; по-друге, шляхи вдосконалення діяльності, спрямованої на протидію кіберзлочинам; по-третє, коло суб’єктів, що здійснюють діяльність у сфері протидії кіберзлочинності, а також перспективні напрямки, рівні, форми та методи їх взаємодії.

Вказаній проблематиці неодноразово приділялась увага і на ріні окремих наукових досліджень. Так, до прикладу, М.О. Кравцова цілком слушно відмічає, що показники динаміки кіберзлочинності в цілому відповідають показникам загальної злочинності в країні, що вказує на особливості детермінантного комплексу кіберзлочинності та на відставання можливостей правоохоронних органів від сучасного рівня технологічного та програмного забезпечення злочинної активності. Серед найбільш ефективних заходів, спрямованих безпосередньо на боротьбу з кіберзлочинністю, можна виділити наступні: збільшення кількості планових та непередбачуваних перевірок; введення жорсткого контролю за обігом технічних засобів, обмежених або заборонених у вільному цивільному обігу; адаптація досвіду правоохоронних органів інших країн у цій сфері; співпраця з відповідними органами інших країн у плані виявлення, розслідування та запобігання злочинам в даній сфері, обмін знань щодо їх правозастосування; виявлення осіб, схильних до вчинення злочинів у вивченій сфері та інше. Реалізація зазначених заходів потребує подальших досліджень для розробки ефективних інструментів протидії сучасним викликам кіберзлочинності [110].

Є.В. Котух у своєму дисертаційному дослідженні дійшов до висновку, що з урахуванням нових кіберризиків та понад 417 складних шкідливих програм, країни і міжнародні організації, такі як НАТО, ENISA та інші, активно розглядають нові способи протидії складним викликам у галузі кібербезпеки. Одним із ключових кроків для країн є розробка національної стратегії кібербезпеки та відповідних політик. Проте, незважаючи на те, що ці стратегії та політики широко охоплюють військові, розвідувальні та критичні інфраструктури, часто виникає проблема ігнорування кібербезпеки на рівні організацій. Однак існують докази того, що забезпечення надійної кібербезпеки на національному рівні вимагає також забезпечення кібербезпеки на рівні окремих організацій. Відповідно до цього було запропоновано модель інституційної кібербезпеки, яка включає в себе різні групи учасників (приватні особи, публічні та приватні установи, національні структури безпеки та міжнародні організації). Відповідно до цієї моделі, інституційна кібербезпека має включати такі ключові компоненти: розробку політики, стратегії та стандартів у сфері кібербезпеки; управління кіберризиками; контроль вразливостей та загроз; централізовану систему реагування на інциденти; підвищення обізнаності з кібербезпеки та освіту; управління журналами та аналіз; створення безпечної архітектури; розробку правового середовища; використання технічних інструментів; забезпечення безперервності діяльності; постійний моніторинг та аудит; підтримку співпраці та кіберстійкості. [109].

О. Коваленко, досліджуючи теоретико-методологічні засади формування механізмів забезпечення кібербезпеки України на сучасному етапі державного будівництва дійшов до ряду цікавих висновків. Так, автор відмічає, що формування механізмів забезпечення кібербезпеки повинно відбуватися в контексті загальної теорії систем, теорій державного та публічного управління, теорій національної безпеки, інформаційної безпеки та кібербезпеки. Засновуючись на теоретико-

методологічних принципах формування механізмів державного та публічного управління, механізмів розробки та впровадження державної та публічної політики, механізмів забезпечення національної безпеки, логіки взаємозв'язку елементів державної політики в галузі кібербезпеки, логіки взаємозв'язку зовнішніх та внутрішніх аспектів кібербезпеки, а також логіки впливу на національний кіберпростір важливих чинників, таких як: глобалізація інформаційної сфери, геополітичні інформаційні конфлікти та кібервійна [94].

Важливим є те, що О. Коваленком також було визначено структуру системи забезпечення кібербезпеки України. Ця система, на думку вченого, включає в себе: організаційно-адміністративний і фінансових механізми, механізм державного реагування на загрози кібербезпеці, механізм запобігання загрозам кібербезпеці, кадровий, науково-методичний та інформаційно-аналітичний механізми забезпечення кібербезпеки, механізм партнерства і співробітництва з питань забезпечення кібербезпеки, механізм інтеграції національного кіберпростору у світовий інформаційний простір, механізм партисипаторної взаємодії у сфері забезпечення кібербезпеки, які використовуються у комплексі з метою забезпечення кібербезпеки. Запропонована структура комплексного механізму забезпечення кібербезпеки України, узагальнює вказаний вище автор, дозволить у подальшому здійснити його змістовне наповнення із чітким визначенням суб’єктів і об'єктів кібербезпеки, функціонально-організаційної структури механізмів забезпечення кібербезпеки в умовах гібридної війни, нормативно-правового і ресурсного забезпечення, інструментів державного реагування на загрози кібербезпеці, а також уникнути суперечностей та дублювання функцій суб'єктів забезпечення кібербезпеки, які сьогодні мають місце у цій специфічній сфері [94].

В.О. Тімашов, розкриваючи правові засади забезпечення кібербезпеки у банківській сфері зазначає, що повністю захиститися від

кібератак неможливо. Однак дотримання принаймні мінімальних правил безпеки мережі значно збільшить шанси на те, що злочинці не зламають систему. Під час проведення транзакцій між банками або в системі «клієнт-банк» в інтернет-банкінгу важливо використовувати криптологічні інструменти, такі як ключі AES з різними бітрейтами, і чим вище бітрейт, тим більший захист. Впровадження та виконання цих заходів дозволить повною мірою отримати переваги цифрового суспільства [211]. В.О. Тімашов також відзначає, що серед питань ефективної протидії кіберзлочинності і сьогодні актуальними є такі: а) розробка відповідних норм права для здійснення обшуку електронних доказів з урахуванням можливості їхнього виявлення в різних юрисдикціях; б) розробка спеціалізованого програмного та апаратного забезпечення для збору, зберігання та аналізу електронних доказів, включаючи великі справи з комп'ютерними доказами; в) організація тісної співпраці між правоохоронними органами та постачальниками для отримання електронних доказів; г) регулярне підвищення кваліфікації слідчих та інших працівників правоохоронних органів з метою вивчення актуальних питань тактики проведення слідчих дій для отримання електронних доказів у розслідуванні кіберзлочинів; ґ) збільшення рівня кібербезпеки як у сфері державного управління, так і в приватному секторі, а також розробка нових технологій захисту та ідентифікації користувачів у кіберпросторі; д) розвиток співпраці між банківськими установами, урядом та правоохоронними органами щодо моделей взаємодії та підвищення довіри приватного сектору до державних службовців та правоохоронців. Це сприятиме збору реальних статистичних даних про кіберзлочини в банківському секторі та підвищить ефективність їх розслідування; е) створення українських кіберсил, чиї дії спрямовані на попередження та боротьбу з кіберзлочинами в кіберпросторі [211].

О.М. Жеребець у своїй науковій праці досить змістовно дослідив Стратегію кібербезпеки України, на основі чого відзначив, що урахування

прогресивного та ефективного міжнародно-правового досвіду у сфері протидії кіберзлочинності є вкрай необхідним для розробки національної системи заходів забезпечення кібербезпеки. Для досягнення проголошених у Стратегії цілей в контексті підвищення ефективності протидії кіберзлочинності доцільно: завершити імплементацію в чинне законодавство України положень Конвенції про кіберзлочинність, зокрема, шляхом встановлення відповідальності за: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних; провести чітке розмежування повноважень суб'єктів забезпечення кібербезпеки; підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів, які використовуються для здійснення кіберзлочинів; підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів, як це передбачено положеннями Стратегії [65].

Отже, проведений аналіз дає змогу констатувати, що вказані вище науковці зробили вагомий внесок у розвиток кібербезпеки в Україні. Разом із тим, варто зауважити декілька важливих аспектів: по-перше, переважна більшість досліджень були спрямовані на опрацювання теоретичних питань кібербезпеки в Україні; по-друге, питання діяльності суб'єктів протидії кіберзлочинності, а також їх взаємодії, досліджувалось досить поверхнево, в межах більш широких проблемних питань.

Таким чином, окрім розробки та прийняття нової «Стратегії кібербезпеки України», з метою вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності вбачається необхідним:

1) Розширити коло суб'єктів, які реалізують діяльність у сфері протидії кіберзлочинності, на основі чого внести доповнення до пункту 4 статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», а також змістовно визначити правовий статус відповідних органів;

2) Доповнити статтю 2 Закону України «Про основні засади забезпечення кібербезпеки України» принципом взаємодії суб'єктів протидії кіберзлочинності, адже вирішити існуючі проблеми у відповідній сфері жоден орган державної влади не може самостійно;

3) в Законі України «Про основні засади забезпечення кібербезпеки України» визначити види кіберзлочинів, що в свою чергу створить основу для опрацювання напрямів взаємодії суб'єктів протидії кіберзлочинності;

4) Розробити та прийняти окремий законодавчий акт «Про основи взаємодії суб'єкті протидії та запобігання кіберзлочинності».

