УНІВЕРСИТЕТ СУЧАСНИХ ЗНАНЬ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

БУХАРЄВ ВЛАДИСЛАВ ВІКТОРОВИЧ

Прим. № ____

УДК 342.95 (477)

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

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

Науковий керівник —
Куліш Анатолій Миколайович,
доктор юридичних наук, професор,
заслужений юрист України

Суми 2018

АНОТАЦІЯ

Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України. — Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук (доктора філософії) за спеціальністю 12.00.07 — адміністративне право і процес; фінансове право; інформаційне право (081 — Право). — Університет сучасних знань; Сумський державний університет. — Суми, 2018.

Зазначається, що одним з основних напрямків розвитку України з моменту проголошення незалежності стали технологічний прогрес та впровадження інформаційних технологій, які сьогодні суттєво полегшують процеси пошуку та оперування інформацією.

Наголошено на відсутності в чинному законодавстві визначень таких понять, як «кібербезпека» та «адміністративно-правова охорона». Запропоновано наступне визначення адміністративно-правової охорони: це системне явище адміністративного права, сутність якого полягає у діяльності публічних органів, спрямованій на забезпечення прав громадян або підтримання відповідного легального режиму в тій чи іншій сфері суспільного буття.

Проаналізовано нормативно-правові та доктринальні джерела на предмет визначення сутнісного змісту та характерних ознак кібербезпеки. Визначено інститут адміністративно-правової охорони кібербезпеки як діяльність окремих державних органів, що здійснюється на засадах імперативності та ієрархічності, направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб’єктів у кіберпросторі. Висвітлено особливості проблеми забезпечення кібербезпеки як об’єкта адміністративно-правової охорони.

Зазначається, що об’єктний склад кібербезпеки становлять суспільні відносини з приводу використання кіберпростору, а також організації

безпечного пошуку, обробки та передачі інформації у цій сфері. У свою чергу, об’єктами механізму кіберзахисту виступають матеріальні та нематеріальні блага, на які спрямовано дію заходів забезпечення кібербезпеки, що входять до складу цього механізму.

До об’єктів кіберзахисту віднесено: об’єкти критичної інформаційної інфраструктури; інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів; інформаційно-телекомунікаційні системи, в яких здійснюється обробка інформації, вимоги щодо захисту якої встановлені законом. Охарактеризовано зміст кожного із зазначених видів об’єктів кіберзахисту.

Проаналізовано чинне законодавство на предмет закріплення у ньому принципів забезпечення кібербезпеки. Виокремлено коло принципів механізму забезпечення кібербезпеки України: 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) пріоритетності запобіжних заходів.

Встановлено, що адміністративно-правове регулювання кібербезпеки являє собою спрямований законодавством вплив норм адміністративного права, в рамках якого використовуються, застосовуються спеціальні засоби та провадяться запобіжні заходи з метою забезпечення відносин суб’єктів у кіберпросторі, а також охорони їх прав та законних інтересів. Визначено співвідношення заходів адміністративного припинення та адміністративних запобіжних заходів.

Наголошено, що надзвичайно важливим аспектом для якісного забезпечення кібернетичної безпеки є правильне визначення основних форм і методів здійснення даного забезпечення. У зв'язку із цим з'ясовна загальнотеоретична сутність понять «форма» та «метод», а також вивчені відповідні наукові та навчальні джерела. Запропоновано під адміністративно-правовими формами забезпечення кібербезпеки України розуміти зовнішній вираз діяльності уповноважених органів державної влади, який виявляється у вчиненні ними комплексу дій, які спрямовані на створення таких умов, за яких буде забезпечено безпеку комп'ютерних систем у всій країні в цілому.

Проаналізовано доктринальні підходи та положення чинного законодавства щодо кола та змісту форм забезпечення кібербезпеки, на підставі чого виокремлено наступні форми зазначеного забезпечення: нормотворчість; прийняття індивідуальних актів у сфері забезпечення кібербезпеки; адміністративний договір; правореалізація. Охарактеризовано сутнісний зміст та значення кожної форми для забезпечення кібербезпеки.

Висвітлено суть та значення для забезпечення кібербезпеки таких методів, як: адміністративний примус; позитивне зобов'язання; дозвіл та заборона; адміністративний контроль; ліцензування діяльності у сфері захисту відомостей, що становлять державну таємницю; сертифікація та стандартизація; реєстрація.

Проаналізовано норми чинного законодавства на предмет урегулювання ним відповідальності за вчинення протиправних дій у кібернетичному просторі. Встановлені види юридичної відповідальності, що можуть бути застосовані за порушення зазначеного законодавства, а саме: цивільна, адміністративна та кримінальна. Розглянуто сутнісний зміст та значення для забезпечення кібербезпеки кожного з указаних видів відповідальності. Висловлено власні думки щодо стану законодавчої регламентації юридичної відповідальності за порушення кібербезпеки.

Виокремлено найбільш характерні особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки.

Проведено дослідження досвіду в зазначеній сфері таких європейських країн, як: Великобританія, Німеччина, Франція, Польща; також проаналізовано досвід США, Японії, КНР. Розглянуто політико-правові та організаційно-управлінські засади діяльності системи кібернетичної безпеки у даних країнах. На підставі проведеного дослідження виокремлено перспективні напрямки розвитку інституту забезпечення кібербезпеки в Україні: збільшення фінансування суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки в державі; кардинальне оновлення Стратегії кібербезпеки України.

За результатами аналізу чинного адміністративного законодавства з питань кібербезпеки виокремлено його недоліки та запропоновано певні кроки щодо його вдосконалення

Взаємодію суб'єктів забезпечення кібербезпеки визначено як їх спільну взаємоузгоджену діяльність, яка спрямована на досягнення єдиної мети – забезпечення належного стану кібернетичної безпеки в Україні. Виокремлено характерні ознаки даної взаємодії. Досліджено положення чинного законодавства на предмет урегулювання ним взаємодії між суб'єктами забезпечення кібербезпеки України. Акцентовано увагу на необхідності більш змістовної законодавчої регламентації: 1) взаємних прав та обов'язків суб'єктів під час здійснення спільної діяльності; 2) напрямків взаємодії; 3) форм та методів взаємодії; 4) повноважень суб'єкта, який буде координувати спільну діяльність суб'єктів забезпечення кібербезпеки в Україні. Наголошується на доцільності розроблення положення «Про порядок взаємодії суб'єктів забезпечення кібербезпеки в Україні».

Ключові слова: кібербезпека, кіберзахист, адміністративно-правова охорона, правовий інститут, адміністративно-правові засади, суб'єкти

забезпечення кібербезпеки, адміністративно-правовий статус, юридична відповідальність, форми, методи, взаємодія.

SUMMARY

Bukhariev V.V. Administrative and Legal Principles of Ensuring Cyber Security of Ukraine. — Qualifying scientific work as the manuscript.

The thesis for a candidate's degree (PhD) by the specialty 12.00.07 — administrative law and procedure; financial law; informational law (081 — Jurisprudence). — The University of Modern Knowledge; Sumy State University. — Sumy, 2018.

It has been noted that one of the main directions of the development of Ukraine since the proclamation of independence is the technological progress and the implementation of information technologies, which nowadays considerably facilitate the processes of information search and operation.

It has been emphasized that the current legislation has no definitions of such concepts as "cyber security" and "administrative and legal protection". The author has offered the following definition of administrative and legal protection: it is a systemic phenomenon of administrative law, the essence of which is the activity of public agencies, aimed at ensuring the rights of citizens or maintaining the corresponding legal regime in any sphere of social life.

Regulatory and doctrinal sources for the purpose of determining the essential content and characteristic features of cyber security have been analyzed. The author has defined the institution of administrative and legal protection of cyber security as an activity of separate state agencies, carried out on the principles of mandatory nature and hierarchy aimed at maintaining and ensuring an adequate state of protecting the rights, interests and information of the relevant subjects in cyberspace. The peculiarities of the problem of providing cyber security as an object of administrative and legal protection have been highlighted.

It has been noted that the object composition of cyber security constitutes the social relations regarding the use of cyberspace, as well as the organization of the safe search, processing and transmission of information in this area. In turn, the objects of the mechanism of cyber protection are material and intangible benefits, which are the orientation for the actions of the measures to ensure cyber security, which are part of this mechanism.

Cyber security objects include: objects of critical information infrastructure; information and telecommunication systems, where the processing of state information resources is carried out; information and telecommunication systems, where processing of information is carried out, the requirements for protection of which are established by the law. The content of each of these types of objects of cyber protection has been characterized.

The author has analyzed the current legislation for the purpose of consolidating the principles of ensuring cyber security. The range of principles of the mechanism of ensuring cyber security of Ukraine has been singled out: 1) the rule of law, legality, respect for human rights and fundamental freedoms and their protection in the manner prescribed by the law; 2) ensuring the national interests of Ukraine; 3) transparency, accessibility, stability and security of cyberspace, development of the Internet and relevant actions in cyberspace; 4) state and private interaction, wide cooperation with civil society in the field of cyber security and cyber protection, in particular through the exchange of information on incidents of cyber security, implementation of joint scientific and research projects, training and professional development of personnel in this area; 5) priority of preventive measures.

It has been established that administrative and legal regulation of cyber security is the influence of the norms of administrative law directed by the legislation, in the framework of which they are used, special means are used and preventive measures are taken in order to secure relations between the subjects in cyberspace, as well as to protect their rights and legitimate interests. The

correlation of administrative cessation measures and administrative preventive measures has been determined.

It has been emphasized that an extremely important aspect for the high-quality provision of cybernetic security is the correct definition of the basic forms and methods of the implementation of this provision. In this regard, the general theoretical essence of the concepts of “form” and “method” has been found out, as well as relevant scientific and educational sources have been studied. The author has suggested to understand administrative and legal forms of ensuring cyber security of Ukraine as the external expression of the activities of authorized state authorities, which is manifested in carrying out a complex of actions aimed at creating such conditions, which ensure the security of computer systems throughout the country in general.

The author has analyzed the doctrinal approaches and provisions of the current legislation concerning the range and content of the forms of ensuring cyber security, on the basis of which the following forms of the mentioned provision have been specified: rule-making; adoption of individual acts in the field of cyber security; administrative agreement; enforcement of the right. Essential content and significance of each form for ensuring cyber security have been characterized.

The author has highlighted the essence and significance of ensuring cyber security of such methods as: administrative coercion; positive commitment; permission and prohibition; administrative control; licensing activities in the field of the protection of information constituting the state secrets; certification and standardization; registration.

The norms of the current legislation have been analyzed for the purpose of resolving their responsibility for the commission of unlawful actions in the cybernetic space. The author has established the types of legal liability that can be applied for violation of the said legislation, namely: civil, administrative and criminal. The author has studied the essential content and significance of ensuring the cyber security of each of the specified types of liability. Own thoughts

regarding the status of legal regulation of legal liability for cyber security violations have been expressed. The most characteristic features of legal liability for the violation of legislation in the field of cyber security have been singled out.

The author has conducted the research of the experience of such European countries in the mentioned sphere as: Great Britain, Germany, France, Poland; has also analyzed the experience of the US, Japan, PRC. The political and legal, organizational and management principles of the cybernetic security system in these countries have been studied. On the basis of the conducted research, the author has specified perspective directions for the development of the institution of ensuring cyber security in Ukraine: increas of financing of the subjects whose activities are aimed at ensuring cyber security in the state; the cardinal renewal of the Cyber Security Strategy of Ukraine.

According to the analysis of the current administrative legislation on cyber security, the author has specified its shortcomings and has suggested certain steps for its improvement.

The interaction of the subjects of ensuring cyber security has been defined as their joint mutually coordinated activity, which is aimed at achieving a single goal – provision of the proper state of cybernetic security in Ukraine. The characteristic features of this interaction have been singled out. The author has researched the provisions of the current legislation in order to regulate interaction between the subjects of ensuring cyber security of Ukraine. The author has emphasized on the need for more substantive legislative regulation of: 1) the mutual rights and obligations of the subjects while carrying out joint activities; 2) areas of interaction; 3) forms and methods of interaction; 4) authorities of the subject, which will coordinate the joint activity of the subjects of ensuring cyber security in Ukraine. The author has emphasized on the expediency of developing the provision “On the Procedure for Interaction of the Subjects of Ensuring Cyber Security in Ukraine”.

Key words: cyber security, cyber protection, administrative and legal protection, legal institution, administrative and legal principles, subjects of ensuring cyber security, administrative and legal status, legal liability, forms, methods, interaction.

Список публікацій здобувача:

Статті у наукових фахових виданнях:

1. Бухарєв В. В. Адміністративно-правові форми забезпечення кібербезпеки в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2015. Вип. 33. Ч. 2. С. 61–66.

2. Бухарєв В. В. Види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2016. Вип. 6-2. Т. 2. С. 188–192.

3. Бухарєв В. В. Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2017. Вип. 43. Т. 3. С. 128–133.

4. Бухарєв В. В. Напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. *Наше право*. 2018. № 2. С. 52–57.

5. Бухарєв В. В. Поняття та особливості кібербезпеки як об’єкту адміністративно-правової охорони. *Європейські перспективи.* 2018. № 3. С.11–16.

Статті у зарубіжних періодичних наукових виданнях:

1. Бухарєв В. В. Напрямки удосконалення взаємодії суб’єктів забезпечення кібербезпеки України. *Верховенство права*. 2018. № 3. С.71–76.

2. Бухарев В. В. Историко-правовой анализ развития законодательства в сфере обеспечения кибербезопасности. *Legea si viata*. 2018. № 11/2. С. 23–26.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Бухарєв В. В. Адміністративно-правові методи забезпечення кібербезпеки в Україні. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи*: Міжнародна науково-практична конференція, м. Київ, 13-14 березня 2015 р. – К.: Центр правових наукових досліджень, 2015. С. 59–62.

2. Бухарєв В. В. Нормотворчість як адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток сучасного права в умовах глобальної нестабільності*: Матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 9-10 вересня 2016 р.) – Одеса: ГО «Причорноморська фундація права», 2016. С. 78–79.

3. Бухарєв В. В. Адміністративний договір як важлива адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток державності та права в Україні: реалії та перспективи*: Матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 вересня 2018 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2018. С. 59–62.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Одним із пріоритетних напрямків розвитку України на її сучасному історичному етапі є розбудова інформаційного суспільства. Заходи із втілення даного кроку передбачають активне впровадження інформаційно-комунікаційних технологій, розвиток кібернетичного простору. Передовий зарубіжний досвід свідчить про те, що переведення частини суспільних відносин у кібернетичний простір має низку переваг, зокрема сприяє підвищенню відкритості та прозорості діяльності суб'єктів публічної влади, оперативності та ефективності їх взаємодії між собою та з представниками громадськості, міжнародною спільнотою. Однак водночас швидкий розвиток інформаційних, інформаційно-телекомунікаційних засобів, технологій, систем і мереж характеризується і значними негативними аспектами, зокрема появою нової сфери для процвітання злочинності. Сприятливість даної сфери для злочинної діяльності обумовлена цілим рядом факторів, наприклад: розвиток комп'ютерних та інформаційно-комунікаційних технологій випереджає розвиток законодавства, яке регулює відносини в даній сфері; необмеженість державними кордонами, що створює сприятливі умови для процвітання транснаціональної злочинності; складність виявлення безпосереднього суб'єкта злочинної діяльності та доведення його вини.

Указані та інші аспекти комп'ютеризації, кібернетизації значної частини суспільного життя змушують кожну сучасну державу особливу увагу приділяти своїй кібернетичній безпеці. Зрозуміло, що Україна в цьому питанні не є виключенням, що обумовлює необхідність суттєвого вдосконалення національного механізму забезпечення кібербезпеки. Одним із основних етапів покращення якості та ефективності організації і функціонування даного механізму є поліпшення його адміністративно-правового забезпечення, яке передбачає покращення відповідного законодавства та перегляд системи

суб'єктів, що опікуються питаннями кібербезпеки. Протягом останніх років у наукових колах все частіше мали місце думки щодо назрілої потреби зміцнення національної кібербезпеки, що є цілком зрозумілим, адже із такими кібернетичними загрозами, які є сьогодні, Україна раніше не зіштовхувалася, як результат – відсутність необхідного досвіду і нездатність ефективно протидіяти даним загрозам. Зазначене вказує на актуальність проведення комплексного вивчення адміністративно-правових засад забезпечення кібернетичної безпеки в Україні з метою виокремлення існуючих проблем у даному механізмі та визначення пріоритетів і перспективних напрямків його подальшого розвитку з урахуванням реалій і викликів сьогодення.

Варто відзначити, що загальним питанням адміністративно-правового забезпечення кібербезпеки присвячено наукові праці Г. О. Андрощук, І. В. Арістової, О. А. Баранова, О. І. Безпалової, Ю. П. Битяка, В. О. Бойко, С. О. Бондаря, С. М. Братуся, В. Л. Бурячка, С. А. Буяджи, Л. Є. Виноградова, О. К. Волох, М. В. Гайворонського, Ю. В. Гаруста, Є. А. Гетьмана, С. О. Гнатюка, Б. В. Деревянка, А. А. Демцова, О. В. Джафарової, Б. В. Дзюндзюк, В. Б. Дзюндзюк, І. В. Діордіци, О. Л. Добржанської, А. В. Долинного, І. В. Європіної, А. В. Кірмач, О. М. Клюєва, Н. В. Коваленка, О. В. Коломоєць, В. К. Колпакова, А. Т. Комзюка, Ю. А. Копитова, О. Є. Користіна, О. Г. Корченка, Т. М. Кравцової, Р. О. Куйбіди, О. В. Кузьменка, А. М. Куліша, В. І. Курила, Є. В. Курінного, О. С. Лагоди, В. А. Ліпкана, М. В. Лошицького, Д. М. Лук'янця, Р. В. Лук'янчука, П. С. Лютікова, В. В. Маркова, О. М. Мельника, О. М. Музичука, В. Я. Настюка, В. І. Олефіра, В. В. Пахомова, Т. О. Проценка, Д. М. Притики, А. В. Руденка, О. Ю. Синявської, М. В. Старинського, В. В. Сухоноса, В. Б. Толубка та ін. Однак, незважаючи на наявність ряду наукових праць, присвячених розвитку кібернетичного простору, забезпеченню кібербезпеки, спеціальні комплексні дослідження, в яких визначаються особливості

адміністративно-правового забезпечення кібербезпеки в Україні, і які ґрунтуються на оновленому законодавстві у цій сфері, є недостатніми.

Таким чином, необхідність удосконалення кібербезпеки в Україні, недосконаліть правового регулювання у зазначеній сфері, з одного боку, та відсутність комплексних досліджень з цієї проблематики – з іншого, обумовлюють своєчасність та актуальність комплексного дослідження адміністративно-правових засад забезпечення кібербезпеки України.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконане відповідно до основних положень Стратегії сталого розвитку «Україна – 2020», схваленої Указом Президента України від 12 січня 2015 р. № 5/2015, Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 р. № 96/2016, Стратегії розвитку наукових досліджень Національної академії правових наук України на 2016 – 2020 роки, затвердженої постановою загальних зборів Національної академії правових наук України від 3 березня 2016 р., Пріоритетних напрямів наукових досліджень Університету сучасних знань на 2017 – 2022 рр. (протокол Вченої ради Університету сучасних знань № 3 від 08.12.2016).

Мета і завдання дослідження. Метою дисертаційного дослідження є визначення сутності та особливостей адміністративно-правових засад забезпечення кібербезпеки в Україні, а також шляхів їх удосконалення.

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

– визначити поняття та з'ясувати особливості кібербезпеки як об'єкта адміністративно-правової охорони;

– здійснити історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки;

– встановити види об'єктів кібербезпеки та кіберзахисту;

– охарактеризувати правові засади забезпечення кібербезпеки України та з’ясувати місце серед них адміністративно-правового забезпечення;

– окреслити систему суб’єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу;

– систематизувати адміністративно-правові форми та методи забезпечення кібербезпеки України;

– виокремити види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України;

– узагальнити зарубіжний досвід забезпечення кібербезпеки та запропонувати можливості його використання в Україні;

– опрацювати напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні;

– встановити способи оптимізації системи суб’єктів забезпечення кібербезпеки України та напрямки вдосконалення взаємодії між ними.

Об’єктом дослідження є суспільні відносини, що виникають під час забезпечення кібербезпеки в Україні.

Предметом дослідження є адміністративно-правові засади забезпечення кібербезпеки України.

Методи дослідження. В дисертаційному дослідженні використано такі методи наукового пізнання: а) логіко-семантичний, за допомогою якого визначено поняття «кібербезпека як об’єкт адміністративно-правової охорони» (підрозділ 1.1), «кібербезпека» та «кіберзахист» (підрозділ 1.3), «адміністративно-правові форми забезпечення кібербезпеки України» та «адміністративно-правові методи забезпечення кібербезпеки України» (підрозділ 2.2), «суб’єкти забезпечення кібербезпеки України» (підрозділ 3.2); б) історико-правовий – під час аналізу становлення та розвитку правового інституту кібербезпеки (підрозділ 1.2); в) системно-структурний, за допомогою якого систематизовано види об’єктів кібербезпеки та кіберзахисту, окреслено коло суб’єктів забезпечення кібербезпеки України, особливості їх

адміністративно-правового статусу та види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України (підрозділи 1.3, 2.1, 2.3); г) порівняльно-правовий, що використовувався з метою з'ясування правових підстав становлення правового інституту кібербезпеки, виявлення особливостей адміністративно-правового забезпечення кібербезпеки України, опрацювання напрямків удосконалення адміністративно-правових засад забезпечення кібербезпеки в Україні (підрозділи 1.2, 1.4, 3.1 – 3.3); г) структурного аналізу, який застосовано під час окреслення особливостей адміністративно-правового статусу суб'єктів забезпечення кібербезпеки та шляхів оптимізації їх системи (підрозділи 2.1, 3.3). В роботі використано низку інших методів наукового пізнання.

Науково-теоретичне підґрунтя дисертації становлять праці вчених різної галузевої належності, які вивчали проблеми теорії та практики забезпечення кібербезпеки в Україні та світі. Нормативною основою дослідження є Конституція України, норми міжнародних нормативно-правових актів, закони та підзаконні нормативно-правові акти, які визначають адміністративно-правові засади забезпечення кібербезпеки в Україні. Інформаційну та емпіричну основу роботи становлять узагальнення практики забезпечення кібербезпеки, довідкові видання, статистичні матеріали.

Наукова новизна отриманих результатів визначається тим, що представлене дисертаційне дослідження є однією з перших спроб комплексно, з урахуванням аналізу наукових праць учених та чинного законодавства України визначити сутність та особливості адміністративно-правових засад забезпечення кібербезпеки України та запропонувати напрямки вдосконалення відповідного законодавства. У результаті проведеного дослідження сформульовано низку нових наукових положень та висновків, запропонованих особисто здобувачем. Основні з них такі:

вперше:

– визначено, що адміністративно-правова охорона у сфері забезпечення кібербезпеки – це діяльність відповідних державних органів, що здійснюється на засадах імперативності та ієрархічності і направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб'єктів у кіберпросторі;

– обґрунтовується, що розмежування адміністративно-правового забезпечення кібербезпеки та адміністративно-правового забезпечення кіберзахисту є принципово важливим питанням, адже воно прямо пов'язане з процесом їх реалізації, що при неправильному підході може завдати шкоди охоронюваним законом інтересам та правам людей, які здійснюють різні операції з інформацією в кіберпросторі;

– доведено позицію автора, згідно з якою суб'єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, оскільки, по-перше, відносини між ними будуються на основі влади і підпорядкування, а по-друге, останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством. Крім цього, аналіз адміністративно-правового статусу суб'єктів забезпечення кібербезпеки просто неможливо здійснювати поза межами адміністративної галузі права;

удосконалено:

– розуміння того, що історія становлення та розвитку кібербезпеки як юридичного інституту прямо пов'язана з еволюцією інформаційних технологій та Інтернету, який дав людству можливість обробляти та обмінюватися колосальною кількістю даних на відстані;

– обґрунтування того, що правові засади забезпечення кібербезпеки – це весь масив керівних ідей, засад та положень, закріплених у нормативно-правових актах різної юридичної сили, які визначають механізм правового регулювання забезпечення кібербезпеки;

– характеристику основних адміністративно-правових форм забезпечення кібербезпеки України, під якими запропоновано розуміти зовнішній вираз діяльності уповноважених органів державної влади, який виявляється у вчиненні ними комплексу дій, які спрямовані на створення таких умов, за яких буде забезпечено безпеку комп'ютерних систем у всій країні в цілому;

– розуміння оптимізації системи суб'єктів забезпечення кібербезпеки, яка являє собою процес, що передбачає: по-перше, створення оптимальної кількості таких суб'єктів, яких буде достатньо для виконання завдань у сфері забезпечення кібербезпеки; по-друге, належну організацію діяльності відповідних суб'єктів шляхом збільшення або зменшення кількості їх повноважень;

– характеристику ознак взаємодії суб'єктів забезпечення кібербезпеки, до яких віднесено: 1) єдину мету спільної діяльності; 2) наявність декількох або більше суб'єктів; 3) обов'язковість законодавчого підґрунтя діяльності; 4) чітко визначений адміністративно-правовий статус кожного суб'єкта; 5) узгодженість заходів щодо мети, місця, часу, методів діяльності;

– розуміння форм взаємодії суб'єктів забезпечення кібербезпеки в Україні, до яких запропоновано віднести: 1) проведення спільних міжвідомчих нарад; 2) обмін оперативною інформацією щодо стану забезпечення кібербезпеки, а також щодо заходів, які були вже реалізовані кожним суб'єктом взаємодії; 3) розроблення спільних програм щодо протидії кіберправопорушенням та окреслення основних напрямків спільної діяльності; 4) спільну участь у проведенні окремих слідчих та розшукових дій; 5) утворення спільних консультативно-дорадчих та експертних органів, рад, комісій;

– визначення поняття «методи взаємодії суб'єктів забезпечення кібербезпеки», під яким запропоновано розуміти сукупність способів та

прийомів, які спрямовуються на налагодження ефективної взаємодії між суб'єктами, що уповноважені забезпечувати кібербезпеку в Україні;

дістали подальшого розвитку:

– обґрунтування того, що кібербезпека є складним правовим явищем, у рамках якого діє механізм кіберзахисту, що являє собою систему заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру;

– розуміння того, що з прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» вперше з'явилось нормативне визначення поняття «кібербезпека», що, у свою чергу, дозволило виробити стратегію захисту кібербезпеки в адміністративно-правовому порядку та закріпити засади, суб'єктний склад механізму забезпечення вказаної категорії, що, безперечно, є позитивною новацією у сфері забезпечення кіберпростору та процесу використання інноваційних технологій;

– обґрунтування того, що питання юридичної відповідальності за порушення законодавства у сфері кібербезпеки України є недостатньо врегульованим, що, безперечно, можна вважати суттєвою прогалиною, яка сприяє зростанню рівня кіберзлочинності в нашій державі. Зокрема, питання притягнення правопорушника у сфері кібербезпеки до цивільної та адміністративної відповідальності регулюється цілою низкою нормативно-правових актів, у кожному з яких містяться різні підстави притягнення особи до відповідальності. Така розгалуженість, у свою чергу, ускладнює застосування стягнень до винних осіб органами державної влади;

– характеристика методів взаємодії суб'єктів забезпечення кібербезпеки, до яких віднесено: 1) кадровий метод, який передбачає активне навчання представників одних органів специфіці роботи інших, що, у свою чергу, сприяє налагодженню ефективної взаємодії між відомствами; 2) метод взаємного інформаційного забезпечення, який полягає в наданні суб'єктами співпраці один одному всієї необхідної інформації для більш відкритої та

ефективної взаємодії; 3) метод контролю, завдяки якому сторони (суб'єкти) взаємодії мають змогу здійснювати взаємне контролювання один одного під час спільної діяльності; 4) методи планування та прогнозування; 5) економічний метод, який передбачає створення відповідної матеріальної бази для проведення спільних заходів.

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

– науково-дослідній сфері – для подальшого розроблення теоретико-методологічних та правових питань забезпечення кібербезпеки України (*акт впровадження Кримінологічної асоціації України від 05.01.2018 р.*);

– правотворчості – як основа для вдосконалення адміністративного законодавства, що регламентує забезпечення кібербезпеки України (*акт впровадження Науково-дослідного інституту публічного права від 17.01.2018 р.*);

– правозастосовній діяльності – з метою удосконалення окремих напрямків, форм та методів забезпечення кібербезпеки України (*акт впровадження результатів дисертаційного дослідження у практичну діяльність Навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору Харківського національного університету внутрішніх справ від 26.01.2018 р.*);

– навчальному процесі – під час підготовки підручників та навчальних посібників із дисциплін «Адміністративне право», «Адміністративний процес», «Публічне адміністрування» та інших дисциплін адміністративно-правового характеру, в ході підготовки відповідних їх розділів (*акт впровадження Сумського державного університету від 10.09.2018 р.*).

Апробація матеріалів дисертації. Підсумки розроблення проблеми в цілому, окремих її аспектів, одержані узагальнення і висновки було оприлюднено на міжнародних, всеукраїнських та регіональних науково-

практичних конференціях, семінарах, круглих столах, зокрема: «Сучасні правові системи світу в умовах глобалізації: реалії та перспективи» (Київ, 2015); «Розвиток сучасного права в умовах глобальної нестабільності» (Одеса, 2016); «Розвиток державності та права в Україні: реалії та перспективи) (Львів, 2018).

Публікації. Основні результати дисертаційного дослідження викладено в семи статтях, опублікованих у наукових фахових виданнях України та наукових періодичних виданнях інших держав, та трьох тезах наукових повідомлень на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що містять 10 підрозділів, висновків, списку використаних джерел, додатків. Повний обсяг дисертації становить 221 сторінку. Список використаних джерел включає 225 найменувань та розміщений на 23-х сторінках, додатки розташовано на дев’яти сторінках.

РОЗДІЛ 1
МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

1.1 Поняття та особливості кібербезпеки як об'єкта адміністративно-правової охорони

Починаючи з моменту надбання Україною незалежності, вектор державного розвитку було спрямовано на технологічний прогрес та імплементацію у людське життя інформаційних технологій, які на сьогоднішній день суттєво полегшують процеси пошуку та обміну інформацією. Велике значення процес «електронного» розвитку відіграє на державному рівні, адже запровадження новітніх технологій відкриває величезні можливості у сфері державобудування. Наразі практично усі органи влади, що існують в Україні, так чи інакше використовують новітні технології, що фактично спричинило перенесення процесу обміну, обробки та пошуку інформації у електронний простір. Нарівні з цим, «цифрова революція» також має низку негативних аспектів, одним з яких є низький рівень кібербезпеки. Ця проблематика неодноразово підіймалася у роботах науковців різних галузей знань. Не є виключенням правова сфера, так як саме у її рамках було розроблено головні механізми охорони кібербезпеки. Вивчення даного питання є пріоритетним напрямком роботи для правників адміністративного, кримінального, цивільного та інформаційного права, адже кібербезпека у вигляді об'єкта правової охорони безпосередньо входить в поле інтересів держави. При цьому, механізми її забезпечення не є однорідними між собою, так як регулюються нормами різних галузей права.

Найбільш доцільним та дієвим «буфером» правової охорони зазначеного об'єкта є адміністративно-правовий, адже він походить від однойменної юридичної галузі, в рамках якої існує державний примус в його

найбільш початковій формі. Іншими словами, дослідження кібербезпеки як об’єкта адміністративно-правової охорони дозволяє визначити рівень правової регламентації її захищеності.

Слід наголосити, що представлена у підрозділі проблематика є комплексною, тобто складається з декількох питань, які потребують детального аналізу таких понять як «кібербезпека» та «адміністративно-правова охорона». Адже відсутність законодавчої дефініції окремих понять перешкоджає аналізу правових інститутів, які вони окреслюють, і, як наслідок, визначенню особливостей їх практичного застосування. Таким чином, визначення поняття та особливостей кібербезпеки як об’єкта адміністративно-правової охорони має не тільки суто теоретичне значення, але і є практичним.

Тож безпосередній розгляд кібербезпеки як об’єкта адміністративно-правової охорони слід починати із визначення поняття та ключових аспектів адміністративно-правової охорони як одного з найбільш значних та функціональних механізмів забезпечення кібербезпеки. Як і будь-яке інше правове явище в державі, основні засади забезпечення кібербезпеки знаходять своє закріплення в нормах Конституції України, тому що цей нормативний акт є основним джерелом національної правової системи. Так, у статті 3 Конституції вказується, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов’язком держави. Тобто наявність адміністративно-правового механізму охорони кібербезпеки та інших подібних об’єктів є проявом виконання державою своїх обов’язків з приводу забезпечення життєдіяльності населення країни [94].

Повертаючись безпосередньо до аналізу адміністративно-правової охорони, необхідно відмітити, що сутність цього терміну розглядається переважно у сукупності з тим благом, на яке спрямовано дію механізму. Іншими словами, в науковій літературі можна зустріти такі терміни як «адміністративно-правова охорона майнових та немайнових прав власності», «адміністративно-правова охорона прав інтелектуальної власності», «адміністративно-правова охорона надр та вод», тощо. Однак, це не свідчить про те, що термін «адміністративно-правова охорона» не розглядається самостійно у сучасному науковому середовищі. Більш того, він характеризується лінгвістичними особливостями.

Термін «адміністративно-правова охорона» складається з двох самостійних понять: «адміністративно-правовий» та «охорона», які мають окремі дефініції. Так, у загальному вигляді під категорією «охороняти» розуміють: оберігати від небезпеки кого-, що-небудь, забезпечувати від загрози нападу, замаху і т. ін.; стояти на варті біля кого-, чого-небудь; вартувати, стерегти; оберігати від руйнування, знищення, завдання шкоди і т. ін.; захищати від чого-небудь [126; 68, с. 183]. Слід наголосити, що досить часто термін «охорона» ототожнюють з терміном «захист», підтвердження чого можна знайти у словнику С. І. Ожегова, відповідно до якого єдність у розумінні «захисту» і «охорони» витікає з пояснення змісту слова «захищати», що, відповідно до С. І. Ожегова, означає охорону, спрямовану на захист від замахів, від ворожих дій та небезпеки [128; 85, с. 119]. Даний аспект нерідко викликає суперечності між вченими з приводу того, чи є інститут адміністративно-правового захисту тотожним інституту адміністративно-правової охорони. Спираючись на дослідження лінгвістів, ми можемо стверджувати, що вказані явища є абсолютно ідентичними, адже відмінність полягає лише у кінцевих термінах, суть яких є однаковою. Різниця є лише у способі впливу, адже захист вимагає активної форми

поведінки, а охорона — пасивної, при цьому мета у обох випадках є тотожною.

Що ж стосується поняття «адміністративно-правовий», то відповідно до Великого тлумачного словника сучасної української мови термін «адмініструвати» означає керувати установою, організацією, підприємством; керувати бюрократично, за допомогою наказів і розпоряджень замість конкретного керівництва [27, с. 12]. Зазначений термін, по-перше, показує приналежність певного інституту чи механізму до галузі адміністративного права, а, по-друге, дає розуміння того, що відповідні дії здійснюються у адміністративному порядку. Таким чином, в найбільш загальному вигляді адміністративно-правова охорона — це захист певних правовідносин у адміністративному порядку. Однак, як ми розуміємо, сутність цього юридичного явища є дещо глибшою, тому розкрити її повністю виключно на лінгвістичному рівні неможливо. Для цього необхідно також скористатися напрацюваннями вчених–адміністраторів.

Наразі існує велика кількість наукових поглядів на проблематику визначення поняття «адміністративно-правова охорона», що пов’язано із тим, що має місце фактична відсутність його дефініції у законодавчих актах. В. В. Галунько у своїх наукових працях визначає, що адміністративно-правова охорона — це система впорядкованої адміністративно-правовими нормами діяльності публічної адміністрації, що спрямована на попередження правопорушень (профілактику злочинів) та відновлення порушених прав, свобод та законних інтересів фізичних і юридичних осіб, що здійснюються засобами адміністративного права з можливістю застосування заходів адміністративного примусу та притягнення винних до адміністративної відповідальності [3, с. 242–247]. Дещо інший погляд на проблематику має С. О. Мосьондз, на думку якого адміністративно-правова охорона вирізняється гуманністю, спрямованістю на переконання населення в доцільності й справедливості заходів, здійснюваних державою, об’єктивній

необхідності тих або інших загальнообов’язкових правил. Вона пов’язана із масштабним використанням перевірених практикою засобів організаційної, масово-політичної та виховної роботи, активним формуванням в суспільній свідомості нетерпимого ставлення до антисоціальних проявів [122, с. 106]. Доволі цікавою є думка О. І. Харитонова, який зосереджує увагу на тому, що явище адміністративно-правової охорони являє собою окремий правовий інститут. Він доводить свій погляд тим, що порушення встановлених законодавством правил поведінки тягне за собою припинення дії регулятивних правовідносин, замість яких виникають охоронні (регулятивні трансформуються в охоронні), підставою до чого є припис норми права та вчинення адміністративного делікту. В цьому випадку йдеться вже не про реалізацію встановлених адміністративно-правових регулятивних норм, якими були визначені вимоги до поведінки зобов’язального суб’єкта, а про реалізацію положень охоронних адміністративно-правових норм, які передбачають встановлення нових прав і обов’язків [203, с. 38]. Отже, підсумовуючи наукові погляди, ми можемо зробити висновок про те, що адміністративно-правова охорона — це системне явище адміністративного права, сутність якого полягає у діяльності публічних органів, спрямованій на забезпечення прав громадян або підтримання відповідного легального режиму в тій чи іншій сфері суспільного буття. Водночас, адміністративно-правова охорона, на нашу думку, трансформується у правовий інститут, коли її застосовують щодо конкретних об’єктів. Це пояснюється тим, що за подібних умов адміністративно-правова охорона перестає бути абстрактним явищем та набуває конкретного механізму реалізації, який визначається окремою групою правових норм. Тобто ми говоримо про строго внормовану, засновану на правових принципах діяльність держави в особі окремих органів влади, яку спрямовану на підтримку об’єктів права: інтелектуальної та промислової власності, надр та вод, окремих правомочностей та законних інтересів громадян, тощо. Наприклад, адміністративно-правовою охороною

права власності визнається імперативно-владна діяльність суб'єктів публічного управління із захисту прав усіх суб'єктів права власності (осіб, які здійснюють управління нею) від протиправних посягань і широкого загалу осіб від майна підвищеної небезпеки, з нормативно прописаною можливістю застосування до порушників режиму власності засобів державного впливу [116, с. 239]. Доволі лаконічно та максимально точно особливості адміністративно-правової охорони конкретного об'єкта (інтелектуальної власності) виділено Є. В. Юрковою, яка зазначила, що інститут охорони інтелектуальної власності відноситься до спеціальної юрисдикційної форми діяльності окремих суб'єктів публічного управління, зокрема: Міністерства внутрішніх справ України, Антимонопольного комітету України, тощо [214, с. 710].