Варто зауважити, що вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності є фактично неможливим без покращення організаційних засад здійснення відповідної діяльності. В даному контексті вбачається необхідним:

1) вдосконалити систему кадрового забезпечення суб'єктів протидії кіберзлочинності. Кадрове забезпечення – це, з одного боку, наявність у керівника об'єктів його управлінської діяльності – виконавців, що є необхідним для підготовки до прийняття управлінського рішення та наступного його виконання. З іншого – кадрове забезпечення – це суто суб'єкти управлінської діяльності, які організують, аналізують, контролюють, координують і здійснюють інші дії в ході державно-управлінської діяльності для досягнення певного результату. Кадри є тим суб'єктивним чинником від якого залежить реальне функціонування механізму управлінської діяльності. Адже життєздатність органу виконавчої влади не тільки в матеріальному забезпеченні, а й у спрямуванні вольових дій і переконань учасників процесу державного

управління в заданому напрямку. Без високого рівня професіоналізму та належних особистих якостей кадрів не виникає того дієвого елементу, який зумовлює динаміку управлінської діяльності [138, с.68]. А відтак, саме від професійності кадрів напряму залежить те, як кожен орган державної влади буде виконувати покладені на нього функції у сфері протидії кіберзлочинності, а відтак і ефективність їх спільної діяльності. Покращення кадрового забезпечення в розрізі представленої проблематики має включати: по-перше, створення системи професійної підготовки фахівців у галузі кібербезпеки; по-друге, постійне підвищення кваліфікації працівників, обмін практичним досвідом між фахівцями різних відомств; по-третє, залучення досвідчених фахівців у галузі кібербезпеки для розв'язання конкретних завдань та передачі знань та практичного досвіду; по-четверте, формування культури безпеки в організаціях та здійснення навчання, тренінгів персоналу щодо правил та процедур безпеки в кіберпросторі; по-п’яте, здійснення постійного моніторингу і аналізу потреб у кадровому забезпеченні та розробка стратегій покращення кадрової політики для ефективної протидії кіберзлочинності.

2) покращити систему інформаційного забезпечення суб’єктів взаємодії. Інформаційне забезпечення – це система одержання, оцінки, зберігання та переробки даних, створена з метою вироблення управлінських рішень. Це стосується різних видів діяльності, наприклад виробничої і збутової, сервісного обслуговування, включаючи підвищення технологічності виробництва, якості вироблюваної продукції, зниження її собівартості, рекламу, інформацію про асортимент продукції, ціни, форми організації сервісу тощо. Отже, узагальнює вчена інформаційне забезпечення є важливим етапом та необхідною умовою організації і проведення економічного аналізу. Це пояснюється тим, що від складу, змісту, якості вихідних даних залежить ефективність аналітичного дослідження, об'єктивність і дієвість його результатів [120]. Покращення інформаційного забезпечення в розрізі протидії кіберзлочинності має

включати: 1) створення системи обміну інформацією в режимі онлайн; 2) розробку науково-методичного забезпечення суб'єктів взаємодії; 3) оновлення програмного та технічного забезпечення.

3) переглянути підхід до фінансового та матеріально-технічного забезпечення взаємодії суб'єктів протидії кіберзлочинності. Зокрема, вбачається необхідним збільшити рівень фінансування відповідної сфери, що обумовлено її високою технологічністю та вартістю праці.

Тож, вирішення зазначених проблем правового та організаційного характеру, як вбачається, дозволить якісно покращити сферу протидії та запобігання кіберзлочинності в нашій державі. Разом із тим, навіть внесення відповідних змін та доповнень не дозволить вирішити всі нагальні проблеми, адже дана сфера постійно розвивається, а відтак потребує постійної уваги збоку науковців та законодавця.

Висновки до Розділу 3

Наголошено, що взаємодія органів державної влади у галузі протидії кіберзлочинності в Сполучених Штатах Америки – це комплексна та багатогранна діяльність, який охоплює різні етапи, від збору й аналізу інформації, а також вчинення спеціально уповноваженими суб'єктами дій, що передбачають реагування на інциденти (кіберзагрози), до державно-приватного партнерства, що також включає можливість активного залучення приватного сектору для вирішення певних задач. Це підкреслює критичну важливість синергії між різноманітними зацікавленими сторонами для ефективної протидії досліджуваному суспільно небезпечному явищу

Узагальнено, що на сьогоднішній день у Світі сформувались досить дієві підходи для протидії кіберзлочинності, втім і вони не стали панацеєю для того, щоб повністю мінімізувати ризики виникнення цього негативного

явища. Втім, це не виключає можливості використання наступного позитивного міжнародного досвіду у сфері протидії кіберзлочинності в українських реаліях:

- по-перше, вбачається необхідним розширити коло суб'єктів протидії кіберзлочинності з чітким розподілом їх ролей у відповідній сфері. Окрім того, вбачається необхідним створити єдиний координаційний центр, який буде відповідати за узгодження діяльності у відповідній сфері (на прикладі Франції та Німеччини);
- по-друге, на прикладі США, доцільно створити розгорнутий та змістовний порядок взаємодії суб'єктів протидії кіберзлочинності, в якому чітко слід розкрити повноваження кожного органу державної влади у відповідній сфері;
- по-третє, в переважній більшості країн ефективність взаємодії напряму залежить від швидкості обміну актуальною інформацією про потенційні та/або існуючі загрози у сфері використання інформаційних технологій. Так, до прикладу, у Великобританії створено систему, за якою суб'єкти протидії постійно отримують актуальну інформацію;
- по-четверте, наявність державах Європи ефективної системи збору даних про кіберзлочини, що в тому числі й на основі отримання скарг від звичайних користувачів;
- по-п'яте, фактично в кожній розвинутій країні важливим елементом протидії кіберзлочинності є співпраця з держави та приватного сектору. Урядові установи тісно співпрацюють із галузями приватного сектора, включаючи енергетику, фінанси, охорону здоров'я та технології.
- по-шосте, суб'єкти взаємодії у США постійно співпрацюють у науковій сфері, зокрема: проводять тренінги, семінари, науково-практичні конференції, тощо. Останнє дозволяє розвивати науковий потенціал у відповідній сфері.

Акцентовано увагу на тому, що «Стратегія кібербезпеки України» 2021 року здійснила вагомий внесок у розвиток сфери протидії та

запобігання кіберзлочинності. Втім, вона, переважно, була орієнтована на подолання проблем, які існували ще до початку повномасштабного вторгнення. Разом із тим, з початком війни система протидії кіберзлочинності в нашій країні виявилась не спроможною повною мірою реагувати на існуючі виклики та загрози. А відтак, незважаючи на відносну новизну, даний нормативно-правовий акт є досить застарілим.

Наголошено на значній зацікавленості законодавця у вирішенні проблем, пов'язаних із протидією кіберзлочинності. Адже зазначене суспільно небезпечне явище негативним чином впливає но фінансово-економічне становище не тільки кожної окремої людини, а й держави і суспільства в цілому. З огляду на це, на сьогоднішній день важливим кроком законодавця має бути розробка та прийняття нової «Стратегії кібербезпеки України». Вказаний нормативно-правовий акт повинен враховувати не тільки існуючі загрози у кіберпросторі, а й визначати: по-перше, окреслити чинники, які обумовлюють виникнення та розвиток кіберзлочинності; по-друге, шляхи вдосконалення діяльності, спрямованої на протидію кіберзлочинам; по-третє, коло суб'єктів, що здійснюють діяльність у сфері протидії кіберзлочинності, а також перспективні напрямки, рівні, форми та методи їх взаємодії.

З метою вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності запропоновано: 1) розширити коло суб'єктів, які реалізують діяльність у сфері протидії кіберзлочинності, на основі чого внести доповнення до пункту 4 статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», а також змістовно визначити правовий статус відповідних органів; 2) доповнити статтю 2 Закону України «Про основні засади забезпечення кібербезпеки України» принципом взаємодії суб'єктів протидії кіберзлочинності, адже вирішити існуючі проблеми у відповідній сфері жоден орган державної влади не може самостійно; 3) в Законі України «Про основні засади забезпечення кібербезпеки України» визначити види

кіберзлочинів, що в свою чергу створить основу для опрацювання напрямів взаємодії суб'єктів протидії кіберзлочинності; 4) розробити та прийняти окремий законодавчий акт «Про основи взаємодії суб'єкті протидії та запобігання кіберзлочинності».

Доведено, що вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності є фактично неможливим без покращення організаційних засад здійснення відповідної діяльності. В даному контексті вбачається необхідним: 1) покращити систему кадрового забезпечення суб'єктів протидії кіберзлочинності; 2) вдосконалити систему інформаційного забезпечення суб'єктів взаємодії; 3) переглянути підхід до фінансового та матеріально-технічного забезпечення взаємодії суб'єктів протидії кіберзлочинності.