Таким чином, ми визначились із тим, що адміністративно-правова охорона певного об'єкта є правовим інститутом. Незважаючи на відсутність єдиного наукового погляду на цю проблематику, вона має доволі широке нормативне підґрунтя, тобто відповідні правові джерела. Найбільше коло норм, спрямованих на охорону певних суспільних відносин, закріплено у Кодексі України про адміністративні правопорушення (далі — КУпАП). Стаття 1 вказаного нормативно-правового акта [84] закріплює, що завданнями кодексу є охорона прав і свобод громадян, власності, конституційного ладу України, прав і законних інтересів підприємств, установ і організацій, встановленого правопорядку, зміцнення законності, запобігання правопорушенням, виховання громадян у дусі точного і неухильного додержання Конституції і законів України, поваги до прав, честі і гідності інших громадян, до правил співжиття, сумлінного виконання своїх обов'язків, відповідальності перед суспільством [84]. Інші положення КУпАП спрямовані на те, щоб забезпечити охорону відповідних об'єктів, що є пріоритетом діяльності державних органів влади, тобто адміністративно-правова охорона є інститутом, який ґрунтується на принципах влади,

превалюванні імперативного методу регулювання, ієрархічності, тощо. Наприклад, у статті 6 КУпАП вказується, що органи виконавчої влади та органи місцевого самоврядування, громадські організації, трудові колективи розробляють і здійснюють заходи, спрямовані на запобігання адміністративним правопорушенням, виявлення й усунення причин та умов, які сприяють їх вчиненню, на виховання громадян у дусі високої свідомості і дисципліни, суворого додержання законів України [84]. Органи місцевого самоврядування, місцеві державні адміністрації, забезпечуючи відповідно до Конституції України додержання законів, охорону державного і громадського порядку, прав громадян, координують на своїй території роботу всіх державних і громадських органів по запобіганню адміністративним правопорушенням, керують діяльністю адміністративних комісій та інших підзвітних їм органів, покликаних вести боротьбу з адміністративними правопорушеннями [84].

Існують також інші законодавчі акти, норми яких є джерелом інституту адміністративно-правової охорони тих чи інших об’єктів, зокрема: Митний Кодекс України, Земельний Кодекс України, Водний Кодекс України, Закони України «Про охорону прав на знаки для товарів і послуг», «Про охорону прав на знаки для товарів і послуг», «Про захист від недобросовісної конкуренції», «Про нафту і газ», тощо.

Підсумовуючи усі наведені вище відомості, ми можемо стверджувати, що адміністративно-правова охорона сама по собі є доволі цікавим явищем. Однак, метою підрозділу є розгляд інституту адміністративного забезпечення конкретного об’єкта — кібербезпеки. Останнє явище також підлягає самостійному аналізу, так як воно характеризується великою кількістю особливостей.

На сьогодні термін «кібербезпека» активно обговорюється у науковій літературі. Це дає нам змогу звернутися до напрацювань вчених, які розглядали цей об’єкт та його особливості. Кібербезпека є абстрактним

поняттям, що виникло у сфері експлуатації комп'ютерної техніки з метою обміну інформацією у віртуальному просторі. Окрім цього, віртуальний простір не має меж і кордонів, в ньому будь-хто набуває широких можливостей у сфері його використання. Саме цей аспект робить віртуальний або ж кіберпростір, як його частіше називають, надзвичайно зручним середовищем для здійснення протиправної діяльності. Сюди можна віднести правопорушення і злочини в різних сферах господарювання та управління, хакерські атаки на урядові сайти та банківські бази даних, інші дії, спрямовані на порушення суспільно-політичного ладу [83, с. 96]. За даних умов кіберпростір слід розглядати як високорозвинену модель об'єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

– подаються в математичному, символічному або в будь-якому іншому вигляді;

– розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації;

– перебувають у постійному русі по сукупності ІТ-систем і мереж [76, с. 8].

Необхідно відмітити, що визначення поняття та особливостей кіберпростору є принципово важливим аспектом нашого дослідження, адже на цьому ґрунтується бачення кібербезпеки. В даному разі логічно було б зазначити, що кібербезпека — це певний стан кіберпростору, який характеризується фактичною відсутністю правопорушень, однак, представлений термін має дещо більший зміст. В. Н. Фурашев визначає кібербезпеку як стан, здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу — несвідомого, негативного впливу (управління) інформації [12; 202, с. 168]. На думку І. В. Діордіца, кібербезпека — це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що

досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [60, с. 110]. Схожої думки дотримується О. А. Баранов, який зазначає, що кібербезпека — це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [12; 59, с. 38]. На нашу думку, останні погляди не зовсім точно відображають сутність досліджуваного явища, адже не зовсім зрозуміло, про які саме важливі інтереси людини і громадянина та системи йдеться мова.

Більш повним є визначення поняття «кібербезпека», яке запропоноване у підручнику В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та С. В. Толюпа. На їх думку, кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечуються їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [26, с. 15]. Підтримка та забезпечення подібного стану здійснюються завдяки сукупності спеціальних захисних дій, реалізаторами яких є окремі органи влади.

Найбільш змістовним ми вважаємо визначення поняття «кібербезпека» О. Г. Корченко, адже він розкриває сутність кібербезпеки через призму ключових ознак цього явища. На його погляд, кібербезпекою є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугрупувань розгортаються навколо інформаційного ресурсу, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем [95, с. 7] та які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об’єктів критично важливої інформаційної і кіберінфраструктури [95, с. 41]. Іншою особливістю даного

визначення є те, що воно подано з урахування технічної сторони явища кібербезпеки, в рамках якого здійснюється використання електронної техніки.

Вказані наукові погляди знайшли свій прояв у Законі України «Про основні засади забезпечення кібербезпеки України». У статті 1 закону зазначається, що 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 [151]. Ми вважаємо, що наведене поняття хоча і є лаконічним, однак, не відображає усю сутність явища кібербезпеки. Хоча, безперечно, нормативне визначення поняття є позитивним фактором для правової системи нашої держави.

Отже, на підставі аналізу понять «адміністративно-правова охорона» та «кібербезпека» вбачається, що «адміністративно-правова охорона у сфері забезпечення кібербезпеки» — це діяльність відповідних державних органів, що здійснюється на засадах імперативності та ієрархічності і направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб’єктів у кіберпросторі. Головною особливістю адміністративно-правового забезпечення кібербезпеки є те, що воно здійснюється в адміністративному порядку, тобто в контексті адміністративно-правових відносин. При цьому, сутність даного інституту є доволі широкою і не обмежується суто захисними нормами та процедурами. Зокрема, доволі часто адміністративно-правова охорона будь-якого об’єкта сприймається як суто «каральний» інститут, що складається з положень Кодексу України про адміністративні правопорушення. Однак, норми цього закону закріплюють адміністративні стягнення для суб’єктів, які порушують легальний стан певного об’єкта, в нашому випадку — кібербезпеки.

Внаслідок здійснення ними правопорушень щодо останніх використовуються норми юридичної відповідальності, метою яких є обмеження прав і свобод. Застосування подібних юридичних механізмів є крайнім заходом, який може мати місце лише за умови вчинення правопорушень, об’єктом яких є правовідносини у сфері кібербезпеки. Інститут адміністративно-правової охорони кібербезпеки в даному разі має набагато ширшу сферу дії, адже забезпечення тих чи інших правовідносин в адміністративному порядку проявляється не тільки у покаранні винних осіб, які їх порушили, а й у діяльності органів влади з метою недопущення виникнення подібних ситуацій та інших негативних факторів.

Нормативне підґрунтя забезпечення кібербезпеки закріплено у Законі України «Про основні засади забезпечення кібербезпеки в Україні», а також в інших положеннях законодавства. Напрямки забезпечення кібербезпеки, що реалізуються у роботі різних органів державної влади, також мають певний нормативно-правовий вираз. Так, у ст. 10 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» розкривається роль державних органів у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. В законі зазначено, що спеціальний центральний орган виконавчої влади з питань організації спеціального зв’язку та захисту інформації має наступні повноваження:

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

– здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі [143].

Необхідно також відмітити діяльність Національного банку України (далі — НБУ) у сфері забезпечення кібербезпеки. Робота даного органу також входить до сфери національної безпеки нашої держави, адже НБУ є центральним банком України, особливим центральним органом державного управління, юридичний статус, завдання, функції, повноваження і принципи організації якого визначаються Конституцією та іншими законами України [147]. Діяльність Нацбанку на сьогоднішній день безпосередньо пов’язана із використанням інноваційних технологій та обробкою інформації у кіберпросторі. Відповідно до цього, на НБУ покладено функцію визначення напряму розвитку сучасних електронних банківських технологій, він створює та забезпечує безперервне, надійне та ефективне функціонування, розвиток створених ним платіжних та облікових систем, контролює створення платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації [147]. Важливість кібербезпеки у діяльності НБУ за даних умов обумовлюються тим, що усі вказані типи електронних систем несуть в собі великий об’єм даних, які за негативних обставин можуть бути використані не за їх цільовим призначенням. До того ж, головним завдання Нацбанку, відповідно до статті 8 Закону України «Про Національний банк України», є розроблення Основних засад грошово-кредитної політики та здійснення контролю за проведенням грошово-кредитної політики [147]. В даному разі робота з інформацією у кіберпросторі представляє собою невід’ємний елемент процесу реалізації

подібного завдання. Цей факт дозволяє нам стверджувати, що забезпечення кібербезпеки у своїй діяльності є одним з головних обов'язків Національного банку України сьогодні.

Отже, кібербезпека як об'єкт адміністративно-правової охорони являє собою певний віртуальний інститут, охорона якого відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності.

На даний час в Україні сформовано специфічну нормативно-правову основу забезпечення кібербезпеки, однак, серед вчених немає єдності у розумінні досліджуваного інституту.

Кібербезпека характеризується великою кількістю особливостей як негативного, так і позитивного забарвлення. Головним негативним моментом кібербезпеки як об'єкта адміністративно-правової охорони є недосконалий понятійний апарат. Відсутність чіткого визначення змісту кібербезпеки фактично призводить, по-перше, до його неоднакового розуміння, а по-друге — застосування, що в окремих випадках дозволяє правопорушнику уникнути відповідальності. Наступною особливістю досліджуваного інституту є те, що адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте, закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державної влади. Іншими словами, забезпеченням кібербезпеки займаються різні відомства в процесі виконання своїх функцій та покладених на них обов'язків. Також особливістю кібербезпеки як об'єкта адміністративно-правової охорони є те, що її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення відповідних порушень, а й їх попередження. І останньою особливістю кібербезпеки як об'єкта адміністративно-правової охорони є те, що основні засади її забезпечення

лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті. З прийняттям цього законодавчого акта в Україні вперше з'явилось нормативне визначення поняття «кібербезпека», що, в свою чергу, дозволить виробити грамотну та надійну стратегію захисту кібербезпеки в адміністративно-правовому порядку. Крім цього, у законі детально визначаються засади та суб'єктний склад механізму забезпечення вказаної категорії, що, безперечно, можна назвати юридичним проривом у сфері забезпечення кіберпростору та процесу використання інноваційних технологій.

1.2 Історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки

В попередньому підрозділі дослідження нами було проаналізовано поняття кібербезпеки та особливості цього явища як одного з об'єктів адміністративно-правової протидії. Відповідна наукова розвідка дозволила побачити його унікальність та особливості тієї сфери, в якій даний інститут існує на сьогоднішній день. На сучасному етапі він є розвиненим правовим явищем, має нормативну основу. Однак, становленню кібербезпеки передувала ціла низка подій, що обумовили розвиток її юридичного виразу у правовій системі держави. Тому з метою більш повного розуміння інституту кібербезпеки та його правової природи необхідно проаналізувати не тільки поточний нормативний стан кібербезпеки на основі положень чинного законодавства, але й провести історико-правове дослідження його появи та становлення.

Поняттям «кібербезпека» описується належний стан роботи у сфері обробки інформації шляхом використання обчислювальної техніки, іншими словами, комп'ютерів. Однак, електронні пристрої самі по собі не становлять

загрози легальному статусу зазначеного вище явища. Усе змінюється в тих випадках, коли мова йде не про самостійні комп'ютерні одиниці, а про цілу систему подібних пристроїв, за допомогою яких здійснюється обмін інформацією через світову мережу. За таких умов ми можемо говорити про існування нового інформаційного простору (кіберпростору), де реально мають місце ситуації фактичного порушення прав і свобод людей. В цьому контексті кібербезпека виступає у вигляді правового механізму забезпечення захисту прав та інтересів людей у кіберпросторі. Таким чином, історія його становлення та розвитку, як юридичного інституту, прямо пов'язана з еволюцією інформаційних технологій та Інтернету, який приніс людству можливість обробляти та обмінюватися колосальною кількістю даних. Звідси виходить, що останні аспекти також підлягають науковому висвітленню у процесі дослідження ґенези кібербезпеки.

Перші обчислювальні машини почали з'являтися вже у середині XX століття, але на той час вони являли собою великі «калькулятори», спектр функцій яких був досить вузьким. Сучасний вид та призначення комп'ютери отримали лише у кінці XX на початку XXI століття, коли їх почали випускати для персонального користування у сфері бізнесу, навчання і навіть розваг. Паралельно з комп'ютерами розвивалась «всесвітня павутина», або ж Інтернет, як його прийнято називати на сьогоднішній день. Важливий крок в історії створення Інтернету було здійснено в 1965 році такими американськими вченими як Т. Меррилл та Л. Дж. Робертс. Вони вперше здійснили підключення віддалених на значну відстань один від одного комп'ютерів, коли одна машина знаходилась у штаті Массачусетс, а інша — в Каліфорнії. Експеримент було проведено з використанням низькошвидкісної телефонної лінії. В результаті цього було створено першу, хоча й невелику, широкомасштабну комп'ютерну мережу. Проведений експеримент приніс розуміння того, що загальні комп'ютери можуть працювати разом, виконувати програми і за необхідності вилучати дані на

видаленому комп'ютері, проте, система комутованих телефонних ліній для цього абсолютно не підходила [175].

З цього моменту починається стрімкий науковий розвиток питання комп'ютерних мереж, який привів до винаходу на початку 90-х років спеціального програмного забезпечення — «WorldWideWeb» («WWW» — всесвітня павутина). У квітні 1993 року було здійснено випуск вихідного коду WorldWideWeb в суспільне надбання, що означало, що кожен може його використовувати і створювати на його основі програмне забезпечення без ліцензійних відрахувань. В цьому ж році Національний центр прикладних систем для суперкомп'ютерів (National Center for Supercomputing Applications) випустив програму Mosaic, яка стала одним з перших браузерів. Спочатку вона була доступна тільки для машин під управлінням операційної системи Unix і у формі вихідного коду, але вже в грудні 1993 Mosaic поставлявся з установниками (інсталяторами) для операційних систем Apple Macintosh і Microsoft Windows. Mosaic дуже швидко ставав популярним, а разом з ним і всесвітня павутина [175].

На сьогоднішній день Інтернет є невід'ємною частиною життєдіяльності людини, адже він використовується у багатьох сферах, зокрема: оборонній, банківській, правоохоронній, тощо. Але подібний розвиток всесвітньої павутини також призвів до появи негативних наслідків, одним з яких є кіберправопорушення. Безмежність інформаційного простору дає можливість окремим суб'єктам здійснювати всілякі маніпулювання даними з метою, наприклад, викрадення певної інформації, порушення роботи суб'єктів влади і т. ін. Саме цей аспект обумовив розвиток правового інституту кібербезпеки як механізму підтримки порядку у кіберпросторі, тобто під час використання можливостей всесвітньої павутини. Розвиток останнього відбувався паралельно еволюції інформаційних технологій. При цьому, на рівні національного законодавства інститут кібербезпеки є новелою, що обумовлено відсутністю належного нормативного закріплення.

З іншого боку, історичні етапи його становлення можна дослідити на основі норм багатьох міжнародних актів, деякі з яких ратифіковано в Україні.

Найпершим в історії законодавчим актом, котрий регулював забезпечення кібербезпеки у кіберпросторі, був «The Computer Fraud and Abuse Act» (Закон про боротьбу з комп'ютерними шахрайством та комп'ютерними зловживанням), прийнятий в 1986 році у Сполучених Штатах Америки [223; 36, с. 146]. Даний акт, по суті, визнавав проблему можливості вчинення неправомірних дій у інформаційній сфері, що дало поштовх до розвитку інституту кібербезпеки. Закон закріпив відповідальність за несанкціоноване втручання у роботу комп'ютерних систем чи викрадення інформації з них. Крім цього, актом передбачено санкції до осіб, які вчиняють дії подібного характеру.

Значним внеском у розвиток інституту кібербезпеки стало прийняття Радою Європи у 1989 році Рекомендації R(89)9, якою було закріплено:

– по-перше, чіткий перелік дій, які набувають ознак кіберправопорушень;

– по-друге, головні аспекти розробки та побудови єдиної стратегії протидії негативним діям у кіберпросторі [219].

Положення вказаного акта фактично запустили механізм еволюції інституту безпеки у сфері використання комп'ютерних технологій з метою обміну даними. Розвиток цього явища в наступні роки до сьогоднішнього дня проходив на рівні як міжнародного права, так і національного, яке приймалося під впливом світового законодавства.

Так, в 2000 році у Відні було прийнято Віденську декларацію про злочинність та правосуддя: відповіді на виклики XXI століття (ООН). Звичайно, цей документ не визначав та не закріплював норми стосовно інституту кібербезпеки у тому вигляді, в якому він існує сьогодні. Однак, на основі положень декларації було прийнято рішення розробити орієнтовані на конкретні дії програмні рекомендації щодо попередження злочинів,

пов’язаних з використанням комп’ютерів, і боротьби з ними. Тобто вже у той час порушення у сфері використання інноваційних технологій характеризувалися суспільною небезпекою, що дозволило говорити про формування кіберзлочинності. Декларація також поклала обов’язок на усіх держав–членів Організації Об’єднаних Націй (далі — ООН) працювати в напрямку зміцнення їх можливостей щодо попередження, розслідування і переслідування злочинів, пов’язаних з використанням високих технологій і комп’ютерів [42]. У тому ж році Європейським Союзом (далі — ЄС) приймається Конвенція про взаємодопомогу в кримінальних справах між членами ЄС, в рамках якої було закріплено процесуальні особливості та нові механізми взаємодії між державами з приводу протидії кіберправопорушенням [91]. Підсумовуючи викладені вище факти, ми можемо стверджувати, що видання двох останніх міжнародних актів фактично змусило світову спільноту поглянути на явище кібербезпеки як на самостійний юридичний осередок, а не елемент системи того чи іншого механізму протидії правопорушенням у сфері використання комп’ютерних технологій.

В подальшому кібербезпека характеризувалась як окремий правовий інститут, в рамках якого здійснюється розробка стратегії подолання антисуспільних дій у кіберпросторі. Ця теза підтверджується положеннями Резолюції Генеральної Асамблеї ООН щодо створення глобальної культури кібербезпеки, прийнятої в 2002 році. В даному акті окреслюються ключові шляхи створення глобальної культури кібербезпеки, а також пояснюються особливі моменти механізму забезпечення цього інституту, наприклад:

– необхідність визнання та охорони правового явища кібербезпеки обумовлено стрімким підвищенням числа залучених до кіберпростору країн;

– ефективна кібербезпека досягається не лише прямою діяльністю державних або правоохоронних органів, направленою на припинення

відповідних протиправних діянь, але й превентивними заходами, крім цього, даний процес повинен підтримуватися суспільством;

– державні органи, в свою чергу, повинні: постійно підвищувати рівень безпеки у сфері використання інформаційних технологій та аналізувати фактори, які на нього негативно впливають [177; 44, с. 105].

Ключовою перевагою резолюції є те, що цей документ закріпив конкретні вимоги до суб'єктів кібербезпеки, які останні повинні неухильно виконувати, адже від цього залежить реальний стан правової забезпеченості інституту. Відповідно до положень акта, існує дев'ять головних вимог:

a) обізнаність, тобто суб'єкти повинні бути інформовані про необхідності безпеки інформаційних систем і мереж і про те, що вони можуть зробити для підвищення безпеки;

b) відповідальність, за безпеку інформаційних систем та мереж згідно з роллю кожного з них;

c) реагування, тобто обов'язковість вживання своєчасних і спільних заходів щодо попередження інцидентів, які зачіпають безпеку, їх виявлення і реагування на них. Суб'єкти повинні обмінюватися в належних випадках інформацією про загрози та фактори уразливості і вводити процедури, що передбачають оперативну і ефективну співпрацю в справі попередження таких інцидентів, тощо;

d) етика, що значить необхідність врахування законних інтересів інших, оскільки інформаційні системи і мережі проникли в усі куточки сучасного суспільства;

e) демократія, яка проявляється у діяльності із забезпечення цінностей, які визнаються демократичним суспільством, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації та комунікації, належний захист інформації особистого характеру, відкритість і гласність;

f) оцінка ризику, яка: дозволяє виявляти загрози та фактори уразливості; має досить широку базу, щоб охопити такі ключові внутрішні та зовнішні аспекти як технологія, фізичні і людські фактори, застосування методик і послуги третіх осіб, що позначається на безпеці; дає можливість визначити допустимий ступінь ризику; допомагає вибрати належні інструменти контролю, що дозволяють регулювати ризик потенційного збитку інформаційним системам і мережам з урахуванням характеру та значущості інформації, що захищається;

g) проектування і впровадження засобів забезпечення безпеки;

h) управління забезпеченням безпеки, тобто здійснення комплексного підходу до управління забезпеченням безпеки, спираючись на динамічну оцінку ризику, що охоплює всі рівні діяльності учасників і всі аспекти їх операцій;

i) переоцінка — учасники повинні піддавати питання безпеки інформаційних систем і мереж огляду і повторній оцінці та вносити належні зміни в політику, практику, заходи і процедури забезпечення безпеки, враховуючи при цьому появу нових, зміну колишніх загроз і чинників уразливості [122].

Представлені вимоги увійшли до положень Женевської декларації принципів побудови інформаційного суспільства, прийнятої на Всесвітньому саміті з питань інформаційного суспільства 12 грудня 2003 року. У статті 35 частини 5 глави в декларації зазначена необхідність формування, розвитку і впровадження глобальної культури кібербезпеки у співпраці з усіма зацікавленими сторонами і компетентними міжнародними організаціями. Такі дії повинні спиратися на розширювану міжнародну співпрацю. В рамках цієї глобальної культури кібербезпеки важливо підвищувати безпеку і забезпечувати захист даних і недоторканність приватного життя, розширюючи при цьому доступ і масштаб торгових операцій. Крім того, необхідно брати до уваги рівень соціально-економічного розвитку кожної

країни і враховувати пов’язані з орієнтацією на розвиток аспекти інформаційного суспільства [55].

Слід відмітити, паралельно розвитку у світовому законодавстві ґенеза правового інституту кібербезпеки також мала місце на національному рівні. Звичайно, на початковому етапі становлення України як незалежної держави самого поняття «кібербезпека» у нормативних документах країни фактично не існувало. Однак, певні основи інституту забезпечення інформаційної безпеки у різних сферах життєдіяльності населення країни вже було імплементовано у національне законодавство з урахування міжнародно-правових стандартів у цій галузі.

Розвиток правових засад організації кібербезпеки в Україні знайшов відображення в наступних нормативних актах, а саме Законах України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року, «Про Національну програму інформатизації» від 2 жовтня 1992 року, «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року, «Про науково-технічну інформацію» від 25 червня 1993 року, «Про охорону прав на топографії інтегральних мікросистем» від 5 листопада 1997 року, тощо.

Відповідні нормативні зрушення у напрямку розвитку системи забезпечення інституту кібербезпеки також простежуються на підзаконному рівні. Зокрема, протягом 2000, 2001 рр. Президентом України було видано Укази «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» та «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні». Положення даних актів визначили вектор розвитку діяльності країни у сфері організації інформаційної безпеки, а також на нормативному рівні закріпили особливості використання інноваційної на той час мережі Internet та механізм її державної підтримки, яка мала прояв у:

– створенні у найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу громадян, органів державної влади та органів місцевого самоврядування, суб'єктів підприємницької діяльності до мережі Інтернет;

– розвитку та впровадженні сучасних комп'ютерних інформаційних технологій у системі державного управління, фінансовій сфері, підприємницькій діяльності, освіті, наданні медичної та правової допомоги та інших сферах;

– вирішенні завдань щодо гарантування інформаційної безпеки держави та недопущенні поширення інформації, розповсюдження якої заборонено відповідно до законодавства, тощо [144; 145].

Найбільшим «проривом» вітчизняного законодавства у сфері забезпечення кібербезпеки стала ратифікація в 2005 році Конвенції про кіберзлочинність, прийнятої Радою Європи. Відповідно до Преамбули, метою створення документу стала необхідність 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, 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 [92]. У конвенції також представлено список протиправних дій, поділених на групи, які, на думку міжнародної спільноти, становлять небезпеку процесу обробки та обміну інформацією у комп'ютерних системах, наприклад:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, зловживання пристроями);

2) правопорушення, пов’язані з комп’ютерами (підробка, пов’язана з комп’ютерами, шахрайство);

3) правопорушення, пов’язані зі змістом (розповсюдження дитячої порнографії);

4) правопорушення, пов’язані з порушенням авторських та суміжних прав [92].

Інші положення конвенції регулюють процедурні особливості міжнародної взаємодії в процесі боротьби із кібернетичними правопорушеннями, а також містять вихідні принципи такої діяльності. Ратифікація цього документу обумовила його включення у структуру джерел правової системи України.

Останні роки характеризуються новим витком еволюції інституту кібербезпеки, який було суттєво модифіковано нормами чинного законодавства. Перейнявши досвід зарубіжних країн у сфері регулювання досліджуваного явища, наша держава створила юридичні основи його регулювання. Так, у 2016 році було видано Указ Президента, який ввів у дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Інноваційність даного акта полягає у тому, що саме в його положеннях вперше було використано термін «кібербезпека».

Згідно із загальними положеннями стратегії, стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Водночас, переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного)

походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [157].

Отже, Стратегією [157] чітко визначається наявна проблема порушення прав і свобод громадян України у кіберпросторі, у зв'язку з чим виникає необхідність, по-перше, запровадження належного механізму правового регулювання цієї сфери, а по-друге, забезпечення охорони суспільного інтересу від протиправних посягань всередині неї. Цікавим є той факт, що даний аспекти було легалізовано на нормативному рівні, адже визначеною метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [157]. Нормативно-правовий акт також закріплює принципи, на яких ґрунтується діяльність із досягнення та забезпечення поставленої мети. В даному разі слід наголосити, що в історії розвитку кібербезпеки на національному рівні засади його ніколи не визначались. Тому Стратегія [157] певним чином посилила легальний статус інституту, надавши йому вихідні принципи, до яких віднесено такі:

– верховенство права і повага до прав та свобод людини і громадянина [157];

– забезпечення національних інтересів України [157];

– відкритість, доступність, стабільність та захищеність кіберпростору [157];

– державно-приватне партнерство, широка співпраця з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту [157];

– пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам [157];

– пріоритетність запобіжних заходів [157];

– невідворотність покарання за вчинення кіберзлочинів;

– пріоритетність розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу [157];

– міжнародне співробітництво 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 протиправних та воєнних цілях [157];

– забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [157].

Ще одним вагомими надбанням Стратегії [157] є те, що в її положеннях кібербезпека хоча і визнається правовим інститутом, однак, напрямки її забезпечення включають в себе не тільки суто юридичні елементи, а й також політичні, економічні, організаційно-технічні, тощо. Наприклад, відповідно до частини 4 Стратегії розвиток безпечного, стабільного і надійного кіберпростору має полягати насамперед у:

– виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

– створенні вітчизняної нормативно-правової та термінологічної бази, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

– формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту;

– розвитку технологій кіберзахисту засобів рухомого зв’язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв’язку;

– залученні експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

– проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;

– розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;

– розвитку мережі команд реагування на комп’ютерні надзвичайні події;

– створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

– розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;

– розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці

України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі;

– створенні умов для впровадження в Україні сучасних технологій кіберзахисту [157].

Незважаючи на доцільність та пріоритетність прийнятої Стратегії [157], інформативність цього підзаконного нормативного акта доволі низька. Зокрема, у його положеннях досить часто терміни «кіберзахист» та «кібербезпека» ототожнюються, що не дає змогу зрозуміти аспекти унікальності даного інституту. Крім цього, вагомий недолік полягає у відсутності в положеннях Стратегії дефініцій таких понять як «кіберпростір», «кіберзлочин», «кіберзагроза», тощо. Іншими словами, нормативний акт створює механізм забезпечення інституту, сутність якого реально залишається незрозумілою.

З іншого боку, Стратегія [157] показує вінець розвитку інституту кібербезпеки, еволюція якого здійснювалась протягом великого відрізку часу. В свою чергу, недоліки вказаного нормативного акта фактично були усунені новим Законом України «Про основні засади забезпечення кібербезпеки в Україні». Його головною метою є визначення правових та організаційних засад державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України [151]. Окрім стратегічно важливої мети, даний нормативний документ характеризується рядом інших особливостей:

– по-перше, закон фактично легалізує усі поняття з префіксом «кібер», які до цього часу існували переважно у наукових роботах вчених чи положеннях міжнародних нормативно-правових актів;

– по-друге, закон на законодавчому рівні закріплює принципи, основні напрямки забезпечення та об’єкти кібербезпеки України;

– по-третє, нормативний документ уточнює поняття суб’єктів механізму забезпечення кібербезпеки, а також більш детально представляє їх повноваження у цій сфері.

Отже, провівши історико-правовий аналіз розвитку і становлення правового інституту кібербезпеки, нами було розглянуто велику кількість нормативних актів як міжнародного, так і національного права. Це дозволило виділити головну особливість ґенези досліджуваного явища — його стійкий взаємозв’язок із еволюцією комп’ютерних технологій. Питання забезпечення кібербезпеки набуло вагомості через підвищення рівня обміну інформацією між різними суб’єктами за допомогою інноваційних технологій та мережі Інтернет. Стрімкий технологічний прогрес призвів до появи осіб, які умисно використовували кіберпростір задля забезпечення власних інтересів, тим самим порушуючи інтереси звичайних користувачів, якими на сьогоднішній день є усі громадяни.

Основний розвиток кібербезпеки здійснювався у нормативній площині Європи, адже підґрунтя інституту було закладено актами ЄС. На рівні національного законодавства інститут почав розвиватися на початку XXI століття. Як ми побачили, його становленню передувало прийняття цілої низки законодавчих актів, які прямо не встановлювали правовий статус кібербезпеки, не кажучи про механізм її забезпечення. Найвизначнішим кроком до імплементації у правову систему України досліджуваного інституту стала ратифікація Конвенції Ради Європи про кіберзлочинність у 2005 році. Цей документ визначив ключові типи правопорушень, що можуть вчинятися у кіберпросторі, а також процедурні особливості міжнародної співпраці у боротьбі з ними.

В останні часи інститут кібербезпеки набув стрімкого розвитку, що пов’язано, на нашу думку, зі зміною зовнішньополітичного вектору держави. Упровадження європейських стандартів різних галузей суспільного життя в країні потребує підвищення рівня інформаційної захищеності. Тому у

2016 році Указом Президента було введено в дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», яке визначило суб'єктів, загрози і напрямки забезпечення кібербезпеки в державі, та прийнято Закон України «Про основні засади забезпечення кібербезпеки України». Крім цього, на сьогоднішній день розвиток досліджуваного інституту все ще триває, тому нам слід очікувати прийняття низки нових законодавчих актів у цій сфері.

1.3 Види об'єктів кібербезпеки та кіберзахисту

Попередньо проведене дослідження поняття кібербезпеки як об'єкта адміністративно-правової охорони, її історії, розвитку та становлення дало розуміння сутності та многогранності цього правового інституту. Відсутність його законодавчого виразу у національній системі права компенсується міжнародними нормами, котрими визначаються головні положення, напрямки дії, суб'єктний склад та завдання кібербезпеки з урахуванням реалій сьогодення. Крім того, в останні роки активізувалась діяльність, направлена на розроблення та імплементацію регулюючих даний інститут норм в державну законодавчу систему. Цей факт привів до суттєвого розширення сфери дії кібербезпеки, що проявляється у появі цілої низки пов'язаних із представленим інститутом явищ та окремого об'єктного складу.

Аналізуючи усі аспекти кібербезпеки, в рамках даного дисертаційного дослідження питання об'єктного складу зазначеного інституту не могло залишитися поза нашою увагою. Наукова розробка даної проблематики з урахуванням сучасної нормативної бази у сфері регулювання кібербезпеки дозволить більш повно побачити сферу її безпосередньої дії. Однак, слід зауважити, що довгий період становлення інституту та неодноманітність

регулюючого законодавства породили багато суміжних йому явищ, які також заслуговують окремої уваги та визначення їх «поля» діяльності. А отже, необхідним є аналіз співвідношення кібербезпеки та кіберзахисту, адже досить часто представлені явища сприймаються як цілком ідентичні, що, в свою чергу, є грубою помилкою. Забігаючи наперед, ми маємо наголосити, що кібербезпека має дещо ширшу дефініцію та сутність, аніж кіберзахист. З іншого боку, останнє явище характеризується наявністю окремого об'єктного складу. Таким чином, наступній розробці, з метою розкриття усіх особливостей інституту кібербезпеки, підлягають питання, пов'язані з:

– по-перше, аналізом сутності явища кіберзахисту, а також його відмінністю та співвідношенням з правовим інститутом кібербезпеки;

– по-друге, окресленням об'єктного складу обох правових категорій.

На сьогодні термін «кіберзахист» не має належного відображення як у науковому середовищі, так і на рівні законодавства. Більшість науковців ототожнюють його із поняттям «кібербезпека», що, на нашу думку, є вкрай невірним судженням. У положеннях чинного законодавства термін застосовується досить часто, але в той же час його дефініцію в жодному офіційному документі не представлено. Наприклад, у тексті Указу Президента, яким вводиться в дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», неодноразово зустрічається поняття «кіберзахист». Зокрема, у загальних положеннях Стратегії говориться, що для досягнення мети цього документу, тобто створення умов безпечного функціонування кіберпростору та його використання, необхідним є забезпечення кіберзахисту державних електронних інформаційних ресурсів та інформації в них [157]. Крім цього, вказаний термін можна також зустріти у положеннях іншого нормативного акта аналогічного типу, а саме: в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». У положеннях документу

вказується, що головна роль у забезпеченні воєнної безпеки України належить Збройним Силам України, водночас, відповідно до своєї компетенції, інші суб'єкти сектору безпеки також виконують важливі функції. Так, Державна служба спеціального зв'язку та захисту інформації України здійснює забезпечення функціонування урядового зв'язку Верховного Головнокомандувача Збройних Сил України з посадовими особами інших військових формувань та правоохоронних органів, а також забезпечення кіберзахисту об'єктів критичної інфраструктури (суспільно важливих підприємств, установ та організацій) [150]. Незважаючи на присутність зазначеного терміну у положеннях цих двох нормативних актів, сутність та інші особливості явища, яке ним описується, не розкриваються взагалі. У зв'язку із відсутністю нормативно-визначеної дефініції поняття кіберзахисту, було б доцільно почати його аналіз, спираючись на лінгвістичне його тлумачення.

Вказаний термін складається з двох складових — «кібернетичний» та «захист». Остання складова, відповідно до Словника української мови за редакцією І. К. Білодіда тлумачиться як оборона чи охорона кого-небудь чи чого-небудь від нападу, замаху, удару чи іншої небезпеки; пильно стежити за недоторканністю чого-небудь і багато робити для цього [19, с. 380]. Схожий за вимовою та формою термін «захищати», за положеннями Словника української мови Б. Грінченко, визначається як заступництво [53, с. 113]. Інша складова поняття походить від назви однієї із сучасних наукових галузей — кібернетики. Остання являє собою науку про закономірності обробки, отримання, зберігання, обміну інформацією в складних системах управління, незважаючи на походження останніх (технічне, біологічне, соціальне, тощо) [48, с. 440].

Враховуючи лінгвістичні особливості складових елементів поняття «кіберзахист», термін можна розтлумачити як захисні дії, направлені на забезпечення безпеки у сфері отримання, обробки, зберігання та передачі

інформації за допомогою складних систем управління. Головною проблемою даного трактування є те, що воно не виділяє особливості явища кіберзахисту та, крім цього, створює плутанину, яка не дає розмежувати його із правовим інститутом кібербезпеки. Однак, в роботах вчених терміни доволі часто вживаються як синоніми, хоча деякі науковці мають дещо іншу точку зору. Як вже було зазначено раніше, даними поняттями описуються різні правові явища та механізми. Зокрема, в попередніх розділах ми визначили, що кібербезпека — це правовий інститут, тобто ціла система юридичних норм, якими регулюється безпечний стан обробки інформації у кіберпросторі. Тут йдеться про цілу сферу діяльності, в рамках якої об'єднуються різні механізми, що функціонують з єдиною метою. Враховуючи цей факт, можна припустити, що кіберзахист є складовим елементом кібербезпеки, тому його розгляд необхідно проводити через призму особливостей останнього інституту. Підтвердження цієї тези ми знайшли у роботах О. В. Коломійця, який стверджує, що поняття кіберзахисту доречно трактувати як сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки [88, с. 8]. Хоча дане визначення певним чином пояснює природу досліджуваного явища, воно повністю не розкриває його внутрішній зміст. Більш широку дифініцію пропонує В. П. Шеломенцев, який під кіберзахистом розуміє систему заходів правового, організаційного, ресурсно-фінансового, програмно-технічного та іншого характеру, спрямовану на створення умов, за яких виключаються або суттєво утрудняються протиправні посягання на об'єкти такого захисту (певні інформаційні об'єкти кіберпростору). Іншими словами, це діяльність у кіберпросторі з охорони певних його об'єктів від протиправних посягань (наприклад, кіберзлочинів) і створення перешкод у реалізації загроз кримінального характеру [210, с. 347].

Останнє визначення ми вважаємо найбільш доречним та правильним доктринальним поглядом, адже воно практично повністю відповідає дефініції

поняття кіберзахисту, яку законодавець представив у Законі України «Про основні засади забезпечення кібербезпеки України». У статті 1 нормативного акта вказано, що кіберзахистом є сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямованих на забезпечення кібербезпеки [151]. Даним поняттям законодавець закріпив на нормативному рівні шляхи регулювання поточного стану кібербезпеки в Україні. При цьому, легальне визначення терміну побудовано досить грамотно, адже воно допускає існування заходів забезпечення «іншого характеру», що суттєво розширює дію правового інституту, задля підтримки якого вони створені.

Розглянемо для прикладу забезпечувальний механізм, який стосується усіх без винятку правових явищ та інститутів сучасної правової системи України. Таким на сьогоднішній день є система політичних заходів забезпечення, що, по суті, являють собою політику держави у певній сфері, в нашому випадку — у галузі кібербезпеки. За сучасних умов політична підтримка інституту має бути спрямована на:

– забезпечення інформаційного суверенітету України у кіберпросторі;

– створення надійного захисту національного сегменту кіберпростору з урахуванням складної військово-політичної ситуації на півночі та сході країни;

– зміцнення обороноздатності держави у кіберпросторі;

– боротьбу з кіберзлочинністю та кібертероризмом;

– недопущення та запобігання втручанню у внутрішні справи України і припинення посягань на її Інтернет-ресурси з боку інших держав, тощо [109, с. 115].