Констатовано, що від професійності кадрів напряму залежить те, як кожен орган державної влади буде виконувати покладені на нього функції у сфері протидії кіберзлочинності, а відтак і ефективність їх спільної діяльності. Підкреслено, що покращення кадрового забезпечення в розрізі представленої проблематики має включати: по-перше, створення системи професійної підготовки фахівців у галузі кібербезпеки; по-друге, постійне підвищення кваліфікації працівників, обмін практичним досвідом між фахівцями різних відомств; по-третє, залучення досвідчених фахівців у галузі кібербезпеки для розв'язання конкретних завдань та передачі знань та практичного досвіду; по-четверте, формування культури безпеки в організаціях та здійснення навчання, тренінгів персоналу щодо правил та процедур безпеки в кіберпросторі; по-п'яте, здійснення постійного моніторингу і аналізу потреб у кадровому забезпеченні та розробка стратегій покращення кадрової політики для ефективної протидії кіберзлочинності.

Обґрунтовано, що покращення інформаційного забезпечення в розрізі протидії кіберзлочинності має включати: 1) створення системи обміну інформацією в режимі онлайн; 2) розробку науково-методичного

забезпечення суб’єктів взаємодії; 3) оновлення програмного та технічного забезпечення.

Узагальнено, що вирішення зазначених проблем правового та організаційного характеру, як вбачається, дозволить якісно покращити сферу протидії та запобігання кіберзлочинності в нашій державі. Разом із тим, навіть внесення відповідних змін та доповнень не дозволить вирішити всі нагальні проблеми, адже дана сфера постійно розвивається, а відтак потребує постійної уваги збоку науковців та законодавця.

ВИСНОВКИ

У висновках наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягає у тому, щоб з'ясувати сутність та особливості адміністративно-правових засад взаємодії суб'єктів протидії кіберзлочинності, на основі чого розробити низку теоретичних та практичних пропозицій і рекомендацій, спрямованих на вдосконалення адміністративного законодавства, норми якого спрямовані на правове врегулювання відповідної взаємодії. У результаті проведеного дослідження сформульовано низку висновків, пропозицій та рекомендацій, спрямованих на досягнення поставленої мети, зокрема:

1. Констатовано, що незважаючи на чималу кількість наукових досліджень, чітко сформульованого підходу до розкриття сутності та оцінки стану правового регулювання взаємодії суб'єктів протидії кіберзлочинності на сьогодні в юридичній літературі досі не сформовано. Поверхнево вказане питання розглядалось в межах багатьох галузевих наук та в рамках більш широких проблематик, присвячених кібербезпеці держави взагалі. Акцентовано увагу, що: а) представники кримінального права та кримінології зосереджують увагу лише на тому, що взаємодія є необхідним організаційним заходом подолання такого негативного явища, як кіберзлочинність; б) представники кримінального процесуального права та криміналістики обмежують свої дослідження виключно рамками існуючих процесуальних механізмів та порядком здійснення відповідних слідчих дій та заходів, вважаючи взаємодію виключно моделлю розвитку процесуальних відносин; в) міжнародники переймаються лише світовою співпрацею у сфері боротьби з кіберзлочинами та її юридичним оформленням; г) теоретики права розглядають взаємодію у контексті дослідження і розкриття особливостей змісту кіберзлочинності загалом. Наголошено, що безумовно, фахівці вказаних вище галузей права зробили вагомий внесок у розвиток даного інституту. Проте відсутність єдиного

сформульованого комплексного бачення природи, змісту, особливостей організації, напрямів здійснення та інших аспектів правового регулювання взаємодії суб'єктів протидії кіберзлочинності ускладнює вироблення її нової концепції та визначення шляхів удосконалення. При цьому підкреслено, що вирішувати відповідні проблеми найбільш доцільно в розрізі адміністративної галузі права, адже саме її нормами регулюється діяльність відповідних суб'єктів, їх правовий статус, мета та завдання діяльності, а відтак і визначаються засади взаємодії спеціально уповноважених органів державної влади у галузі протидії кіберзлочинності.

2. Визначено, що взаємодія суб'єктів протидії кіберзлочинності – це регламентована нормами адміністративного права модель суспільних відносин, яка передбачає тісну інформаційно-організаційну співпрацю, об'єднання ресурсів, реалізацію спільних заходів, а також поділ відповідальності у процесі здійснення державно-значущої діяльності у напрямку протидії та запобігання суспільно-небезпечним діянням, які складають структуру кіберзлочинності.

До характерних особливостей даної взаємодії віднесено наступне: а) головною її ціллю є протидія комплексному суспільно-небезпечному явищу, яке наносить шкоду правам, свободам та інтересам громадян України, а також включає негативні дії, за які законодавством передбачено найсуворіший різновид покарання – кримінальний; б) відбувається в рамках протидії кіберзлочинності – спеціальної комплексної діяльності, спрямованої на реалізацію заходів та процедур із попередження, виявлення та припинення дій окремих осіб та груп, що містять ознаки кіберзлочинів, а також факторів, які сприяють їх вчиненню; в) вступати у дані відносини можуть виключно спеціально-уповноважені суб'єкти, які мають права та обов'язки у сфері реалізації правоохоронної функцію держави; г) взаємодія суб'єктів протидії кіберзлочинності є об'єктом адміністративно-правового регулювання.

3. Доведено, що на сьогоднішній день стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності не можна оцінити однозначно, адже, 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: фактичну відсутність нормативно-правового закріплення ефективних та злагоджених механізмів взаємодії спеціально уповноважених суб'єктів у відповідній сфері; форм та методів такої взаємодії тощо.

4. Під механізмом адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності запропоновано розуміти формалізовану систему спеціальних, взаємодіючих та взаємозалежних між собою юридичних елементів, за рахунок яких встановлюються матеріальні та процедурні засади впливу права на суспільно-правові відносини, що виникають в сфері спільної діяльності суб'єктів, які уповноважені на виявлення, припинення та профілактику кіберзлочинів.

5. Аргументовано, що принципи взаємодії суб'єктів протидії кіберзлочинності представляють собою сукупність вихідних засад, основоположних, розчинених у адміністративно-правових нормативних актах, стабільних, загальнообов'язкових ідей, які визначають призначення, вектори, цілі та особливості правового регулювання суспільно-правових відносин, що виникають в контексті взаємодії уповноважених суб'єктів протидії кіберзлочинності в Україні. До вказаних принципів віднесено принципи: законності; поєднання цілей; визначеності суб'єктного складу; координації та контролю; плановості; науковості; достатності.

6. Наголошено, що адміністративно-правовий статус суб'єктів протидії кіберзлочинності в Україні – це сукупність визначених нормами адміністративного права елементів, які в своїй єдності визначають положення та роль суб'єктів протидії кіберзлочинності у суспільно-правових відносинах, що виникають в процесі здійснення ними спільної

діяльності у досліджуваному напрямку. До елементів адміністративно-правового статусу відповідних суб'єктів віднесено: компетенцію, повноваження, гарантії діяльності та юридичну відповідальність.

7. Під формами взаємодії суб'єктів протидії кіберзлочинності запропоновано розуміти зовнішній вираз спільної, взаємоузгодженої практичної діяльності спеціально уповноважених органів державної влади та їх посадових осіб, яка спрямована на досягнення єдиної мети – протидія та запобігання правопорушенням та злочинним діям, які відбуваються в кіберпросторі або з використанням комп'ютерних технологій і мереж. Зауважено, що в науковій літературі не сформовано єдиного підходу щодо переліку відповідних форм, а відтак останні запропоновано поділити на дві групи: 1) нормативно-правові форми: нормотворчість; адміністративний договір; правозастосування; 2) організаційно-управлінські форми: підготовка і реалізація спільних заходів; створення спільних робочих груп; адміністративний нагляд; просвітницька робота з громадськістю.

Методи взаємодії суб'єктів протидії кіберзлочинності запропоновано визначити як сукупність закріплених нормами чинного законодавства інструментів та засобів, які в своїй діяльності використовують спеціально уповноважені органи державної влади задля здійснення відповідної спільної діяльності. До вказаних методів віднесено такі: переконання, примус, координацію, планування, прогнозування, роботу з кадрами та інформаційний метод.

8. Узагальнено, що на сьогоднішній день у світі сформувались досить дієві підходи у сфері протидії кіберзлочинності, втім і вони не стали панацеєю для того, щоб повністю мінімізувати ризики виникнення цього негативного явища. Втім, це не виключає можливості використання такого позитивного міжнародного досвіду у сфері протидії кіберзлочинності в українських реаліях:

– по-перше, вбачається необхідним розширити коло суб'єктів протидії кіберзлочинності з чітким розподілом їх ролей у відповідній сфері. Окрім

того, необхідним є створення єдиного координаційного центру, який буде відповідати за узгодження діяльності у відповідній сфері (на прикладі Франції та Німеччини);

– по-друге, на прикладі США доцільно розробити розгорнутий та змістовний порядок взаємодії суб'єктів протидії кіберзлочинності, в якому слід чітко розкрити повноваження кожного органу державної влади у відповідній сфері;

– по-третє, в переважній більшості у зарубіжних країнах ефективність взаємодії напряму залежить від швидкості обміну актуальною інформацією про потенційні та/або існуючі загрози у сфері використання інформаційних технологій. Так, до прикладу, у Великобританії створено систему, за якою суб'єкти протидії постійно отримують актуальну інформацію про існуючі та потенційні загрози кібербезпеці в режимі «он-лайн», отже доцільно створити відповідну систему й в Україні;

– по-четверте, слід створити ефективну систему збору даних про кіберзлочини, в тому числі й на основі отримання скарг від звичайних користувачів;

– по-п'яте, фактично в кожній розвинутій країні важливим елементом протидії кіберзлочинності є співпраця держави та приватного сектору у відповідній сфері. Урядові установи тісно співпрацюють із галузями приватного сектора, включаючи енергетику, фінанси, охорону здоров'я та технології, що є теж доцільним для запровадження в Україні.

– по-шосте, на прикладі США запровадити постійну співпрацю у науковій сфері, зокрема: проводити тренінги, семінари, науково-практичні конференції тощо. Останнє дозволяє розвивати науковий потенціал у сфері протидії кіберзлочинності.

9. З метою вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності запропоновано:

1) розробити та прийняту нову «Стратегію забезпечення кібербезпеки», яка повинна враховувати не тільки існуючі загрози у кіберпросторі, а й: по-перше, окреслити чинники, які обумовлюють виникнення та розвиток кіберзлочинності; по-друге, виокремити шляхи вдосконалення діяльності, спрямованої на протидію кіберзлочинам; по-третє, закріпити коло суб'єктів, що здійснюють діяльність у сфері протидії кіберзлочинності, а також перспективні напрямки, рівні, форми та методи їх взаємодії;

2) розширити коло суб'єктів, які реалізують діяльність у сфері протидії кіберзлочинності, задля чого слід внести доповнення до пункту 4 статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», а також змістовно визначити правовий статус відповідних органів;

3) доповнити статтю 2 Закону України «Про основні засади забезпечення кібербезпеки України» принципом взаємодії суб'єктів протидії кіберзлочинності, адже вирішити існуючі проблеми у відповідній сфері жоден орган державної влади самостійно не може;

4) в Законі України «Про основні засади забезпечення кібербезпеки України» визначити види кіберзлочинів, що в свою чергу створить основу для опрацювання напрямів взаємодії суб'єктів протидії кіберзлочинності;

5) розробити та прийняти окремий законодавчий акт «Про основи взаємодії суб'єкті протидії та запобігання кіберзлочинності».

Доведено, що вдосконалення адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності є фактично неможливим без покращення організаційних засад здійснення відповідної діяльності. В даному контексті вбачається необхідним: 1) покращити систему кадрового забезпечення суб'єктів протидії кіберзлочинності; 2) вдосконалити систему інформаційного забезпечення суб'єктів взаємодії; 3) переглянути підхід до фінансового та матеріально-технічного забезпечення взаємодії суб'єктів протидії кіберзлочинності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративна діяльність органів внутрішніх справ. Загальна частина: Підручник / Під загальною редакцією І.П.Голосніченка, Я.Ю.Кондратьєва. К., 1995. 179с.

2. Адміністративне право України: словник термінів. за заг. ред. Т. О. Коломоєць, В. К. Колпакова. К.: Ін Юре, 2014. 520 с.

3. Адміністративне право України [Підручник для юрид. вузів і фак. / АЗІ Ю. П. Битяк, В. В. Богуцький, В. М. Гаращук та ін.]; За ред. Ю.П. Битяка. Харків: Право, 2000. 520 с.

4. Адміністративне право України. Академічний курс: Підруч.: У двох томах: Том 1. Загальна частина. Ред. колегія: В. Б. Авер'янов (голова). К.: Видавництво «Юридична думка», 2004. 584 с.

5. Адміністративне право України: Підручник. Битяк Ю.П., Гаращук В.М., Дьяченко О. В., Зима О. Т., Зуй В. В.; під ред. Ю.П. Битяка. К.: Юрінком Інтер, 2005. 544 с.

6. Азаров Д.С. Злочини у сфері комп’ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. 304 с.

7. Алтуніна О.М. Адміністративно-правовий статус органів місцевого самоврядування. Право і безпека. 2010. №4(36).С.89-92.

8. Алфьоров С. М., Ващенко С. В., Долгополова М. М., Купін А. П. Адміністративне право. Загальна частина. Навч. посіб. К.: Центр учбової літератури, 2011. 216 с.

9. Андреєв А. Механізм правового регулювання суспільних відносин: окремі аспекти щодо визначення поняття та особливостей. Підприємництво, господарство і право. 2019. №6. С.125-128 с.

10. Андрійко О.Ф. Державний контроль в Україні: організаційно-правові засади / О.Ф. Андрійко. К.: Наук. думка, 2004. 304 с.

11. Бабич І. Г. Принцип справедливості в римському праві і у сучасному зобов'язальному праві України: дис... канд. юрид. наук: 12.00.03

/ Бабич Ірина Григорівна; Одеська національна юридична академія. О., 2006. 183 арк.

12. Бабійчук О.М. Адміністративно-правове регулювання та юридичні аспекти в паліативній і хоспісній медицині. Адміністративне право і процес. 2014. №4(10). С.132-140.

13. Бандурка О. М., Давиденко Л. М. Преступность в Украине: причины и противодействие : монографія. Харків, 2003. 368 с.

14. Бандурка О. М., Литвинов О. М. Протидія злочинності та профілактика злочинів: монографія. Харків, 2011. 308 с.

15. Бандурка О.М. Управління в органах внутрішніх справ України: Підручник. Харків: Ун-т внутр. справ, 1998. 480 с.

16. Барандич С. Правозастосування в сучасному вимірі юридичної науки. Науковий часопис Національної академії прокуратури України. 2014. № 4. С. 1–7 URL:http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2015/barandych.pdf

17. Батраченко О.В. Адміністративно-правові засади діяльності Національної поліції України щодо забезпечення публічної безпеки і порядку: дис. ... канд. юрид. наук: Суми. Сумський державний університет. 2019. 218 с.

18. Бедрак Н.О. Адміністративно-правове регулювання туристичною галуззю: автореферат. дис. ... канд. юрид. наук: Київ. Київський національний університет внутрішніх справ. 2010. 18 с.

19. Безпалова О.І., Горбач Д.О. Поняття та структура адміністративно-правового статусу Національної гвардії України. Форум права. 2017. № 5. С. 31–38.

20. Березовська І.Р. Поняття і характеристика структурних елементів механізму застосування адміністративно-правових засобів забезпечення інформаційної безпеки України. Науковий вісник Національної академії внутрішніх справ. 2013. №2. С.31-35.

21. Битяк Ю. П. Адміністративне право України [конспект лекцій] / Ю. П. Битяк, В. В. Зуй. Х.: Націон. юрид. акад. України імені Ярослава Мудрого, 1996. 160 с.

22. Битяк Ю., Константий О. Правова природа адміністративних договорів // Вісник Академії правових наук України. 2001. № 3 (26). С. 101-109

23. Білик П.П. Організаційно-правове забезпечення управління соціально-економічним розвитком регіону: дис. ... канд. юрид. наук: Одеса: Одеський національний університет ім. І.І. Мечникова. 2003. 188 с.

24. Білодід І.К. Словник української мови: в 11 томах. Том 8, 1977. Стор. 317.

25. Білодід І.К. Словник української мови: в 11 томах. Том 9, 1978. Стор. 671.

26. Богатирьов І.Г., Литвинов О.М. Кримінальна політика як наукова стратегія у сфері протидії злочинності. Вісник Кримінологічної асоціації України. 2013.№ 4. С. 6–12.

27. Богуцький В. В., Богуцька А. В. Адміністративне право України як галузь права: навч. посіб. Х.: ФІНН, 2010. 59 с.

28. Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : науково-практичний посібник. Київ : Національна академія прокуратури України, 2015. 202 с.

29. Бондаренко К.В. До визначення категорії «правовий стан». Юридичний науковий електронний журнал. 2014. №4. С.16-18.

30. Борисова Л.В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження: дис. ... канд. юрид. наук: Київ: Київський національний університет внутрішніх справ. 2007. 217 с.

31. Боровик А.В., Копотун І.М. Кібезлочини в Україні (кримінально-правова характеристика): навчальний посібник. Волинь. Вид.-во: «Поліграф». 2019. 304 с.

32. Бузунов Р.А. Адміністративно-правове регулювання кредитно-модульної системи організації навчального процесу (в ВНЗ системи МВС): дис. ... канд. юрид. наук. Ірпінь: Донецький юридичний інститут Луганського державного університету внутрішніх справ. 2007. 434 с.

33. Буяджа С. Позитивний досвід правового регулювання боротьби з кіберзлочинністю в країнах ЄС / С. Буяджа // Evropský politický a právní diskurz. 2017. Sv. 4, Vyd. 4. С. 41-46. URL: http://nbuv.gov.ua/UJRN/evrpol_2017_4_4_7

34. Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект: дис. ... канд. юрид. наук: Київ: ПВНЗ Університет Короля Данила. 2018. 203 с.