Слід відмітити особливості інших заходів, котрі входять до системи кіберзахисту, адже з їх допомогою також можна дослідити його специфіку. Наприклад, оперативні заходи в більшості випадків є прерогативою правоохоронних органів. Їх головна особливість — це швидкоплинність

застосування та висока ефективність. Як правило, такі заходи використовуються для попередження кіберправопорушень у конкретних ситуаціях, тобто вони мають превентивний характер. В цьому контексті слід відзначити точку зору більшості іноземних вчених, які вважають, що попередження кіберправопорушень (зокрема, злочинів) є простішим та легшим, аніж наступний розгляд питання за фактом їх вчинення [41].

Отже, підсумовуючи вищенаведене, ми можемо стверджувати: під поняттям кіберзахисту слід розуміти систему (механізм) засобів різного характеру, за допомогою яких здійснюється підтримка та забезпечення інституту кібербезпеки. Кіберзахист здійснюється за допомогою використання досить широкого кола правових інструментів, порядок використання яких врегульовано нормами багатьох законодавчих та підзаконних нормативно-правових актів. Розмежування кібербезпеки та кіберзахисту є принципово важливим питанням, адже воно прямо пов’язане із процесом їх реалізації, який при неправильному підході може нанести шкоду охоронюваним законом інтересам та правам людей, які здійснюють різні операції з інформацією в кіберпросторі.

Проведення границі між сутністю інституту кібербезпеки та механізму кіберзахисту також має велике значення для висвітлення їх об’єктного складу, який, між іншим, є вкрай різним. Неоднакова природа та цільове призначення двох представлених явищ доводять те, що вони мають різні об’єкти правового впливу. Варто зазначити, що цей аспект знайшов відображення у національному законодавстві України. Однак, перш ніж зосередити увагу на різниці об’єктного складу інституту кібербезпеки та механізму кіберзахисту, слід спершу відповісти на питання, що собою представляє об’єкт цих двох явищ у загальному розумінні.

Правовий об’єкт в загальному вигляді можна розглядати як об’єкт тієї чи іншої правової галузі чи об’єкт правовідносин певного типу. Об’єкт галузі являє собою сукупність суспільних відносин, в сфері яких між окремими

суб’єктами виникають відповідні права і обов’язки. В рамках нашого дослідження таке визначення можна використати для виділення об’єктного складу кібербезпеки, котра є правовим інститутом, предмет впливу якого є досить широким.

Дещо інший теоретичний вираз мають об’єкти кіберзахисту. Їх слід представити як складовий елемент правовідносин, що виникають в процесі реалізації вищенаведених заходів з метою забезпечення кібербезпеки. З цього приводу доцільно було б представити наукові погляди теоретиків права, які безпосередньо досліджували особливості об’єктів правовідносин в їх загальному вигляді. На сьогодні можна виділити декілька основних точок зору з цього питання. Наприклад, Н. М. Крестовська та Л. Г. Матвєєва стверджують, що об’єкти правовідносин — це соціальні цінності та блага, з приводу володіння якими суб’єкти вступають у правовідносини, здійснюють свої права та обов’язки [96, с. 432]. Інший погляд на цю проблематику мають О. О. Тихомиров, Ю. А. Іванов та М. М. Мікуліна, на думку яких об’єктами правовідносин виступають певні інтереси суб’єктів правовідносин, закріплені (передбачені) правовими нормами, на задоволення яких спрямована поведінка цих суб’єктів (реалізація суб’єктивних прав і виконання обов’язків) [185, с. 191]. Найбільш лаконічним та влучним є науковий погляд О. Ф. Скакун, яка наголошує на тому, що об’єктами правовідносин виступають матеріальні і нематеріальні блага, з приводу яких суб’єкти вступають у правовідносини, здійснюють свої суб’єктивні права і юридичні обов’язки [170, с. 533]. Беручи до уваги останнє визначення, ми можемо класифікувати подібні блага, з приводу яких люди вступають у взаємовідносини юридичного характеру, на дві групи:

1) матеріальні об’єкти;
2) нематеріальні об’єкти.

До першої групи відносяться усі без винятку речі, рухоме та нерухоме майно, грошові цінності, а також майнові права. До нематеріальних включено дещо ширше коло об’єктів, а саме:

– нематеріальні об’єкти правовідносин, пов’язані з матеріальними об’єктами (інформація — матеріальний носій інформації; результати інтелектуальної творчої діяльності — книга, промисловий зразок);

– нематеріальні об’єкти правовідносин, не пов’язані з матеріальними об’єктами (здоров’я, життя, честь, гідність);

– поведінка суб’єктів правовідносин (голосування за законопроект депутатів у Верховній Раді України; робота акторів під час вистави);

– результати поведінки суб’єктів (будівництво будинку, ремонт побутової техніки);

– охоронюваний законом інтерес суб’єкта (визнання права власності в судовому порядку, позов про усунення перешкод у здійсненні власником права користування та розпорядження майном), тощо [170, с. 192].

Зважаючи на представлені наукові погляди, вбачається, що об’єктний склад кібербезпеки становлять суспільні відносини з приводу використання кіберпростору, а також організації безпечного пошуку, обробки та передачі інформації у цій сфері. В свою чергу, об’єктами механізму кіберзахисту виступають матеріальні та нематеріальні блага, на які спрямовано дію заходів забезпечення кібербезпеки, що входять до складу цього механізму.

Для більш точного розуміння об’єктний склад кібербезпеки необхідно розглядати через призму напрямків забезпечення цього правового інституту в Україні. Зокрема, у згаданому раніше нами Законі «Про основні засади забезпечення кібербезпеки України», а саме статті 4, зазначається, що основними напрямами забезпечення кібербезпеки України є:

– розвиток інформаційної інфраструктури держави, забезпечення безпечного функціонування об’єктів критичної інформаційної інфраструктури;

– 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;

– забезпечення ефективного застосування Збройних Сил України для адекватної відповіді реальним та потенційним кіберзагрозам національному сегменту кіберпростору;

– розвиток пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій;

– підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників;

– адаптація законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення її стійкості до кібератак, спроможності держави більш ефективно захищати національні інтереси у кіберпросторі;

– 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 [151].

З урахуванням наведених напрямів забезпечення кібербезпеки можна зробити висновок, що до об’єктного складу кібербезпеки входять:

– правовідносини у сфері розвитку належної інформаційної інфраструктури у державі;

– правовідносини у сфері налагодження міжнародних зав’язків з метою обміну досвідом у сфері розбудови кібербезпеки;

– правовідносини з приводу регулювання, координації і контролю діяльності правоохоронних органів та інших суб’єктів забезпечення кібербезпеки в процесі виконання покладених на них обов’язків;

– правовідносини у сфері впровадження інформаційних технологій в основних галузях життєдіяльності суспільства та налагодження процесу їх безпечного використання;

– правовідносини у сфері розвитку науки та техніки з метою розбудови предметної основи інституту кібербезпеки, тобто розробки новітніх технологій, які б сприяли підвищенню безпеки при роботі у кіберпросторі;

– правовідносини у сфері імплементації у законодавство України правових механізмів забезпечення кібербезпеки з урахуванням міжнародного досвіду у цій галузі;

– правовідносини у сфері підвищення інформаційної обізнаності суспільства при роботі з інформацією у кіберпросторі, тощо.

Звичайно, представлене коло об’єктів не є сталим, адже суспільні відносини у галузі кібербезпеки стрімко розвиваються на сьогоднішній день. Вектор еволюції цього правового інституту направляється процесом євроінтеграції, тож його особливості та, зокрема, об’єктний склад будуть приведені у повну відповідність європейським стандартам.

Об’єкти кібербезпеки у порівнянні із кіберзахистом є більш широкими та самостійними. Кіберзахист, як ми визначили раніше, розповсюджує свою дію не на окремі групи правовідносин, а на певні матеріальні та нематеріальні блага. Таким чином, ми можемо стверджувати, що об’єкти кіберзахисту характеризуються високим рівнем конкретики. Ця особливість знайшла своє відображення на нормативному рівні. У статті 2 Рішення Ради Національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» зазначено, що на Кабінет Міністрів України, Службу Безпеки України та

Національну поліцію України покладається забезпечення регулювання та охорони окремих об’єктів кіберзахисту, до яких віднесено:

– об’єкти критичної інформаційної інфраструктури;

– інформаційно-телекомунікаційні системи фінансового сектору держави, тощо [140].

Головним здобутком зазначеного вище нормативно-правового акта є те, що представлені об’єкти кіберзахисту лише згадуються у його положеннях, крім того, їх повний перелік фактично не представлено. Відповідь на питання про те, що входить до об’єктного складу механізму кіберзахисту, міститься у статі 5 Закону України «Про основні засади забезпечення кібербезпеки України». Відповідно до положень зазначеної статті, об’єктами кіберзахисту є об’єкти критичної інформаційної інфраструктури та інші інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом. При цьому, об’єкти критичної інформаційної інфраструктури потребують першочергового (пріоритетного) захисту від кібератак [151]. Тож стаття Закону України дає чіткий перелік об’єктів кіберзахисту, до яких віднесено:

– по-перше, об’єкти критичної інформаційної інфраструктури;

– інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів;

– інформаційно-телекомунікаційні системи, в яких здійснюється обробка інформації, вимоги щодо захисту якої встановлені законом.

Першою ланкою, тобто об’єктами критичної інфраструктури, виступають підприємства та установи (незалежно від форми власності) таких галузей як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та

населення [142]. Їх дефініція подається у постанові Кабінету Міністрів України № 563 від 23 серпня 2016 року «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави». Забезпечення охорони даних об'єктів є першочерговим завданням. Головною загрозою порушення цілісності останніх визнаються, як законом, так і іншими нормативними актами, кібератаки — несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи [151].

Другу групу об'єктів кіберзахисту становлять інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів. Останні, по суті, є головними цілями державної охорони від кібератак. За загальним визначенням, запропонованим О. Д. Довгань, інформаційні ресурси — це документи і масиви документів в інформаційних системах: бібліотеках, архівах, фондах, банках даних, депозитаріях, музейних сховищах і т. ін. Існують інформаційні ресурси спільного користування — сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання [64]. В свою чергу, визначення саме державних інформаційних ресурсів є дещо іншим. Так, у Законі України «Про державну службу спеціального зв'язку та захисту інформації України» вказано, що державні інформаційні ресурси — це систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України,

державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень [138]. До державних інформаційних ресурсів висуваються вимоги щодо актуальності та достовірності наведених у них даних; вичерпної повноти інформаційних джерел; компактності викладу; оперативності пошуку. На сьогодні в науковому колі існує певний підхід до класифікації цього об'єкта, який умовно розподіляється на дві групи:

1) інформаційні ресурси, призначені для вирішення завдань конкретного органу управління певної ланки;

2) інформаційні ресурси, орієнтовані на зовнішнього користувача [64; 137].

Найбільш яскравим прикладом даного об'єкта є інформаційні системи та ресурси, які будуть використовуватися в процесі імплементації у систему управління нашою державою електронного урядування. Останнє являє собою форму організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [158]. Кіберзахист даної форми публічної взаємодії влади, громадян та різних сфер життєдіяльності останніх є пріоритетним завданням, адже від цього прямо залежить якість надання публічних послуг фізичним і юридичним особам, мобільність такого процесу та його безпека для законних інтересів та прав населення України.

До об'єктів третьої ланки відносяться інформаційно-телекомунікаційні системи, в яких здійснюється обробка охоронюваної законодавством інформації, тобто таких відомостей, які не призначено для загального користування. З положень чинного законодавства можна виділити декілька видів подібної інформації. Однією з найбільш важливих є державна

таємниця, тобто таємна інформація, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані державною таємницею і підлягають охороні державою [139]. В даному разі штучне порушення роботи інформаційно-телекомунікаційних систем, в яких містяться подібні відомості, може нанести вагому шкоду не тільки приватним, а й державним інтересам у відповідних галузях діяльності України.

Окрім державної таємниці, у кіберпросторі також обробляється інша охоронювана законом інформація, зокрема:

1) інформація, що знаходиться у володінні засобу масової інформації або журналіста і надана їм за умови нерозголошення авторства або джерела інформації;

2) відомості, які можуть становити лікарську таємницю;

3) відомості, які можуть становити таємницю вчинення нотаріальних дій;

4) конфіденційна інформація, в тому числі така, що містить комерційну таємницю;

5) відомості, які можуть становити банківську таємницю;

6) особисте листування особи та інші записи особистого характеру;

7) інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв’язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст, маршрути передавання, тощо;

8) персональні дані особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних [98; 124].

Розголошення або викрадення вищенаведених відомостей під час кібератаки чи порушення роботи інформаційно-телекомунікаційних систем

іншим чином, звичайно, не матиме такої шкоди, як у випадку з державною таємницею. Однак, уся інформація, відповідно до якої існує законодавча вимога щодо охорони, автоматично стає об’єктом кіберзахисту в тих випадках, коли її обробка здійснюється з використанням комп’ютерних технологій.

Отже, кібербезпека є складним правовим явищем, в рамках якого діє механізм кіберзахисту, що являє собою систему заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, метою яких є забезпечення вищенаведеного інституту. Об’єктами кібербезпеки виступають відносини правового характеру, які виникають у сфері обміну та обробки інформації у кіберпросторі, а також відносини, пов’язані із розвитком цього правового інституту, зокрема, правовідносини із розвитку інформаційної структури держави, тощо. Об’єктний склад кіберзахисту становлять матеріальні блага, інформаційні системи, за допомогою яких здійснюється обробка та передача інформації у кіберпросторі, а саме: інформаційно-телекомунікаційні системи, в яких обробляється інформація з обмеженим доступом, об’єкти критичної інфраструктури, інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів. Забезпечення охорони об’єктів кібербезпеки є стратегічно важливим питанням для сучасного стану національної безпеки України, при цьому охорона об’єктів кіберзахисту має тактичне значення.

1.4 Правові засади забезпечення кібербезпеки України та місце серед них адміністративно-правового забезпечення

Регулювання всіх суспільних відносин в державі відбувається відповідно до вимог нормативно-правових актів, прийнятих у встановленому

законом порядку. Але законодавча база є лише зовнішнім виразом права та інститутів, які входять до його структури, іншими словами, він надає правовій системі держави матеріальний вигляд. Реальною ж основою будь-якої юридичної галузі є принципи чи засади, які містяться у положеннях нормативно-правових актів різної ієрархічної підпорядкованості. Не є виключенням в даному разі кібербезпека, яка з кожним днем розвивається у нашій державі. Дане явище представляє собою доволі широкий правовий інститут, об’єктом якого є правовідносини у сфері обробки інформації у кіберпросторі. Не менш цікавою є структура кібербезпеки, до складу якої входить механізм кіберзахисту. Останній являє собою систему різного типу заходів забезпечення вказаного вище правового інституту, які застосовуються задля його стабільності та дієвості. Однак, механізм забезпечення кібербезпеки є цілком правовим явищем, що, в свою чергу, обумовлює існування відповідних правових засад, на яких ґрунтується його дія. Сучасна нормативна база дає можливість виділити велику кількість правових засад забезпечення інституту, але враховуючи особливості нашого дослідження, необхідним є освітлення місця адміністративно-правового регулювання в системі принципів вказаного механізму.

Слід зауважити, що правові засади будь-якої юридичної галузі, інституту чи норми беруть свій початок у положеннях Конституції України. Тож розглядаючи адміністративно-правові засади забезпечення кібербезпеки, необхідно також враховувати особливості правової системи, принципи побудови якої у цілому закладено в нормах Конституції України. У Основному Законі держави закріплено, що Україна — суверенна і незалежна, демократична, соціальна, правова держава. Відповідно до даних особливостей наша країна функціонує та розвиває усі внутрішні галузі життєдіяльності суспільства. Велику особливість має останній термін представленої конституційної норми — правова держава. У науковому середовищі точаться спори стосовно його ролі та сутності у правовій системі

України, але в рамках цього дослідження нас цікавить принцип, дію якого було започатковано вказаним поняттям. Стаття 8 Конституції України закріплює, що в нашій державі визначається та діє засада верховенства права, яка розкривається у наступних аспектах:

– по-перше, Конституція України має найвищу юридичну силу;

– по-друге, закони та інші нормативно-правові акти приймаються на основі Конституції і повинні відповідати їй;

– по-третє, норми основного закону є нормами прямої дії [94].

Таким чином, дана норма Конституції фактично проголошує право єдиним та головним регулятором суспільних відносин. Цей аспект дає нам можливість стверджувати, що механізм забезпечення інституту кібербезпеки має юридичне підґрунтя — правові засади, принципи, вагому частину яких складають адміністративно-правові.

Самі по собі юридичні засади є доволі цікавою теоретичною конструкцією. У науковій літературі їх частіш за все окреслюють поняттям «правові принципи». Якщо навести найпростішу дефініцію, то вона буде виглядати наступним чином: це керівні ідеї, основи певної правової галузі, інституту чи окремого механізму. Проте, таке тлумачення є доволі вузьким та не дає цілком зрозуміти їх сутність. У вітчизняній юридичній літературі існує багато різних дефініцій принципів права. Безумовно, це зумовлюється тим, що принципи права — неодноманітне і неоднозначне явище, до дослідження якого можна і треба підходити з різних боків [87, с. 42]. Даний факт підтверджується неоднорідністю його наукових визначень.

Наприклад, такі вчені як Л. С. Явич, В. М. Ронжин та А. М. Васильєв вказують, що принципи права — це ідеї, теоретичні, нормативно-керівні положення того чи іншого виду людської діяльності, які конкретизуються в змісті правових норм та об’єктивно зумовлені матеріальними умовами існування суспільства [215; 163; 180, с. 40]. Інший погляд на цю проблематику пропонує нам Г. В. Анісімова, яка вказує, що правові засади є

загальнонауковою категорією, якою оперують, як правило, в двох значеннях: по-перше, як основним вихідним положенням якої-небудь теорії, вчення, науки, світогляду; по-друге, як внутрішнім переконанням людини, визначальним її ставленням до дійсності, норм поведінки й діяльності [9, с. 486]. Схожої думки дотримується велика кількість вітчизняних та зарубіжних вчених. Якщо проаналізувати наукову та навчальну літературу то можемо побачити, що під принципами права в більшості випадків розуміють загальні вимоги до суспільних відносин і їх учасників, а також вихідні керівні засади, відправні установлення, що виражають сутність права і випливають з ідей справедливості й свободи, визначають загальну спрямованість і найістотніші риси чинної правової системи [20, с. 53]. Найбільш влучною, на наш погляд, є концепція розуміння сутності основних засад О. Ф. Скакун, П. М. Рабіновича, В. А. Козлова, К. Є. Ліванцева, В. С. Грекул, Ю. А. Ведернікова та ін. Відповідно до неї, принципи права розуміють як керівні ідеї, об'єктивно властиві праву відправні начала, незаперечні вимоги (позитивні зобов'язання), які ставляться до учасників суспільних відносин із метою гармонійного поєднання індивідуальних, групових і громадських інтересів та визначають зміст і спрямованість правового регулювання, відображають найважливіші закономірності соціально-економічної формації [180, с. 40; 169; 160]. Певним чином підсумовує даний погляд визначення М. І. Козюбра, на думку якого правові принципи — це відправні ідеї, основні засади, що визначають зміст і спрямованість правового регулювання [86, с. 66].

Необхідно відмітити, що на сьогодні масив правових принципів у юридичній системі держави є доволі широким, адже вихідні начала мають усі без винятку галузі та інститути права. У зв'язку з цим, класифікація керівних засад набуває вигляду окремої та досить значущої проблематики. У науковій літературі принципи права частіш за все класифікують залежно від сфери дії на загальні, міжгалузеві, галузеві, а також на принципи підгалузей та

інститутів права. Вони притаманні, відповідно, праву в цілому, декільком галузям права, окремим галузям, підгалузям або інститутам права [86, с. 70]. Доволі цікавою є думка В. В. Копейчикова та С. Л. Лисенкова, які класифікують принципи права за їх функціональним призначенням і об'єктом відображення. За цим критерієм принципи права об'єднані в дві групи:

1) соціально-правові — відображають систему цінностей, що властиві суспільству і мають правову форму виразу (домінування загальнолюдських цінностей над інтересами класів, націй, єдність суспільних і особистих інтересів);

2) спеціально-правові — узагальнюють засади формування та існування власне права як специфічного соціального явища.

Останні включають загальноправові (принципи гуманізму, рівності громадян перед законом, демократизму, законності, взаємної відповідальності держави і особи), міжгалузеві і галузеві принципи права [20; 186, с. 135–136].

Повертаючись до проблематики даного підрозділу, ми можемо стверджувати, що правові засади забезпечення кібербезпеки — це весь масив керівних ідей, засад та положень, закріплених в нормах нормативно-правових актів різної юридичної сили, які визначають механізм правового регулювання забезпечення кібербезпеки.

Визначальне місце в системі правових засад забезпечення кібербезпеки посідають принципи правого регулювання. Слід зазначити, що до цього часу в законодавстві не існувало сталої системи принципів забезпечення кібербезпеки. Вони були окреслені лише у доктринальній сфері правниками–теоретиками, які займалися дослідженням вказаного інституту. Однак, певні засади забезпечення кібербезпеки все ж таки містились у нормативних актах, якими регулювалися питання інформаційної безпеки в України. Їх положення на сьогоднішній день виступають правовою основою забезпечення

кібербезпеки, про що говориться у новоприйнятому Законі України «Про основні засади забезпечення кібербезпеки України». Відповідно до статті 3 Закону України «Про основні засади забезпечення кібербезпеки України», правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України. Крім того, якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені положеннями вищенаведеного Закону, то застосовуються положення міжнародного договору України [151]. Окрім цього, вказана норма у Законі України «Про основні засади забезпечення кібербезпеки України» не містить перелік актів, положення яких, по суті, становлять механізм забезпечення кібербезпеки. До них відносяться: Кримінальний кодекс України та Кодекс України про адміністративні правопорушення. Важливість цих офіційних документів проявляється в тому, що вони становлять «буфер» протидії правопорушенням у сфері кібербезпеки. У даних кодексах містяться норми, котрі дозволяються застосовувати до порушників найбільш суворі заходи примусу, а також запобігати або припиняти відповідні правопорушення.

В положеннях усіх зазначених нормативних актів містяться основи, вихідні начала механізму забезпечення кібербезпеки України. Усі вони були уніфіковані у Законі України «Про основні засади забезпечення кібербезпеки України», тож на сьогодні правові засади забезпечення кібербезпеки України ґрунтується на наступних десяти 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.

Якщо провести паралель між принципами та правовою основою забезпечення кібербезпеки, то стає зрозумілим що практично кожна засада знаходить своє більш детальне закріплення у нормах тих або інших

нормативно-правових актів. Тобто одні принципи відображають конституційність механізму забезпечення кібербезпеки, інші — особливості його застосування. Наприклад, перший принцип — верховенства права і законності — уособлює головні основи буд-якої демократичної держави та знаходить своє закріплення безпосередньо у Конституції України. Сутність верховенства права була розглянута нами вище, тож питання виникають з приводу другого елементу — законності. Досить часто ці поняття плутають або ж ототожнюють, що є серозною помилкою, хоча законність та верховенство права дійсно є пов'язаними між собою юридичними конструкціями. Наразі в юридичній науці сформувалось загальне концептуальне розуміння як поняття законності в цілому (мається на увазі законність як принцип, як правовий режим, законність як метод), так і законності як принципу організації і діяльності механізму держави. Так, законність часто характеризується як суворе і неухильне слідування державними органами та посадовими особами закону в процесі застосування права або ж як слідування праву органами держави і її громадянами [117; 16, с. 86]. У сфері забезпечення кібербезпеки законність необхідно розуміти як вимогу щодо відповідності цього механізму нормам Конституції, іншого законодавства та міжнародно-правовим актам, ратифікованим у визначеному законом порядку. Крім того, суб'єкти забезпечення кібербезпеки в процесі виконання своїх функцій не можуть діяти поза законом.

Не менш цікавим принципом є засада щодо невідворотності покарання за вчинення кіберзлочинів. Він походить від основоположного завдання всього кримінального права щодо забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України від злочинних посягань, забезпечення миру і безпеки людства, а також запобігання злочинам [97]. Безпосередньо зміст принципу невідворотності покарання за вчинення кіберзлочинів доволі повно розглянуто П. Л. Фрісом. На думку останнього,

ця засада визначає необхідність: виявлення та розкриття всіх без винятку вчинюваних у реальній дійсності злочинів; притягнення до кримінальної відповідальності всіх осіб, винних у їх вчиненні; застосування до кожного з них заходів кримінального покарання або таких заходів, що його замінюють, або звільнення від кримінальної відповідальності і (або) від покарання у випадках і на підставах, передбачених кримінальним законом; відшкодування заподіяної злочином шкоди там, де це можливо; покликаний продемонструвати соціально нестійким елементам «невигідність» порушення кримінального закону [200; 209, с. 465].

Адміністративно-правові засади забезпечення кібербезпеки нашої держави також знайшли свій прояв у переліку принципів забезпечення кібербезпеки в Україні. Як приклад, можна навести пункт 6 статті 7 Закону України «Про основні засади забезпечення кібербезпеки України», в якому закріплено пріоритетність запобіжних заходів забезпечення кібербезпеки Сутність зазначеного принципу забезпечення кібербезпеки полягає в тому, що запобіжні заходи закріплені саме в нормах адміністративного законодавства, адже вони здійснюються державними органами та використовуються з метою попередження правопорушень у тій чи інший сфері та недопущення вчинення правопорушень в майбутньому. Крім того, в рамках механізму забезпечення кібербезпеки адміністративно-правове регулювання набуває більш широкого розуміння.

Слід зазначити, що адміністративне право як окрема галузь — це сукупність правових норм, що регулюють з метою реалізації завдань і функцій держави суспільні відносини управлінського характеру, які складаються у сфері виконавчої влади, внутрішньоорганізаційній діяльності інших державних органів, а також у процесі здійснення громадськими організаціями, їх органами зовнішніх юридично-владних повноважень. Інакше кажучи, адміністративне право — це управлінське право, яке

відрізняється від інших галузей права специфікою предмета, методу регулювання та структурними особливостями [5, с. 19; 8, с. 7].

Наявність управлінського фактору та особливий предмет регулювання обумовлюють привалювання імперативного методу впливу на правовідносини. Останній складається із управлінських відносин, які виникають, розвиваються та припиняються між:

– органами виконавчої влади;

– органами виконавчої влади і підпорядкованими їм підприємствами, установами, організаціями;

– органами виконавчої влади, які не пов’язані безпосередньою підпорядкованістю;

– органами управління й органами громадських організації;

– органами виконавчої влади і громадянами [8].

Слід зазначити, що процес координації відносин, які входять до предмету адміністративного права, має свої особливості та самостійність. У законодавстві сутність адміністративно-правового регулювання не розкривається, однак, зазначений термін досить детально проаналізовано у працях вчених. Зокрема, В.В. Галунько та О.М. Єщук визначають його як цілеспрямований вплив норм адміністративного права на суспільні відносини з метою забезпечення за допомогою адміністративно-правових засобів прав, свобод і публічних законних інтересів фізичних та юридичних осіб, нормального функціонування громадянського суспільства та держави [46; 50, с. 61]. Інші вчені розглядають адміністративно-правове регулювання як сукупність відповідних засобів, які застосовуються з метою забезпечення прав, свобод і публічних законних інтересів фізичних та юридичних осіб, функціонування громадянського суспільства і держави [119, с. 278; 69, с. 124]. На нашу думку, останнє визначення досить широке та недоречне, адже воно не є інформативним, так як належним чином не розкриває внутрішні особливості адміністративно-правового регулювання. На наше

переконання, більш вдале визначення поняття адміністративно-правового регулювання запропонував В. І. Теремецький. Він вказує, що адміністративно-правове регулювання являє собою цілеспрямований вплив правових норм, що прийняті державою і є відповідними адміністративними засобами забезпечення прав та законних інтересів фізичних, юридичних осіб та держави у суспільних відносинах з метою підпорядкування їх юридично встановленому правопорядку, а також охорони та розвитку в інтересах суспільства і держави [190, с. 52].

Враховуючи представлені погляди вчених, ми можемо стверджувати, що адміністративно-правове регулювання кібербезпеки — це цілеспрямований вплив норм адміністративного законодавства на суспільні відносини, які виникають у сфері забезпечення кібербезпеки, в межах якого використовуються, застосовуються спеціальні засоби та провадяться запобіжні заходи з метою недопущення правопорушень у кіберпросторі.

Роль адміністративно-правового регулювання у сфері забезпечення кібербезпеки полягає в тому, що саме відповідно до норм адміністративного законодавства здійснюється правове регулювання діяльності суб’єктів забезпечення кібербезпеки в Україні. Як приклад, у статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» зазначається, що 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 [151]. Дана норма наглядно показує, що законодавець має на меті створення впорядкованої структури суб’єктів забезпечення кібербезпеки, тобто владних суб’єктів, які наділені відповідною компетенцією та повноваженнями, що дозволять їм регулювати

правовідносини у сфері обробки інформації в кіберпросторі шляхом застосування державного примусу. Прикладом виступає Державний центр кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань [151].

Іншим яскравим прикладом ролі адміністративно-правового регулювання у системі забезпечення кібербезпеки є створення урядової команди реагування на комп'ютерні надзвичайні події України «CERT-UA». Відповідно до статті 9 Закону України «Про основні засади забезпечення кібербезпеки України», завданнями команди є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти;

7) 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;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

9) 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.

Слід зауважити, що функціонування «CERT-UA» здійснюється Державною службою спеціального зв'язку та захисту інформації України [151].

Таким чином, адміністративно-правове регулювання виступає однією з головних засад забезпечення кібербезпеки України. Більш того, заходи, які складають систему управлінського регулювання, мають пріоритетний характер, так як їх дія направлена на попередження порушень прав і законних інтересів суб'єктів у сфері обробки інформації в кіберпросторі. Крім цього, адміністративно-правова складова забезпечення кібербезпеки проявляється у створенні ієрархічної структури суб'єктів його реалізації, яких наділено владними повноваженнями. Останні входять до Національної системи кібербезпеки України та відповідно до законодавства у межах своїх повноважень здійснюють підтримку належного стану вказаного інституту за допомогою спеціальних заходів, у тому числі адміністративних. Отже, адміністративно-правове регулювання є ключовою правовою засадою забезпечення кібербезпеки, так як проявляється у роботі великої кількості

владних суб’єктів та процесі реалізації державної політики у сфері кібербезпеки.

Висновки до розділу 1

Визначено, що адміністративно-правова охорона — це системне явище адміністративного права, сутність якого полягає у діяльності публічних органів, спрямованій на забезпечення прав громадян або підтримання відповідного правового режиму в тій чи іншій сфері суспільних відносин. Наголошено, що адміністративно-правова охорона трансформується у правовий інститут, коли її застосовують щодо конкретних об’єктів у суворій відповідності до чинного законодавства.

Під поняттям адміністративно-правова охорона, суто із юридичної точки зору, запропоновано розуміти суворо внормовану, засновану на правових принципах діяльність держави, в особі окремих органів державної влади, яку спрямовану на підтримку об’єктів права: інтелектуальної та промислової власності, надр та вод, окремих правомочностей та законних інтересів громадян, тощо.

Встановлено, що «адміністративно-правова охорона у сфері забезпечення кібербезпеки» — це діяльність відповідних державних органів, що здійснюється на засадах імперативності та ієрархічності і направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб’єктів у кіберпросторі. Головною особливістю адміністративно-правового забезпечення кібербезпеки є те, що воно здійснюється в адміністративному порядку, тобто в межах адміністративно-правових відносин.

Визначено, що кібербезпека як об’єкт адміністративно-правової охорони являє собою певний віртуальний інститут, охорона якого

відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності.

Наведено такі особливості кібербезпеки як об'єкта адміністративно-правової охорони: а) відсутність чіткого визначення змісту адміністративно-правової охорони кібербезпеки; б) адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте, закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державно влади; в) її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення відповідних порушень, а й їх попередження; г) основні засади забезпечення кібербезпеки лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті — Законі України «Про основні засади забезпечення кібербезпеки України»; ґ) власний понятійний апарат.

Обґрунтовано, що з прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» вперше з'явилось нормативне визначення поняття «кібербезпеки», що, в свою чергу, дозволить виробити грамотну та надійну стратегію захисту кібербезпеки в адміністративно-правовому порядку. Крім цього, у законі детально визначаються засади та суб'єктний склад механізму забезпечення вказаної категорії, що, безперечно, можна назвати юридичним проривом у сфері забезпечення кіберпростору та процесу використання інноваційних технологій.

Доведено, що історія становлення та розвитку кібербезпеки як юридичного інституту прямо пов'язана із еволюцією інформаційних технологій та Інтернету, який приніс людству можливість обробляти та обмінюватися колосальною кількістю даних на відстані.

Історико-правовий аналіз становлення та розвитку інституту «кібербезпеки» дозволив переконатись в тому, що досить довгий час

інституту кібербезпеки на території України фактично не існувало. Його основи вперше було закладено на Заході, де комп'ютерні технології розвивалися швидше, ніж у Європі. Наголошено, що становлення інституту кібербезпеки безпосередньо пов'язане з еволюцією інформаційних технологій. Тож найпершим комп'ютерним законом, положеннями якого вже було передбачено різного роду правопорушення із використанням комп'ютерів, став Закон «Про боротьбу з комп'ютерними шахрайствами та комп'ютерними зловживаннями», прийнятий у 1986 році в США. В подальшому розвиток правового інституту кібербезпеки здійснювався на міжнародному рівні, зокрема, у: Віденській декларації про злочинність та правосуддя, Конвенції про взаємодопомогу в кримінальних справах між членами ЄС, Резолюції Генеральної Асамблеї ООН щодо створення глобальної культури кібербезпеки від 2002 року, Женевській декларації принципів побудови інформаційного суспільства, тощо. В Україні кібербезпеку як окремий правовий інститут з'явилася після ратифікації в 2005 році Конвенції про кіберзлочинність. Наступним кроком на шляху його розвитку стало розроблення Стратегії кібербезпеки України, яка була введена в дію рішенням Ради національної безпеки і оборони України. На даний момент досліджуване явище набуло легального правового закріплення, так як на законодавчому рівні визначено його поняття, механізм забезпечення та засади функціонування. На сучасному етапі кібербезпека у повній мірі отримала нормативний прояв в положеннях Закону України «Про основні засади забезпечення кібербезпеки України».

Кіберзахист у загальному розумінні визначено як захисні дії, направлені на забезпечення безпеки у сфері отримання, обробки, зберігання та передачі інформації за допомогою складних систем управління.

У вузькому сенсі під поняттям кіберзахисту запропоновано розуміти систему (механізм) засобів різного характеру, за допомогою яких здійснюється підтримка та забезпечення інституту кібербезпеки.

Акцентовано увагу, що кіберзахист здійснюється за допомогою використання досить широкого кола правових інструментів, порядок використання яких врегульовано нормами багатьох законодавчих та підзаконних нормативно-правових актів. Розмежування кібербезпеки та кіберзахисту є принципово важливим питанням, адже воно прямо пов'язане із процесом їх реалізації, який при неправильному підході може нанести шкоду охоронюваним законом інтересам та правам людей, які здійснюють різні операції з інформацією в кіберпросторі.

Встановлено, що об'єктний склад кібербезпеки становлять суспільні відносини з приводу використання кіберпростору, а також організації безпечного пошуку, обробки та передачі інформації у цій сфері. В свою чергу, об'єктами механізму кіберзахисту виступають матеріальні та нематеріальні блага, на які спрямовано дію заходів забезпечення кібербезпеки, що входять до складу цього механізму.

Доведено, що до об'єктного складу кібербезпеки входять: а) правовідносини у сфері розвитку належної інформаційної інфраструктури у державі; б) правовідносини у сфері налагодження міжнародних зав'язків з метою обміну досвідом у сфері розбудови кібербезпеки; в) правовідносини з приводу регулювання, координації і контролю діяльності правоохоронних органів та інших суб'єктів забезпечення кібербезпеки в процесі виконання покладених на них обов'язків; г) правовідносини у сфері впровадження інформаційних технологій в основних галузях життєдіяльності суспільства та налагодження процесу їх безпечного використання; ґ) правовідносини у сфері розвитку науки та техніки з метою розбудови предметної основи інституту кібербезпеки, тобто розробки новітніх технологій, які б сприяли підвищенню безпеки при роботі у кіберпросторі; д) правовідносини у сфері імплементації у законодавство України правових механізмів забезпечення кібербезпеки з урахуванням міжнародного досвіду у цій галузі;

е) правовідносини у сфері підвищення інформаційної обізнаності суспільства при роботі з інформацією у кіберпросторі, тощо.

З'ясовано, що об'єктами кіберзахисту є: а) об'єкти критичної інформаційної інфраструктури; б) інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів; в) інформаційно-телекомунікаційні системи, в яких здійснюється обробка інформації, вимоги щодо захисту якої встановлені законом.

Обґрунтовано висновок, що кібербезпека є складним правовим явищем, в рамках якого діє механізм кіберзахисту, що являє собою систему заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, метою яких є забезпечення вищенаведеного інституту. Об'єктами кібербезпеки виступають відносини правового характеру, які виникають у сфері обміну та обробки інформації у кіберпросторі, а також відносини, пов'язані із розвитком цього правового інституту, зокрема, правовідносини із розвитку інформаційної структури держави, тощо. Об'єктний склад кіберзахисту становлять матеріальні блага, інформаційні системи, за допомогою яких здійснюється обробка та передача інформації у кіберпросторі, а саме: інформаційно-телекомунікаційні системи, в яких обробляється інформація з обмеженим доступом, об'єкти критичної інфраструктури, інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів. Забезпечення охорони об'єктів кібербезпеки є стратегічно важливим питання для сучасного стану національної безпеки України, при цьому охорона об'єктів кіберзахисту має тактичне значення.

Визначено, що правові засади забезпечення кібербезпеки — це весь масив керівних ідей, засад та положень, закріплених в нормах нормативно-правових актів різної юридичної сили, які визначають механізм правового регулювання забезпечення кібербезпеки.

Встановлено, що адміністративно-правове регулювання кібербезпеки — це цілеспрямований вплив норм адміністративного законодавства на суспільні відносини, які виникають у сфері забезпечення кібербезпеки, в межах якого використовуються, застосовуються спеціальні засоби та провадяться запобіжні заходи з метою недопущення правопорушень у кіберпросторі.

Наголошено, що роль адміністративно-правового регулювання у сфері забезпечення кібербезпеки полягає в тому, що саме відповідно до норм адміністративного законодавства здійснюється правове регулювання діяльності суб’єктів забезпечення кібербезпеки в Україні.