35. Васильєв А.С. Адміністративне право України (загальна частина): навч. посіб. Х.: Одисей, 2002. 356 с.

36. Васильковський І.І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2018. Вип. 1-2 (10-11). С.276-282.

37. Великий тлумачний словник сучасної української мови. уклад. і голов. ред. В. Т. Бусел. К., Ірпінь : Перун, 2005. 1728 с.

38. Венедіктов С.В. Матеріальне та моральне стимулювання ефективної професійної діяльності працівників органів внутрішніх справ України: теоретичний аспект: дис. ... канд. юрид. наук: Харків: Національний університет внутрішніх справ. 2004. 186 с.

39. Вербець В.В., Субота О.А., Христюк Т.А. Соціологія: навчальний посібник. К.: КОНДОР. 2009. 550 с.

40. Віхров О.Л. та Віхрова І.О. Теорія держави і права: курс лекцій. Чернігів : Десна Поліграф, 2015. 303 с.

41. Войциховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і безпека 2011. №4(41). С.107-112.

42. Галунько В.В. Адміністративно-правові основи організації та діяльності державної служби охорони при Міністерстві внутрішніх справ України. Київ: Національна академія внутрішніх справ України. 2003. 207 с.

43. Гаруст Ю.В. Правове регулювання контрольної діяльності податкових органів України: дис. ... канд. юрид. наук: Харків: Харківський національний університет внутрішніх справ. 2007. 181 с.

44. Гончарук С. Т. Адміністративне право України. Загальна та Особлива частини : навч. посіб. К. : Нац. акад. внутр. справ ; Нац. акад. упр., 2000. 240 с.

45. Горінецький Й.І. Правоохоронна функція держав Центральної Європи: теоретичні і практичні аспекти: Автреф. дис. … канд. юрид. наук: 12.00.01. Національна академія внутрішніх справ України. К., 2005. 20 с.

46. Городянко С.В. Організаційно-правове забезпечення безпеки діяльності працівників ОВС України: дис. ... канд. юрид. наук: Харків. Харківський національний університет внутрішніх справ. 2007. 189 с.

47. Гриценко С. П. Латинська мова й основи римського права : навч. посіб. К. : Центр навчал. літератури, 2005. 336 с.

48. Грохольський В.Л. Принципи державного управління у сфері боротьби з організованою злочинністю. Право і безпека. 2003. №2/3. С.65-69.

49. Гук Б. М. Особливості адміністративно-правового статусу Державної виконавчої служби України в умовах адміністративної реформи. Публічне право. 2010. № 3 С. 86-92.

50. Гумін О.М., Пряхін Є.В. Адміністративно-правовий статус особи: поняття та структура. Наше право. 2014. №5. С.32-37.

51. Дегтярьов О.Ф. Адміністративно-правове забезпечення реалізації прав громадян на вільний вибір місця проживання: дис. ... канд. юрид. наук. Київ: Київський національний університет внутрішніх справ. 2006. 181 с.

52. Дергільова О.Г. Правові акти: поняття, класифікація та соціальне призначення. Актуальні проблеми вітчизняної юриспруденції. 2016. №3. С.3-8.

53. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: постанова, порядок від 04.04.2023 №299. Офіційний вісник України. 2023. №39. Ст.2061.

54. Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. С. 4 - 12.

55. Дмитренко, С. М. Адміністративно-правове забезпечення самоврядного контролю у сфері земельних відносин: дис. ... канд. юрид. наук : 12.00.07. Суми, 2021. 242 с.

56. Добкін М. М. Адміністративно-правовий статус виконавчих органів міських рад : автореф. дис. … канд. юрид. наук. Київ, 2009. 26 с

57. Добровольська Н.В. Адміністративний договір: осмислення нормативної дефініції. Правова позиція 2020. № 3 (28). С. 28–34

58. Дрозд О.Ю. Співвідношення норм трудового та адміністративного права при регулюванні проходження державної служби в Україні : монографія. О.Ю. Дрозд. Дніпро : Видавничий дім «Гельветика», 2016. 420 с.

59. Дручек О.В., Легенький В.В. Протидія злочинам, здійсненим на ґрунті ненависті: поняття, зміст, ознаки. Юридичний науковий електронний журнал. 2021. №4. С.450-453.

60. Дрьомін В.М. Злочинність як соціальна практика: інституціональна теорія криміналізації суспільства: монографія. О.: Юридична література, 2009. 616 с.

61. Дрьомін В.М. Інституціональна теорія злочинності та криміналізації суспільства: дис. ... д-ра. юрид. наук: Одеса: Одеська національна юридична академія. 2010. 442 с.

62. Дубінчак В.М. Правоохоронна діяльність сутність, суб’єкти, засоби забезпечення (теоретико-правовий аспект): дис. ... д-ра. юрид. наук:

Київ: Національна академія наук України Інститут держави і права ім. В.М. Корецького. 2010. 425 с.

63. Дулепа В.П. Кримінологічна характеристика кіберзлочинності. 2021. №11. С.592-595.

64. Енциклопедичний словник з державного управління уклад. : Ю.П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін. ; за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. К. : НАДУ, 2010. 820 с.

65. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект / О. М. Жеребець // Інформація і право. 2021. № 4. С. 129-134

66. Жидченко К.П. Сутність механізму адміністративно-правового регулювання реалізації військовослужбовцями права на виплату одноразової грошової допомоги. Юридичний вісник. 2016. №3(40). С.67-72.

67. Завальний А.М. Юридичні факти в сфері здійснення правоохоронної діяльності: дис. ... канд. юрид. наук: Київ. Київський національний університет внутрішніх справ. 2007. 192 с.

68. Завальний М.В. Принципи взаємодії державних та недержавних суб'єктів правоохорони в Україні. Правовий часопис Донбасу. 2018. №1(62). С.114-119.

69. Загальна теорія держави і права: підруч. для студ. юрид. спец. вищ. навч. закл. / [М. В. Цвік та ін.] ; за ред. д-ра юрид. наук, проф., акад. АПрН України М. В. Цвіка, д-ра юрид. наук, проф, акад. АПрН України О. В. Петришина ; Нац. юрид. акад. України ім. Ярослава Мудрого. Х.: Право, 2010. 583 с.

70. Загальна теорія держави і права: Підручник для студентів юридичних спеціальностей вищих навчальних закладів. М. В. Цвік, В. Д. Ткаченко, Л. Л. Богачова та ін.; За ред. М. В. Цвіка, В. Д. Ткаченка, О. В. Петришина. Харків : Право, 2002. 432 с.

71. Загуменний О.О. Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини». Харків: Процесуальне та техніко-криміналістичне забезпечення досудового розслідування. 2019. С.67-70.

72. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 172–177

73. Іващенко О.М. Адміністративно-правове регулювання корпоративних прав держави: дис. ... канд. юрид. наук: Київ: Київський міжнародний університет. 2008. 189 с.

74. Ісаков М. Г. До визначення адміністративно"правового статусу суб'єктів державного контролю у сфері підприємницької діяльності. Публічне право. 2013. № 2 (10). С. 91-98.

75. Йона О. О. Світові тенденції боротьби з кіберзлочинністю / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. 2013. № 15(1). С. 59-61

76. Кабанець В.О. Теоретичні аспекти удосконалення інституту трудових спорів в Україні: дис. ... канд. юрид. наук: Харків: Харківський національний університет внутрішніх справ. 2009. 189 с.

77. Кабиш О.О. До проблеми визначення поняття протидії кіберзлочинності. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення:* матеріали міжнародної науково-практичної конференції (Київ, 22–23 вересня 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 37–39.

78. Кабиш О.О. До характеристики принципів адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Виклики сучасності та наукові підходи до їх вирішення:* матеріали міжнародної науково-практичної конференції (Київ, 12–13 серпня 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 42–45.

79. Кабиш О. Особливості взаємодії суб'єктів протидії кіберзлочинності. *KELM*. 2022. № 7(51). С. 250–254.

80. Кабиш О.О. Стан дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Держава та регіони. Серія Право.* 2021. № 4(74). С. 205–209.

81. Кабиш О.О. Сутність та зміст координації та контролю, як принципів взаємодії суб'єктів протидії кіберзлочинності. *Проблемні питання юридичної науки в контексті реформування правової системи України:* матеріали міжнародної науково-практичної конференції (Київ, 19–20 жовтня 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 21–23.

82. Кабиш О.О. Сутність та зміст механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Юридична наука.* 2020. № 8. С. 185–189.

83. Кабиш О.О. Сучасний стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Науковий вісник публічного та приватного права.* 2023. Вип. 4. С. 113–118.

84. Карпечкін П.Ф. Принципи права та виключення у праві: поняття, значення, співвідношення та класифікація. Електронний веб-портал Апеляційного суду міста Києва. URL: https://kia.court.gov.ua/sud2690/1j/4q/51101/.

85. Кельман М.С., Мурашин О.Г. Загальна теорія держави і права : підручник. Київ: Кондор, 2008. 477 с.