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

2.1 Система суб'єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу

Правова система України складається з багатьох галузей права, які, в свою чергу, включають в себе окремі підгалузі, юридичні інститути, механізми, явища, тощо. Іншими словами, правова система — це досить розгалужена та многогранна структура, основою якої виступає чинне законодавство на чолі з Конституцією. Однак, будь-яке правове явище незалежно від галузевої приналежності набуває реальної юридичної сили у двох випадках: по-перше, якщо воно прописано у нормах офіційних документів, тобто має законодавче забезпечення, по-друге, реалізовано в установленому законом порядку. Останній аспект далеко не завжди має місце, що породжує ситуації, коли той чи інший інститут перебуває у стані правової інертності.

Реалізація норм законодавства покладається на державні органи в залежності від сфери діяльності та повноважень останніх. Вказаний раніше негативний аспект виникає, коли подібні суб'єкти не мають відповідних прав щодо реалізації окремих правових інститутів або ж виконують свою роботу неналежним чином. Якщо звернути увагу на досліджуване явище кібербезпеки, то на сьогодні воно має структуровану законодавчу основу. Інститут, а також усі супутні йому явища, повністю легалізовано на території України. Крім того, визначною перевагою законодавчої бази, котра регулює кібербезпеку, є те, що в ній детально прописані суб'єкти забезпечення інституту, а також їх повноваження. Тож враховуючи особливості даного дослідження, ми маємо змогу детально розібрати систему суб'єктів

забезпечення кібербезпеки, їх адміністративно-правовий статус, а також повноваження у сфері реалізації механізму кіберзахисту відповідних об’єктів.

Слід пам’ятати, що коли мова йде про суб’єктів забезпечення кібербезпеки, то в даному контексті маються на увазі учасники правових відносин відповідного типу. Звідси виходить, що аналізувати їх адміністративно-правовий статус необхідно крізь класичний погляд на суб’єктів правовідносин. Якщо не брати до уваги галузеві відмінності, то в цілому подібні учасники є однаковими між собою. Однак, це виключає існування декількох наукових поглядів на тлумачення юридичного статусу суб’єктів правовідносин.

Відповідно до загальної правової теорії, суб’єктами правових відносин є учасники суспільних відносин, які виступають носіями юридичних прав та обов’язків [71, с. 229; 167, с. 90]. З цього приводу влучно зазначив В. М. Шаповал, який наголошував на тому, що певні особи чи органи, наділені правами та обов’язками, вступають у відношення, використовуючи свою правосуб’єктність. Даний факт робить їх учасникам конкретних правовідносин та змінює їх правовий статус [207; 168, с. 92]. Ураховуючи ці наукові погляди, доцільно було б вказати, що найбільш повно та явно особливості суб’єктів правовідносин розкриваються, якщо проводити їх дослідження в рамках тієї галузі, де відношення були започатковані. При цьому, варто пам’ятати про відмінність вказаної категорії від суміжних понять та явищ. Так, слід відмежовувати суб’єктів правовідносин від суб’єктів права взагалі (маються на увазі суб’єкти правової системи держави, а не конкретної галузі). В цьому контексті варто згадати думку С. С. Алексєєва, який вказав на те, що суб’єкти права — це особи, що володіють «правосуб’єктністю», тобто громадяни, організації, суспільні утворення, які можуть бути носіями прав і обов’язків, брати участь у правових відношеннях [163, с. 91; 6]. Таким чином, суб’єкта правовідносин

можна визначити як учасника відносин певного характеру, на якого у зв'язку з цим покладаються спеціальні права і обов'язки.

Слід відзначити, що суб'єктів забезпечення кібербезпеки окремі науковці розглядають як учасників інформаційних відносин. Зокрема, подібну думку висловлює у своїх працях І. В. Діордіца. Доводячи свій погляд, він спирається на визначення учасників інформаційних відносин, подане у Словнику стратегічних комунікацій В. А. Ліпкана, де зазначено, що суб'єкт інформаційної діяльності — це юридична або фізична особа, задіяна в інформаційному процесі [61, с. 161; 106, с. 365]. Цей науковий погляд заслуговує право на життя, однак, на нашу думку, є не зовсім правильним. Суб'єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, так як, по-перше, відносини між ними будуються на основі влади і підпорядкування, а, по-друге, останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством. Крім цього, аналіз адміністративно-правового статусу суб'єктів забезпечення кібербезпеки просто неможливо здійснювати поза межами адміністративної галузі права.

У науковому правничому середовищі поняття суб'єктів наведеної вищі юридичної галузі визначається неоднаково. Наприклад, Ю. М. Старілов бачить суб'єктів адміністративного права як реальних учасників адміністративно-правових відносин, які, маючи відповідний адміністративно-правовий статус, беруть участь в організації публічного управління, в управлінській діяльності, а також у процесі управління, тобто адміністративних процедурах [104; 176, с. 419]. Більш лаконічно з цього приводу висловився Д. М. Бахрах, який зазначив, що суб'єктами адміністративного права потрібно визнати учасників управлінських відносин, які адміністративно-правовими нормами наділені правами і обов'язками, здатністю вступати в адміністративні правовідносини [14, с. 124; 201, с. 550]. Найбільш влучним є визначення суб'єктів адміністративного права,

синтезоване І. С. Гриценко, Р. С. Мельником, А. А. Пухтецькою. Останні наголошують на тому, що суб'єктами адміністративного права слід розуміти носіїв (фізичних чи юридичних осіб) прав і обов'язків у сфері публічного управління, передбачених адміністративно-правовими нормами, які здатні надані права реалізовувати, а покладені на них обов'язки — виконувати [72, с. 226].

Під представлену дефініцію підпадає велике коло осіб, які входять до єдиної системи. Слід зазначити, що структура суб'єктів адміністративного права складається із сукупності індивідуальних та колективних осіб, але вона не вичерпується їх механічною кількістю. Кожен із суб'єктів адміністративного права займає відповідне місце в системі, яке пов'язане з його адміністративно-правовим статусом, що зумовлює можливість взаємодії з іншими суб'єктами. Аналіз суб'єктів адміністративного права дозволяє зробити висновок про наявність у системі двох підсистем, критерієм виокремлення яких є публічно-владні повноваження [118, с. 128]. Найбільш класичний погляд на це питання дає змогу виділити дві групи учасників правовідносин управлінського характеру:

– індивідуальні суб'єкти адміністративного права (громадяни, іноземці, особи без громадянства та посадові особи);

– колективні суб'єкти адміністративного права (органи публічної адміністрації, органи місцевого самоврядування, громадські організації).

Суб'єкти забезпечення кібербезпеки є учасниками правовідносин управлінського характеру, що обумовлюється їх правовим статусом. Отже, якщо перенести вищенаведену інформацію у сферу забезпечення кібербезпеки, то можна зробити висновок про те, що суб'єктами забезпечення кібербезпеки є державні органи та посадові особи останніх, наділені владними повноваженнями та відповідними обов'язками щодо охорони об'єктів кібербезпеки. Крім цього, дані суб'єкти знаходяться у законній підпорядкованості між собою. Звичайно, представлене авторське

визначення повністю не розкриває сутність адміністративно-правового статусу учасників механізму забезпечення кібербезпеки, однак, воно відображає теоретичне уявлення даної проблематики. З метою її більш повного та глибокого аналізу необхідно звернутись до норм чинного законодавства, де представлено перелік суб'єктів забезпечення кібербезпеки, а також їх права та обов'язки у цій сфері.

На нормативному рівні перелік вищевказаних осіб не є однорідним. Одним із перших офіційних актів, в положеннях якого говориться про систему суб'єктів забезпечення кібербезпеки, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». У цьому нормативному документі вперше було використано термін «національна система кібербезпеки». Саме у цю систему входять головні учасники процесу захисту прав і свобод осіб у відносинах з приводу обробки та обміну інформацією у кіберпросторі. Тож у главі 3 Стратегії вказано, що основу системи суб'єктів забезпечення кібербезпеки мають становити Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому законом порядку спеціальні завдання [157]. Інший перелік суб'єктів закріплено у ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», відповідно до якої до основних суб'єктів забезпечення кібербезпеки віднесено: Раду національної безпеки і оборони України, Міністерство внутрішніх справ України, Міністерство оборони України, Генеральний штаб Збройних Сил України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, розвідувальні органи, тощо [151]. В свою чергу, відповідно до ч. 4 статті 5 Закону України «Про основні засади забезпечення кібербезпеки 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 [151].

Таким чином, в нормах Закону України «Про основні засади забезпечення кібербезпеки України» окреслено загальну систему суб’єктів забезпечення кібербезпеки України. Звичайно, кожен учасник правовідносин у сфері забезпечення кібербезпеки володіє повноваженнями, які допомагають йому реалізувати напрями діяльності та відповідні заходи з метою підтримки належного стану вказаного інституту. Простіше кажучи, адміністративно-правовий статус кожного суб’єкта забезпечення кібербезпеки є суто індивідуальним та характеризується певними особливостями, що найбільш яскраво проявляється у правах та обов’язках відповідних суб’єктів. Нарівні з цим законодавець визначив мінімальний масив повноважень, котрі притаманні усім без винятку учасникам забезпечення кібербезпеки. У межах свої компетенції суб’єкти забезпечення кібербезпеки:

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 [151].

Окрім вказаних загальних повноважень, суб’єкти забезпечення кібербезпеки володіють спеціальними правами і обов’язками, що обумовлюють їх особливий адміністративно-правовий статус. На наше переконання, основними суб’єктами забезпечення кібербезпеки в Україні є:

– Державна служба спеціального зв’язку та захисту інформації України;
– Національна поліція України;
– Служба безпеки України;
– Міністерство оборони України;
– Генеральний штаб Збройних Сил України;
– розвідувальні органи;
– Національний банк України.

Ключова роль даних відомств, з-поміж інших суб’єктів забезпечення кібербезпеки, обумовлена особливими напрямками їх діяльності та можливістю застосовувати спеціальні заходи щодо підтримки легального

рівня кібербезпеки, які фактично не доступні іншим органам. Однак, на нашу думку, представлений список суб'єктів не є повним, адже у нього не включено Кабінет Міністрів України (далі — КМУ). Відповідно до положень законодавства, Кабінет Міністрів України є вищим органом у системі органів виконавчої влади. КМУ реалізує свої функції безпосередньо та через міністерства, інші центральні органи виконавчої влади [146]. Повноваження вищого органу виконавчої влади у сфері забезпечення кібербезпеки є доволі широкими, адже Уряд формує та реалізує державну політику у сфері кібербезпеки, захисту прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьби 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 [146]. Відповідно до цих правових норм, Кабінет Міністрів України не тільки входить до національної системи забезпечення кібербезпеки, тобто системи основних суб'єктів відповідних правовідносин, а й фактично очолює її. Однак, в положеннях чинної нормативної бази Уряд не входить до національної системи суб'єктів кібербезпеки, а є суб'єктом підтримки інституту із загальним статусом. Тому необхідно сподіватися, що у майбутньому дану нормативну помилку буде виправлено.

Продовжуючи аналіз ключових суб'єктів забезпечення кібербезпеки та особливостей їх адміністративно-правового статусу, необхідно відмітити Державну служба спеціального зв'язку та захисту інформації України, адже цей орган найбільше опікується проблемами регулювання правовідносин, об'єктом яких є інформація практично в усіх її проявах. Відомство призначене для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування

радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону. Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України [138]. У сфері забезпечення кібербезпеки Державна служба спеціального зв'язку та захисту інформації України займається формуванням та реалізацією політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, тощо [200]. До компетенції Державної служби спеціального зв'язку та захисту інформації України, відповідно до положень чинного законодавства, входить не тільки реалізація запобіжних заходів щодо охорони інформаційних ресурсів та інформації в цілому, а також велике коло контрольних повноважень.

Доволі специфічними є адміністративно-правовий статус Національної поліції України (далі — НПУ) та Служби безпеки України (далі — СБУ) у сфері забезпечення кібербезпеки. Дані правоохоронні органи наділенні повноваженнями щодо припинення правопорушень та притягнення винних осіб до відповідальності. Їх діяльність принципово відрізняється від роботи Державної служби спеціального зв'язку та захисту інформації України, адже

цей орган створює належні умови використання інформаційних ресурсів та інформації в цілому. При цьому, повноваження та завдання СБУ та НПУ суттєво різняться між собою, хоча сфери функціонування органів є доволі близькими. Зокрема, Національна поліція України є центральним органом виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку.

Завданнями поліції є надання поліцейських послуг у сферах:

1) забезпечення публічної безпеки і порядку;

2) охорони прав і свобод людини, а також інтересів суспільства і держави;

3) протидії злочинності;

4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [149].

Безпосередньо у галузі забезпечення кібербезпеки НПУ наділена повноваженнями щодо забезпечення прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [149]. Діяльність Нацполіції спрямовується та координується КМУ через підпорядковуваний орган — Міністерство внутрішніх справ (далі — МВС). Слід відзначити, що МВС як орган виконавчої влади також відіграє значну роль у процесі забезпечення кібербезпеки. До речі, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», МВС було включено до національної системи суб’єктів забезпечення кібербезпеки. У зв’язку з цим, на МВС було покладено повноваження щодо: створення і забезпечення функціонування підрозділів з протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на

боротьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів, тощо [149]. В положеннях Закону «Про основи забезпечення кібербезпеки України» МВС віднесено до загальних суб'єктів забезпечення інституту.

Дещо іншими повноваженнями у сфері забезпечення кібербезпека наділена Служба безпеки України. У своїй роботі СБУ також наділена повноваженнями щодо протидії правопорушенням і припинення злочинів, однак, її можливості є дещо ширшими, враховуючи функціональну направленість відомства. Відповідно до законодавства, Служба безпеки України — це державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України. В своїй роботі СБУ підпорядковується безпосередньо Президенту України. На Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входять попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України [155]. Як ми бачимо, діяльність СБУ безпосередньо спрямовано на підтримку національної безпеки держави, що також відображається у повноваженнях органу у сфері забезпечення кібербезпеки. У Законі України «Про основні засади забезпечення кібербезпеки України» закріплено, що Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів 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; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [155].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», окремим суб'єктом забезпечення кібернетичної безпеки є Міністерство оборони України (далі — Міноборони) та Генеральний штаб Збройних Силу України (далі — Генеральний штаб). У галузі забезпечення кібербезпеки повноваження даних органів є цілком ідентичними. Вони 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 [155]. Але необхідно відзначити, що наведені повноваження Міноборони та Генеральний штаб реалізують у відповідності до інших повноважень кожного з них, які суттєво різняться. Зокрема, Міноборони є головним органом у системі центральних органів виконавчої влади, який забезпечує формування та реалізацію державної політики з питань національної безпеки у воєнній сфері, сфері оборони і військового будівництва у мирний час та особливий період. Міноборони є органом військового управління, у

підпорядкуванні якого перебувають Збройні Сили. Основними завданнями Міноборони є:

1) забезпечення формування та реалізація державної політики з питань національної безпеки у воєнній сфері, сфері оборони і військового будівництва у мирний час та особливий період;

2) здійснення військово-політичного та адміністративного керівництва Збройними Силами;

3) здійснення в установленому порядку координації діяльності державних органів та органів місцевого самоврядування щодо підготовки держави до оборони;

4) забезпечення в межах повноважень, передбачених законом, реалізації державної політики з оборонних питань, що пов’язані з використанням повітряного простору України та захистом суверенітету держави [141].

В свою чергу, Генеральний штаб Збройних сил України підпорядковується Міноборони та є головним військовим органом з планування оборони держави, управління застосуванням Збройних Сил України, координації та контролю за виконанням завдань у сфері оборони іншими утвореними відповідно до законів України військовими формуваннями, правоохоронними органами, тощо. Завданнями Генерального штабу є:

1) участь у формуванні та реалізації державної політики у сфері оборони, стратегії воєнної безпеки;

2) стратегічне планування застосування Збройних Сил, інших військових формувань, правоохоронних органів, координація їх підготовки до виконання завдань у сфері оборони, організація територіальної оборони та оперативного обладнання території держави;

3) безпосереднє військове керівництво Збройними Силами;

4) організація і контроль за здійсненням заходів, спрямованих на підтримання військ (сил) Збройних Сил та інших військових формувань і правоохоронних органів у постійній бойовій та мобілізаційній готовності [152].

Отже, Міноборони є координаційним політичним центром, який реалізує політику держави у сфері забезпечення кібербезпеки, у той час як Генеральний штаб є оперативним органом, діяльність якого спрямовано на подолання реальної агресії та виконання бойових завдань у випадках, передбачених законодавством.

Схожі із Міноборооною та Генеральним штабом повноваження у сфері забезпечення кібербезпеки мають розвідувальні органи. У сфері забезпечення кібербезпеки останні здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки [200]. При цьому, до кола розвідувальних можна віднести досить незначну кількість існуючих відомств. Даним правовим статусом володіють: Служба зовнішньої розвідки України, розвідувальні органи Міноборони, розвідувальні органи спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону [154].

Одне з ключових місць у системі забезпечення кібербезпеки займає Національний банк України (далі — НБУ). У попередніх підрозділах дослідження ми вказували, що НБУ розробляє та впроваджує у свою діяльність сучасні електронні банківські технології, новітні платіжні та облікові системи, тощо [147]. Крім того, враховуючи той факт, що основною функцією Нацбанку, відповідно до Конституції України, є забезпечення стабільності грошової одиниці України, його повноваження у галузі забезпечення кібербезпеки доволі широкі. У зв’язку з цим, НБУ:

– здійснює формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

– визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням;

– створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України, тощо [16; 200].

Використання даних повноважень, порівняно з іншими органами, здійснюється НБУ дещо простіше, адже він є центральним банком України, особливим центральним органом державного управління, головною метою якого є забезпечення фінансової стабільності у державі. Тож на основі саме цієї особливості формується його роль у механізмі підтримки інституту кібербезпеки.

Отже, всі суб'єкти забезпечення кібербезпеки наділені як комплексом специфічних, так і комплексом загальних повноважень. Серед загальних рис суб'єктів забезпечення кібербезпеки варто відзначити те, що вони: по-перше, в своїй діяльності використовують владний примус з метою реалізації передбачених законодавством функцій; по-друге, суб'єкти забезпечення кібербезпеки перебувають у системному взаємозв'язку з іншими учасниками адміністративних правовідносин, який будується на засадах ієрархічності; по-третє, діяльність суб'єктів забезпечення кібербезпеки спрямовано не тільки на припинення правопорушень у цій сфері, а й на забезпечення умов, коли такі порушення неможливі, що реалізується шляхом проведення контрольних заходів, і т.п.

На наше переконання, суб'єктів забезпечення кібербезпеки слід об'єднати у дві групи: загальну та спеціальну. До загальної відносяться усі органи державної влади, органи місцевого самоврядування, 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. До кола спеціальних нами віднесено органи влади, котрі становлять систему суб'єктів кібербезпеки України, перелік яких закріплено в Закони України «Про основні засади забезпечення кібербезпеки України».

2.2 Адміністративно-правові форми та методи забезпечення кібербезпеки України

На сьогодні необхідність забезпечення кібербезпеки в Україні та усьому світі не викликає жодних сумнівів, адже інформаційні технології проникли фактично у всі сфери суспільного життя. Без них складно уявити діяльність будь-якого державного органу, суб'єкта господарювання, а також звичайного пересічного громадянина. А відтак, обов'язком держави стає забезпечення конфіденційності, цілісності та доступності даних. Втім, доводиться констатувати, що стан реалізації заходів із забезпечення кібербезпеки в Україні залишає бажати кращого, що, в свою чергу, обумовлює необхідність комплексного дослідження та удосконалення багатьох аспектів такої діяльності, одним із яких є розгляд адміністративно-правових форм та методів забезпечення кібербезпеки України. Адже саме зазначені категорії у своїй сукупності утворюють своєрідний інструмент, за допомогою якого суб'єкти забезпечення кібербезпеки можуть вирішити складні завдання, які стоять перед ними у досліджуваній сфері.

У загальному розумінні форма — це об'єктивне вираження змісту будь-якого явища чи процесу. У лінгвістичному тлумаченні «форма» — це типова будова, спосіб організації чого-небудь, структура, спосіб побудови думки [37, с. 1328]. В «Сучасному тлумачному словнику української мови» дане поняття пояснюється так: «форма (лат. forma — зовнішність, устрій):

1. Контури, зовнішні межі предмета, які визначають його зовнішній вигляд. … 4. Спосіб організації чого-небудь. 5. Спосіб існування певної внутрішньої структури, зовнішнє вираження… 7. Спосіб виявлення будь-якої дії… 8. Установлений зразок чого-небудь (заповнення певного документа, звернення, тощо)» [182, с. 906]. У філософському словнику за редакцією І. Т. Фролова форма визначається як категорія, що відображає внутрішню організацію змісту, і в цьому значенні проблематика форми отримує подальший розвиток в понятті структури [198, с. 519–520]. О. П. Рябченко цілком обґрунтовано доводить, що «форма» виражає спосіб існування, розвиток. Вона впливає на зміст управління позитивно або негативно: стимулює або гальмує реалізацію змісту, його розвиток. У свою чергу, зміст визначає форму. Зміст управління являє собою сукупність взаємопов'язаних внутрішніх, суттєвих для якісної характеристики управління, властивостей та ознак [164, с.19–20].

А. В. Сурілов вважає, що у праві категорія «форма» застосовується у двох значеннях: а) правової форми (наприклад, соціально-економічних відносин). У цьому контексті формою є зміст права, правосвідомість та правовідносини; б) форми самого права у двох її аспектах: форми внутрішньої та форми зовнішньої [181, с. 206; 24]. В. М. Горшеньов та І. Б. Шахов справедливо відзначають, що правова форма — це специфічна організаційна форма діяльності органів держави, посадових осіб та інших уповноважених суб'єктів, що: по-перше, здійснюється на основі найсуворішого дотримання вимог закону та інших нормативних актів; по-друге, її результати завжди тягнуть визначені наслідки, що мають юридичне значення або пов'язані з їх настанням. Зазначені два моменти виступають в органічній єдності і є головними визначальними властивостями, а у своїй сукупності кваліфікують кожну організаційну форму діяльності як правову [51]. На думку О. М. Шульги, правова форма — це організаційна форма діяльності органів держави, їх посадових осіб, яка, по-перше,

передбачена правом і йому відповідає, по-друге, спричиняє юридично значущі наслідки для суб'єктів права [212, с. 29].

Переходячи до розгляду поняття адміністративно-правових форм, варто зазначити, що в юридичній літературі не існує єдиного підходу щодо розуміння вказаного терміну, що, в свою чергу, обумовлює чималу кількість точок зору щодо його тлумачення. Так, Ю. П. Битяк вважає, що адміністративно-правова форма — це зовнішній вияв конкретних дій, що здійснюються органами виконавчої влади для реалізації поставлених перед ними завдань [4]. Досліджуючи адміністративно-правові форми протидії корупції, В. І. Литвиненко пропонує під вказаним терміном розуміти об'єктивне зовнішнє вираження адміністративно-правових норм і актів, а також інституційно-правову структуру органів публічної адміністрації, які виявляються в повноваженнях суб'єктів публічної адміністрації та здійснюваних на їхній основі діях щодо запобігання, виявлення й боротьби з корупцією, спрямованих на створення потенційно несприятливих умов для здійснення корупційних діянь, обмеження можливості розвитку корупції, виявлення наявної корумпованості в суспільстві, сприяння подоланню та викоріненню корупції з державно-владного апарату й інших сфер суспільного життя шляхом усунення наслідків корупції, притягнення винних у корупційних правопорушеннях до юридичної відповідальності, поновлення прав та інтересів осіб, що були порушені корупційним діянням [105, с. 50]. В свою чергу, Т. А. Кобзєва під адміністративно-правовими формами управління фінансовою системою України розуміє спрямовану ззовні й засновану на приписах норм адміністративного права діяльність уповноважених державою на здійснення управління фінансовою системою суб'єктів, що спричиняє юридично значимі наслідки для правовідносин в межах фінансової системи [82].

В контексті представленого дисертаційного дослідження заслуговує на увагу точка зору О. В. Логінова, який під адміністративно-правовою формою

забезпечення інформаційної безпеки Кабінету Міністрів України, центральних та місцевих органів виконавчої влади пропонує розуміти: 1) однорідну діяльність цих органів по забезпеченню інформаційної безпеки, через яку реалізуються їх функції; 2) основні, конкретні, здійснювані в межах певних правових, організаційних та організаційно-правових рамок дії цих органів, їх посадових осіб, за допомогою яких реалізується їх компетенція; 3) здійснення передбачених нормативно-правовими актами та практикою державного управління видів дій посадових та службових осіб органів виконавчої влади, за допомогою яких реалізується їх завдання по забезпеченню інформаційної безпеки. Таким чином, продовжує думку науковець, адміністративно-правовою формою забезпечення інформаційної безпеки є здійснення передбачених нормативно-правовими актами, теорією та практикою державного управління однорідної діяльності посадовими та службовими особами органів виконавчої влади, за допомогою якої реалізується їх компетенція по забезпеченню інформаційної безпеки [108, с. 128].

Таким чином, узагальнюючи вказані вище точки зору, вважаємо, що під адміністративно-правовими формами забезпечення кібербезпеки України необхідно розуміти зовнішній вираз діяльності уповноважених органів державної влади, який виявляється у вчиненні ними комплексу дій, які спрямовані на створення таких умов, за яких буде забезпечено безпеку комп'ютерних систем у всій країні в цілому. Варто підкреслити, що в юридичній літературі не існує єдиного підходу до визначення конкретних форм забезпечення кібербезпеки, а відтак, спираючись на аналіз наукової літератури та норм чинного законодавства України, нами буде запропоновано власне бачення щодо переліку таких форм.

Так, в першу чергу необхідно вказати таку адміністративно-правову форму забезпечення кібербезпеки України як нормотворчість (тобто прийняття нормативно-правових актів у сфері забезпечення кібербезпеки).

О. Ф. Скакун вважає, що під нормотворчістю слід розуміти офіційну діяльність уповноважених суб'єктів держави та громадянського суспільства щодо встановлення, зміни, призупинення і скасування правових норм, їх систематизації [171, с. 342]. Досить розгорнуте визначення нормотворчості надає О. В. Петришин, який зазначає, що це діяльність уповноважених на це суб'єктів з розроблення, розгляду, прийняття та офіційного оприлюднення нормативно-правових актів, яка здійснюється за визначеною процедурою [187]. Науковець сформулював наступні характерні ознаки вказаного поняття: 1) нормотворчість є етапом правоутворення. Під час нормотворчості в нормативно-правових актах мають закріплюватися норми права, які є результатом узагальнення найбільш важливих повторювальних суспільних відносин, а також засобом витіснення шкідливої суспільної практики; 2) нормотворчість є правовою формою діяльності публічної влади поряд із правозастосуванням, тлумаченням права, контрольно-наглядовою та установчою діяльністю. Тому нормотворча діяльність урегульована правом і є юридично значущою, тобто породжує правові наслідки. Основна відмінність нормотворчості від інших правових форм діяльності полягає в тому, що її метою є створення, зміна або скасування норм права; 3) результатом нормотворчої діяльності є нормативно-правові акти, за допомогою яких формально закріплюються норми права. Загальним результатом нормотворчості є законодавство як джерело права; 4) нормотворчість здійснюється уповноваженими на це суб'єктами — органами і носіями публічної впади: органами державної влади та органами місцевого самоврядування, їх посадовими особами, народом та територіальними громадами; 5) нормотворчість здійснюється за певною процедурою, яка регламентується законодавством. Процедурний характер нормотворчої діяльності (тобто її здійснення в установленому порядку) зменшує вірогідність свавілля та помилкових рішень, забезпечує створення справедливих та ефективних норм права. Суттєві порушення процедури

нормотворчості можуть призвести до визнання нормативно-правового акта недійсним у судовому порядку [187].

Слід також вказати точку зору В. І. Риндюка, який справедливо підкреслює, що поняття «нормотворчість» («правотворчість») слід відрізняти від поняття «нормоутворення» («правоутворення»). Нормоутворення — це найбільш широка категорія, яка включає всі форми і засоби виникнення, розвитку та зміни права, у тому числі і нормотворчість. Нормотворчість — це завжди офіційно оформлений процес діяльності держави, посадових осіб, органів місцевого самоврядування, а нормоутворення (формування права) — це неоформлений соціальний процес становлення правових ідей про необхідність упорядкування суспільних відносин, зумовлений різними факторами і поглядами. Головною відмінністю нормотворчості від нормоутворення, продовжує В. І. Риндюк, є те, що творчість права здійснюється державними органами або з їх санкції, дозволу. Нормоутворення відбувається і поза нормотворчістю державою, у рамках громадянського суспільства — у правосвідомості, конкретних правовідносинах, правомірній поведінці, правових теоріях і т. ін. [162, с. 22].

Узагальнюючи все вказане вище, можна із впевненістю стверджувати, що нормотворчість є однією з ключових форм забезпечення кібербезпеки в Україні, оскільки за її допомогою вбачається можливим створити таке правове поле, яке буде виключати будь-які можливості для суб’єктів відповідних правовідносин вчинити правопорушення у досліджуваній сфері. А відтак, нормотворчість, через процес створення правового припису, дозволяє досягти певної поведінки людей у конкретній сфері суспільних правовідносин, що, в свою чергу, має важливий соціальний, економічний та політичний ефект. Якісна та своєчасна нормотворча діяльність дозволяє не лише забезпечити необхідний стан якоїсь сфери суспільних відносин, вона також сприяє підвищенню рівня довіри до суб’єкта нормотворчості

(держави), а також підвищує відчуття захищеності громадян у своїй країні [35].

Наступною формою забезпечення кібербезпеки, на яку хотілося б звернути увагу, є прийняття індивідуальних актів у сфері забезпечення кібербезпеки. Так, на переконання С. С. Алєксєєва, індивідуальний акт — це припис, який розрахований на конкретний, чітко визначений, одиничний випадок і, виходячи з цього, являє собою акт «одноразової дії»; такі акти здебільшого персоніфіковані і їх дія завершується із настанням відповідних наслідків або фактів, що безпосередньо ними передбачені [7, с. 208; 6, с. 82–83]. У своєму дисертаційному дослідженні О.О . Мандюк дійшов висновку, що індивідуальний акт — це одностороннє волевиявлення адміністративного органу зовнішньої дії, що безпосередньо впливає на права, свободи чи інтереси конкретних осіб або стосується конкретної ситуації. До основних ознак вказаного поняття автор відносить такі: односторонність, індивідуальність (конкретність), зовнішня дія, породження правових наслідків, приймається адміністративним органом [114, с. 6–7]. Інший науковець — К. І. Бриль — доводить, що під індивідуальним актом слід розуміти вольову дію суб’єктів права, яка здійснюється ними в передбачених законом випадках, закріплюється в установленій законом формі (у формі акта–документа) та спрямована на реалізацію вимог правових норм в конкретних суспільних відносинах і конкретних ситуаціях. Автор підкреслює, що індивідуальні акти належать до різних частин механізму правового регулювання. Разом з тим, всіх їх об’єднує те, що кожний акт поширюється на конкретний випадок. Оскільки всі індивідуальні акти є дуже різноманітними і критеріїв їх класифікації можна виділити досить багато, то ми виберемо найбільш загальний і важливий критерій — за місцем в механізмі правового регулювання [23].

Таким чином, індивідуальні акти у сфері забезпечення кібербезпеки дозволяють оперативно вирішити нагальні проблеми, що з’являються у

вказаній сфері суспільних відносин. Їх перевага полягає у тому, що вони спрямовані на конкретного суб'єкта, а тому за їх допомогою можливо вирішити більш конкретні проблемні питання. В якості прикладу таких документів В. В. Марков слушно наводить такі: протокол засідання Кабінету Міністрів України від 11.04.2012 р. № 27 та лист Державної служби спеціального зв'язку та захисту інформації України від 21.05.2012 р. № 16/1/1-1543 стосовно підготовки законопроекту щодо вдосконалення порядку отримання правоохоронними органами інформації про споживачів телекомунікаційних послуг та порядку придбання SIM-карт споживачами [115, с. 44].

Наступна адміністративно-правова форма забезпечення кібербезпеки в Україні, на нашу думку, — адміністративний договір. Стосовно вказаного терміну О. Ю. Прокопенко слушно підкреслює, що адміністративний договір — 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 [159, с. 81]. Однак, незважаючи на відносну новизну вказаного поняття, в науковій літературі існує чимала кількість підходів щодо його тлумачення. Так, В. С. Стефанюк визначає адміністративний договір як договір, побудований на публічно-правових нормах, який регулює добровільне погодження волі двох (або більше) суб'єктів права, один із яких є суб'єктом управління, про встановлення взаємних адміністративних правовідносин [179]. 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, як продовжує автор, учасники правовідносин визначають правила власного поводження і встановлюють послідовність своїх дій, досягають необхідного для них правового результату [172, с. 12].

Відомий український вчений Ю. П. Битяк вважає, що адміністративний договір — це правовий акт між двома (або більше) суб'єктами адміністративного права, один із яких обов'язково є органом виконавчої влади, і може включати в себе загальнообов'язкові правила поведінки або встановлювати конкретні правовідносини між його учасниками [17, с. 5]. В іншій науковій праці Ю. П. Битяк та О. В. Константий констатують, 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) [18, с. 106; 10].

Характерними ознаками адміністративного договору, на слушну думку О. В. Дьоміна, є: виникнення у сфері публічної влади у зв'язку і з приводу реалізації органом виконавчої влади або органом місцевого самоврядування своїх владних повноважень; підставою виникнення є правозастосовчий акт, прийнятий згаданими органами; організуючий характер; метою є задоволення публічних інтересів, досягнення публічного блага, тобто домінування суспільних цілей. В адміністративному договорі, продовжує автор, неможлива (за будь-яких умов) одностороння відмова від виконання договірних умов або їх зміна, такий договір або окремі його положення не може бути визнано конфіденційним. У деяких випадках необхідною умовою чинності є його опублікування [56, с. 18].

Таким чином, адміністративний договір, як адміністративно-правова форма забезпечення кібербезпеки, представляє собою добровільну угоду між декількома суб'єктами адміністративного права, які наділені владними повноваження, з метою координації їх спільної діяльності, яка в результаті призводить до виникнення, зміни або припинення взаємних прав та обов'язки сторін відповідного договору. Отже, за допомогою адміністративного договору вбачається можливим скоординувати роботу різних державних структур, однак, лише у випадках, коли в цьому існує об'єктивна необхідність, а координація діяльності призведе до отримання кінцевого бажаного результату [29].

І остання адміністративно-правова форма забезпечення кібербезпеки, на яку, на нашу думку, необхідно звернути окрему увагу, — правореалізація, яка представляє собою втілення вимог правових норм у суспільних відносинах. Реалізація норм права, як зазначає Ю. А. Ведєрніков, протікає в правомірній поведінці, тобто під час здійснення або утримання від здійснення відповідних учинків. Але ця поведінка не є кінцевим результатом реалізації правомірного припису. Як і правомірна поведінка, правореалізація нерозривно пов'язана з досягненням соціального ефекту [188]. Результати правореалізації — це кінцевий результат правомірної поведінки суб'єктів, який характеризується як соціально цінні наслідки правового регулювання [112]. Таким чином, в контексті представленого наукового дослідження правореалізація передбачає безпосереднє втілення норм адміністративного права в діяльність суб'єктів, функції яких полягають у забезпеченні кібербезпеки в Україні. При цьому, кожен із таких суб'єктів повинен в обов'язковому порядку дотримуватись визначених суб'єктивних прав та виконання своїх зобов'язань.

Таким чином, саме адміністративно-правові форми є об'єктивним практичним відображенням дій, що вчиняють суб'єкти, які уповноважені реалізовувати заходи із забезпечення кібербезпеки в Україні. Можна також

говорити про те, що форми діяльності відображають характерні особливості правового статусу конкретного суб'єкта, адже в них фактично відображається те, яким чином вони (суб'єкти) реалізують свою суб'єктивні права та юридичні обов'язки [31].

На наступному етапі нашого дослідження приділимо увагу адміністративно-правовим методам забезпечення кібербезпеки в Україні. У загальному розумінні метод — це шлях до мети, спосіб її досягнення [199, с. 241]. З точки зору філософії, як зазначає В. Л. Петрушенко, поняття методу, 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. Сам термін «метод» сходить до давньогрецького виразу «мета — одоїс», що можна перекласти як «через вистежений (або підготовлений) шлях» [135, с. 223]. В. С. Зеленецький під методами розуміє сукупність взаємопов'язаних правил, технологічних прийомів і наукових положень, які визначають оптимальні шляхи та способи реалізації пізнання й перетворення дійсності. На його думку, відповідні методи можуть бути реалізовані лише за допомогою конкретних дій, тобто тактичних прийомів їх реалізації [74, с. 213; 24]. Поняття методу активно використовується у багатьох сферах суспільного життя, втім, найбільш дослідженим воно є саме в галузі права, а в залежності від галузі права воно набуває своїх характерних особливостей.

Адміністративно-правові методи, як зазначає В. О. Бурбика, — це сукупність прийомів впливу, що містяться в адміністративно-правових нормах, за допомогою яких встановлюється юридичне владне і юридичне підвладне становище сторін у правовідносинах [24]. На нашу думку, слід погодитись із точкою зору В. К. Колпакова та О. В. Кузьменко, які доводять, що адміністративно-правові методи — це способи та прийоми

безпосереднього і цілеспрямованого впливу органів державного управління (посадових осіб) на підпорядковані їм об’єкти управління [90, с. 36]. Методи, підкреслюють вчені, є досить різноманітними, однак, вони мають загальні риси, а саме: способи впливу органів державного управління на підпорядковані їм об’єкти управління; вираження державного публічного інтересу; засоби досягнення мети; способи організації, прийоми здійснення функцій, що виникають в процесі спільної діяльності; способи реалізації компетенції [81, с. 36].

Варто вказати на той факт, що в науковій літературі не існує єдиного підходу щодо визначення конкретних адміністративно-правових методів забезпечення кібербезпеки в Україні. А тому на основі аналізу норм чинного законодавства та наукових поглядів вчених нами були визначені такі методи забезпечення кібербезпеки:

– адміністративний примус. У найбільш загальному розумінні це метод психічного чи фізичного впливу державних органів (посадових осіб) на свідомість і поведінку певних осіб з метою спонукати, примусити їх виконувати правові норми [2, с. 151]. Р. С. Мельник відзначає, що адміністративний 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» [120, с. 5; 165]. Таким чином, ключове значення вказаного методу полягає у тому, що він спрямований на попередження виникнення правопорушень у досліджуваній сфері. Однак, справедливо буде також підкреслити, що застосування методу адміністративного примусу не лише спрямоване на попередження виникнення протиправної поведінки, а й покликане забезпечити захист інформаційних, приватних, комп’ютерних ресурсів, тощо;

– метод позитивного зобов’язання. Позитивне зобов’язання — це категорія, що включає та доповнює інше поняття — моральне зобов’язання. Позитивне в юриспруденції означає встановлення (правила) волею чи силою панівного, господарюючого суб’єкта; зобов’язання, відповідно, означає дію чи бездіяльність (що рідше), обов’язковість якої випливає внаслідок вольового акту чи внутрішнього переконання, що відповідає: перше — державному закону, друге — моральному закону [47];

– метод дозволу та заборон. В контексті представленого наукового дослідження метод дозволу означає надання суб’єктам відповідних правовідносин можливості (права) здійснювати активні дії та/або бездіяльність, тобто мати свободу вибору напрямку (варіанта) поведінки. Однак, при цьому не слід забувати, що така поведінка все одно не повинна виходи за межі, визначені чинним законодавством. Щодо методу заборон, то він передбачає покладання на суб’єкта обов’язку певної пасивної поведінки, утримання від вчинення якихось дій під загрозою настання відповідальності [171];

– метод адміністративного контролю. В. М. Кудрявцев визначає адміністративний контроль як перевірку якості адміністративної діяльності за допомогою співставлення фактично досягнутих результатів цієї діяльності з цілями, поставленими в нормативних актах при вирішенні актуальних соціальних проблем, а також з рівнем вирішення цих проблем. Адміністративний контроль дає можливість не тільки виявляти відхилення, помилки і недоліки, але й запобігати їм, шукати нові резерви і можливості [99, с. 140]. Таким чином, застосування вказаного методу є важливим з точки зору забезпечення ефективного функціонування суб’єктів забезпечення кібербезпеки в Україні, що, в свою чергу, прямо впливає на вказану сферу суспільних відносин;

– метод контролю доступу, який хоча і є специфічним способом забезпечення кібербезпеки, однак, водночас є одним із найефективніших. Він

передбачає можливість встановити обмеження та/або заборону до доступу певних суб'єктів до якоїсь інформації. Втім, справедливо буде відмітити, що реалізація вказаного методу ускладнюється відсутністю належної матеріально-технічної бази;

– метод ліцензування діяльності у сфері захисту відомостей, що становлять державну таємницю. Взагалі ліцензування — це «форма контролю за законністю передбачуваних дій громадянина чи організації дозволом робити тільки законні дії і відмовленням у здійсненні протиправних дій, що обумовлює вид і міру припустимої активності, а так само реалізацію нагляду за фактично здійснюваними діями» [127, с. 32]. А відтак, ліцензування, беззаперечно, можна вважати одним із найважливіших методів забезпечення інформаційної безпеки, оскільки воно дозволяє: по-перше, контролювати осіб, що мають доступ до конкретної інформації; по-друге, забезпечити захист інформації, яка не повинна буди доступною для загалу;

– метод сертифікації та стандартизації. Стандартизація та сертифікація — це необхідні заходи, які пов'язані із встановленням мінімальних вимог до певних небезпечних засобів. Стандартизація — діяльність, що полягає в установленні положень для загального та неодноразового використання щодо наявних чи потенційних завдань і спрямована на досягнення оптимального ступеня впорядкованості в певній сфері [156]. А відтак, зазначений метод зазвичай використовується з метою стандартизації та сертифікації системи телекомунікаційного обладнання й програмного забезпечення автоматизованих систем обробки інформації згідно з вимогами інформаційної безпеки;

– реєстраційний метод, який ґрунтується на використанні інформації, яку отримують шляхом підрахунку кількості процесів, предметів або витрат на створення, споживання продукції [174].

Таким чином, завершуючи представлений підрозділ дисертаційного дослідження, слід констатувати, що вказаний нами перелік форм та методів забезпечення кібербезпеки в Україні не претендує на вичерпність, однак, на нашу думку, саме вони найбільш якісно та всебічно характеризують зміст такої діяльності. Разом із тим, справедливо буде відмітити, що для забезпечення кібербезпеки в нашій державі необхідним є комплексне використання таких форм і методів. Як суттєвий недолік слід визнати те, що жодна із вказаних категорій не дістала законодавчого закріплення, що, беззаперечно, потребує негайного вирішення шляхом внесення змін до відповідних нормативно-правових актів [30].

2.3 Види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України

На сьогоднішній день можна із впевненістю констатувати, що одними із найпоширеніших правопорушень є порушення у кіберпросторі. Варто підкреслити, що вчинення таких правопорушень може не тільки мати негативні наслідки для кожного окремого громадянина, а й нести небезпеку для всієї держави взагалі. Саме тому важливого значення набуває інститут юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. Взагалі ж «відповідальність» у науковій літературі в більшості випадків трактується лише як підзвітність (accountability) і усвідомлення осудності (immutability). У юридичній ж науці феномен відповідальності вивчається головним чином у плані покарання (punishability). Цікаво також відзначити той факт, що термін «відповідальність» вперше ввів у науковий обіг Альфред Бен, який тлумачив її саме в значенні «покарання» [13]. Тривалий час проблема відповідальності

була в основному предметом уваги правознавців, що, в свою чергу, обумовило чималу кількість підходів до його розуміння.

Так, відповідно до точки зору В. Н. Хропанюка, юридична відповідальність — це важливий захід захисту інтересів особистості, суспільства і держави. Вона наступає в результаті порушення приписів правових норм та виявляється у формі застосування до правопорушника заходів державного примусу. Найважливішою ознакою юридичної відповідальності є те, що вона визначається державою і застосовується її компетентними органами. Для правопорушника юридична відповідальність означає застосування до нього санкцій правових норм, вказаних в них певних заходів відповідальності [204, с. 334; 40]. На переконання Д. М. Лук'янця, юридична відповідальність — це регламентована правовими нормами реакція з боку уповноважених суб'єктів на діяння фізичних або юридичних осіб (колективних суб'єктів), що проявляються в недотриманні встановлених законом заборон, невиконанні встановлених законом обов'язків, порушенні цивільно-правових зобов'язань, нанесенні шкоди або завданні збитків, і виражена в застосуванні до осіб, які вчинили такі діяння, засобів впливу, що тягнуть за собою позбавлення особистого, майнового або організаційного характеру [110, с. 15].

М. І. Матузова та А. В. Малько зазначають, що юридична відповідальність являє собою виникле з правопорушення правове відношення між державою в особі її спеціальних органів і правопорушником, на якого покладається обов'язок зазнати відповідні втрати та негативні наслідки за скоєне правопорушення, за порушення вимог, які містяться в нормах права; автори дійшли висновку, що під юридичною відповідальністю слід розуміти передбачений законом обов'язок правопорушника зазнати в процесуально визначеному порядку державно-владного примусового впливу, кінцевим наслідком якого є позбавлення особи, яка вчинила правопорушення, благ особистого, майнового або організаційного

характеру [208, с. 425; 206]. Б. Т. Базильов доводить, що інститут юридичної відповідальності — це загальний, комплексний за своїм змістом (складається з норм різних галузей), своєрідний за структурою (включає в себе інститути і галузь в цілому), охоронний за призначенням, функціональний інститут права, що регулює деліктні відносини методом покарання правопорушників [11, с. 47]. О. С. Літошенко пише, що юридична відповідальність — це один із видів соціальної відповідальності, являє собою встановлений державою примусовий захід (покарання) за скоєне правопорушення, що застосовується до винної особи державними органами або за їх дорученням громадськими органами, та обов'язок правопорушника перетерпіти відповідні негативні наслідки, що визначені чинним законодавством [107, с. 16].

Розкриваючи сутність поняття «юридична відповідальність», не можна не звернути увагу на характерні ознаки вказаної категорії. В цьому контексті ми поділяємо точку зору О. В. Зайчука та Н. М. Оніщенко, які цілком слушно зазначають, що для всіх різновидів юридичної відповідальності спільними є наступні ознаки [184]: 1. Підставою відповідальності є правопорушення як конкретний факт поведінки, юридична кваліфікація якого вміщена у законі. Ознаки правопорушення та санкції, що визначають засоби примусу за його вчинення, не підлягають звужувальному чи розширювальному тлумаченню. У процесі застосування відповідальності повинно бути доведено, що особа, яка притягнута до відповідальності, вчинила правопорушення, ознаки якого вміщені у законі. Цей вид відповідальності не може бути застосований за наміри, вислови, погрози чи вчинення моральних проступків. Чіткість підстав відповідальності у правовій сфері забезпечує її реальність, справедливість та законність. Правопорушення не завдає шкоди нормам закону, які продовжують діяти, поширюючись на всіх суб'єктів. Воно завдає шкоди охоронюваним державою правам, свободам та законним інтересам суб'єктів суспільних відносин. 2. Наявність правової основи, яку складають

правові норми. Саме вони характеризують поведінку як протиправну та у санкції вміщують вичерпний перелік видів відповідальності та засобів, що можуть бути застосовані до порушника. Вказана норма права вміщається у документі, який має форму нормативно-правового акта, що виходить від органу публічної влади. 3. Наявність визначеного суб'єкта — фізичної чи юридичної особи, що в силу вікового та психічного стану може власноруч відповідати за вчинене. Тому такий суб'єкт повинен володіти певними характеристиками, а вчинене правопорушення має пов'язуватись із наявністю вини, тобто психологічним ставленням до скоєного. Саме це і визначає можливість покладення відповідальності та впливає на її види і форму. 4. Юридична відповідальність спирається на державний примус та пов'язується із досягненням певної мети — перевиховання, покарання правопорушника та поновлення порушених прав. Державний примус є специфічним впливом на поведінку людей, заснованим на організованій силі. Особливістю такого примусу є націленість на примусове виконання норм права, нормативна регламентованість його законом, наявність чітко встановлених меж та здійснення лише компетентними державними органами. Однак, потрібно пам'ятати, що державний примус є більш широким поняттям, ніж юридична відповідальність, оскільки він може здійснюватися різними способами, не пов'язаними з відповідальністю (наприклад, митний огляд багажу, стягнення аліментів та ін.). 5. Метою відповідальності є охорона правопорядку, що здійснюється шляхом примусового поновлення порушених прав, припинення протиправного стану чи покарання правопорушника. Дієвість цього інституту забезпечує реальну можливість безперешкодного здійснення суб'єктивних прав та можливість досягнення правового результату правомірною поведінкою суб'єктів суспільних відносин. Своєчасне застосування відповідальності забезпечує можливість перевиховання правопорушника та реалізацію виховної функції у суспільстві. 6. Відображається у настанні певних негативних наслідків для

правопорушника, що мають особистий, майновий, організаційний характер. Юридична відповідальність є підставою виникнення у суб'єкта, винного у скоєнні правопорушення, додаткового обов'язку зазнати певних втрат відповідно до санкції норми права та рішення правозастосовчого органу держави. 7. Наявність особливої процесуальної форми покладення та реалізації відповідальності. Вона має нормативне закріплення та виявляється у наявності певних стадій відповідальності, кожна з яких має певне значення, межі та відповідає певним вимогам. Основними з них є виникнення юридичної відповідальності, вияв правопорушення; офіційне визнання правопорушення як підстави відповідальності актом компетентного органу; реалізація юридичної відповідальності [184]. Стосовно вказаних вище характерних ознак О. В. Зайчук та Н. М. Оніщенко наголошують, що їх наявність є обов'язковою, а відсутність хоча б однієї з них свідчить про відсутність юридичної відповідальності та можливість застосування певного різновиду неправової соціальної відповідальності [184].

Таким чином, під юридичною відповідальністю за порушення законодавства у сфері кібербезпеки України слід розуміти застосування заходів примусового характеру, які визначені нормами чинного законодавства, до осіб, що вчинили правопорушення у кіберпросторі. Заходи юридичної відповідальності застосовуються лише у випадку винного діяння відповідного суб'єкта, а санкції повинні відповідати рівню шкоди вчиненого проступку. Відповідно до нещодавно прийнятого Закону України «Про основні засади забезпечення кібербезпеки України» [151], особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом [151]. Виходячи із вказаного положення, до суб'єктів, що вчинили правопорушення у досліджуваній

сфері, можуть бути застосовані таки види юридичної відповідальності: цивільна, адміністративна та кримінальна. Далі приділимо окрему увагу кожному із вказаних видів відповідальності.

Розглядаючи перший вид відповідальності, в першу чергу зазначимо, що цивільна відповідальність — це самостійний вид юридичної відповідальності, який полягає у застосуванні державного примусу до правопорушника шляхом позбавлення особи певних благ чи покладення обов'язків майнового характеру. До правопорушника застосовуються санкції майнового характеру, які спрямовані на відновлення порушених прав та полягають у відшкодуванні збитків, стягненні неустойки чи пені. Особливості даного виду юридичної відповідальності, на думку Р. О. Стефанчука, є: 1) майновий характер; 2) стягується на користь потерпілої сторони; 3) компенсаційна природа, тобто спрямованість на відновлення майнової сфери потерпілого [178]. Цивільна відповідальність, як підкреслює Н. В. Іванчук, — це насамперед компенсаційна відповідальність, яка означає, що одна із сторін компенсує завдані нею втрати, тому її називають майновою. Одночасно вона є і відновлювальною відповідальністю, тому що завдяки їй часто відновлюються порушені раніше певні права громадян, правове становище суб'єктів (повернення боргів, недійсні окремі види угод, тощо). Особливістю цивільної відповідальності є її чітко виражена позитивна, добровільна форма юридичної відповідальності, що передбачає можливість і належність добровільного виконання взятих на себе обов'язків, без використання примусу з боку держави. Сторона, що порушила взяті на себе обов'язки чи завдала збитків, може самостійно відшкодувати ці збитки, якщо потерпіла сторона на це погодиться [75, с. 47–48].

Варто вказати точку зору О. О. Тихомирова, який зазначає, що юридичний зміст цивільно-правової відповідальності виявляється у взаємозв'язку двох її сутнісних компонентів [191]: 1) права потерпілого

(кредитора) на відновлення власного порушеного становища шляхом відшкодування (компенсації) збитків, майнової та моральної шкоди, здійснення інших правовідновлювальних дій; 2) обов'язку правопорушника (боржника) добровільно чи примусово перетерпіти негативні наслідки майнового чи особистого характеру, передбачені законом чи договором, а у випадку застосування примусу — підтверджені рішенням суду, що забезпечує захист та відновлення прав потерпілого [191]. Отже, як продовжує автор, реалізація цивільно-правової відповідальності — це передусім виконання обов'язку по відновленню порушеного права (становища) особи або компенсації нанесених правопорушенням шкоди, реальних збитків, упущеної вигоди, тощо, що забезпечується передбаченими нормами цивільного права заходами державного примусу (їх можливістю або безпосередньою реалізацією) [191].

Відзначимо, що незважаючи на законодавче закріплення можливості притягнення осіб до цивільно-правової відповідальності за порушення законодавства у сфері забезпечення кібербезпеки, на сьогодні відсутній механізм притягнення осіб до вказаного виду відповідальності. Крім того, не визначено чіткого переліку підстав притягнення правопорушника до вказаного виду відповідальності, про них лише опосередковано говориться в окремих статтях Цивільного кодексу України. Так, особу може бути притягнено до цивільно-правової відповідальності за порушення прав інших учасників відповідних правовідносин, зокрема: права на інформацію (ст. 302 ЦКУ); права на свободу літературної, художньої, наукової і технічної творчості (ст. 309 ЦКУ); обов'язок фізичної особи, яка поширює інформацію, переконатися в її достовірності (ст. 302 ЦКУ); обов'язок правоволодільця передавати інформацію користувачеві для здійснення прав, наданих йому за договором комерційної концесії (ст. 1120 ЦКУ); право на таємницю особистого життя (ст. 301 ЦКУ); майнові права інтелектуальної власності на комерційну таємницю (ст. 506 ЦКУ); обов'язки виконавця за договором на

виконання науково-дослідних або дослідно-конструкторських та технологічних робіт утримуватися від публікації без згоди замовника науково-технічних результатів, одержаних при виконанні робіт (ст. 897 ЦКУ); тощо [205].

Справедливо буде відзначити, що цивільна відповідальність найрідше застосовується за порушення законодавства у досліджуваній сфері. Найбільш поширеними є санкції, передбачені адміністративним та кримінальним законодавством. Переходячи до наступного виду відповідальності за порушення законодавства у сфері кібербезпеки України, в першу чергу зазначимо, що у найбільш загальному розумінні адміністративна відповідальність — це застосування до осіб, які вчинили адміністративні проступки, адміністративних стягнень, що тягнуть для цих осіб обтяжливі наслідки майнового, морального, особистого чи іншого характеру і накладаються уповноваженими на те органами чи посадовими особами на підставах і в порядку, встановлених нормами адміністративного права [132]. І. О. Галаган доводить, що адміністративна відповідальність — це застосування у встановленому порядку уповноваженими на це органами і службовими особами адміністративних стягнень, сформульованих у санкціях адміністративно-правових норм, до винних у вчиненні адміністративних проступків, що містять державний і громадський осуд, засудження їх особи і протиправного діяння, що виявляється у негативних для них наслідках, які вони зобов`язані виконати, і переслідують цілі їх покарання, виправлення і перевиховання, а також охорони суспільних відносин у сфері радянського державного управління [45, с. 41].

Адміністративна відповідальність, на переконання В. К. Колпакова, — це специфічне реагування держави на адміністративне правопорушення, що полягає у застосуванні уповноваженим органом або посадовою особою передбаченого законом стягнення до суб’єкта правопорушення. Як явище правової дійсності, вона характеризується двома видами ознак: по-перше, це

ознаки, властиві юридичній відповідальності в цілому (основні); по-друге, ознаки, що відмежовують адміністративну відповідальність від інших видів юридичної відповідальності (похідні). Основні ознаки адміністративної відповідальності, як зазначає автор, полягають у тому, що вона: 1) є засобом охорони встановленого державою правопорядку; 2) нормативно визначена і полягає в застосуванні (реалізації) санкцій правових норм; 3) є наслідком винного антигромадського діяння; 4) супроводжується державним і громадським осудом правопорушника і вчиненого ним діяння; 5) пов'язана з примусом, з негативними для правопорушника наслідками (морального або матеріального характеру), яких він має зазнати; 6) реалізується у відповідних процесуальних формах [89].

Більш вичерпний перелік характерних ознак адміністративної відповідальності, на нашу думку, надає С. Т. Гочарук. Автор вказує, що для вказаного виду юридичної відповідальності є характерними такі властивості: 1) це один із самостійних видів правової відповідальності (поряд з кримінальною, дисциплінарною та цивільно-правовою); 2) це специфічна форма правового регулювання з боку держави в особі її компетентних органів на певну категорію протиправних проявів; 3) це державно-репресивний захід як результат протиправної поведінки особи; 4) це один із видів державного примусу, зокрема, адміністративний його різновид (одна із ланок заходів адміністративного примусу); 5) це водночас правовий обов'язок правопорушника дати відповідь перед повноважним державним органом щодо своїх неправомірних дій і понести за це певне покарання; 6) юридичною підставою для настання адміністративної відповідальності, як правило, є окремий вид правопорушень — адміністративні проступки; 7) засобами реалізації адміністративної відповідальності є самостійні юридично-репресивні (примусові) заходи — адміністративні стягнення; 8) адміністративна відповідальність — це своєрідні правовідносини між органами (посадовими особами), що її застосовують, та правопорушниками,

причому в таких правовідносинах відсутні елементи службового підпорядкування; 9) певними правами щодо встановлення та застосування адміністративної відповідальності наділене значне коло державних органів (посадових осіб); 10) це один із важливих адміністративно-правових інститутів, нормами якого значною мірою охороняється велика кількість суспільних відносин, урегульованих як адміністративно-правовими нормами, так і нормами інших галузей права; 11) адміністративна відповідальність реалізується в установлених законом формах та порядку, чітко визначених адміністративно-процесуальними нормами; 12) суб'єктами адміністративно-правової відповідальності можуть бути як фізичні, так і юридичні особи (наприклад, при порушенні правил пожежної безпеки, законодавства про об'єднання громадян, тощо) [49, с. 20–21; 102].

Таким чином, адміністративна відповідальність за порушення законодавства у сфері кібербезпеки — це застосування до особи, що вчинила правопорушення, санкцій, передбачених нормами адміністративного права. Зазвичай санкції за вчинення адміністративного проступку носять матеріальний (грошовий) характер. Відзначимо, що у чинному Кодексі України про адміністративні правопорушення не виокремлено окремий розділ, який було б присвячено адміністративним проступкам за порушення законодавства у сфері кібербезпеки. Однак, окремими статтями така відповідальність все ж таки передбачена. Наприклад, стаття 51-2 КУпАП встановила, що незаконне використання об'єкта права інтелектуальної власності, зокрема: комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка, знака для товарів і послуг, топографії інтегральної мікросхеми, тощо, привласнення авторства на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом, — тягне за собою накладення штрафу від десяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовленої продукції та обладнання і матеріалів,

які призначені для її виготовлення; стаття 164^9 — розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних, упаковки яких не марковані контрольними марками або марковані контрольними марками, що мають серію чи містять інформацію, які не відповідають носію цього примірника, або номер, який не відповідає даним Єдиного реєстру одержувачів контрольних марок, — тягне за собою накладення штрафу від десяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією цих примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних; тощо [84].

Крім того, справедливо буде відмітити, що КУпАП містить більше сотні статей, якими врегульовані питання відповідальності за порушення порядку створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації [192, с. 81]. Такі правопорушення, на слушну думку Т. С. Перуна, можна поділити на три основні групи, а саме: а) забезпечення доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; б) забезпечення обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб або національній безпеці; в) забезпечення безпеки у сфері медіа-інформації [133].

Завершуючи розгляд адміністративної відповідальності за порушення законодавства у сфері забезпечення кібербезпеки в Україні, слід відзначити неоднозначність законодавства, яке визначає засади даного виду юридичної відповідальності у досліджуваній сфері. Враховуючи зростання кількості правопорушень у кіберпросторі (зокрема, за 2017 рік в Україні було вчинено понад 3 тисячі правопорушень у цій сфері), на сьогодні не викликає сумнівів необхідність систематизації положень про притягнення до адміністративної відповідальності осіб, що порушили законодавство про кібербезпеку. А

відтак, пропонуємо у чинному КУпАП передбачити окремий розділ, присвячений адміністративним проступкам у кіберпросторі.

І останній, найбільш «суворий», вид юридичної відповідальності за порушення законодавства у сфері кібербезпеки України — кримінальна. На думку А. В. Наумова, кримінальна відповідальність — це особливий правовий інститут, у межах якого здійснюється офіційна оцінка поведінки особи як злочинної. Кримінальна відповідальність матеріалізується в обвинувальному вироку суду і зазвичай включає засудження особи за вчинений злочин, призначення їй покарання, його відбування, судимість, тощо [125, с. 17]. П. М. Давидов вказує, що кримінальна відповідальність — це такий, що реалізується, покладається на винну у вчинені злочину особу, обов`язок, що полягає у перетерпіванні засудження, покарання, судимості; оскільки в законі кримінальна відповідальність не прирівнюється до покарання, обов`язковим і основним компонентом кримінальної відповідальності є засудження, яке визнається в теорії права елементом не лише кримінальної, але і будь-якої іншої юридичної відповідальності, а основним кримінально-процесуальним актом, в якому виражається осуд, є вирок [54, с. 35]. Таким чином, кримінальна відповідальність за порушення законодавства у сфері кібербезпеки України настає у випадку вчинення особою злочину, тобто вчинку, здійснення якого мало найбільш шкідливі наслідки для іншої особи, суспільства, держави, тощо. Такий злочин у досліджуваній сфері має назву «кіберзлочин» (комп’ютерний злочин).

За останні 10–15 років поняття «комп’ютерна злочинність» трансформувалось у термін «кіберзлочинність» — поняття, яке охоплює власне комп’ютерну злочинність та інші протиправні діяння, де комп’ютер є знаряддям або способом вчинення злочину проти власності, авторських прав, громадської безпеки, моралі, тощо. Відтак, кіберзлочин — це будь-який злочин, який може вчинятися за допомогою комп’ютерної системи або мережі, в рамках комп’ютерної системи або мережі чи проти інформації в

комп’ютерній системі або мережі. В принципі, цей термін охоплює будь-який злочин, який може бути скоєно в електронному середовищі [43]. Справедливо буде відзначити, що на сьогодні поняття «кіберзлочин» дістало законодавче закріплення, зокрема, у Законі України «Про основні засади забезпечення кібербезпеки України». Відповідно до вказаного нормативно-правового акта, кіберзлочин (комп’ютерний злочин) — суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена Законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [151].

Однією з найбільш характерних особливостей кримінальної відповідальності за кіберзлочини є те, що вона як у вузькому, так і широкому розумінні врегульовується Конвенцією про кіберзлочинність від 2001 року. При цьому, варто підкреслити, що кримінальне законодавства окремо взятих країн світу визначає карну відповідальність за кіберзлочини лише у вузькому розумінні, не є виключенням і Україна [67, с. 129]. Держави–члени Ради Європи та інші держави, які підписали цю конвенцію, обґрунтовують, що вона є необхідною 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 [92]. Вказаний вище міжнародний нормативно-правовий акт передбачає чотири групи злочинів, пов’язаних з використанням комп’ютерних технологій як інструменту їх учинення. До першої групи віднесено злочини проти конфіденційності, цілісності й доступності комп’ютерних даних і систем (протизаконний доступ,

протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв і комп'ютерних програм). До другої групи — злочини, пов'язані з використанням комп'ютерних засобів (підроблення, шахрайство). До третьої групи віднесено злочини, пов'язані зі змістом даних (дитяча порнографія). До четвертої — злочини, пов'язані з порушенням авторського права та суміжних прав [131, с. 5; 92].

Отже, підписуючи Конвенцію про кіберзлочинність, Україна взяла на себе зобов'язання привести вітчизняне законодавство у відповідність до її положень. Все це віднайшло своє відображення у Кримінальному кодексі України, зокрема, Розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем комп'ютерних мереж і мереж електрозв'язку». Відповідно до положень вказаного розділу, передбачаються наступні санкції за вчинення кіберзлочинів: «Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, — карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого. Стаття 361-1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, — караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на

строк до двох років, або позбавленням волі на той самий строк. Стаття 361-2. 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 п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. Стаття 362. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, — караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. Стаття 363-1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, — карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років; тощо» [97].

Втім, як справедливо відмічає Ю. Ю. Орлов, перелік кіберзлочинів не вичерпується діяннями, визначеними в розділі XVI Особливої частини КК України. Певні злочини, що існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. Використання комп'ютерів спрощує вчинення злочину або уможливлює його вчинення в нових формах. Отже, наголошує вчений, ці злочини можна розглядати як такі, що підпадають під дію конвенції. Зокрема, ідеться про такі злочинні діяння: різні види підроблення: грошей, цінних паперів, платіжних карток, знаків поштової оплати, марок акцизного збору,

контрольних марок, номерів вузлів та агрегатів транспортних засобів, документів на отримання наркотиків, інших документів, тощо (ст.ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України); шахрайство з різними предметами (ст.ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України); увезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України); порушення авторського права й суміжних прав (ст. 176 КК України) [131, с. 5; 97].

Завершуючи представлений підрозділ дисертаційного дослідження, слід констатувати, що питання юридичної відповідальності за порушення законодавства у сфері кібербезпеки України є недостатньо врегульованим, що беззаперечно можна вважати суттєвою прогалиною, яка сприяє зростанню рівня кіберзлочинності в нашій державі. Зокрема, питання притягнення правопорушника у сфері кібербезпеки до цивільної та адміністративної відповідальності регулюється цілою низкою нормативно-правових актів, в кожному із яких містяться різні підстави притягнення особи до відповідальності. Така розгалуженість, в свою чергу, ускладнює застосування стягнень до винних осіб органами державної влади. Таким чином, з огляду на все зазначене вище, вбачаємо за доцільне внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», зокрема, більш детально окреслити види правопорушень та кіберзлочинів, через які особу може бути притягнено до того чи іншого виду юридичної відповідальності [32]. Все вказане зробить відповідне законодавство більш узгодженим, а відтак, і позитивно вплине на якість забезпечення кібербезпеки в державі.

Все зазначене вище дає нам змогу виокремити найбільш характерні особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки:

– специфічний предмет правопорушення та/або кіберзлочину, яким є інформація, тобто відомості та/або дані, які зберігаються у мережі Інтернет або на якихось носіях (серверах, жорстких дисках, картах пам’яті, тощо);

– складність виявлення суб’єкта правопорушення, що потребує серйозного матеріально-технічного та кадрового забезпечення;

– найбільш поширеним видом відповідальності є кримінальна, що обумовлюється високим рівнем шкоди, в результаті здійснення кіберзлочину;

– зазвичай правопорушення у вказаній сфері спрямовуються не на конкретну особу, тобто не є персоніфікованими;

– шкода від вчинення кіберзлочину, зазвичай, має матеріальний характер, та не шкодить фізичному здоров’ю людини.

Висновки до розділу 2

Доведено, що суб’єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, так як, по-перше, відносини між ними будуються на основі влади і підпорядкування, а по-друге, останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством. Крім цього, аналіз адміністративно-правового статусу суб’єктів забезпечення кібербезпеки просто неможливо здійснювати поза межами адміністративної галузі права.

Визначено, що суб’єктами забезпечення кібербезпеки є державні органи та посадові особи останніх, наділені владними повноваженнями та відповідними обов’язками щодо охорони об’єктів кібербезпеки.

Наголошено, що всі суб’єкти забезпечення кібербезпеки наділені як комплексом специфічних, так і комплексом загальних повноважень. Серед загальних рис суб’єктів забезпечення кібербезпеки варто відзначити те, що вони: по-перше, в своїй діяльності використовують владний примус з метою

реалізації передбачених законодавством функцій; по-друге, суб'єкти забезпечення кібербезпеки перебувають у системному взаємозв'язку з іншими учасниками адміністративних правовідносин, який будується на засадах ієрархічності; по-третє, діяльність суб'єктів забезпечення кібербезпеки спрямовано не тільки на припинення правопорушень у цій сфері, а й на забезпечення умов, коли такі порушення неможливі, що реалізується шляхом проведення контрольних заходів і т.п.

Суб'єктів забезпечення кібербезпеки запропоновано об'єднати у дві групи: загальну та спеціальну. До загальної відносяться усі органи державної влади, органи місцевого самоврядування, 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. До кола спеціальних нами віднесено органи влади, котрі становлять систему суб'єктів кібербезпеки України, перелік яких закріплено в Закони України «Про основні засади забезпечення кібербезпеки України».

Під адміністративно-правовими формами забезпечення кібербезпеки України запропоновано розуміти зовнішній вираз діяльності уповноважених органів державної влади, який виявляється у вчиненні ними комплексу дій, які спрямовані на створення таких умов, за яких буде забезпечено безпеку комп'ютерних систем у всій країні в цілому.

Виокремлено та охарактеризовано такі форми забезпечення кібербезпеки України: а) нормотворчість (тобто прийняття нормативно-правових актів у сфері забезпечення кібербезпеки); б) прийняття індивідуальних актів у сфері забезпечення кібербезпеки.

Доведено, що нормотворчість є однією із ключових форм забезпечення кібербезпеки в Україні, оскільки за її допомогою вбачається можливим

створити таке правове поле, яке буде виключати будь-які можливості для суб'єктів відповідних правовідносин вчинити правопорушення у досліджуваній сфері. А відтак, нормотворчість, через процес створення правового припису, дозволяє досягти певної поведінки людей у конкретній сфері суспільних правовідносин, що, в свою чергу, має важливий соціальний, економічний та політичний ефект. Якісна та своєчасна нормотворча діяльність дозволяє не лише забезпечити необхідний стан якоїсь сфери суспільних відносин, вона також сприяє підвищенню рівня довіри до суб'єкта нормотворчості (держави), а також підвищує відчуття захищеності громадян у своїй країні.

Акцентовано увагу, що індивідуальні акти у сфері забезпечення кібербезпеки дозволяють оперативно вирішити нагальні проблеми, що з'являються у вказаній сфері суспільних відносин. Їх перевага полягає у тому, що вони спрямовані на конкретного суб'єкта, а тому за їх допомогою можливо вирішити більш конкретні проблемні питання

Визначено, що адміністративний договір, як адміністративно-правова форма забезпечення кібербезпеки, представляє собою добровільну угоду між декількома суб'єктами адміністративного права, які наділені владними повноваження, з метою координації їх спільної діяльності, що в результаті призводить до виникнення, зміни або припинення взаємних прав та обов'язків сторін відповідного договору. За допомогою адміністративного договору вбачається можливим скоординувати роботу різних державних структур, однак, лише у випадках, коли в цьому існує об'єктивна необхідність, а координація діяльності призведе до отримання кінцевого бажаного результату.

З'ясовано, що правореалізація передбачає безпосереднє втілення норм адміністративного права в діяльність суб'єктів, функції яких полягають у забезпеченні кібербезпеки в Україні. При цьому, кожен із таких суб'єктів

повинен в обов’язковому порядку дотримуватись визначених суб’єктивних прав та виконання своїх зобов’язань.

Зроблено висновок, що адміністративно-правові форми є об’єктивним практичним відображенням дій, що вчиняють суб’єкти, які уповноважені реалізовувати заходи із забезпечення кібербезпеки в Україні. Можна також говорити про те, що форми діяльності відображають характерні особливості правового статусу конкретного суб’єкта, адже в них фактично відображається те, яким чином вони (суб’єкти) реалізують свою суб’єктивні права та юридичні обов’язки.

На основі аналізу норм чинного законодавства та наукових поглядів вчених виокремлено та охарактеризовано такі методи забезпечення кібербезпеки: а) адміністративний примус (ключове значення вказаного методу полягає у тому, що він спрямований на попередження виникнення правопорушень у досліджуваній сфері. Проте, застосування методу адміністративного примусу не лише спрямоване на попередження виникнення протиправної поведінки, а й покликане забезпечити захист інформаційних, приватних, комп’ютерних, ресурсів, тощо); б) метод позитивного зобов’язання; в) метод дозволу та заборон; г) метод адміністративного контролю; ґ) метод контроль доступу; д) метод ліцензування діяльності; е) метод сертифікації та стандартизації; є) реєстраційний метод.

Запропоновано на законодавчому рівні закріпити адміністративно-правові форми та методи забезпечення кібербезпеки України.

Під юридичною відповідальністю за порушення законодавства у сфері кібербезпеки України запропоновано розуміти застосування заходів примусового характеру, які визначені нормами чинного законодавства, до осіб, що вчинили правопорушення у кіберпросторі. Заходи юридичної відповідальності застосовуються лише у випадку винного діяння

відповідного суб'єкта, а санкції повинні відповідати рівню шкоди вчиненого проступку.

Визначено, що адміністративна відповідальність за порушення законодавства у сфері кібербезпеки — це застосування до особи, що вчинила правопорушення, санкцій, передбачених нормами адміністративного права. Зазвичай санкції за вчинення адміністративного проступку носять матеріальний (грошовий) характер.

Констатовано, що питання юридичної відповідальності за порушення законодавства у сфері кібербезпеки України є недостатньо врегульованим, що беззаперечно можна вважати суттєвою прогалиною, яка сприяє зростанню рівня кіберзлочинності в нашій державі. Зокрема, питання притягнення правопорушника у сфері кібербезпеки до цивільної та адміністративної відповідальності регулюється цілою низкою нормативно-правових актів, в кожному із яких містяться різні підстави притягнення особи до відповідальності. Така розгалуженість, в свою чергу, ускладнює застосування стягнень до винних осіб органами державної влади.

Запропоновано внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», зокрема, більш детально окреслити види правопорушень та кіберзлочинів, через які особу може бути притягнено до того чи іншого виду юридичної відповідальності. Все вказане зробить відповідне законодавство більш узгодженим, а відтак, і позитивно вплине на якість забезпечення кібербезпеки в державі.

Виокремлено найбільш характерні особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки:

а) специфічний предмет правопорушення та/або кіберзлочину, яким є інформація, тобто відомості та/або дані, які зберігаються у мережі Інтернет або на якихось носіях (серверах, жорстких дисках, картах пам'яті, тощо);

б) складність виявлення суб'єкта правопорушення, що потребує серйозного матеріально-технічного та кадрового забезпечення;

в) найбільш поширеним видом відповідальності є кримінальна, що обумовлюється високим рівнем шкоди в результаті здійснення кіберзлочину;

г) зазвичай правопорушення у вказаній сфері спрямовуються не на конкретну особу, тобто не є персоніфікованими;

ґ) шкода від вчинення кіберзлочину зазвичай має матеріальний характер та не шкодить фізичному здоров’ю людини.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВИХ ЗАСАД ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

3.1 Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні

На сьогоднішній день вже ні в кого не викликає сумнівів, що існуючий в Україні механізм забезпечення кібербезпеки є недосконалим та потребує удосконалення. В цьому контексті відмітимо, що визначення шляхів удосконалення такого механізму є неможливим без вивчення зарубіжного досвіду, що особливо є актуальним у прагненні України адаптувати вітчизняне законодавство до європейських та світових стандартів. Саме тому в контексті представленого наукового дослідження ми не лише приділимо увагу досвіду найспішніших країн Європи, а й розглянемо інші провідні держави світу, наприклад, США, Японію, Китай, тощо. Розглядаючи країни Європи, в першу чергу приділимо увагу досвіду Великобританії, адже сьогодні в цій країні питання кібербезпеки виходить на першочергові місця, що підтверджується тим, що у листопаді 2016 року Уряд Великої Британії оприлюднив 5-річний план реалізації Стратегії національної кібербезпеки і виділив на це рекордні 1,9 млрд. фунтів.

Основними законодавчими актами у сфері забезпечення кібербезпеки у Великобританії є Конституція — як Основний Закон, та Закони «Про боротьбу з комп'ютерними злочинами» (1990); «Про захист даних» (1998); «Про шахрайство» (2006), тощо. Британська Конституція представляє собою сукупність нормативно-правових актів, судових прецедентів, конституційних угод, доктринальних джерел, які встановлюють права і свободи людини, визначають порядок формування і повноважень органів публічної влади у сфері ІБ, а також принципи взаємовідносин між державою, суспільством і

людиною. Відсутність конституції у вигляді єдиного писаного акта дозволяє стверджувати, що конституція є неписаною за формою. Конституція складається з наступних частин: а) статутне право; б) прецедентне право; в) доктринальні джерела або труди авторитетних науковців у галузі юриспруденції; г) конституційні угоди [134]. Що ж стосується вказаних вище законів, то їх положення, як правило, містять норми, що визначають кримінальну відповідальність за вчинення кіберзлочинів.

Основним же документом, що спрямований на забезпечення кібербезпеки у Великобританії, є Стратегія національної кібербезпеки 2016–2021 рр., яку було прийнято замість аналогічної стратегії 2011–2015 рр. Основна мета Стратегії на 2021 рік полягає в тому, щоб зробити Великобританію безпечною і стійкою до кіберзагроз, процвітаючою і впевненою в цифровому світі. Для цього, на думку законодавців країни, є необхідним: 1) виділяти достатньо коштів для захисту Великобританії від розвитку кіберзагроз; ефективно реагування на інциденти і забезпечувати захист і стійкість мереж і даних у Великобританії; 2) виявляти, розуміти, розслідувати ворожі дії, що вживаються проти Британії; 3) розробляти та сприяти розвитку інноваційних технологій та індустрії кібербезпеки; 4) сприяти розвитку кадрового потенціалу. Слід також відмітити, що ця Стратегія стосується кіберзлочинності в контексті двох взаємопов’язаних форм злочинної діяльності: 1) кіберзалежність злочинів, тобто злочинів, які можуть бути здійснені тільки з використанням пристроїв інформаційно-комунікаційних технологій (ІКТ), де ці пристрої є інструментом для вчинення злочину і метою злочину (наприклад, розробка та поширення шкідливого програмного забезпечення для фінансової вигоди, зламати, щоб вкрасти, пошкодити, спотворити або знищити дані та/або мережу або діяльність); а також 2) злочини, пов’язані з використанням кібератаки, — традиційні злочини, які можуть бути збільшені в масштабі або охоплені за

допомогою комп’ютерів, комп’ютерних мереж або інших видів ІКТ (таких як шахрайство з використанням кібертехнологій і крадіжка даних).