86. Кириченко Т. Недоліки правового регулювання трудових відносин в Україні. Підприємництво, господарство і право. 2020. №12. С.96-103

87. Кириченко Ю.М. Поняття та структура адміністративно-правового статусу органів місцевого самоврядування. Юридичний бюлетень. 2018. Випуск 7. Ч.2. С.41-47.

88. Кіберзлочинність коштує Британії 27 млрд. URL: https://www.bbc.com/ukrainian/news/2011/02/110217_cybercrime_uk_oh

89. Ківалов С. В. Адміністративне право України : навч.-метод. посіб. С. В. Ківалов, Л. Р. Біла. 2-ге вид., переробл. і доп. О. : Юрид. л-ра, 2002. 312 с.

90. Ківалова Т.С. Зобов'язання відшкодування шкоди за цивільним законодавством України: теоретичні проблеми: дис. ... д-ра. юрид. наук: Одеса: Одеська національна юридична академія. 2008. 458 с.

91. Клемпарський М.М. Державні службовці як суб'єкти трудового права України: дис. ... д-ра. юрид. наук. Харків: Харківський національний університет внутрішніх справ. 2014. 403 с.

92. Клюєв О.М. Форми та методи профілактичної діяльності органів внутрішніх справ на місцевому рівн. Форум права. 2007. № 1. С. 99-103.

93. Князька Л.А. Адміністративно-правове регулювання в галузі соціального захисту населення: дис. ... канд. юрид. наук: Київ: Національний університет біоресурсів і природокористування України. 2010. 215 с.

94. Коваленко О. Теоретико-методологічні засади формування механізмів забезпечення кібербезпеки України на сучасному етапі державного будівництва. Věda a perspektivyNo 6(13) 2022URL: http://perspectives.pp.ua/index.php/vp/article/view/1795/1792

95. Коваль В. Елементи адміністративно-правового статусу військовослужбовців. Підприємництво, господарство і право. 2018. №11. С.92-95.

96. Ковальов В.В. Взаємодія слідчого з працівниками експертної служби МВС України: дис. ... канд. юрид. наук: Київ: Київський національний університет внутрішніх справ. 2007. 227 с.

97. Ковальська В.В. Міліція в системі правоохоронних органів держави (адміністративно-правові аспекти): дис. ... д-ра. юрид. наук: Київ: Київський міжнародний університет. 2008. 422 с.

98. Кодекс адміністративного судочинства України : Закон України від 6 липня 2005 р. № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15

99. Кожухар О.В. Адміністративно-правове забезпечення взаємодії інститутів громадян-ського суспільства з органами і підрозділами Національної поліції України : дис. ... канд. юрид. наук : спец. 12.00.07. Київ, 2021. 278 с.

100. Козюбра М. Принципи права: методологічні підходи до розуміння природи та класифікації в умовах сучасних глобалізаційних трансформацій. Право України. 2017. №11. С.142-164.

101. Колесніченко В.В. Принципи права Європейського Союзу: загальнотеоретичне дослідження: автореферат. дис. ... канд. юрид. наук: Одеса: Одеський національний університет внутрішніх справ. 2010. 22 с.

102. Коломоєць Т.О. Адміністративне право України. Академічний курс: підруч. К: Юрінком Інтер, 2011. 576 с.

103. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності: конвенція від 15.11.2000 №14. Ст.340.

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

105. Конопльов В.В. Організаційно-правовий механізм підготовки та прийняття управлінських рішень в адміністративній діяльності органів внутрішніх справ: дис. ... д-ра. юрид. наук: Харків: Кримський юридичний інститут ХНУВС. 2006. 413 с.

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

107. Коржанський М.Й. Кримінальне право України. Частина загальна : курс лекцій. К.: Наукова думка та українська видавнича група, 1996. 336 с.

108. Корсун С.І. Механізм адміністративно-правового регулювання запобігання фінансуванню тероризму. Науковий вісник Міжнародного гуманітарного університету. 2013. №6-2. Том.1. С.116-118.

109. Котух Є.В. Кібербезпека у публічному секторі : монографія / Є.В. Котух. Харків : Колегіум, 2021. 272 с.

110. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. Вісник кримінологічної асоціації України. 2018. № 2(19). С. 155–166

111. Кравченко О.О. Кримінально-правова характеристика контрабанди (ст.201 КК України): дис. ... канд. юрид. наук: Київ: Київський міжнародний університет. 2010. 203 с.

112. Кравченко Ю.Ф. Свобода як принцип демократичної правової держави: дис. ... д-ра. юрид. наук. Харків: Національний університет внутрішніх справ. 2003. 411 с.

113. Крестовська Н.М. Ювенальне право України: генезис та сучасний стан: дис. ... канд. юрид. наук: Одеса. Одеська національна юридична академія. 2008. 468 с.

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

115. Кримінальний процесуальний кодекс України: закон від 13.04.2012 № 4651-VI. Відомості Верховної Ради України. 2013. №9-10. Ст.474.

116. Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків). МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. 244 с.

117. Круглий В.М. Теоретико-правові засади взаємодії працівників оперативних підрозділів органів внутрішніх справ з населенням. Науковий вісник НАВСУ К. 2002. № 3. С. 130-136.

118. Кудін А. Адміністративний договір у сфері адміністративно-правового забезпечення патентної діяльності в Україні. 6 Knowledge, Education, Law, Management 2020 № 4 (32), vol. 2, c.59-64 URL: http://kelmczasopisma.com/viewpdf/1539

119. Кулик О. Правоохоронні органи України. Міжнародна поліцейська енциклопедія: у 10-ти т. К.: Концерн "Видавничий Дім "Ін Юре", 2003 Т.1. 2003. 1232 с.

120. Купалова Г.І. Теорія економічного аналізу: Навч. посіб. К.: Знання, 2008. 639 с.

121. Куракін О.М. Структура механізму правового регулювання. Науковий вісник Ужгородського національного університету. 2015. Випуск 35. Частина ІІ. Том І. С.46-49.

122. Курило В.І. Адміністративні правовідносини у сільському господарстві України: дис. ... д-ра. юрид. наук: Київ: Національний аграрний університет. 2007. 487 с.

123. Куц В. Загальна характеристика механізму протидії злочинності та його понятійного апарату. Актуальні проблеми кримінального права та кримінології: матеріали всеукраїнської науково-практичної конференції. Донецький юридичний інститут ЛДУВС ім. Е.О. Дідоренка. Донецьк: Норд Комп'ютер, 2009. С. 12–15.

124. Куц В. Зміст та рівні протидії злочинності. Тенденції та пріоритети реформування законодавства України: матеріали всеукраїнської науково-практичної конференції (м. Херсон, 11–12 грудня 2015 р.). Херсон: Гельветика, 2015 С. 152–156.

125. Кучук А.М., Перепьолкін С.М. Принципи права як категорії внутрішньодержавного й міжнародного права. Право і суспільство. 2015. №3 частина 3. С.22-26.

126. Лавренко П.Є. Особливості діяльності кіберполіції: досвід країн Європи та США / П.Є.Лавренко // Актуальні проблеми

державотворення, правотворення та правозастосування: матеріали наук. семінару (м. Дніпро, 8 грудня 2017 р.). Дніпро: ДДУВС, 2018. С. 380-385

127. Леган І.М. Теоретико-правові засади міжнародного співробітництва щодо запобігання та протидії транснаціональній злочинності: автореферат. дис. ... д-ра. юрид. наук: Ірпінь: Університет державної фіскальної служби України. 2021. 41 с.

128. Лисенко В.В. Проблеми криміналістичного забезпечення розслідування податкових злочинів: дис. ... д-ра. юрид. наук: Ірпінь: Національна академія Державної податкової служби України. 2005. 499 арк.

129. Литвин І.І. Сутність поняття правового статусу. Науковий вісник Ужгородського національного університету. 2016. Випуск 36. Том 1. С.18-21.

130. Литвинов О.М. Соціально-правовий механізм протидії злочинності в Україні (теоретичні та практичні засади): дис. ... д-ра. юрид. наук: Харків: Харківський національний університет внутрішніх справ. 2010. 432 с.

131. Лютіков П.С. Державний контроль у галузі чорної металургії в Україні: організаційно-правовий аспект: дис. ... канд. юрид. наук: Запоріжжя: Запорізький національний університет. 2009.212 с.

132. Люх В.В. Адміністративно-правовий статус правоохоронних органів як суб'єктів забезпечення фінансової безпеки держави. Юридична наука. 2020. №1(103). С.193-204.

133. Мандибура В.О. Рівень життя населення України та проблеми реформування механізмів його регулювання. К. : Парламент. вид-во, 1998. 256 с.

134. Марков В. В. Актуальні проблеми інформаційної безпеки України в системі міжнародної координації. Право і Безпека. 2013. № 1. С. 78-80.

135. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. Право і безпека. 2015. №2(57). С.107-113.

136. Марков В.В., Караченцев О.В. Напрями діяльності НАТО у справі протидії кіберзлочинності. Право і безпека. 2014. №4(55). С.119-123.