Відповідно до положень чинного законодавства, основний обов'язок уряду Великобританії полягає в тому, щоб захистити країну від нападів інших держав, захистити громадян і економіку від шкоди і встановити внутрішні і міжнародні рамки для захисту інтересів країни. Будучи власником значних даних і постачальником послуг, уряд приймає суворі заходи для забезпечення гарантій для своїх інформаційних активів. Уряд також несе відповідальність за консультування та інформування громадян про стан виконання Національної стратегії кібербезпеки 2016 року. Крім того, уряд повинен інформувати громадян про те, що потрібно зробити, щоб захистити себе в Інтернеті, а за необхідності встановити стандарти, дотримання яких Великобританія очікує від ключових компаній і організацій. В Стратегії підкреслюється, що хоча ключові сектори економіки країни знаходяться в приватних руках, уряд в кінцевому рахунку несе відповідальність за забезпечення національної безпеки.

Особливу увагу слід звернути на те, що з метою реалізації Стратегії 1 жовтня 2016 року було створено Національний центр кібербезпеки (NCSC). NCSC надає унікальну можливість для створення ефективних партнерських відносин в області кібербезпеки між урядом, промисловістю і громадськістю, щоб у результаті забезпечити безпеку Великобританії в Інтернеті. Вперше ключові сектори зможуть безпосередньо взаємодіяти з Центром для отримання найкращих можливих рекомендацій і підтримки щодо захисту мереж і систем від кіберзагроз. NCSC забезпечує: 1) єдине джерело консультацій для попередження загрози кібербезпеки і забезпечення інформації; 2) ефективну та прозору роботу уряду по боротьбі з кіберзагрозами, працюючи рука об руку з промисловістю, науковими колами та міжнародними партнерами, щоб захистити Великобританію від

кібератаки. В процесі виконання Стратегії буде встановлено поетапний підхід до побудови можливостей NCSC.

Не можна не звернути увагу на той факт, що Британське Національне агентство по боротьбі зі злочинністю (NCA), в рамках Стратегії національної кібербезпеки 2016 року, відкрило перший реабілітаційний центр для людей, які були засуджені до ув'язнення за кіберзлочини. Як пише BBC, у ньому їх вчать використовувати свої навички у більш конструктивних цілях та готують до роботи в спецслужбах. Нині центр відвідують восьмеро молодих людей, які потрапили в поле зору правоохоронців за нелегальні дії в он-лайні ще у підлітковому віці. Деякі з них ламали сайти чи сервери, здійснювали кібератаки, змушували користувачів розкривати свої персональні дані, зламували шкільні мережі або ж іншим чином порушували британське законодавство про використання комп'ютерів [193]. Серед слухачів центру є й ті, хто в грудні 2016 року брав участь в атаці на британського провайдера TalkTalk. Тоді було зламано майже 5 мільйонів роутерів. За словами самих хлопців, вони здебільшого робили подібні дії «для веселощів». Більшість учасників центру отримали умовні терміни, але їх також зобов'язали ходити на реабілітацію кожні вихідні. Вони відвідують лекції про судово-медичний аналіз та захист мереж компаній від атак. Також їх вчать шукати лазівки в системах безпеки і повідомляти про них керівництву за винагороду. Крім того, хакерам розповідають про вакансії в службі кібербезпеки [193].

Взагалі глибинний аналіз Стратегії національної кібербезпеки Великобританії на 2016–2021 роки дає змогу говорити про те, що вона містить низку інноваційних та цікавих положень та взагалі потребує окремого наукового дослідження. Позитивними моментами вказаної Стратегії, на які хотілося б також звернути увагу, є те, що в ній: 1) визначено та закріплено офіційне тлумачення низки понять у сфері забезпечення кібербезпеки (наприклад, кібернетична оборона, активна кібернетична оборона, тощо); 2) детально окреслено напрямки та етапи запровадження

інновацій у сфері забезпечення кібербезпеки; 3) суттєва увага приділена навчанню населення щодо того, як захистити себе від можливих порушень їх прав у досліджуваній сфері; 4) виокремлено напрямки навчання персоналу, адже забезпечення кібербезпеки є неможливим без відповідного кадрового забезпечення.

Наступна європейська країна, досвіду якої ми приділимо увагу, — Німеччина, адже саме ця держава є однією з ключових країн, форми державно-приватного партнерства якої працюють як один із основних інструментів ефективної системи кіберзахисту країни [21]. Однак, в останні декілька років у Німеччині спостерігається різке зростання кіберзлочинності. 2016 року кількість скоєних кримінальних діянь з використанням Інтернет-технологій сягнула 82649 випадків, у той час як в 2015 році поліція зареєструвала 45793 кіберзлочини. Водночас, дані кримінальної статистики вказують на зростання показників розкриття подібних злочинів. У цілому кількість розкритих правопорушень такого типу зросла на 5,9%, досягнувши рівня в 38,7%. І така тенденція в державі продовжується й досі [194]. В силу цього А. Меркель наголосила, що кібербезпека має «надзвичайно важливе значення». Вона зазначила, що уряд Німеччини актуалізував стратегію кібербезпеки. Крім того, федеральний уряд готовий співпрацювати з містами та громадами. Вона також закликала представників органів місцевої влади та підприємств звертатися до Федеральної служби безпеки в сфері інформаційних технологій у разі виявлення підозрілих випадків [121].

Як і у Великобританії, у 2011 р. в Німеччині було прийнято Стратегію кібербезпеки Німеччини, відповідно до якої федеральний уряд застосовує заходи на основі вже створених структур до відповідних рівнів загроз за наступними стратегічними напрямками [63, с. 113–115]:

1. Захист найважливіших інформаційних інфраструктур. В центрі уваги кібербезпеки лежить захист найважливіших інформаційних структур, адже

безпека має важливе значення в постійно зростаючих майже всіх найважливіших інфраструктурах [218; 63, с. 114].

2. IT-системи безпеки ФРН. Захист інфраструктур потребує більшої надійності IT-систем громадян, а також малих та середніх підприємств. Користувачі потребують інформацію, яка відповідала б їхнім потребам і не суперечила б сама собі про ризики, які пов'язані з IT-системами і самостійно застосовувати заходи безпеки, щодо безпеки належної поведінки у кіберпросторі.

3. Посилення IT-безпеки в публічному управлінні. Публічне управління ще сильніше захистить свої IT-системи. Державні установи повинні бути зразком щодо захисту даних. Основою електронного обміну даними і вербальної комунікації буде загальна, універсальна і надійна мережева інфраструктура Федеральної адміністрації («федеральна мережа») [218; 63, с. 114].

4. Для оптимізації оперативної співпраці усіх державних установ і покращення координації заходів щодо захисту проти IT-випадків було створено Національний центр кіберзахисту. Він працює під керівництвом Федерального відомства з інформаційної безпеки (BSI) і за безпосередньою участю Федерального відомства захисту конституції (BfV), а також Федерального відомства з питань захисту населення і допомоги при стихійних лихах (BBK) [224; 63, с. 113].

5. Створено Національну раду кібербезпеки, діяльність якої спрямована на виявлення і усунення конструктивних причин криз — важливий превентивний інструмент у кібербезпеці. Тому, відповідно до Стратегії, буде організована співпраця в рамках федерального уряду, а також між державою і економікою під відповідальністю уповноважених осіб федерального уряду з IT–питань. Представники — відомство федерального канцлера, а також заступник міністра, департаменти закордонних справ, Міністерство внутрішніх справ, Міністерство оборони, Міністерство економіки і

технології, Міністерство юстиції, Міністерство фінансів, Міністерство освіти, а також представники інших державних органів.

6. Ефективна боротьба зі злочинністю у кіберпросторі. Посилюються можливості правоохоронних органів, Федеральної служби безпеки в сфері ІТ і економіки в контексті подолання ІКТ-злочинності (стосовно захисту від шпіонажу і диверсій).

7. Ефективна співпраця у кібербезпеці в Європі та у світі. Безпека в глобальному кіберпросторі досягається лише за допомогою сукупності узгоджених засобів та методів на національному і міжнародному рівнях.

8. Використання надійних і достовірних інформаційних технологій. Потрібно забезпечити можливість доступу до надійних ІТ-систем і ІТ-компонентів. Розвиток інноваційних програм захисту для покращення безпеки буде прискорюватись, враховуючи суспільні та економічні аспекти. Тому ФРН буде продовжувати розвивати відповідні дослідження в ІТ-безпеці і найважливіших інфраструктурах [63, с. 113–115].

У липні 2015 р. у Німеччині був прийнятий Закон «Про інформаційну безпеку» з метою запобігання атакам на важливі інформаційні системи. Закон визначає мінімальні стандарти кібербезпеки для більш ніж 2 тисяч компаній — операторів критичної інфраструктури. Відповідно до закону, ці мінімальні вимоги до безпеки мають забезпечуватися шляхом вдосконалення доступності, автентичності, конфіденційності та цілісності ІТ-безпеки у всій Німеччині; підвищення безпеки Інтернету для громадян; кращого захисту критично важливої інфраструктури національного значення [225; 21]. Цей закон мав на меті врегулювати низку попередніх недоопрацювань правових положень, втім, для бізнесу та підприємств галузі залишається під питанням, хто є частиною KRITIS і якими є наслідки закону про ІТ-безпеку. Відтак, за відгуком індустрії та бізнес-спільноти, визначення оператора критичної інфраструктури не є достатньо прозорим, зокрема, через те, що у законі 2015 р. для компаній малого і середнього бізнесу не було розмежування

сфери застосування закону. За опитуванням PwC36, близько 18% компаній, зареєстрованих в Німеччині, юридично можуть підпадати під поняття оператора, визначеного у законодавстві. Згідно із аналізом KPMG37, кількість «непевних» компаній є ще вищою [225; 21].

Таким чином, в Німеччині досить багато уваги приділяється питанню забезпеченню кібербезпеки, про що яскраво свідчить розгалужена система органів державної влади у досліджуваній сфері. Крім того, в державі активно застосовується міжнародне співробітництво, що, в свою чергу, дозволяє більш ефективно та оперативно виявляти загрози у досліджуваній сфері та розвивати вітчизняне законодавство і технології. Із позитивного також слід вказати те, що в країні постійно відбувається розширення заходів, спрямованих на реалізацію державної політики у сфері забезпечення кібербезпеки.

Розглядаючи досвід Франції, відзначимо, що базовими нормативними актами, в яких визначаються стратегічні напрями державної політики Франції у сфері забезпечення безпеки, є Біла книга оборони та національної безпеки від 2008 р. та Національна стратегія цифрової безпеки 2015 року. Так, в Білій книзі серед найбільш ймовірних загроз територіям Франції та європейській спільноті (тероризм, використання балістичних ракет, організована злочинність, ризики природного характеру та ускладнення епідеміологічної ситуації у великих містах, прихована імміграція) названі: масштабні атаки на інформаційні системи; шпіонаж та стратегічний вплив [134]. Що ж стосується Стратегії, то вона покликана супроводжувати цифровий перехід французького суспільства і відповідає новим викликам, які пов’язані зі зміною використання цифрових технологій і пов'язаними з ними загрозами за п’ятьма цілями: 1) гарантувати національний суверенітет; 2) забезпечити сильну відповідь на акти кіберзлочинності; 3) інформувати громадськість в цілому; 4) забезпечити цифрову безпеку, адже це є конкурентною перевагою для французьких підприємств; 5) посилити позиції

Франції на міжнародній арені. Відповідно до національної стратегії кібербезпеки, французька держава працює над забезпеченням безпеки ІТ-систем в напрямку колективного реагування, цифрової довіри, що є необхідним для стабільності держави, економічного розвитку і захисту громадян.

Таким чином, зміцнення стратегічної стабільності і міжнародної безпеки в кіберпросторі є однією з ключових цілей Франції. Тому вона відіграє активну роль в просуванні безпечного, стабільного і відкритого кіберпростору. Міністерство Європи і закордонних справ координує роботу Франції в сфері «кібердипломатії». Франція особливо активна в рамках ООН, де обговорюються правила відповідальної поведінки в кіберпросторі. Франція брала участь в останніх п’яти групах урядових експертів ООН (GGE) з кібербезпеки, чия робота допомогла розмістити кіберпростір в міжнародній системі, створеній Статутом Організації Об’єднаних Націй, і направляти держави до запобігання, співпраці і нерозповсюдження в кіберпросторі злочинності.

Досліджуючи зарубіжний досвід забезпечення кібербезпеки, не можна не звернути увагу на країну–сусіда Польщу, яка на сьогодні активно займається розвитком кіберзахисту на державному рівні [80]. За прогнозами аналітиків, через два-три роки Польща буде лідером в ІТ-галузі в країнах Центрально-Східної Європи. А вже нині півмільйона осіб працює в польському секторі високих технологій, а вартість ринку ІТ-послуг у Польщі сягнула майже 3,5 мільярда доларів і продовжує зростати. Динамічний розвиток цього сектору приваблює в країну закордонних інвесторів та програмістів–іноземців, зокрема, українців. Причини успіху польського ІТ-сектору аналітики вбачають у продуманій політиці державної влади та органів місцевого самоврядування. Якщо тенденції розвитку польського ІТ-сектору зберігатимуться, то в 2019 році його вартість досягне 4 мільярдів доларів, тоді як ринок ІТ-послуг усієї Центрально-Східної Європи

коштуватиме 11 мільярдів доларів. Такі дані оприлюднила дослідницька фірма IDC. Через позитивну динаміку багато фірм з різних країн світу вирішують розмістити свої підприємства саме у Польщі [166].

Тривалий час зусилля влади Польщі щодо боротьби з кіберзагрозами були недостатніми. Однак, низка масштабних атак на тлі відсутності єдиного координованого центру ухвалення рішень стали стимулом для дій. Отже, що зробила Польща? [216]. По-перше, ухвалила зміни до законодавства, які дозволяють запроваджувати у країні надзвичайний стан в разі атаки у віртуальному просторі. Такими юридичними новаціями можуть похвалитися небагато держав. По-друге, влада погодилася з недоцільністю функціонування кількох інституцій з боротьби з кіберзагрозами, які лише дублювали одна одну. У 2011 році було створене Міністерство адміністрації і цифровізації, завданнями якого стали забезпечення кібербезпеки у військовій сфері, захист конфіденційності громадян, побудова національної освітньої платформи, залучення до Інтернету людей похилого віку і жителів віддалених районів країни. По-третє, в рамках Міністерства цифровізації у 2016 році створили Національний центр кібербезпеки. Його ключовим завданням стало попередження загроз, реакція на них та координація дій. Робота центру — вдалий приклад державно-приватного партнерства у сфері кіберзахисту. Працює центр цілодобово. По-четверте, Польща опрацювала нову стратегію кібербезпеки. Вона передбачає, що до 2022 року влада гарантуватиме безпеку громадян, суб’єктів економічної діяльності і державних установ у галузі кібербезпеки [216]. Більш конкретними цілями вказаної стратегії є: 1) досягти здатності координувати дії на національному рівні, спрямовані на запобігання, виявлення, боротьбу та мінімізацію наслідків та/або інцидентів, що порушують безпеку систем ІКТ, необхідних для функціонування держави; 2) посилення здатності протистояти кіберзагрозам; 3) підвищення національного потенціалу та компетенції в

галузі безпеки в кіберпросторі; 4) формування сильної міжнародної позиції Республіки Польща у сфері кібербезпеки.

Окрему увагу хотілося б звернути на Міністерство адміністрації і цифровізації, до завдань якого відносяться: розробка та реалізація стратегічних документів і правових актів в області кібербезпеки, проведення національного і міжнародного співробітництва, розробка керівних принципів для створення відповідних заходів щодо захисту інформаційних систем, підготовка аналізу щодо стану кібербезпеки на національному рівні та ризиків для держави кібербезпека, а також розробка центральних навчальних планів, вправ та випробувань. Міністерство активно співпрацює з іншими відомствами, університетами, інститутами, неурядовими організаціями та приватним сектором при виконанні завдань. Міністерство у співпраці з іншими організаціями є вкрай важливими суб'єктами для забезпечення безпеки кіберпростору, зокрема, підготовлено два документи для вдосконалення та розвитку національної системи кібербезпеки. 27 квітня 2017 р. Рада міністрів прийняла стратегічний документ — Національні рамки політики кібербезпеки Республіки Польща на 2017–2022 роки. 31 жовтня минулого року політика була спрямована на громадські консультації та міжміністерські консультації щодо проекту закону про національну систему кібербезпеки [220].

Наступною країною, досвіду якої ми хотіли б приділити увагу в контексті представленої наукової праці, є Сполучені Штати Америки. Сьогодні законодавство США у сфері забезпечення інформаційної безпеки складається з федеральних законів та законів штатів, які створили правову основу для формування єдиної державної політики в галузі захисту інформації для забезпечення інтересів національної безпеки. Це, насамперед, такі Закони: «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.), «Про комп'ютерне шахрайство та зловживання» (1986 р.), «Про свободу інформації» (1967 р.), «Про

висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю» (1974 р.), «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп'ютерних систем» (1987 р.) [28].

Нова американська адміністрація послідовно підтримує напрацьовані раніше зусилля. Наприклад, наприкінці липня 2018 року у Вашингтоні було оголошено про зміну статусу Кіберкомандування ЗС США. Перш за все, цю структуру планується вивести з підпорядкування Стратегічному командуванню ЗС США та підняти її на рівень окремого функціонального командування збройних сил. Це дозволить централізувати керівництво кібернапрямом з боку Міноборони та Об'єднаного комітету начальників штабів США. Тепер Кіберкомандування отримає більші повноваження щодо розвитку спроможностей діяти в кіберпросторі, підготовки кадрів, виконання бюджету, безпосереднього оперативного планування дій в кіберпросторі та їх реалізації. Також було оголошено про відокремлення Кіберкомандування від Агентства національної безпеки. Не є таємницею, що до теперішнього часу посаду керівника обох відомств (на основі суміщення) займала одна людина. Але тепер очікується призначення двох окремих керівників. Експерти оцінили таке рішення переважно як позитивний крок до розширення потенціалу США щодо дій в кіберпросторі [79]. Одночасно тривають зміни на рівні видів американських збройних сил США. Наприклад, в Армії США (тобто в сухопутних військах) за кілька останніх років також відбулося перезавантаження кібернапряму. Усвідомлення нових загроз разом із розумінням цінності власних операцій в кіберпросторі у вересні 2014 року призвело до появи директиви про створення фактично нового роду військ — Кіберкомандування сухопутних військ. Причина такого кроку дуже нагадує українські реалії: існувало безліч невеликих підрозділів різної підпорядкованості, але їхні зусилля не були об'єднаними та мали відношення переважно до розвідників або зв'язківців. Створення нового роду військ

дозволило інтегрувати підрозділи для спільних дій та розширити можливості для активного впливу в кіберпросторі. На сьогодні Кіберкомандування сухопутних військ вже має у підпорядкуванні щонайменше дві бойові структури рівня бригади [79].

Окремо хотілося б звернути увагу на те, що у Конгресі представлений законопроект, що передбачає створення посади посла США по кіберпростору, а також впровадження американської міжнародної кібердипломатії. У разі прийняття закону Держдепартамент США буде зобов'язаний включати в щорічні доповіді про дотримання прав людини в світі оцінки про свободу Інтернету. Останнім часом відносини Росії, Китаю і США помітно погіршилися, особливо стосовно кіберпростору. США звинувачують російську владу у втручанні у вибори Президента навесні, влітку і восени минулого року, що виразилося у зломі пошти штабу кандидата в Президенти Хілларі Клінтон, а також створенні фейкових акаунтів в соціальних мережах і спробах впливати на думку виборців через рекламу на Facebook [217, с. 31]. Якщо ж вказаний законопроект буде запроваджено у життя, то це в кінцевому результаті суттєво вплине на забезпечення кібербезпеки не лише в США, а й в усьому світі.

Таким чином, на сьогодні не викликає сумніву, що США є тією державою, яка володіє всіма необхідними матеріальними та технічними ресурсами для того, щоб забезпечити необхідний рівень кібербезпеки у своїй державі та допомогти у цьому іншим країнам світу, в тому числі і Україні. Крім того, у розпорядженні Кіберкомандування і спецслужб США сьогодні є достатній арсенал засобів протидії, які розроблені за попередні роки. Слід також відмітити, що в Сполучених Штатах особлива увага приділяється навчанню населення того, як захистити себе від правопорушень у досліджуваній сфері, що, в свою чергу, беззаперечно впливає на загальний стан забезпечення кібербезпеки у державі. З позитивного боку хотілося б

відмітити активну діяльність спецслужб у сфері забезпечення кібербезпеки, досвід роботи яких, беззаперечно, був би корисним і для нашої держави.

Ще одна країна, на яку не можна не звернути увагу, — Японія. Як і більшість розвинених країн світу, Японія має спеціальний закон про кібербезпеку під назвою «Основний закон про кібербезпеку», який був прийнятий 6 листопада 2014 року (і оприлюднений 12 листопада 2014 року). Основний закон про кібербезпеку — це перший закон про захист кібербезпеки, який був прийнятий серед країн «Великої сімки». Ключовим завданням вказаного нормативно-правового акта є забезпечення кібербезпеки, а також забезпечення вільного розповсюдження інформації. Мета Основного закону про кібербезпеку полягає в тому, щоб поширювати політику, пов’язану з кібербезпекою, всебічно та ефективно, а також сприяти створенню більш енергійного та такого, що постійно розвивається, економічного суспільства, що, як наслідок, сприяє національній безпеці Японії [221]. Слід підкреслити, що наразі в державі є інші закони, що стосуються кіберзлочинності, зокрема, це: Кримінальний кодекс, Закон про недобросовісну конкуренцію, Закон про несанкціонований доступ до комп’ютерних прав, Закон про спеціальний захист, Закон про захист особистої інформації, що був прийнятий ще у 2003 році з метою захисту особистої інформації та ідентифікації; у 2013 році було прийнято Закон про соціальний захист та податкове навантаження [221].

Уряд Японії нещодавно розгорнув план своєї наступної стратегії кібербезпеки. Цей документ має на меті визначити пріоритети в галузі кібербезпеки в Японії. Уряд оновлює свою стратегію кожні кілька років з моменту випуску першої в 2013 році. Нова стратегія спрямована на покращення стану кібербезпеки та відповідної інфраструктури, а також на заохочення японського бізнесу до досягнення найкращих практик в галузі кібербезпеки, що сприятиме економічному зростанню та інноваціям в Японії. Основна увага в новій стратегії приділяється поліпшенню кібербезпеки в

приватному секторі, адже на сьогодні японська промисловість відстає від американських та європейських аналогів. Згідно з державною статистикою, лише 55% японських компаній проводять оцінку ризику кібербезпеки, порівняно з приблизно 80% у Сполучених Штатах та 65% у Європі. Аналогічним чином, лише 27 відсотків японських компаній мають у штаті працівника з питань інформаційної безпеки (CISO), що є критичною позицією, яка, як правило, контролює зусилля компанії з кібербезпеки. Для порівняння, 78% американських компаній та 67% європейських компаній мають CISO. На відміну від Сполучених Штатів, інтеграція кібербезпеки в корпоративне управління є відносно новою концепцією в Японії [222]. А тому стратегія кібербезпеки на 2019 р. закликає бізнес-лідерів підвищити обізнаність та інвестувати більше в кібербезпеку. Однак, Японія потребує більше, ніж просто податкових чи фінансових стимулів. Необхідною є частіша та більш продуктивна взаємодія між урядом та промисловістю, що, в свою чергу, вимагає від країни створення кардинально нових органів державної влади у цій сфері, а також навчання професійних кадрів, консолідації бюджетів, щоб зрештою конкурувати з іншими державами світу.

І остання країна, якій ми приділимо увагу, — Китайська Народна Республіка, діяльність якої у сфері забезпечення кібербезпеки пов’язана в першу чергу із жорстким контролем над будь-якою інформацією у мережі Інтернет. 7 листопада 2016 року Уряд Китаю схвалив новий закон щодо кібербезпеки, спрямований на подальше посилення і централізацію державного контролю над Інтернетом, в тому числі над роллю, яку відіграють іноземні компанії в китайському кіберпросторі. Закон, прийнятий в постійному комітеті законодавчого органу Китаю, дає завдання установам і підприємствам поліпшити їх здатність захищатися від мережевих вторгнень, вимагаючи перевірки безпеки обладнання і даних в стратегічних секторах. Закон, зокрема, містить положення, що зобов’язує інтернет-операторів надавати «технічну допомогу» владі в справах, пов’язаних з національною

безпекою. Він також вимагає перевірки безпеки устаткування для «критичної інфраструктури», яка визначається як така, що стосується інформаційних послуг, енергетики, транспорту, фінансів та інших важливих секторів [78]. Під час розробки закон критикували деякі іноземні бізнес-групи і технічні експерти, називаючи його основою для подальшого відгородження вже ізольованого Інтернету у Китаї. Китайські законодавці описали закон як необхідність для зміцнення безпеки в Інтернеті у часи поширення великої кількості загроз [78].

Не можна не звернути увагу на те, що в Китаї особлива увага приділяється кадровому забезпеченню у досліджуваній сфері. Вказане підтверджується тим, що в країні розпочату будівництво першого інституту з підготовки фахівців кібербезпеки, на який буде витрачено близько 800 млн дол. США, а до 2027 року в КНР планується побудувати 4–6 таких навчальних закладів. Все це, беззаперечно, підтверджує серйозність намірів країні щодо забезпечення кібербезпеки. А відтак, незважаючи на те, що в більшості країн світу політика Китаю вбачається н вірною та такою, що суперечить деяким міжнародним нормативно-правовим актам, втім, не можна не погодитись, що така політика країни є доволі ефективною, що в тому числі підтверджує статистика вчинення кіберзлочинів у державі [33].

Таким чином, узагальнюючи весь наведений матеріал у представленому підрозділі дисертаційного дослідження, можемо із впевненістю констатувати, що на сьогодні світові тенденції розвитку інформаційного суспільства спонукають всі держави світу для прийняття заходів щодо забезпечення кібербезпеки. Не є виключенням і Україна, яка нині знаходиться лише на перших етапах розвитку цього інституту. Аналіз досвіду вказаних вище країн дає змогу виокремити наступні напрямки розвитку інституту забезпечення кібербезпеки в Україні:

– по-перше, необхідно збільшити фінансування суб’єктів, діяльність яких спрямована на забезпечення кібербезпеки в державі;

– по-друге, слід покращити якість освіти працівників кіберполіції;

– по-третє, кардинального оновлення потребує Стратегія кібербезпеки України. На наше переконання, вона повинна бути ширшою та охоплювати більше коло питань у цій сфері а не обмежуватись лише базовими питаннями. В цьому контексті цікавим є досвід Великобританії та Німеччини, чиї стратегії забезпечення кібербезпеки охоплюють практично всі питання та є основними документами у цій сфері;

– по-четверте, необхідно розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки, не обмежуючись співпрацею з однією конкретною країною (в нашому випадку — США);

– по-п’яте, необхідно посилити контроль у мережі Інтернет (на прикладі Китаю). Така наша пропозиція в першу чергу обґрунтовується тим, що на сьогоднішній день в мережу «викидається» дуже багато так званих «фейкових» новин, які лише вводять в оману населення та підривають довіру до окремих органів державної влади (досить часто ними є правоохоронні органи) та держави взагалі.

3.2 Напрямки удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні

В ході проведення дисертаційного дослідження ми неодноразово наголошували, що законодавство, яке регулює забезпечення кібербезпеки в Україні, є недосконалим та потребує удосконалення, що, в свою чергу, обумовлює необхідність проведення ґрунтовних наукових досліджень, присвячених вказаній проблемі. В першу чергу відзначимо, що наявність недоліків у чинному законодавстві пов’язана з існуванням в ньому такого явища як «прогалини». У найбільш загальному розумінні «прогалина» — це пропуск у змісті чого-небудь, те, що потребує заповнення. Зазначений термін

активно використовується саме в юридичній літературі у сполученні із словом «законодавство». Під останнім поняттям зазвичай розуміють сукупність нормативно-правових актів вищої юридичної сили в державі, якими є закони як результат безпосереднього волевиявлення народу (референдуму) або його представницького органу (Верховної Ради), а також чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України [103, с. 97].

Переходячи до розгляду поняття прогалин в законодавстві, варто підкреслити, що в науковій літературі існує чимала кількість підходів щодо його тлумачення. Так, у своєму дисертаційному дослідженні Д. М. Величко дійшов висновку, що прогалина в законодавстві — це відсутність конкретної норми, що необхідна для регулювання відносин, які входять до сфери правового регулювання. Така ситуація складається, коли з'являються нові суспільні відносини, що на момент прийняття закону ще не існували або ще не були враховані законодавцем, або коли при розробці закону чи іншого нормативного акта були зроблені певні упущення [38]. Більш точною та цікавою, на наше переконання, видається точка зору О. Ф. Скакун, яка зазначає, що прогалини у законодавстві — повна або часткова відсутність (пропуск) необхідних юридичних норм у чинних законодавчих актах, якими, виходячи з принципів права, мають бути врегульовані певні суспільні відносини [171]. Серед причин виникнення прогалин у законодавстві вчена називає: 1) невміння відобразити в нормативних актах усе різноманіття сучасних життєвих ситуацій, що потребують правового регулювання і можуть бути врегульовані правом; 2) відставання нормотворчості від розвитку суспільних відносин як наслідок невміння передбачити появу нових життєвих ситуацій; 3) наявність деформацій у процесі нормотворчості, спричинених, наприклад, лобіюванням голосування в парламенті в інтересах певних бізнесових груп; 4) технічні помилки законодавця, допущені при розробці нормативних актів та застосуванні прийомів юридичної техніки.

Прогалини в законодавстві виникають зазвичай там, де існує: а) неповнота правових норм; б) суперечність норм однакової юридичної сили, коли одна з них «знищує» іншу; в) повна відсутність правової норми [171].

Досить розгорнуто поняття прогалин в законодавстві розглядають Є. О. Гіда, Є. В. Білозьоров, А. М. Завальний та ін. Науковці вказують, що «прогалина в законодавстві» — це повна або часткова відсутність нормативно-правового регулювання суспільних відносин, що зумовлює прийняття нового нормативно-правового акта або внесення змін до вже існуючого. Автори наголошують, що при визначенні поняття «прогалина в законодавстві» слід мати на увазі, що йдеться лише про ті відносини, які можливо врегулювати за допомогою норм права [189]. Цікавою є думка вказаних вище вчених щодо того, що неврегульованість окремих суспільних відносин має як об'єктивний, так і суб'єктивний характер та обумовлюється розвитком суспільства, іншими причинами. В часи, коли правова система розвивається послідовно, повільно, вона має сталий характер, суспільні відносини максимально врегульовані. В періоди революційних змін в суспільстві правова система не встигає своєчасно врегульовуватися, заповнити відсутні елементи, що і призводить до появи прогалин в законодавстві. Водночас, зближення держав веде до трансформації національних правових систем, виникнення нових суспільних відносин, які потребують юридичного врегулювання. Крім перерахованих об'єктивних причин, Є. О. Гіда також виділяє окремі суб'єктивні причини прогалин в законодавстві: невміння законодавця відобразити в нормативних актах усе різноманіття життєвих ситуацій, які вимагають правового регулювання; невміння законодавця передбачити появу нових життєвих ситуацій у результаті постійного розвитку суспільних відносин, здійснити щодо них певні законодавчі дії; технічні помилки законодавця, допущені при розробці нормативно-правових актів і у використанні прийомів юридичної техніки [189]. Прогалини потрібно відрізняти від: незрозумілості змісту норм

права, що усувають компетентні органи шляхом офіційного тлумачення; «кваліфікованої мовчанки» законодавця, коли він навмисно залишає питання по врегулюванню певних відносин відкритим, утримується від прийняття норми, виносячи вирішення справи за межі законотворчої сфери; випадків, коли законодавець віддає вирішення питання на розгляд суб'єктів права, розраховуючи на те, що його законотворча воля буде конкретизована іншими правовими актами, наприклад, деякі цивільні відносини можуть бути урегульовані договором; «помилок в законодавстві» [189].

Відмітимо, що в юридичній літературі ставлення науковців до явища прогалин в законодавстві є неоднозначним. Одні вчені стверджують, що прогалини є виключно негативним явищем, яке суттєво погіршує стан правового регулювання тих чи інших суспільних відносин. Однак, є група науковців, які вважають, що окрім негативних сторін, прогалини мають і позитивний бік, зокрема, вони: по-перше, є показником активного розвитку певних суспільних відносин; по-друге, активізують наукові пошуки, а також роботу законодавця по вдосконаленню різних нормативно-правових актів. Ми ж, в свою чергу, вважаємо, що перш ніж говорити про позитивні та/або негативні сторони прогалин в законодавстві, слід враховувати специфіку сфери суспільних відносин. Тож ми переконані, що в контексті забезпечення кібербезпеки необхідно говорити про прогалини в законодавстві як про суто негативне явище. Адже їх наявність апріорі загрожує безпеці кожного окремого громадянина, органам державної влади та державі взагалі. А тому законодавець повинен в якомога коротші строки здійснювати всі необхідні заходи для подолання та усунення прогалин в законодавстві, яке регулює забезпечення кібербезпеки в Україні.

Отже, визначаючи напрямки вдосконалення законодавства у сфері забезпечення кібербезпеки, в першу чергу слід звернути увагу на прийнятий нещодавно Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. І в першу чергу відмітимо досить широке

коло суб'єктів забезпечення кібербезпеки в Україні, однак, при цьому у вказаному вище нормативно-правовому акті не визначено єдиного (ключового) органу, до повноважень якого повинно бути віднесене оперативне командування всіма іншими суб'єктами у цій сфері. Взагалі питання оптимізації суб'єктів забезпечення кібербезпеки в Україні є дуже актуальним, а тому йому буде приділено окрему увагу у наступному підрозділі дисертаційного дослідження.

Ще один суттєвий недолік, на який хотілося б звернути увагу, — це термінологічна недосконалість вказаного вище закону, адже деякі терміни вбачаються занадто «простими» та не відображають всю специфіку окремих категорій. Так, законодавець визначає кібертероризм як «терористичну діяльність, що здійснюється у кіберпросторі або з його використанням». На нашу думку, більш вдале визначення «кібертероризму» надає Б. В. Кузьменко, який вказує, що це поняття слід розуміти як один з напрямків тероризму, в якому об'єктом деструктивної дії для досягнення цілей використовують інформаційно-обчислювальну техніку, комплекси та мережеві сегменти, які підтримують критично важливі, з точки зору національної безпеки, системи [100, с. 22]. Не можна не звернути увагу на те, що законодавець надає визначення поняття «індикатори кіберзагроз», яке визначає як показники (технічні дані), що використовуються для виявлення та реагування на кіберзагроз [151]. Зазначене беззаперечно заслуговує на увагу, однак, законодавцю необхідно було уточнити, про які саме показники йде мова.

З позитивного боку слід відмітити, що в Законі України «Про основні засади забезпечення кібербезпеки України» було законодавчо закріплено поняття кіберзагроз — це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [151]. Однак, надаючи визначення

вказаного терміну, законодавець залишив поза увагою те, які все ж таки існують конкретні види кіберзагроз. А тому, поділяючи точку зору І. В. Діордіца, вважаємо, що основними видами кіберзагроз є [58]: 1) націлені атаки (advanced persistent threat), які можуть здійснюватись: по-перше, через застосування програмного забезпечення (вірус, троянський кінь), маючи на меті компрометацію якомога більшої кількості систем; по-друге, через проведення атак прицільно для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів; 2) кібертероризм (вплив на системи керування); 3) кібервійни. Stuxnet — це прообраз кіберзброї для ведення кібервійни, використовується для здійснення диверсій або відключення систем (наприклад, комплексів протиповітряної чи протиракетної оборони); 4) хактивізм, тобто зловживання інформацією у соціальних мережах (вплив на суспільство); 5) атаки на банківські системи (викрадення грошей); 6) атаки на електронний уряд; 7) апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання [52, с. 17; 58]. Таким чином, закріплення видів кіберзагроз на законодавчому рівні має важливе значення не лише з теоретичної, а й з практичної точки зору, адже це: по-перше, унеможливлює неоднозначне тлумачення окремих правових норм; по-друге, дозволяє більш якісно формулювати положення інших нормативно-правових актів у цій сфері, наприклад, положення Стратегії кібербезпеки України.

Не можна також не звернути увагу на те, що в законі відсутнє тлумачення деяких понять, зокрема, «кіберправопорушення» та «кіберпроступок», що є неприпустимим, оскільки законодавством передбачено такі види відповідальності як цивільна та адміністративна. А тому пропонуємо до Закону України «Про основні засади забезпечення кібербезпеки України» додати вказані вище терміни та викласти їх у наступній редакції: «Кіберправопорушення — це суспільно небезпечне діяння, яке було здійснено за допомогою застосування кіберпростору через

використання, створення, обробку чи знищення інформації (комп'ютерних даних, носіїв інформації, тощо), здійснення якого тягне за собою настання негативних наслідків у вигляді юридичної відповідальності. Що ж стосується кібепроступку, то під ними необхідно розуміти кіберправопорушення, яке не несе в собі суспільну небезпеку та за яке передбачена відповідальність.

Наступний проблемний аспект Закону України «Про основні засади забезпечення кібербезпеки України», на який хотілося б звернути увагу, — це відсутність переліку видів кіберзлочинів. А тому, погоджуючись із точкою зору В. Б. Дзюндзюка, до таких злочинів пропонуємо віднести [57]: 1) злочини проти конституційних прав і свобод людини і громадянина, такі як порушення недоторканності приватного життя, порушення таємниці листування, телефонних переговорів, поштових, телеграфних і інших повідомлень, порушення авторських і суміжних прав; 2) злочини проти життя і здоров'я. Першим зафіксованим фактом вбивства, здійсненим за допомогою Інтернет, був випадок, що відбувся в лютому 1998 р. в США. Важко поранений свідок злочину був захований в закритому госпіталі на території військової бази, проте, злочинці через Інтернет змінили режими роботи кардіостимулятора і апарату вентиляції легенів, що призвело до смерті свідка [57; 77]. Крім того, загрозливі масштаби в Інтернет отримали сайти, що пропагують наркоманію, публікують технологію виготовлення наркотичних препаратів в домашніх або промислових масштабах, які розповсюджують наркотичні засоби, психотропні речовини і їх аналоги; 3) злочини проти честі і гідності особи. Анонімність, широка аудиторія Інтернет дають безмежні можливості в розповсюдженні інформації будь-яких видів, у тому числі і наклепницької, такої, що порочить честь і гідність особи; 4) злочини проти власності. Одним з найпоширеніших видів злочинів сучасності в Інтернет є Інтернет-шахрайство, при цьому з кожним днем з'являються все нові його форми, види і способи; 5) злочини у сфері комп'ютерної інформації, в першу чергу такі як неправомірний доступ до

інформації і створення, використання і розповсюдження шкідливих програм; 6) злочини проти суспільної моральності. Так, широкого поширення в Глобальній мережі набув порнобізнес, при цьому порносайти в Інтернет доступні для будь-якої точки світу і для будь-якої категорії населення, а розповсюджувачі аморальної продукції відчувають себе безкарно, оскільки діють анонімно; 7) злочини проти безпеки держави. Із зростанням використання Інтернет в державних структурах стає можливим нелегально дістати доступ не тільки до приватної і корпоративної інформації, але також до інформації, що є державною таємницею, і за допомогою Інтернет скоювати такі злочини як шпигунство, державна зрада або розголошування державної таємниці; 8) звичайно ж, головне місце серед таких видів злочинів займає кібертероризм, який набуває все більш загрозливих масштабів, маючи тенденцію зрощення із «звичайним» тероризмом [57].

Наступний недолік нормативно-правового акта, що розглядається, — це те, що, формулюючи деякі положення, законодавець використав принцип «від зворотного» та недвозначно вказав в ч. 1 ст. 2 Закону 2163Л/ІІІ, що «цей Закон не поширюється на [213; 151]: 1) відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; 2) діяльність, пов’язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; 3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів; 4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем)» [151]. Аналізуючи лише

дану норму, неможливо дати відповідь на питання, чи поширюється закон на приватні мережі суб'єктів господарювання, адже такі мережі все ж таки підключені до мережі Інтернет. Проте, якщо розглядати вказану норму в сукупності з нормою ч. 2 ст. 4 Закону 2163-VIII, котра визначає перелік об'єктів кіберзахисту (серед яких закріплено об'єкти критичної інформаційної інфраструктури), то можна зробити попередній висновок, що все ж таки даний закон поширює свою дію на приватні мережі суб'єктів господарювання у разі, коли того чи іншого господарюючого суб'єкта буде віднесено до об'єктів критичної інфраструктури [213]. А відтак, зазначене вище потребує уточнення та внесення відповідних змін до ч. 1 ст. 2 Закону 2163Л/III. Це дозволить уникнути неоднозначного тлумачення вказаних норм та сприятиме якісному покращенню механізму забезпечення кібербезпеки в Україні.

Ще один суттєвий недолік Закону України «Про основні засади забезпечення кібербезпеки України», на який слід звернути увагу, — це відсутність норм, які б детально визначали організаційні та процедурні засади забезпечення кібербезпеки в України. Крім того, як ми вже вказували, невизначеними залишаються форми та методи забезпечення кібербезпеки. А тому на сьогодні існує нагальна необхідність внесення відповідних змін до вказаного нормативно-правового акта, що, в свою чергу, створить більш сприятливе поле для подальшої діяльності уповноважених суб'єктів у сфері забезпечення кібербезпеки.

Таким чином, незважаючи на те, що Закон України «Про основні засади забезпечення кібербезпеки України» було прийнято та запроваджено в дію не так давно, а його розробка та обговорення тривали декілька років, в ньому залишається досить багато проблемних та невирішених питань, які потребують уваги з боку як законодавця, так і вітчизняних науковців. Звісно, запропонований нами перелік змін до досліджуваного нормативного-правового акта не претендує на вичерпність, однак, ми переконані, що вони

дозволять якісно покращити практичну діяльність суб'єктів забезпечення кібербезпеки в Україні, а як результат — позитивним чином вплинуть на стан кіберзахисту в нашій державі.

Розглядаючи можливості удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні, слід звернути увагу і на інші нормативно-правові акти, серед яких обов'язково необхідно вказати новий Закон України «Про національну безпеку України», який містить чимало цікавих та нових положень про кібербезпеку та є досить прогресивним у порівнянні з аналогічним законом від 2003 року. Зокрема, важливим аспектом є те, що стаття 31 визначає, що Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, тощо [148]. Однак, вказаний нормативно-правовий акт також не позбавлений певних недоліків. Зокрема, не зовсім зрозумілим є виключення (у порівнянні з попереднім Законом «Про національну безпеку України») статті, яка визначала основні реальні та потенційні загрози внутрішньо- та зовнішньополітичній національній безпеці України та стабільності в суспільстві. Натомість, в законі як загрози національній безпеці закріплені різні негативні чинники розвитку суспільства та держави, попри те, що їх подолання не може бути забезпечене діяльністю органів сектору безпеки. Закріплений на законодавчому рівні перелік загроз національній безпеці України та заходів реагування на них не відповідає практикам держав — членів Європейського Союзу та НАТО, ускладнює визначення пріоритетів державної політики у сфері національної безпеки та вчасну реакцію на зміни безпекової ситуації.

В контексті представленого наукового дослідження слід вказати позицію керівництва СБУ, яке підтримує необхідність прийняття Верховною Радою України проекту Закону «Про внесення змін до деяких законодавчих

актів України щодо протидії загрозам національній безпеці в інформаційній сфері». СБ України вважає, що внесення змін у чинне законодавство в частині забезпечення інформаційної безпеки та кібербезпеки забезпечить впровадження правового механізму блокування інформаційного ресурсу (сервісу) на підставі рішення слідчого судді та суду у кримінальному провадженні. Блокування можливе за рішенням РНБО України, прийнятим відповідно до Закону України «Про санкції». Застосування РФ під час гібридної війни новітніх технологій проти України перетворило інформаційну сферу та кіберпростір на одну з ключових арен протиборства з агресором. Починаючи з 2014 року, відбулися численні кібератаки з використанням шкідливого програмного забезпечення на об'єкти інформаційної критичної інфраструктури та державні установи. Ініційовані спецслужбами РФ кібератаки викликали тимчасове припинення енергопостачання, що створило реальні передумови для надзвичайних ситуацій техногенного характеру, вивели з ладу десятки серверів й електронних систем, блокували систему бюджетних виплат та надання банківських і адміністративних послуг. Передбачене проектом закону унормоване ведення відкритого у загальному доступі Єдиного реєстру виконання судових рішень і застосування санкцій у сфері телекомунікацій, наявність прозорої процедури прийняття процесуальних рішень про тимчасове блокування доступу до інформаційних ресурсів (сервісів) забезпечать демократичний цивільний контроль над діями СБУ для зміцнення національної безпеки України. Крім того, відповідно до прийнятого Закону України «Про національну безпеку України» також здійснюватиметься парламентський контроль за діяльністю органів сектору безпеки і оборони [195].

Ще один нормативно-правовий акт, якому ми приділимо увагу, — Указ Президента України «Про Доктрину інформаційної безпеки України» [66]. Метою Доктрини є уточнення засад формування та реалізації державної

інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Але, на думку Т. Попової, така мета більше підходить для іншого документа, який має визначати основні засади державної інформаційної політики, особливо її структуру і зміст. Поки що такого документа на державному рівні в Україні не існує. Крім того, експерт вважає відкритими питання щодо методології підходів до проблематики забезпечення інформаційної безпеки, які закріплені в Доктрині [183]. Зокрема, Т. Попова вбачає за необхідне поставити на перше місце співвідношення понять «інформаційна безпека» та «кібербезпека». Вона констатує, що українська наука чітко обґрунтувала необхідність розгляду національного сегмента кіберпростору як складової частини інформаційного простору держави, з чого випливає і логічність розгляду питань кібербезпеки в контексті інформаційної безпеки. Але в ряді країн застосовуються інші підходи до цього питання, наголошує експерт [183]. Ще один медіа експерт — Н. Лігачова — також зазначає, що: «Один з її (Доктрини) недоліків, що положення доктрини пов'язані насамперед з агресією Росії, мені здається, що це свідчить про те, що в України і авторів доктрини поки немає уявлення, яким чином повинна забезпечуватися інформаційна безпека України, з урахуванням всіх загроз». Крім того, експерт до недоліків відносить факт закріплення на законодавчому рівні позасудового та досудового блокування сайтів [65].

Наступний суттєвий недолік, який також виділяє Т.Попова, — відсутність реально працюючих механізмів координації діяльності у сфері інформаційної безпеки. Деякі успішні приклади горизонтальної взаємодії органів влади, волонтерські проекти, проекти у форматі «ручного управління» є винятком з правил, які лише підтверджують необхідність офіційної координації з боку держави. Безумовно, необхідність централізації діяльності, дієвих алгоритмів координації та контролю в тексті Доктрини

задекларована. Але, з іншого боку, механізми зазначеного не прописані. Це є підставою говорити про певні ризики, бо РНБО отримала завдання координації діяльності, не маючи при цьому необхідних повноважень і ресурсів, які притаманні центральним органам виконавчої влади. Мінінформполітики в існуючому вигляді також не зможе виконати певні завдання, не будучи до того ж офіційною складовою частиною сектору безпеки та оборони держави і суб'єктом боротьби з тероризмом [183]. А відтак, головним, можна навіть говорити «концептуальним», недоліком вказаної Доктрини є її орієнтованість лише на Російську Федерацію. А тому, на наше переконання, можна говорити про необхідність ґрунтовного переосмислення положень вказаного нормативно-правового акта, враховуючи не лише ті загрози, які можуть поступати з боку держави–сусіда, а й інші наявні виклики у цій сфері, як внутрішні, так і зовнішні.

І останній нормативно-правовий акт, на який ми хотіли звернути особливу увагу, — Стратегія кібербезпеки України від 15 березня 2016 року [153]. У попередньому підрозділі дисертаційного дослідження ми відмічали недосконаліть цієї Стратегії, а тому хотіли б зупинитись на найважливіших її аспектах, які, на наше переконання, потребують удосконалення:

1. Перший недолік, на який ми хотіли звернути увагу, — це відсутність конкретних термінів (строків), на які приймається Стратегія. Ми вважаємо, що найбільш оптимальним строком прийняття Стратегії кібербезпеки в Україні є 3–5 років. Така наша пропозиція обґрунтовується декількома фактами: по-перше, у всіх найбільш успішних країнах (у сфері забезпечення кібербезпеки) такі стратегії приймаються щонайменше на 3 роки, а найбільше — на 5; по-друге, кіберпростір — це така сфера, яка постійно розвивається, в ній виникають нові виклики та проблемні питання, які стосуються кібербезпеки. А відтак, і законодавство у цьому напрямку повинно оновлюватись якомога частіше, щоб уникати прогалин в ньому.

2. В Стратегії повинна визначатись сума грошових коштів, яка може бути витрачена на її реалізацію, тобто повинен визначатись бюджет. Так, наприклад, у Великобританії, Франції, Польщі та інших країнах, перш ніж затвердити стратегію, визначається бюджет, від якого законодавець відштовхується при формуванні плану реалізації останньої. Справедливо буде відзначити, що в Законі України «Про основні засади забезпечення кібербезпеки України» вказується, що джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством [151]. Однак, при цьому, на нашу думку, в Стратегії має бути чітко визначено, куди повинні бути використані кошти державних та місцевих бюджетів, тобто окреслено їх цільове призначення.

3. На відміну від більшості держав, у Стратегії забезпечення кібербезпеки в Україні не приділена увага кадровому питанню суб'єктів, що уповноважені забезпечувати кібербезпеку в Україні. Кадрове забезпечення — це система підготовки, що передбачає навчання та виховання фахівців, які здатні розв'язувати складні завдання у сфері забезпечення кібербезпеки [15]. Кадрове забезпечення характеризується низкою ознак, серед яких варто особливо відмітити такі: 1) являє собою триваючий в часі динамічний процес, який має неоднорідну структуру; 2) здійснюється на постійній основі, починається з професійної підготовки (період до призначення) та закінчується звільненням із подальшим призначенням пенсії або переведенням до іншого місця роботи (період після звільнення); 3) основний період кадрового забезпечення починається після призначення; здійснюється кадровими службами відповідної управлінської структури; 4) його організація на конкретному підприємстві, установі, організації регламентується законодавством, підвідомчими нормативно-правовими актами, а також локальними актами; 5) метою кадрового забезпечення є

укомплектування підприємства, установи або організації кваліфікованими кадрами, постійна робота з кадрами, що включає підвищення кваліфікації, перепідготовку, забезпечення службової або трудової дисципліни, тощо [196]. Кадрове забезпечення виступає невід'ємною складовою управлінського процесу, оскільки воно включається в структуру управління, а його стан безпосередньо впливає на ефективність управління [196]. Отже, питання кадрового забезпечення повинно бути невід'ємною складовою Стратегії забезпечення кібербезпеки. В ній повинні бути вказані наступні аспекти:

– по-перше, кількість фахівців, яку планується підготувати для здійснення діяльності у досліджуваній сфері;

– по-друге, напрямки підготовки фахівців;

– по-третє, відповідальні особи (державні органи), які повинні відповідати за розробку програм підготовки та перепідготовки кадрів;

– по-четверте, джерела фінансування.

4. Не можна також не звернути увагу на те, що в Стратегії недостатньо повно розкрито питання взаємодії суб'єктів забезпечення кібербезпеки як один з одним, так і з громадськістю та суб'єктами господарської діяльності [34].

Отже, з аналізу наведеного матеріалу видно, що на сьогодні Стратегія забезпечення кібербезпеки в Україні є занадто «простою» та практично не відповідає тим викликам, які стоять перед сучасною державою у сфері забезпечення кібербезпеки.

Таким чином, завершуючи представлений підрозділ дисертаційного дослідження, слід вказати, що в останні декілька років фахівці та політики наголошують на суттєвому покращенні вітчизняного законодавства у сфері забезпечення кібербезпеки в Україні. З цим твердженням складно не погодитись, однак, зазвичай вони відмічають поліпшення законодавства у порівнянні із тим, що було в Україні до 2013 року. Це, на наше переконання,

є не зовсім справедливим, адже відправною точкою у цій сфері повинно бути не застаріле законодавство, а найбільш вдала практика зарубіжних країн, які є своєрідним взірцем забезпечення кібербезпеки. А тому не викликає сумнівів, що запропоновані нами зміни дозволять якісно покращити діяльність суб'єктів забезпечення кібербезпеки в Україні, а як результат — і рівень кібербезпеки в державі взагалі.

3.3 Оптимізація системи суб'єктів забезпечення кібербезпеки України та удосконалення взаємодії між ними

Одним із перспективних напрямків удосконалення забезпечення кібербезпеки в Україні є оптимізація системи суб'єктів, що уповноважені здійснювати діяльність у цій сфері, а також налагодження ефективної взаємодії між ними. Досвід іноземних країн та особливості українських реалій свідчать, що розв'язання основних завдань кібербезпеки неможливе без створення [25, с. 8–9; 60]: 1) міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки. Кібератака 27 червня 2017 року на Україну довела неефективність діяльності Національного координаційного центру кібербезпеки, поставила питання не про демагогічні та популістські формування недієздатних центрів / органів, а про формування відповідно до національних інтересів національної системи кібербезпеки, власне, як на те вказується безпосередньо в Стратегії кібербезпеки України; 2) центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії

кібератакам протиборчих сторін та впливу на їх ІТС; 3) органів власної інформаційної і кібербезпеки — державних установ (відомств) та комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпростору [25, с. 8–9; 62]. Із зазначеного слідує, що система вказаних органів повинна бути якомога оптимальнішою.

Терміном «оптимізація» в літературі позначають процес або послідовність операцій, що дозволяє отримати уточнене рішення [39, с. 4]. У найбільш загальному розумінні оптимізація — це процес приведення системи в найкраще (оптимальне) становище [173, с. 483]. О. С. Розумовський зазначає, що оптимізація — це перехід від одного — несприятливого чи малосприятливого стану — до іншого — бажаного, кращого в певному відношенні, що відповідає меті, нормам і програмам у керованих системах різного роду [161, с. 71]. Таким чином, оптимізація системи суб'єктів забезпечення кібербезпеки представляє собою процес, який передбачає: по-перше, створення оптимальної кількості таких суб'єктів, яких буде достатньо для виконання завдань у сфері забезпечення кібербезпеки; по-друге, належну організацію діяльності відповідних суб'єктів шляхом збільшення або зменшення кількості їх повноважень.

Однак, перше, на що хотілося б звернути увагу, — це необхідність створення єдиного державного органу, який був би наділений повноваженнями щодо координації діяльності всіх суб'єктів забезпечення кібербезпеки України. Відмітимо, що РНБО здійснює лише координацію та стратегічне управління. Генштаб — оперативне управління в «особливий період». Але на практиці кібервійну ніхто ніколи не об'являє. А тому, на нашу думку, цікавим є досвід країни–сусіда Польщі, яка створила Міністерство цифровізації, одним із завдань якого є координація діяльності всіх без винятку суб'єктів забезпечення кібербезпеки в державі.

Крім того, цікавою вбачається точка зору, відповідно до якої з метою оптимізації діяльності суб'єктів забезпечення кібербезпеки пропонується [73] обмежити повноваження Держспецзв'язку та СБУ об'єктами критичної інфраструктури, що є власністю держави, які на сьогодні мають надмірні повноваження з аудиту об'єктів критичної інфраструктури, що знаходяться в приватній власності. По суті, це буде весь великий та середній бізнес. Водночас, Держспецзв'язок має право визначати вимоги для аудиторів та порядок їх атестації. Це створює можливості для зловживань, тиску на бізнес з боку держави, передумови для корупції, наприклад, ліцензії для аудиту будуть видаватися тільки «своїм» фірмам, які, в свою чергу, будуть робити перевірки «на папері», та взагалі суперечить політиці держави з дерегуляції. На жаль, практика показує, що наявність ліцензіата не гарантує високого рівня якості. Водночас, міжнародні професійні сертифікації з кібербезпеки та IT-аудиту на визнаються [73]. Щодо приватних об'єктів, то слушно пропонується віддати повноваження з регулювання та контролю кібербезпеки галузевим регуляторам, міністерствам або саморегулюючим організаціям, створеним учасниками відповідних галузей, у відповідності до моделі, яка працює в США [73].

Взагалі, говорячи про оптимізацію суб'єктів забезпечення кібербезпеки, слід відзначити, що на сьогодні чисельність таких суб'єктів в Україні є чи не однією із найбільших у Європі та світі, що, в свою чергу, суттєво ускладнює налагодження взаємодії між ними. Переходячи до розгляду питання удосконалення взаємодії суб'єктів забезпечення кібербезпеки в Україні, слід відзначити, що аналіз положень Стратегії кібербезпеки України вказує, що сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі [109, с. 88]. Зазначене свідчить про доцільність, в рамках

організаційного забезпечення реформування системи державного управління кібербезпекою, об'єднання спільних зусиль усіх відповідальних структур — Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, Національного банку України, розвідувальних органів, з метою прискорення проведення їхньої функціональної оптимізації, впровадження організаційно-технічної моделі оперативного управління національною системою кіберзахисту, налагодження між вказаними суб'єктами механізмів оперативної та комплексної взаємодії, обміну інформацією у режимі реального часу з метою реагування на кіберзагроз та кіберінциденти, у тому числі й у напрямі запровадження заходів державної підтримки власних розробок кіберзброї [109, с. 88].

Поняття «взаємодія» надзвичайно багатозначне. З погляду філософії ця категорія являє собою одну із загальних форм взаємозв'язку між явищами. Її суть полягає у зворотному впливі одного предмета чи явища на інше. Отже, взаємодія відтворює процеси впливу об'єктів один на одного, їх взаємну зумовленість і породження одним об'єктом іншого. В соціології вживається дефініція «соціальна взаємодія» для визначення такої форми спілкування осіб, соціальних спільнот, угруповань, за якою систематично здійснюється їхній вплив один на одного, реалізується соціальна дія кожного з партнерів, досягається пристосування дій одного до дій іншого, спільність у розумінні ситуації, сенсу дій і певний ступінь солідарності або згоди між ними [130].

Д. Г. Заброда звертає увагу на те, що взаємодія — це категорія, що відображає процеси впливу різних об'єктів один на одного, їхню взаємну обумовленість і зміну стану або взаємоперехід, а також породження одним об'єктом іншого. Взаємодія являє собою вид прямого або опосередкованого, зовнішнього або внутрішнього відношення зв'язку [22, с. 7; 70, с. 44]. На думку І. Т. Фролова, взаємодія — це процес взаємного впливу різних об'єктів один на одного, їх взаємообумовленість і навіть у певному сенсі перехід один

в одного. Як одна з найбільш загальних та універсальних характеристик буття, взаємодія визначає сутність і структурну організацію будь-якої матеріальної системи. Саме взаємодії лежать в основі матеріальних утворень, виступають джерелом, двигуном їх змін та розвитку [197, с. 93]. Л. Г. Шморгун вказує, що взаємодія — це процес безпосереднього чи опосередкованого впливу об'єктів (суб'єктів) один на одного, що породжує їх взаємні зумовленість і зв'язок [211]. У взаємодії, як підкреслює автор, реалізується відношення людини до іншої людини як до суб'єкта, в якого є власний світ. Під взаємодією в соціальній філософії та психології, а також теорії менеджменту, крім того, розуміється не лише вплив людей один на одного, а й безпосередня організація їх спільних дій, що дає змогу групі реалізувати спільну для її членів діяльність. Взаємодія людини з людиною в суспільстві — це також взаємодія їх внутрішніх світів: обмін думками, ідеями, образами, вплив на цілі та потреби, дія на оцінки іншого індивіда, його емоційний стан. Науковець також вказує на те, що взаємодія є систематичним і постійним учиненням дій, спрямованих на те, щоб викликати відповідну реакцію з боку інших людей. Спільне життя і діяльність людей як у суспільстві, так і в організації, на відміну від індивідуального, має більш жорсткі обмеження будь-яких виявів активності чи пасивності. В процесі реальної взаємодії формуються також адекватні уявлення працівника про себе та інших людей. Взаємодія людей — провідний фактор у регуляції їх самооцінок і поведінки в суспільстві [211].

Цікавою видається точка зору В. М. Олійника стосовно того, що в залежності від мети діяльності взаємодія може бути умовно поділена на негативну та позитивну. Негативна взаємодія — функціонування суб'єктів спрямоване на досягнення протилежних цілей, вплив та дія кожного з них спрямовані на перешкоджання розвитку іншого об'єкта. Позитивна взаємодія — елементи у своїй діяльності прагнуть досягнення однієї мети (у нашому випадку — протидії злочинності), зусилля об'єктів спрямовані в

один бік, при цьому відбувається найбільш повне використання їх можливостей для виконання спільних завдань. Як наслідок, створюються необхідні передумови для успішної реалізації поставлених перед ними завдань. Отже, позитивна взаємодія породжує нові якості та можливості, які відсутні у взаємодіючих суб'єктів поодинці [129, с. 512].

Таким чином, під взаємодією суб'єктів забезпечення кібербезпеки слід розуміти їх спільну взаємоузгоджену діяльність, яка спрямована на досягнення єдиної мети — забезпечення належного стану кібернетичної безпеки в Україні. До характерних ознак такої взаємодії необхідно віднести: 1) єдину мету спільної діяльності; 2) наявність двох або більше суб'єктів; 3) обов'язковим є законодавче підґрунтя діяльності; 4) чітко визначений адміністративно-правовий статус кожного суб'єкта; 5) узгодженість заходів щодо цілі, місця, часу, методів. Питанню взаємодії у сфері забезпечення кібербезпеки приділяється особлива увагу, оскільки і науковці, і законодавець усвідомлюють, що без взаємодії досягнення кінцевого результату у цій сфері просто неможливе.

Так, відповідно до Стратегії кібербезпеки України, Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [153]. Однак, на жаль, доводиться констатувати, що на цьому увага законодавця до питання взаємодії суб'єктів забезпечення кібербезпеки в Україні і обмежується.

Не можна не звернути увагу на статтю 7 Закону України «Про основні засади забезпечення кібербезпеки України» від 2017 року, яка визначила, що

однією з основних засад забезпечення кібербезпеки в Україні є принцип державно-приватної взаємодії, тобто 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 [151]. В статті 10 цього ж нормативно-правового акта уточнюється, що державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом: 1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій; 2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту; 3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів; 4) партнерства та координації команд реагування на комп'ютерні надзвичайні події; 5) залучення експертного потенціалу наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки; 6) надання консультативної та практичної допомоги з питань реагування на кібератаки; 7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет; 8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки; 9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки; 10) створення системи підготовки кадрів та

підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки; 11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі [151].

Отже, із зазначеного вище дійсно слідує, що законодавець досить багато уваги приділив питанню взаємодії. Однак, при цьому, на законодавчому рівні мало уваги приділяється взаємодії конкретних суб'єктів забезпечення кібербезпеки. Зокрема, недостатньо розробленим є механізм такої взаємодії, який включає: 1) визначання взаємних прав та обов'язків суб'єктів під час здійснення спільної діяльності; 2) визначення напрямків взаємодії; 3) окреслення форм та методів взаємодії; 4) визначення повноважень суб'єкта, який буде координувати спільну діяльність суб'єктів забезпечення кібербезпеки в Україні. Таким чином, враховуючи постійну динаміку розвитку кіберпростору, на сьогодні постала нагальна необхідність прийняття окремого положення «Про порядок взаємодії суб'єктів забезпечення кібербезпеки в Україні», в якому необхідно передбачити всі вказані нами аспекти такої взаємодії.

Так, говорячи про права та обов'язки суб'єктів взаємодії, то вони можуть змінюватись в залежності від того, в якому напрямку здійснюється така взаємодія та реалізовуються заходи забезпечення кібербезпеки. Так, наприклад, якщо Служба безпеки України здійснює контррозвідувальні та/або оперативно-розшукові заходи та виникає необхідність взаємодії з кіберполіцією, то у такому випадку СБУ у будь-якому випадку буде мати більше прав, а поліція — більше обов'язків, тощо. В свою чергу, визначення форм і методів взаємодії матиме важливе значення з точки зору практичної реалізації заходів із забезпечення кібербезпеки.

Взагалі форми взаємодії — це зовнішні, постійно і типізовано фіксовані вирази (прояви) практичної активності уповноважених державних органів з формування та реалізації управлінських цілей і функцій і

забезпечення їх взаємодії [123]. До конкретних форм взаємодії суб'єктів забезпечення кібербезпеки в Україні, на наше переконання, слід віднести: 1) проведення спільних міжвідомчих нарад; 2) обмін оперативною інформацією щодо стану забезпечення кібербезпеки, а також щодо заходів, які були вже реалізовані кожним суб'єктом взаємодії; 3) розробку спільних програм щодо протидії кібеправопорушенням та окреслення основних напрямків спільної діяльності; 4) спільну участь у проведенні окремих слідчих та розшукових дій; 5) утворення спільних консультативно-дорадчих та експертних органів, рад, комісій.

В свою чергу, методи взаємодії — це сукупність способів та прийомів, які спрямовуються на налагодження ефективної взаємодії між суб'єктами, що уповноважені забезпечувати кібербезпеку в Україні. До таких методів взаємодії слід віднести: 1) кадровий метод, який передбачає активне навчання представників одних органів специфіки роботи інших, що, в свою чергу, сприяє налагодженню ефективної взаємодії між відомствами; 2) метод взаємного інформаційного забезпечення, який полягає у наданні суб'єктами співпраці один одному всієї необхідної інформації для більш відкритої та ефективної взаємодії; 3) метод контролю, тобто сторони (суб'єкти) взаємодії мають змогу здійснювати взаємний контроль одна одної під час спільної діяльності; 4) методи планування та прогнозування; 5) економічний метод, який передбачає створення відповідної матеріальної бази для проведення спільних заходів; тощо.

Ще один аспект, на який слід звернути увагу, — це створення органу, який би координував спільні дії суб'єктів забезпечення кібербезпеки в Україні. Взагалі, координація — це діяльність щодо організації взаємодії, поняттям «координація» охоплюється поняття «взаємодія» [113, с. 105]. О. Є. Луньов вказував, що координація означає погодження та об'єднання дій з метою найбільш швидкого і найбільш правильного вирішення завдань із найменшими витратами сил, коштів та матеріальних цінностей. Учений

виділяв два види координації: вертикальну і горизонтальну. Вертикальна координація — це управлінські відносини, які виникають між вищим і нижчим органами виконавчої влади. При цьому, суб'єкти зв'язків можуть перебувати в організаційній залежності (один із них підпорядкований іншому), а можуть і не перебувати в ній. Горизонтальна координація виникає між двома або більше органами, що перебувають на одному організаційному рівні системи органів: наприклад, вищезазначене Міністерство юстиції координує діяльність центральних органів виконавчої влади щодо правової освіти населення [111, с. 148; 1]. В контексті представленого наукового дослідження цікавою є позиція В. П. Пивненка, який справедливо підкреслює, що координація — це функція одного із суб'єктів системи, а взаємодія — принцип діяльності, засіб їх контактів із суб'єктами інших служб і підрозділів [136, с. 157–159].

Таким чином, все вказане вище підтверджує необхідність прийняття єдиного «Порядку взаємодії суб'єктів забезпечення кібербезпеки в Україні» з урахуванням всіх вказаних нами вище пропозицій, які, як вбачається, здатні суттєво покращити взаємодію між суб'єктами забезпечення кібербезпеки в Україні, а як результат — створити всі необхідні умови для розвитку безпечного кіберпростору в державі та захистити її від зовнішніх та внутрішніх кіберзагроз.

Узагальнюючи весь наведений у представленому підрозділі дисертаційного дослідження матеріал, можемо із впевненістю констатувати той факт, що оптимізація суб'єктів забезпечення кібербезпеки неминуче матиме позитивний вплив і на взаємодію між ними. А відтак, комплексна робота законодавця щодо оптимізації та удосконалення взаємодії між суб'єктами забезпечення кібербезпеки на сьогодні є об'єктивною необхідністю, яка здатна якісно удосконалити відповідну сферу суспільних правовідносин.

Висновки до розділу 3

На підставі узагальнення зарубіжного досвіду забезпечення кібербезпеки констатовано, що на сьогодні світові тенденції розвитку інформаційного суспільства спонукають всі держави світу для прийняття заходів щодо забезпечення кібербезпеки. Не є виключенням і Україна, яка нині знаходиться лише на перших етапах розвитку цього інституту. Аналіз досвіду вказаних вище країн дав змогу виокремити наступні напрямки розвитку інституту забезпечення кібербезпеки в Україні: по-перше, необхідно збільшити фінансування суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки в державі; по-друге, слід покращити якість освіти працівників кіберполіції; по-третє, кардинального оновлення потребує Стратегія кібербезпеки України. На наше переконання, вона повинна бути ширшою та охоплювати більше коло питань у цій сфері а не обмежуватись лише базовими питаннями. В цьому контексті цікавим є досвід Великобританії та Німеччини, чиї стратегії забезпечення кібербезпеки охоплюють практично всі питання та є основними документами у цій сфері; по-четверте, необхідно розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки, не обмежуючись співпрацею з однією конкретною країною (в нашому випадку — США); по-п'яте, необхідно посилити контроль у мережі Інтернет (на прикладі Китаю). Така наша пропозиція в першу чергу обґрунтовується тим, що на сьогоднішній день в мережу «викидається» дуже багато так званих «фейкових» новин, які лише вводять в оману населення та підривають довіру до окремих органів державної влади (досить часто ними є правоохоронні органи) та держави взагалі.

Окреслено такі недоліки законодавства у сфері забезпечення кібербезпеки: а) в Законі України «Про основні засади забезпечення кібербезпеки України» закріплено занадто широке коло суб'єктів

забезпечення кібербезпеки в Україні, однак, при цьому у вказаному нормативно-правовому акті не визначено єдиного (ключового) органу, до повноважень якого повинно бути віднесене оперативне командування всіма іншими суб'єктами у цій сфері; б) термінологічна недосконаліть Закону України «Про основні засади забезпечення кібербезпеки України», адже деякі терміни вбачаються занадто «простими» та не відображають всю специфіку окремих категорій; в) законодавець залишив поза увагою те, які все ж таки існують конкретні види кіберзагроз; г) в Законі України «Про основні засади забезпечення кібербезпеки України» відсутнє тлумачення деяких понять, зокрема, «кіберправопорушення» та «кіберпроступок», що є неприпустимим, оскільки законодавством передбачено такі види відповідальності як цивільна та адміністративна; ґ) законодавець не окреслив перелік видів кіберзлочинів; д) у Законі України «Про основні засади забезпечення кібербезпеки України» відсутні норми, які б детально визначали організаційні та процедурні засади забезпечення кібербезпеки в України, а також форми та методи забезпечення кібербезпеки; е) не зовсім зрозумілим є виключення у Законі України «Про національну безпеку України» (у порівнянні з попереднім Законом «Про національну безпеку України») статті, яка визначала основні реальні та потенційні загрози внутрішньо- та зовнішньополітичній національній безпеці України та стабільності в суспільстві; є) спрямованість Доктрини інформаційної безпеки лише на Російську Федерацію. А тому, на наше переконання, можна говорити про необхідність ґрунтовного переосмислення положень вказаного нормативно-правового акта, враховуючи не лише ті загрози, які можуть поступати з боку держави–сусіда, а й інші наявні виклики у цій сфері, як внутрішні, так і зовнішні; ж) відсутність закріплення строків реалізації Стратегії кібербезпеки України, розмірів видатків на її реалізацію, не вирішено питання кадрового забезпечення суб'єктів забезпечення кібербезпеки, не розкрито питання взаємодії суб'єктів забезпечення

кібербезпеки як один з одним, так і з громадськістю та суб'єктами господарської діяльності.

Запропоновано: а) закріпити види кіберзагроз на законодавчому рівні, що має важливе значення не лише з теоретичної, а й з практичної точки зору, адже це: по-перше, унеможливлює неоднозначне тлумачення окремих правових норм; по-друге, дозволяє більш якісно формулювати положення інших нормативно-правових актів у цій сфері, наприклад, положення Стратегії кібербезпеки України; б) внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України» та додати терміни «кіберправопорушення» та «кіберпроступок» і викласти їх у наступній редакції: «Кіберправопорушення» — це суспільно небезпечне діяння, яке було здійснене за допомогою застосування кіберпростору через використання, створення, обробку чи знищення інформації (комп'ютерних даних, носіїв інформації, тощо), здійснення якого тягне за собою настання негативних наслідків у вигляді юридичної відповідальності. Що ж стосується кібепроступку, то під ними необхідно розуміти кіберправопорушення, яке не несе в собі суспільну небезпеку та за яке передбачена відповідальність»; в) у Стратегії кібербезпеки України: по-перше, чітко закріпити строки реалізації стратегії; по-друге, приділити увагу кадровому питанню суб'єктів, що уповноважені забезпечувати кібербезпеку в Україні. В ній повинні бути вказані наступні аспекти: кількість фахівців, яку планується підготувати для здійснення діяльності у досліджуваній сфері; напрямки підготовки фахівців; відповідальні особи (державні органи), які повинні відповідати за розробку програм підготовки та перепідготовки кадрів; джерела фінансування.

Доведено, що оптимізація системи суб'єктів забезпечення кібербезпеки представляє собою процес, який передбачає: по-перше, створення оптимальної кількості таких суб'єктів, яких буде достатньо для виконання завдань у сфері забезпечення кібербезпеки; по-друге, належну організацію

діяльності відповідних суб'єктів шляхом збільшення або зменшення кількості їх повноважень.

З метою оптимізації системи суб'єктів забезпечення кібербезпеки України запропоновано створити єдиний державний орган, який був би наділений повноваженнями щодо координації діяльності всіх суб'єктів забезпечення кібербезпеки України.

Під взаємодією суб'єктів забезпечення кібербезпеки запропоновано розуміти їх спільну взаємоузгоджену діяльність, яка спрямована на досягнення єдиної мети — забезпечення належного стану кібернетичної безпеки в Україні. До характерних ознак такої взаємодії віднесено: 1) єдину мету спільної діяльності; 2) наявність двох або більше суб'єктів; 3) обов'язковим є законодавче підґрунтя діяльності; 4) чітко визначений адміністративно-правовий статус кожного суб'єкта; 5) узгодженість заходів щодо цілі, місця, часу, методів діяльності.

З'ясовано, що на законодавчому рівні мало уваги приділяється взаємодії конкретних суб'єктів забезпечення кібербезпеки. Зокрема, недостатньо розробленим є механізм такої взаємодії, який включає: 1) визначання взаємних прав та обов'язків суб'єктів під час здійснення спільної діяльності; 2) визначення напрямків взаємодії; 3) окреслення форм та методів взаємодії; 4) визначення повноважень суб'єкта, який буде координувати спільну діяльність суб'єктів забезпечення кібербезпеки в Україні.

Враховуючи постійну динаміку розвитку кіберпростору, обґрунтована необхідність прийняття окремого положення «Про порядок взаємодії суб'єктів забезпечення кібербезпеки в Україні», в якому необхідно передбачити всі аспекти такої взаємодії.

До форм взаємодії суб'єктів забезпечення кібербезпеки в Україні запропоновано віднести: 1) проведення спільних міжвідомчих нарад; 2) обмін оперативною інформацією щодо стану забезпечення кібербезпеки, а також

щодо заходів, які були вже реалізовані кожним суб'єктом взаємодії; 3) розробку спільних програм щодо протидії кібеправопорушенням та окреслення основних напрямків спільної діяльності; 4) спільну участь у проведенні окремих слідчих та розшукових дій; 5) утворення спільних консультативно-дорадчих та експертних органів, рад, комісій.

Визначено поняття «методи взаємодії суб'єктів забезпечення кібербезпеки» — це сукупність способів та прийомів, які спрямовуються на налагодження ефективної взаємодії між суб'єктами, що уповноважені забезпечувати кібербезпеку в Україні. До таких методів взаємодії віднесено: 1) кадровий метод, який передбачає активне навчання представників одних органів специфіки роботи інших, що, в свою чергу, сприяє налагодженню ефективної взаємодії між відомствами; 2) метод взаємного інформаційного забезпечення, який полягає у наданні суб'єктами співпраці один одному всієї необхідної інформації для більш відкритої та ефективної взаємодії; 3) метод контролю, тобто сторони (суб'єкти) взаємодії мають змогу здійснювати взаємний контроль одна одної під час спільної діяльності; 4) методи планування та прогнозування; 5) економічний метод, який передбачає створення відповідної матеріальної бази для проведення спільних заходів; та інші.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягає у визначенні сутності та особливостей адміністративно-правових засад забезпечення кібербезпеки України, а також опрацюванні напрямків удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. У результаті дослідження сформульовано низку нових теоретичних та практичних положень, основні з них такі:

1. Аргументовано, що кібербезпека як об’єкт адміністративно-правової охорони являє собою певний правовий інститут, охорона якого відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності.

Наведено такі особливості кібербезпеки як об’єкта адміністративно-правової охорони: а) відсутність чіткого визначення змісту адміністративно-правової охорони кібербезпеки; б) адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державної влади; в) її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення відповідних порушень, а також їх попередження; г) основні засади забезпечення кібербезпеки лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті – Законі України «Про основні засади забезпечення кібербезпеки України»; ґ) має місце спеціальний понятійний апарат.