137. Мельник Р.С. Забезпечення законності застосування заходів адміністративного примусу, не пов'язаних з відповідальністю: Автореф. дис... канд. юрид. наук. Харків, 2002. 19 с.

138. Мельничук М. В. Адміністративно-правовізасади управлінської діяльності керівників органів виконавчої влади : дис. ... канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / М. В. Мельничук. К., 2009. 197 с.

139. Мещерякова О. В. Щодо визначення елементів адміністративно-правового статусу учасників операцій ООН з підтримання миру. Форум права. 2011. № 2. С. 609–612.

140. Міловська Н.В. Структура механізму правового регулювання договірних страхових відносин. Право і суспільство. 2018. №3. С.98-104.

141. Міщенко С. Г. Роль кримінальної юстиції в протидії злочинності : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2011. 19 с

142. Науковий коментар Кримінального кодексу України. проф. М.Й. Коржанський. К. : Атіка, Академія, Ельга, 2001. 656 с.

143. Несімко О.Д. Економічна культура юриста: правовий аспект: дис. ... канд. юрид. наук. Львів: Львівський державний університет внутрішніх справ. 2009. 205 с.

144. Нечипоренко А. О. Нормотворчість в Україні: поняття, види, напрямки удосконалення: автореф. дис. ... канд. юрид. наук : 12.00.01 / А. О. Нечипоренко; наук. кер. І. В. Процюк; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2015. 21 с.

145. Німко О. Б. Адміністративно-правове регулювання державного молодіжного житлового кредитування : дис. ... канд. юрид. наук : 12.00.07 / Німко Ольга Борисівна. К., 2008. 201 с.

146. Новий тлумачний словник української мови : у 4 т. уклад. В. Яременко, О. Сліпушко. К.: Аконіт. Т. 4. 1998. 941 с.

147. Новий тлумачний словник української мови. У чотирьох томах. Т.2. Укладачі В. В. Яременко, О. М. Сліпушко. Київ: “Аконіт”, 2000. 912 с.

148. Ольховська С.М. Поняття та зміст адміністративного договору / С. М. Ольховська // Право і Безпека. 2011. № 3. С. 86-88

149. Оніщенко О.В. Конституція України як основне джерело конституційного права України: дис. ... канд. юрид. наук: Київ: Київський національний університет імені Тараса Шевченка. 2005. 216 с.

150. Основи інформаційного права України: Навч. посіб. В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.; За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К.: Знання, 2004. 274 с.

151. Основи менеджменту: навч, посібн. [для студ. вищ.навч. закл.] / І.О. Щебликіна, Д.В. Грибова. Мелітополь: Видавничий будинок Мелітопольської міської друкарні, 2015. 480 с.

152. Основи методології та організації наукових досліджень : навч. посіб. для студентів, курсантів, аспірантів і ад’юнтів. за ред. А. Є. Конверського. К. : Центр учбової літератури, 2010. 352 с.

153. Пархоменко Н.М. Джерела права: теоретико-методологічні засади: дис. ... д-ра. юрид. наук: К., 2009. 442 с.

154. Пасічна І.О. Навчальний посібник з дисципліни «Законотворчість, нормотворчість та правореалізація» для студентів спеціальності 281 Публічне управління та адміністрування. Полтава : ПолтНТУ, 2019. 113 с.

155. Петров Є. В. Інформація як об’єкт цивільно-правових відносин : автореф. дис. на здобуття наук. ступеня канд. юрид. наук: 12.00.03

«Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / Є. В. Петров. Х., 2003. 20 с.

156. Петрушенко В.Л. Філософія: [Навчальний посібник, 2-е видання, виправлене і доповнене] / П.П. Петрушенко. К.: "Каравела", 2002. 544 с.

157. Пєтков С.В. Теорія адміністративного права: навч. посіб. К.: КНТ, 2014, 304 с.

158. Погрібний С. О. Механізм та принципи регулювання договірних відносин у цивільному праві України : дис. ... д-ра юрид. наук : 12.00.03. Погрібний Сергій Олексійович. К., 2009. С. 144.

159. Подковенко Т. Протидія злочинності: аксіологічний аспект. Актуальні проблеми правознавства. 2020. №1(21). С.32-39.

160. Подоляка А.М. Адміністративно-правове регулювання охорони громадського порядку в Україні: дис. ... д-ра. юрид. наук: Київ: Інститут законодавства Верховної Ради України. 2009. 381 с.

161. Подоляка А.М. Адміністративно-правовий статус Державної автомобільної інспекції МВС України: автореф. дис. … канд. юрид. наук : 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право»; Національний університет внутрішніх справ. Харків, 2004. 19 с.

162. Подорожній Є.Ю. Особливості юридичної відповідальності у трудовому праві України: дис. ... д-ра. юрид. наук: Харків: Харківський національний університет внутрішніх справ. 2016. 426 с.

163. Попадюк О.І. Особливості планування як пріоритетної функції управління. Інвестиції: практика та досвід. 2012. №5. С.86-87.

164. Попович Є.М. Нагляд і контроль за дотриманням трудового законодавства України: дис. ... канд. юрид. наук: Харків. Національний університет внутрішніх справ. 2003. 192 с.

165. Правдюк А.Л. Організаційно-правові засади реєстрації і ідентифікації сільськогосподарських тварин: дис. ... канд. юрид. наук:

Київ. Національний університет біоресурсів і природокористування. 2009. 200 с.

166. Примуш М. В. Загальна соціологія: навч. Посібник. К.: Професіонал, 2004. 590 с.

167. Про затвердження Положення про організаційно-технічну модель кіберзахисту: постанова від 29.12.2021 №1426. Урядовий портал. Єдиний веб-портал органів виконавчої влади України. [Електронний ресурс]. Режим доступу: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-polozhennya-pro-a1426.

168. Про затвердження Порядку координації діяльності правоохоронних органів у сфері протидії злочинності: наказ, перелік від 08.02.2021 №28.

169. Про Кабінет Міністрів України: закон від 27.02.2014 №794-VII. Відомості Верховної Ради України. 2014. №13. Ст.828.

170. Про Національний координаційний центр кібербезпеки: указ, положення від 07.06.2016 №242/2016. Офіційний вісник Президента України. 2016. №17. Ст.468.

171. Про Національну поліцію: закон від 02.07.2015 №580-VIII. Відомості Верховної Ради України. 2015. №40-41. Ст.379.

172. Про оперативно-розшукову діяльність: закон від 18.02.1992 №2135-XII. Відомості Верховної ради України. 1992. №22. Ст.303.

173. Про організаційно-правові основи боротьби з організованою злочинністю: закон від 30.06.1993 №3341-XII. Відомості Верховної Ради України. 1993. №35. Ст.358.

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

175. Про прокуратуру: закон від 14.10.2014 №1697-VII. Відомості Верховної Ради України. 2015. №2-3. Ст.12.

176. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» /

Указ Президента України; Стратегія від 14.09.2020 № 392/2020 URL: https://zakon.rada.gov.ua/laws/show/392/2020#n5

177. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента України; Стратегія від 26.08.2021 № 447/2021 URL: https://zakon.rada.gov.ua/laws/show/447/2021/conv#Text

178. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.2021 року №685/2021 / Президент України Офіційне інтернет-представництво. https://www.president.gov.ua/documents/6852021-41069

179. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки" / Указ Президента України; Стратегія від 16.02.2022 № 56/2022 URL: https://zakon.rada.gov.ua/laws/show/56/2022/conv#Text

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

181. Про Службу безпеки України: закон від 25.03.1992 №2229-XII. Відомості Верховної Ради України. 1992. №27. Ст.382.

182. Прокопенко О.Ю. Завдання органів внутрішніх справ як суб’єктів забезпечення правопорядку в регіоні / О.Ю. Прокопенко // Пріоритетні проблеми реформування системи законодавства України : Матеріали міжнародної науково-практичної конференції (м. Київ, 23-24 липня 2015 р.). К. : «Науково-дослідний інститут публічного права», 2015. С. 174- 176

183. Резнік О. М. Адміністративно-правові засади діяльності правоохоронних органів із забезпечення фінансово-економічної безпеки України : дис..докт. юрид. наук : 12.00.07. Суми, 2019. 509 с.

184. Рущак І.Я. Проблеми адміністративно-правового становища органів місцевого самоврядування в Україні. Право. 2014. Випуск 26. С.143-147.

185. Савчук Р.М. Поняття та структура адміністративно-правового статусу правоохоронних органів України. Право та державне управління. 2022. №3. С.81-86.

186. Сажнев І.В. До питання щодо визначення поняття “правоохоронна функція держави” Вісник Запорізького юридичного інституту МВС України. 2000. Вип.4. С. 62-71.

187. Салманова О.Ю. Правові акти в управлінській діяльності Національної поліції України: дис. ... д-ра. юрид. наук: Харків: Харківський національний університет внутрішніх справ. 2016. 455 с.

188. Сергєєв А.А. Поняття та особливості механізму забезпечення права на захист честі, гідності та ділової репутації працівників ОВС України. Право і безпека 2013. №2(49). С.182-188.

189. Сидоров М. В.-С. Використання індексів з композитними змінними для визначення соціального статусу громадян України. Актуальні проблеми соціології, психології, педагогіки. 2013. Вип. 18. С. 103-111.

190. Синицький П.В. Контрольно-наглядова діяльність державної служби охорони при МВС України: дис. ... канд. юрид. наук. Харків: Харківський національний університет внутрішніх справ. 2010. 209 с.

191. Сільченко С.О. Механізм правового регулювання соціального страхування: теоретичні аспекти. Юридичні і політичні науки. Держава і право. Випуск 56. С.256.

192. Скакун О. Ф. Теория государства и права : учебник. Харьков : Консум ; Ун-т внутр. дел, 2000. 704 с.

193. Скакун О. Ф. Теорія права і держави: Підручник. 3-те видання. К.: Алерта; ЦУП, 2011. 524 с.

194. Скакун О.Ф. Теорія держави і права: Підручник / Перекл. з рос. Х.: Консум, 2001. 656 с.

195. Скворцов С.С. Адміністративний договір як засіб управлінської діяльності Автореф. дис. … канд.юрид.наук: 12.00.07. Х.: НУВС, 2005. 25 с.

196. Скворцов С.С. Адміністративний догорів як засіб управлінської діяльності: дис. ... канд. юрид. наук. Одеса: Одеський національний університет ім. І.І. Мечникова. 2004. 218 с.

197. Словник української мови : в 11 т. / ред. колег. І. К. Білодід (голова) [та ін.]. К. : Наукова думка, 1970–1980. Т. 5. 832 с.

198. Словник української мови. К., 1973. Т.4. С.92; [246] Словник української мови. К., 1978. Т.9. С.578.

199. Смокович М.І. Проблеми розмежування судової юрисдикції та визначення компетенції адміністративних судів: дис. ... канд. юрид. наук: Київ. Міжрегіональна академія управління персоналом. 2009. 231 с.

200. Сокуренко В.В. Поняття адміністративно-правового статусу органів публічного управління в сфері оборони. EUROPEAN POLITICAL AND LAW DISCOURSE. 2015. Volune 2. Issue 4. С.298-301.

201. Старицька О.О. Поняття та критерії класифікації правового статусу споживача: теоретико-правове дослідження. Юридичний вісник. 2012. №3(24). С.49-52.

202. Стеценко С.Г. Адміністративне право України: навч. посіб. – вид. 2-ге, перероб. та доп. К.: Атіка, 2009. 640 с.

203. Стеченко Д.М. Державне регулювання економіки: Навч. посіб. 3-тє вид., випр. / Стеченко Д.М. К., 2006. 262 с.

204. Тацишин І.Б. Адміністративно-правове забезпечення інформаційних відносин в галузі реклами: дис. ... канд. юрид. наук: Львів: Львівський державний університет внутрішніх справ. 2009. 198 с.

205. Теорія держави і права. Академічний курс: підручник. О. В. Зайчук, Н. М. Оніщенко. К.: Юрінком Інтер, 2008. 688 с.

206. Теорія держави і права: підруч. для студ. юрид. вищ. навч. закл. / О. В. Петришин, С. П. Погребняк, В. С. Смородинський та ін.; за ред. О. В. Петришина. Х.: Право, 2014. 368 с.

207. Теорія управління органами внутрішніх справ: Підручник. За ред. канд. юрид. наук Ю.Ф. Кравченка. К.: Національна академія внутрішніх справ України, 1999. 978 с.

208. Теплицький Б.Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: дис. ... канд. юрид. наук: Київ: Національна академія внутрішніх справ. 2021. 21 с.

209. Тернопільська В.І. Система виховання соціально-комунікативної культури учнів загальноосвітньої школи у позаурочній діяльності: дис. ... д-ра. юрид. наук: Київ: Інститут проблем виховання АПН України. 2009. 573 с.

210. Тихомирова Т.О. Реалізація державної політики охорони здоров'я в системі МВС України: адміністративно-правовий аспект: дис. ... канд. юрид. наук: Київ: Відкритий міжнародний університет розвитку людини «Україна». 2010. 217 с.

211. Тімашов В.О. Правові засади забезпечення кібербезпеки у банківській сфері. Юридичний науковий електронний журнал. № 3/2021. URL: http://lsej.org.ua/3_2021/60.pdf

212. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: угода, міжнародний документ від 27.06.2014. Офіційний вісник України. 2014. №75. Ст.83.

213. Ундір В.О. Принципи взаємодії органів державної влади і громадських структур як основа гармонізації суспільства. Ефективність державного управління. 2020. Вип. 3(64). Ч.1. С.66-78.

214. УСЕ : Універсальний словник-енциклопедія. Гол. ред. ради чл.-кор. НАНУ М. Попович. К. : Ірина, 1999. УІІ+1551 с.

215. Федорова К.І. Адміністративно-правове регулювання приватної нотаріальної діяльності в Україні: дис. ... канд. юрид. наук: Запоріжжя. Запорізький національний університет. 2008. 209 с.

216. Фелик В.І. Адміністративно-правове забезпечення профілактичної діяльності Національної поліції України: дис. ... д-ра. юрид. наук: Харків: Харківський національний університет внутрішніх справ. 2017. 479 с.

217. Форос Г.В. Правове регулювання протидії кіберзлочинам. Правова держава. 2016. №24. С.164-169.

218. Фудорова О.М. Теорія соціального статусу: пізнавальні можливості і дослідницькі стратегії. Вісник Харківського національного університет імені В.Н. Каразіна. 2009. №881. С.110-116.

219. Чернишов Г.М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. Прикарпатський юридичний вісник. 2018. Випуск 3(24). С.158-162.

220. Чернявський А.Д. Організація управляння: Навчальний посібник. К.: МАУП, 1998. 136с.

221. Чумак В. В. Взаємодія та координація між суб'єктами охорони державного кордону. Право і безпека. 2011. № 2 (39). С. 161–165.

222. Шахов С.В. Адміністративно-правова норма: аналіз поняття та характерних ознак. Прикарпатський юридичний вісник. 2017. Випуск 1(16). Том 3. С.212-218.

223. Шиян Т.В. Формування відповідальності старшокласників у процесі факультативних занять гуманітарного профілю в загальноосвітніх навчальних закладах. : Дис... канд. наук: 13.00.07 2000. 230 с.

224. Шнурко Я.В. Принципи взаємодії національної поліції та засобів масової інформації. Нове українське право. Вип. 6. 2021. С.143-147.

225. Щербакова А.К. До питання співвідношення основних понять і категорій протидії злочинності. Науковий вісник Ужгородського національного університету. 2017. С.146-148.

226. Юридична енциклопедія: В 6 т. Редкол.: Ю. С. Шемшученко (голова редкол.) та ін. К.: «Укр. енцикл.», 1998. Т. 1 : А–Г. К. : Вид-во «Юридична думка», 2011. 656 с.

227. Якимчук М.Ю. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. Нове українське право. 2021. Вип.4. С.182-186.

228. Яцишин М.Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю: автореферат. дис. ... канд. юрид. наук: Київ: Київський національний університет імені Тараса Шевченка. 2019. 23 с.

229. Kabysh O.O. Administrative and legal status of the subjects of interaction in the field of combating cybercrime. Entrepreneurship, Economy and Law. 2023. № 9. pp. 101-106.

230. The Latest 2023 Cyber Crime Statistics (updated October 2023) URL: https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Headline%20Cyber%20Crime%20Statistics&text=1%20in%202%20American%20internet,the%20first%20half%20of%202022.

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Кабиш О.О. Стан дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Держава та регіони. Серія Право.* 2021. № 4(74). С. 205–209.

2. Кабиш О.О. Сутність та зміст механізму адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Юридична наука.* 2020. № 8. С. 185–189.

3. Кабиш О. Особливості взаємодії суб'єктів протидії кіберзлочинності. *KELM*. 2022. № 7(51). С. 250–254.

4. Кабиш О.О. Сучасний стан адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Науковий вісник публічного та приватного права.* 2023. Вип. 4. С. 113–118.

5. Kabysh, O.O. Administrative and legal status of the subjects of interaction in the field of combating cybercrime. *Entrepreneurship, Economy and Law.* 2023. № 9. pp. 101–106.

які засвідчують апробацію матеріалів дисертації:

6. Кабиш О.О. До характеристики принципів адміністративно-правового регулювання взаємодії суб'єктів протидії кіберзлочинності. *Виклики сучасності та наукові підходи до їх вирішення:* матеріали міжнародної науково-практичної конференції (Київ, 12–13 серпня 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 42–45.

7. Кабиш О.О. До проблеми визначення поняття протидії кіберзлочинності. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення:* матеріали міжнародної науково-практичної конференції (Київ, 22–23 вересня 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 37–39.

8. Кабиш О.О. Сутність та зміст координації та контролю, як принципів взаємодії суб’єктів протидії кіберзлочинності. *Проблемні питання юридичної науки в контексті реформування правової системи України:* матеріали міжнародної науково-практичної конференції (Київ, 19–20 жовтня 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 21–23.