2. Історико-правовий аналіз становлення та розвитку інституту кібербезпеки дозволив переконатись у тому, що достатньо тривалий час

інституту кібербезпеки на території України фактично не існувало. Наголошено, що становлення інституту кібербезпеки безпосередньо пов’язане з еволюцією інформаційних технологій. Тож, найпершим комп’ютерним законом, положеннями якого вже було передбачено різного роду правопорушення з використанням комп’ютерів, став Закон «Про боротьбу з комп’ютерними шахрайствами та комп’ютерними зловживаннями», прийнятий у 1986 р. у США. Відзначено, що у подальшому розвиток правового інституту кібербезпеки здійснювався на міжнародному рівні, зокрема, у: Віденській декларації про злочинність та правосуддя, Конвенції про взаємодопомогу в кримінальних справах між членами ЄС, Резолюції Генеральної Асамблеї ООН (щодо створення глобальної культури кібербезпеки від 2002 р.), Женевській декларації принципів побудови інформаційного суспільства тощо. З’ясовано, що в Україні кібербезпека як окремий правовий інститут з’явилася після ратифікації у 2005 р. Конвенції про кіберзлочинність. Наступним кроком на шляху її розвитку стало розроблення Стратегії кібербезпеки України, яка була введена в дію рішенням Ради національної безпеки і оборони України. На сучасному етапі кібербезпека повною мірою отримала нормативний прояв у положеннях Закону України «Про основні засади забезпечення кібербезпеки України».

3. Доведено, що до об’єктного складу кібербезпеки входять: а) правовідносини у сфері розвитку належної інформаційної інфраструктури у державі; б) правовідносини у сфері налагодження міжнародних зав’язків з метою обміну досвідом у галузі розбудови кібербезпеки; в) правовідносини з приводу регулювання, координації і контролю діяльності правоохоронних органів та інших суб’єктів забезпечення кібербезпеки в процесі виконання покладених на них обов’язків; г) правовідносини у сфері впровадження інформаційних технологій в основних галузях життєдіяльності суспільства та налагодження процесу їх безпечного використання; ґ) правовідносини у сфері розвитку науки та техніки з метою розбудови предметної основи

інституту кібербезпеки, тобто розроблення новітніх технологій, які б сприяли підвищенню безпеки при роботі у кіберпросторі; д) правовідносини у сфері імплементації у законодавство України правових механізмів забезпечення кібербезпеки з урахуванням міжнародного досвіду у цій галузі; е) правовідносини у сфері підвищення інформаційної обізнаності суспільства при роботі з інформацією у кіберпросторі.

З'ясовано, що об'єктами кіберзахисту є: а) об'єкти критичної інформаційної інфраструктури; б) інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів; в) інформаційно-телекомунікаційні системи, в яких здійснюється обробка інформації, вимоги щодо захисту якої встановлені законом.

4. Встановлено, що адміністративно-правове регулювання кібербезпеки – це цілеспрямований вплив норм адміністративного законодавства на суспільні відносини, які виникають у сфері забезпечення кібербезпеки, в межах якого застосовуються спеціальні засоби та запобіжні заходи з метою недопущення правопорушень у кіберпросторі.

Роль адміністративно-правового регулювання у сфері забезпечення кібербезпеки полягає в тому, що саме відповідно до норм адміністративного законодавства здійснюється правове регулювання діяльності суб'єктів забезпечення кібербезпеки в Україні.

5. Суб'єктів забезпечення кібербезпеки запропоновано об'єднати у дві групи: загальні та спеціальні. До загальної належать усі органи державної влади, органи місцевого самоврядування, 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. До кола спеціальних суб'єктів віднесено органи влади, котрі становлять систему суб'єктів кібербезпеки

України, перелік яких закріплено в Законі України «Про основні засади забезпечення кібербезпеки України».

Наголошено, що всі суб'єкти забезпечення кібербезпеки наділені як комплексом специфічних, так і комплексом загальних повноважень. Серед загальних ознак суб'єктів забезпечення кібербезпеки виділено наступні: по-перше, вони у своїй діяльності використовують владний примус з метою реалізації передбачених законодавством функцій; по-друге, суб'єкти забезпечення кібербезпеки перебувають у системному взаємозв'язку з іншими учасниками адміністративних правовідносин, який будується на засадах ієрархічності; по-третє, діяльність суб'єктів забезпечення кібербезпеки спрямована не тільки на припинення правопорушень у цій сфері, а й на забезпечення умов, коли такі порушення неможливі, що реалізується шляхом проведення контрольних заходів.

6. Виокремлено та охарактеризовано такі форми забезпечення кібербезпеки України: а) нормотворчість (тобто прийняття нормативно-правових актів у сфері забезпечення кібербезпеки); б) прийняття індивідуальних актів у сфері забезпечення кібербезпеки; в) укладення адміністративних договорів; г) правореалізація.

Доведено, що нормотворчість є однією з ключових форм забезпечення кібербезпеки в Україні, оскільки за її допомогою вбачається можливим створити таке правове поле, яке буде виключати будь-які можливості для суб'єктів відповідних правовідносин вчинити правопорушення у досліджуваній сфері. Акцентовано увагу на тому, що індивідуальні акти у сфері забезпечення кібербезпеки дозволяють оперативно вирішити нагальні проблеми, що з'являються у вказаній сфері суспільних відносин. Їх перевага полягає у тому, що вони спрямовані на конкретного суб'єкта, а тому за їх допомогою можливо вирішити більш конкретні проблемні питання. Визначено, що адміністративний договір, як адміністративно-правова форма забезпечення кібербезпеки, являє собою добровільну угоду між декількома

суб’єктами адміністративного права, які наділені владними повноваженнями, з метою координації їх спільної діяльності, що в результаті приводить до виникнення, зміни або припинення взаємних прав та обов’язків сторін відповідного договору. З’ясовано, що правореалізація передбачає безпосереднє втілення норм адміністративного права в діяльність суб’єктів, функції яких полягають у забезпеченні кібербезпеки в Україні. При цьому кожен із таких суб’єктів повинен в обов’язковому порядку дотримуватись визначених суб’єктивних прав та виконання своїх зобов’язань.

На основі аналізу норм чинного законодавства та наукових поглядів учених виокремлено та охарактеризовано такі методи забезпечення кібербезпеки: а) адміністративний примус (ключове значення вказаного методу полягає в тому, що він спрямований на попередження виникнення правопорушень у досліджуваній сфері. Проте застосування методу адміністративного примусу спрямовано не лише на попередження виникнення протиправної поведінки, а й покликано забезпечити захист інформаційних, приватних, комп’ютерних ресурсів тощо); б) метод позитивного зобов’язання; в) метод дозволу та заборон; г) метод адміністративного контролю; ґ) метод контролю доступу; д) метод ліцензування діяльності; е) метод сертифікації та стандартизації; є) реєстраційний метод.

7. Виокремлено найбільш характерні особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки: а) специфічний предмет правопорушення та/або кіберзлочину, яким є інформація, тобто відомості та/або дані, які зберігаються у мережі Інтернет або на якихось носіях (серверах, жорстких дисках, картах пам’яті тощо); б) складність виявлення суб’єкта правопорушення, що потребує серйозного матеріально-технічного та кадрового забезпечення; в) найбільш поширеним видом відповідальності є кримінальна, що обумовлюється високим рівнем шкоди в результаті здійснення кіберзлочину; г) зазвичай, правопорушення у

вказаній сфері спрямовуються не на конкретну особу, тобто не є персоніфікованими; ґ) шкода від вчинення кіберзлочину, як правило, має матеріальний характер та не шкодить фізичному здоров'ю людини.

Розкрито сутність та особливості таких видів юридичної відповідальності за порушення законодавства у сфері кібербезпеки, як адміністративна, кримінальна та цивільно-правова. Основний акцент зроблено на характеристиці адміністративної відповідальності за порушення законодавства у сфері кібербезпеки, у зв'язку з чим визначено, що адміністративна відповідальність за порушення законодавства у сфері кібербезпеки – це застосування до особи, що вчинила правопорушення, санкцій, передбачених нормами адміністративного права. Зазвичай, санкції за вчинення адміністративного проступку мають матеріальний (грошовий) характер.

8. На підставі узагальнення зарубіжного досвіду забезпечення кібербезпеки констатовано, що сьогодні світові тенденції розвитку інформаційного суспільства спонукають всі держави світу вжити заходів щодо забезпечення кібербезпеки. Не є виключенням і Україна, яка нині знаходиться лише на перших етапах розвитку цього інституту. Аналіз досвіду вказаних вище країн дав змогу виокремити наступні напрямки розвитку інституту забезпечення кібербезпеки в Україні: по-перше, необхідно збільшити фінансування суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки в державі; по-друге, покращити якість освіти працівників кіберполіції; по-третє, кардинального оновлення потребує Стратегія кібербезпеки України. На наше переконання, вона повинна бути ширшою та охоплювати більше коло питань у цій сфері, а не обмежуватись лише базовими питаннями. В цьому контексті цікавим є досвід Великобританії та Німеччини, чиї стратегії забезпечення кібербезпеки охоплюють, практично, всі питання та є основними документами у цій сфері; по-четверте, необхідно розширювати міжнародне співробітництво у сфері

забезпечення кібербезпеки, не обмежуючись співпрацею з однією конкретною країною (в нашому випадку – США); по-п’яте, слід посилити контроль у мережі Інтернет (на прикладі Китаю). Така наша пропозиція, в першу чергу, обґрунтовується тим, що сьогодні в мережу «викидається» дуже багато так званих «фейкових» новин, які лише вводять в оману населення та підривають довіру до окремих органів державної влади (досить часто ними є правоохоронні органи) та держави взагалі.

9. З метою вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні, запропоновано: а) закріпити види кіберзагроз на законодавчому рівні, що має важливе значення не лише з теоретичної, а й з практичної точки зору, адже це, по-перше, унеможливлює неоднозначне тлумачення окремих правових норм; по-друге, дозволяє більш якісно формулювати положення інших нормативно-правових актів у цій сфері, наприклад положення Стратегії кібербезпеки України; б) внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України» та додати терміни «кіберправопорушення» та «кіберпроступок», вказавши, що кіберправопорушення – це суспільно небезпечне діяння, яке було здійснено за допомогою застосування кіберпростору через використання, створення, обробку чи знищення інформації (комп’ютерних даних, носіїв інформації тощо) та здійснення якого тягне за собою настання негативних наслідків у вигляді юридичної відповідальності. Що ж стосується кібепроступку, то під ним необхідно розуміти кіберправопорушення, яке не несе в собі суспільну небезпеку та за яке передбачена відповідальність; в) у Стратегії кібербезпеки України, по-перше, чітко закріпити строки реалізації стратегії; по-друге, приділити увагу кадровому питанню суб’єктів, що уповноважені забезпечувати кібербезпеку в Україні. В ній повинні бути вказані наступні аспекти: кількість фахівців, яку планується підготувати для здійснення діяльності у досліджуваній сфері; напрямки підготовки фахівців; відповідальні особи (державні органи), які повинні відповідати за

розроблення програм підготовки та перепідготовки кадрів; джерела фінансування.

10. З метою оптимізації системи суб'єктів забезпечення кібербезпеки України запропоновано створити єдиний державний орган, який був би наділений повноваженнями щодо координації діяльності всіх суб'єктів забезпечення кібербезпеки України.

З'ясовано, що на законодавчому рівні мало уваги приділяється взаємодії конкретних суб'єктів забезпечення кібербезпеки. Зокрема, недостатньо розробленим є механізм такої взаємодії, який включає: 1) визначення взаємних прав та обов'язків суб'єктів під час здійснення спільної діяльності; 2) визначення напрямків взаємодії; 3) окреслення форм та методів взаємодії; 4) визначення повноважень суб'єкта, який буде координувати спільну діяльність суб'єктів забезпечення кібербезпеки в Україні.

Враховуючи постійну динаміку розвитку кіберпростору обґрунтована необхідність прийняття окремого положення «Про порядок взаємодії суб'єктів забезпечення кібербезпеки в Україні», в якому необхідно передбачити всі аспекти такої взаємодії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аблязов Д. Е. Взаємодія та координація в державному управлінні. *Право і Безпека*. 2011. № 5. С. 39–42.

2. Административная деятельность органов внутренних дел. Часть Общая: учебное пособие 3-е изд. / под ред. А. П. Коренева. Москва, 2000. 367 с.

3. Адміністративне право України: навчальний посібник у 4-х томах / В.В. Галунько //Херсон: ХМТ, 2011. Т. 1. 334 с

4. Адміністративне право України: підручник / за заг. ред. проф. Ю. П. Битяка. Харків: Право, 2000. 526 с.

5. Адміністративне право України: підручник для юридичних вузів і фак. / Ю. П. Битяк, В. В. Богуцький, В. М. Гаращук та ін.; за ред. Ю. П. Битяка. Х., 2000. 520 с.

6. Алексеев С. С. Право: азбука теория философия: Опыт комплексного исследования. Москва: Статут, 1999. 712 с.

7. Алексеев С. С. Проблемы теории права: курс лекций в двух томах. Свердловск, 1972. Т. I. 396 с.

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

9. Анісімова Г. В. Принципи екологічного права: поняття та види. *Правова доктрина основа формування правової системи держави*: матеріали Міжнар. наук.-практ. конф., присвяч. 20-річчю НАПрН України та обговоренню п’ятитом. моногр. «Правова доктрина України» (Харків, 20–21 листоп. 2013 р.) / Нац. акад. прав. наук України. 2013. С. 485–488.

10. Афанасьєв К. К. Адміністративний договір як форма державного управління (теоретико-правовий аспект): дис… канд. юрид. наук: 12.00.07 /

Луганська академія внутрішніх справ МВС ім. 10-річчя Незалежності України. Луганськ, 2002. 191 с.

11. Базылев Б. Т. Юридическая ответственность: теоретические вопросы: [учебное пособие]. Красноярск: Изд-во Красноярского университета, 1985. 120 с.

12. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 1–9.

13. Баранова Н. М. Етика: навч, посіб. Ніжин: НДУ ім. М. Гоголя, 2015. 323 с.

14. Бахрах Д. Н., Россинский Б. В., Старилов Ю. Н. Административное право: учебник для вузов. 3-е изд., пересмотр, и доп. Москва: Норма. 2007. 816 с.

15. Берлач А. І. Біржове право України: [навч. посіб.]. Київ: Університет «Україна», 2008. 316 с.

16. Бистрик Г. М. Принцип законності і засоби його правового забезпечення у функціонуванні механізму держави. *Наукові праці МАУП*. 2014. Вип. 1. С.85–90.

17. Битяк Ю. П. Правова природа адміністративних договорів. *Вісник Академії правових наук України.* 2001. № 3. С. 5–26.

18. Битяк Ю., Константий О. Правова природа адміністративних договорів. *Вісник Академії правових наук України*. 2001. № 3. С. 101–109.

19. Білодід І. К. Словник української мови: в 11 т. Київ: Наукова думка. 1970–1980. Т. 3. 580 с.

20. Богачова Л. Л. Принципи європейського і національного права (порівняльно-правовий аналіз критеріїв класифікація). *Державне будівництво та місцеве самоврядування.* 2013. Вип. 26. С. 47–60.

21. Бойко В. О. Державно-приватне партнерство у сфері кібербезпеки: кейс Німеччина: аналітична записка. Київ: Національний інститут стратегічних досліджень, Відділ інформаційної безпеки та розвитку

інформаційного суспільства Національного інституту стратегічних досліджень 2018. 18 с.

22. Большая Советская Энциклопедия. 3-е изд. Москва, 1971. Т. 5. 640 с.

23. Бриль К. І. Правозастосовний акт як особливий вид індивідуальних правових актів: дис ... канд. юрид. наук: 12.00.01. Київ: Б.в., 2008. 214 с.

24. Бурбика В. О. Адміністративно-правові засади взаємодії органів місцевого самоврядування з правоохоронними органами: дисертація ... канд. юрид. наук, спец.: 12.00.07 адміністративне право і процес; фінансове право; інформаційне право. Суми: СумДУ, 2017. 251 с.

25. Бурячок В. Л., Гнатюк С. О., Корченко О. Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. *Інформаційна безпека: виклики і загрози сучасності*: зб. матеріалів наук.-практ. конф. (5 квітня 2013 року, м. Київ). Київ: Наук.-вид. центр НА СБ України, 2013. 416 с.

26. Бурячок В. Л., Корченко О. Г., Хорошко В. О., Кудінов В. А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. *Захист інформації*. 2013. Том 15, № 1. С. 5–12.

27. Бусел В. Т. Великий тлумачний словник сучасної української мови. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.

28. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України: офіційний web-сайт Центру досліджень соціальних комунікацій НБУВ. URL: http://www.nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350. (дата доступу – 13.03.2017).

29. Бухарєв В. В. Адміністративний договір як важлива адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток державності та права в Україні: реалії та перспективи*:

Матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 вересня 2018 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2018. С. 61–64.

30. Бухарєв В. В. Адміністративно-правові методи забезпечення кібербезпеки в Україні. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи*: Міжнародна науково-практична конференція, м. Київ, 13-14 березня 2015 р. – К.: Центр правових наукових досліджень, 2015. С. 59–62.

31. Бухарєв В. В. Адміністративно-правові форми забезпечення кібербезпеки в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2015. Вип. 33. Ч. 2. С. 61–66.

32. Бухарєв В. В. Види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2016. Вип. 6-2. Т. 2. С. 188–192.

33. Бухарєв В. В. Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2017. Вип. 43. Т. 3. С. 128–133.

34. Бухарєв В. В. Напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. *Наше право*. 2018. № 2. С. 52–57.

35. Бухарєв В. В. Нормотворчість як адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток сучасного права в умовах глобальної нестабільності*: Матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 9-10 вересня 2016 р.) – Одеса: ГО «Причорноморська фундація права», 2016. С. 78–79.

36. Буяджа С. А. Генезис правового регулювання боротьби з кіберзлочинністю у світі. *Науковий вісник Ужгородського національного університету*. 2014. Вип. 29, ч. 2, том 4/2. С. 145–149.

37. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В. Т. Бусел]. Ірпінь: ВТФ «Перун», 2004. 1440 с.

38. Величко Д. М. Джерела міжнародно–правового регулювання праці: дис. канд. юрид. наук: 12.00.05 «Трудове право; право соціального забезпечення». Харкыв, 2008. 199 с.

39. Велігоцька Ю. С. Конспект лекцій з курсу «Методи оптимізації архітектурно-містобудівельних рішень» (для студентів 6 курсу спеціальностей 7.06010202 і 8.06010202 «Містобудування») / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків: ХНУМГ, 2015. 58 с.

40. Венедиктов В. С. Статус працівників органів внутрішніх справ України як державних службовців: наук.-практ. посіб. / В. С. Венедиктов, М. І. Іншин; Національний ун-т внутрішніх справ. Харків: Видавництво НУВС, 2003. 187 с.

41. Вехов В. Б., Голубєв В.А. Расследование компьютерных преступлений в странах СНГ. *ВА МВД России*. 2004. 300 с.

42. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI століття: міжнародний документ, декларація від 17.04.2000. URL: http://zakon3.rada.gov.ua/laws/show/995_443. (дата доступу – 31.03.2016).

43. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО Издательство «Юрлитинформ», 2002. 86 с.

44. Волох О. К. Питання кібернетичної безпеки в умовах розбудови інформаційного суспільства. *Юридичний науковий електронний журнал*. 2016. № 4. С. 104–107.

45. Галаган И. А. Административная ответственность в СССР. Изд. Воронежского ун-та, 1970, 251 с.

46. Галунько В. В., Єщук О. М. Поняття та зміст адміністративно-правового регулювання. *Actual problems of corruption prevention and*

counteraction. 2011. URL: http://www.law-property.in.ua. (дата доступу – 31.04.2016).

47. Гетьман-П’ятковська І. А. Право та мораль: теоретико правові проблеми співвідношення та взаємодії: дис ... канд. юрид. наук. Київ: б. в., 2007. 210 с.

48. Глушков В. М. Енциклопедія кібернетики у т. 1. Київ, 1974. 596 с.

49. Гончарук С. Т. Адміністративна відповідальність за законодавством України. Київ: КМУЦА, 1995. 78 с.

50. Городецька І. А. Сутність адміністративно-правового регулювання суспільних відносин у галузі охорони, використання і відтворення тваринного світу. *Форум права*. 2016. № 1. С. 60–66.

51. Горшенев В. М., Шахов И. Б. Контроль как правовая форма деятельности. Москва: Юрид. лит., 1987. 176 с.

52. Грайворонський М. В. Сучасні підходи до забезпечення кібернетичної безпеки. Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (м. Київ, 21–23 травня 2015). Київ: НТУУ «КПІ», 2015. С. 10–17.

53. Грінченко Б. Словник української мови. Київ: Видавництво Академії Наук Української РСР, 1958. Том № 2. 766с

54. Давыдов П. М. Обвинительный приговор основная форма реализации уголовной ответственности. Свердловск: СЮИ, 1979. 142 с.

55. Декларація принципів «Побудова інформаційного суспільства глобальне завдання у новому тисячолітті»: міжнародний документ, декларація від 12.12.2003. URL: http://zakon3.rada.gov.ua/laws/show/995_c57. (дата доступу – 21.05.2016).

56. Демин А. В. Нормативный договор как источник административного права. *Государство и право*. 1998. № 2. С. 18.

57. Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3. (дата доступу – 15.06.2017).

58. Діордіца І. В. Класифікація кіберзагроз та їх легітимізація у нормативно-правових актах України. *Підприємництво, госп-во і право*. 2017. № 10. С. 206–211.

59. Діордіца І. В. Поняття та зміст національної системи кібербезпеки. *Національний юридичний журнал: теорія та практика*. 2016. С. 37–42.

60. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. *Інформаційне право*. 2017. № 7. С. 109–110.

61. Діордіца І. В. Суб'єкти забезпечення кібербезпеки. *Науковий вісник Ужгородського національного університету.* 2017. Вип. 45. Том 1. С. 160–165.

62. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. URL: http://goal-int.org/sistemazabezpechennya-kiberbezpeki-sutnist-ta-priznachennya. (дата доступу – 17.08.2017).

63. Добржанська О. Л., Демцов А. А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102 (1). С. 111–116.

64. Довгань О. Д. Інформаційні ресурси: національні та державні, зміст, поняття. *Інформація і право*. 2015. № 3 (15). С. 85–91.

65. Доктрина інформаційної безпеки України: медіаексперт вказала на недоліки документа. *Інтернет видання «Апостроф».* URL: https://apostrophe.ua/ua/news/society/media/2017-02-28/doktrina-informacionnoj-bezopasnosti-ukrainy-mediaekspert-ukazala-na-nedostatki-dokumenta/88336. (дата доступу – 31.09.2017).

66. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017. URL: http://zakon2.rada.gov.ua/laws/show/47/2017. (дата доступу – 24.08.2017).

67. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України*. 2010. № 3. С. 129–136.

68. Єшук Є. О. Адміністративно-правова охорона: деякі теоретичні аспекти. *Порівняльно-аналітичне право*. 2013. № 4. С. 183–185.

69. Жила С. Ю. Механізм адміністративно-правового регулювання діяльності Національної поліції із забезпечення громадської безпеки. *Південноукраїнський правовий часопис*. 2015. № 3. С. 123–126.

70. Заброда Д. Г. Взаємодія суб'єктів боротьби з корупцією (адміністративно-правовий аспект): дис. … канд. юрид. наук: 12.00.07. Київ, 2005. 235 с.

71. Загальна теорія держави і права: підручник / М. В. Цвік, О. В. Петришин, Л. В. Авраменко. Харків: Право. 2011. 584 с.

72. Загальне адміністративне право: підручник / І. С. Гриценко, Р. С. Мельник, А. А. Пухтецька Київ: Юринком Інтер. 2015. 568 с.

73. Закон «Про кібербезпеку» як спроба тотального контролю. *Електронне видання газети «Українська правда»*. URL: https://www.pravda.com.ua/columns/2017/06/10/7146438/. (дата доступу – 20.11.2017).

74. Зеленецкий В. С. Общая теория борьбы с преступностью: ч. 1 Концептуальные основы. Харків: Основа, 1994. 375 с.

75. Іванчук Н. В. Взаємна відповідальність особи і держави в контексті розбудови сучасної української держави: дис... канд. юрид. наук: 12.00.01 / Київський національний ун-т внутрішніх справ. Київ, 2007. 185 арк.

76. Інформаційна кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Київ: ДУТ, 2015. 288с.

77. Кесареева Г. П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид.наук: 12.00.08. Москва, 2002. 236 с.

78. Китай схвалив новий закон про кібербезпеку. *Українські національні новини «інформаційне агентство UNN»*. URL: http://www.unn.com.ua/uk/news/1616273-kitay-skhvaliv-noviy-zakon-pro-kiberbezpeku. (дата доступу – 23.11.2017).

79. Кібербезпека на порядку денному. URL: https://www.radiosvoboda.org/a/28722877.html. (дата доступу – 02.01.2018).

80. Кібербезпека: віртуальна зброя держави. URL: https://biz.nv.ua/ukr/experts/kutsenko1/kiberbezpeka-zbroja-derzhavi-u-virtualnij-ploshchini-2014774.html. (дата доступу – 10.01.2018).

81. Ківалов С. В., Біла Л. Р. Адміністративне право України: навчально-методичний посібник. Вид. друге, перероб. і доп. Одеса: Юридична література, 2002. 312 с.

82. Кобзєва Т. А. Адміністративно-правове забезпечення управління фінансовою системою України: монографія. Суми: СумДУ, 2018. 433 с.

83. Коваленко Н. В. Про правовий режим кібербезпеки в Україні. *Актуальні проблеми вітчизняної юриспруденції.* 2016. № 3. С. 96–100.

84. Кодекс України про адміністративні правопорушення: кодекс від 07.12.1984 № 8073 X. *Відомості Верховної Ради України*. 1984. № 51. Ст. 1122. URL: http://zakon2.rada.gov.ua/laws/show/80731-10/conv. (дата доступу – 14.01.2018).

85. Кожура Л. О. Адміністративно-правовий захист та охорона: поняття та співвідношення. *Науковий вісник Ужгородського національного університету.* 2015. Вип. 35, Ч. 1, Т. 2. С. 119–122.

86. Козюбр М. І. Загальна теорія права: підручник. Київ: Ваіте. 2015. 392 с.

87. Колодій А. М. Принципи права: генеза, поняття, класифікація та реалізація. *Альманах права*. 2012. Вип. 3. С. 42–46.

88. Коломієць О. В. Проблеми національного законодавства в сфері боротьби з кіберзлочинністю та шляхи їх вирішення. *Гілея*. 2012. Вип. 57 (№ 2). С. 546–551.

89. Колпаков В. К. Адміністративне право України. Київ: Юрінком-Інтер, 2004. 724 с.

90. Колпаков В. К., Кузьменко О. В. Адміністративне право України: підручник. Київ: Юрінком Інтер, 2003. 544 с.

91. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу: міжнародний документ, конвенція від 29.05.2000. URL: http://zakon5.rada.gov.ua/laws/show/994_238/page. (дата доступу – 23.01.2018).

92. Конвенція про кіберзлочинність: міжнародний документ, конвенція від 23.11.2001. *Офіційний вісник України*. 2007. № 65. Ст. 107. URL: http://zakon3.rada.gov.ua/laws/show/994_575/conv. (дата доступу – 22.11.2017).

93. Кондаков Н. И. Логический словарь. Москва: Наука, 1971. 656 с.

94. Конституція України: закон від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

95. Корченко О. Г., Бурячок В. Л., Гнатюк С. О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Ukrainian Scientific Journal of Information Security.* 2013. № 19. С. 40–44.

96. Крестовська Н. М., Матвеева Л. Г. Теорія держави і права: підручник. Практикум. Київ: Юрінком Інтер, 2015. 584 с.

97. Кримінальний кодекс України: кодекс, закон від 05.04.2001 № 2341 III. *Відомості Верховної Ради України*. 2001. № 25. Ст. 131. URL: http://zakon3.rada.gov.ua/laws/show/2341-14/conv. (дата доступу – 11.07.2017).

98. Кримінальний процесуальний кодекс України: науково-практичний коментар: у 2 т. Т. 1 / О. М. Бандурка, Є. М. Блажівський, Є. П. Бурдоль та

ін.; за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків: Право, 2012. 768 с.

99. Кудрявцев В. Н. Правовое поведение: норма и патология. Москва, 1997. 223 с.

100. Кузьменко Б. В. Інформаційна диверсія та інформаційний саботаж інструменти кібертероризму. *Роль правоохоронних органів у формуванні правової держави в умовах євроінтеграції України*: матеріали Всеукр. підсумк. наук.-практ. конф. (м. Київ, 12 березня 2015 р.). Київ: Нац. акад. внутр. справ, 2015. Ч. 1. С. 20–22.

101. Кулешов О. О. Діяльність адміністративної служби міліції по припиненню правопорушень (організаційно-правовий аспект): дисертація. Ірпінь, 2005. 198 с.

102. Курінний Є. В. Предмет і об’єкт адміністративного права України: характеристика категорій в умовах системного реформування: дис... д-ра юрид. наук: 12.00.07 / Національна академія внутрішніх справ України. Київ, 2004. 428 с.

103. Лисенкова О. Законодавство України: необхідне нормативне визначення поняття. *Право України*. 1999. № 11. С. 93–97.

104. Литвин І. Сутність системи суб’єктів адміністративно-правових відносин у сфері надання освітніх послуг. *Підприємництво, господарство і право.* 2016. № 5. С. 63–66.

105. Литвиненко В. І. Адміністративно-правові форми протидії корупції в Україні. *Наук. вісн. Херсон. держ. ун-ту.* Вип. 2 (№ 3-2). С. 50–55.

106. Ліпкан В. А. Стратегічні комунікації: словник. Київ: ФОП Ліпкан О. С., 2016. 416 с.

107. Літошенко О. С. Адміністративна відповідальність в системі юридичної відповідальності: дис... канд. юрид. наук: 12.00.07 / Київський національний економічний ун-т. Київ, 2004. 221 с.

108. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: дис. … канд. юрид. наук: спец. 12.00.07. Київ, 2005. 2010 с.

109. Лук'янчук Р. В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник Національної академії державного управління при Президентові України*. 2015. № 3. С. 110–117.

110. Лук'янець Д. М. Інститут адміністративної відповідальності: проблеми розвітку: монографія. Київ: Інститут держави і права ім. В. М. Корецького НАН України, 2001. 136 с.

111. Лунев А. Е. Теоретические проблемы государственного управления. Москва: Наука, 1974. 247 с.

112. Макаренко Л. О. Теоретичні закономірності дії правових приписів: дис... канд. юрид. наук: 12.00.01 / НАН України; Інститут держави і права ім. В. М.Корецького. Київ, 2004. 191 с.

113. Мангутов И. С., Уманский Л. И. Организатор и организаторская деятельность. Л.: ЛГУ, 1975. С. 103–127.

114. Мандюк О. О. Індивідуальні адміністративні акти: теорія та практика застосування: дисертація на здобуття наукового ступеня кандидата юридичних наук: 12.00.07 адміністративне право і процес; фінансове право; інформаційне право / Міністерство освіти і науки України, Національний університет «Львівська політехніка». Львів, 2017. 213 с.

115. Марков В. В. Поняття та види форм адміністративно-правової протидії кіберзлочинності в Україні. *Європейські перспективи*. 2015. Вип. 7. С. 43–47.

116. Марущак Ю. В. Адміністративно-правова охорона майнових та немайнових прав власності в Україні. *Науковий вісник Національного університету біоресурсів і природокористування України*. 2014. Вип. 197, ч. 2. С. 238–242.

117. Марченко М. Н. Проблемы теории государства и права. Москва: Проспект. 2001. 687 с.

118. Мацелик Т. О. Суб'єкти адміністративного права: поняття та система (монографія). Ірпінь.: Видавництво Національного університету податкової служби України. 2013. 342 с.

119. Мельник О. М. Проблеми охорони прав суб'єктів інтерелктуальної власності в Україні. Харків: Видавництво ХНУВС, 2002. 362 с.

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

121. Меркель: уряд Німеччини актуалізував стратегію кібербезпеки. URL: http://vgolos.com.ua/news/merkel_uryad_nimechchyny_aktualizuvav_strategiyu_kiberbezpeky_256173.html. (дата доступу – 13.02.2018).

122. Мосьондз С. О. Адміністративно-правова охорона сфери науки в Україні: концептуальне бачення. *Науково-аналітичний журнал «Митна справа»*. 2012. № 5 (83), частина 2, книга 2. С. 102–107.

123. Муравйов К. В. Проблеми реалізації державної політики у сфері виконання кримінальних покарань: монографія. Київ: МП Леся, 2016. 412 с.

124. Науково-практичний коментар Кримінального процесуального кодексу України / В.М. Тертишник. Київ: Правова Єдність, 2017. 824 с.

125. Наумов А. В. Реализация уголовного права и деятельность следователя. Волгоград: ВСШ, 1987. 83 с.

126. Новий тлумачний словник української мови: у 3 т. / В. Яременко, О. Сліпушко. Київ: Аконіт, 2003. Т. 3: ОБЕ-РОБ. 927 с.

127. Новоселов В. И. Правовое положение граждан в отраслях советского государственного управления. Саратов: Изд-во Сарат. ун-та, 1977. 166 с.

128. Ожегов С. И. Словарь русского языка. Москва: Русский язык, 1984. 797 с.

129. Олійник В. М. Поняття та принципи взаємодії при виявленні та розкритті злочинів у сфері господарської діяльності. *Форум права*. 2012. № 2. С. 511–518.

130. Орбан-Лембрик Л. Е. Соціальна психологія: підручник: у 2 кн. Кн. І: Соціальна психологія особистості і спілкування. Київ: Либідь, 2004. 576 с.

131. Орлов Ю. Ю. Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України. *Наук. вісн. Нац. акад. внутріш. справ.* 2011. № 6. С. 3–9.

132. Педешко А. І. Адміністративна відповідальність за порушення митних правил: дис... канд. юрид. наук: 12.00.07 / Університет внутрішніх справ. Харків, 2000. 176 с.

133. Перун Т. С. Адміністративна відповідальність в системі заходів забезпечення інформаційної безпеки. URL: http://aphd.ua/publication-229/. (дата доступу – 14.02.2018).

134. Петрик В. М. Забезпечення інформаційної безпеки держави: підручник / за заг. ред. О. А. Семченка та В. М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.

135. Петрушенко В. Л. Філософія: навчальний посібник, 2-е видання, виправлене і доповнене. Київ: Каравела, 2002. 544 с.

136. Пивненко В. П. Проблеми підвищення ефективності роботи правоохоронних органів в Україні у боротьбі з організованою злочинністю. *Вісник Академії правових наук*. 1997. Вип. 1. С. 157–159.

137. Приймак Ю. Ю. Національні інформаційні ресурси джерело державних інформаційних продуктів та послуг. *Державне управління: теорія та практика.* 2009. № 2. С.15–25.

138. Про Державну службу спеціального зв’язку та захисту інформації України: закон від 23.02.2006 №3475-IV. *Відомості Верховної Ради України*. 2006. № 30. Ст. 1094.

139. Про державну таємницю: закон від 21.01.1994 № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 422.

140. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: рішеня від 29.12.2016. *Офіційний вісник України*. 2017. № 16. Ст. 10.

141. Про затвердження Положення про Міністерство оборони України: постанова від 26.11.2014 № 671. *Офіційний вісник України*. 2014. № 97. Ст. 51.

142. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: постанова від 23.08.2016 № 563. *Офіційний вісник України.* 2016. № 69. Ст. 50.

143. Про захист інформації в інформаційно-телекомунікаційних системах: закон від 05.07.1994 № 80/94 ВР. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286.

144. Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України: указ від 06.12.2001 № 1193/2001. *Офіційний вісник України*. 2001. № 50. Ст. 25.

145. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: від 31.07.2000 № 928/2000. *Офіційний вісник України*. 2000. № 31. Ст. 11.

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

147. Про Національний банк України: закон від 11.10.2017 № 679 XIV. *Відомості Верховної Ради України*. 1999. № 29. Ст. 238.

148. Про національну безпеку України: закон України від 21.06.2018 № 2469-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2469-19/conv. (дата доступу – 23.07.2018).

149. Про Національну поліцію: закон від 02.07.2015 № 580-VII. *Офіційний вісник України*. 2015. № 63. Ст. 33.

150. Про нову редакцію Воєнної доктрини України: указ від 24.09.2015 №555/2015. *Офіційний вісник України*. 2015. № 22. Ст. 19.

151. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 №2163-VIII. *Голос України.* 2017. № 208. URL: http://zakon2.rada.gov.ua/laws/show/2163-19. (дата доступу – 24.07.2018).

152. Про Положення про Міністерство оборони України та Положення про Генеральний штаб Збройних Сил України: указ від 06.04.2011 №406/2011. *Офіційний вісник України*. 2011. № 29. Ст. 153.

153. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», затверджена Указом Президента України від 15.03.2016 № 96/2016. URL: http://zakon5.rada.gov.ua/laws/show/96/2016. (дата доступу – 29.07.2017).

154. Про розвідувальні органи України: закон від 22.03.2001 №2331-III. *Офіційний вісник України*. 2001. № 15. Ст. 642.

155. Про Службу безпеки України: закон від 25.03.1992 №2229-XI. *Відомості Верховної ради України*. 1992. № 27. Ст. 382.

156. Про стандартизацію: Закон України від 05.06.2014. URL: http://zakon2.rada.gov.ua/laws/show/1315-18. (дата доступу – 12.08.2018).

157. Про Стратегію кібербезпеки України: указ від 15.03.2016 № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 69.

158. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження від 20.09.2017 № 649-р. *Офіційний вісник України*. 2017. № 78. Ст. 109.

159. Прокопенко О. Ю. Завдання органів внутрішніх справ як суб'єктів забезпечення правопорядку в регіоні. *Пріоритетні проблеми реформування системи законодавства України*: матеріали міжнародної науково-практичної конференції (м. Київ, 23–24 липня 2015 р.). Київ: Науково-дослідний інститут публічного права, 2015. С. 174–176.

160. Рабінович П. М. Основи загальної теорії права і держави: навчальний посібник. Київ: ІСДО, 1995. 393 с.

161. Разумовский О. С. Закономерности оптимизации в науке и практике. Новосибирск: Наука, 1990. 174 с.

162. Риндюк В. І. Нормотворча діяльність: навч.-метод. посіб. для самост. вивч. дисц. Київ: КНЕУ, 2009. 162 с.

163. Ронжин В. Н. О понятии и системе принципов социалистического права. *Вестник МГУ*. Сер.11. Право. 1977. № 2. С. 34.

164. Рябченко О. П. Держава і економіка: адміністративно-правові аспекти взаємовідносин: монографія / за заг. ред. О. М. Бандурки. Харків: Вид-во Ун-ту внутр. справ, 1999. 304 с.

165. Ряшко О. В. Законність у контексті профілактики правопорушень в службовій діяльності міліції України: дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07. Київ, 2006. 217 с.

166. Савицькиій Ю. Досвід Польщі для України: чому варто робити ставку на високі технології? URL: https://www.radiosvoboda.org/a/27631224.html. (дата доступу – 24.08.2017).

167. Самілик Л. О. Співвідношення понять «суб'єкт права», «особа», «суб'єкт правовідносин», «учасник відносин». *Право і суспільство*. 2016. № 1. С. 89–93.

168. Санжарук Т. О. Поняття «суб'єкт права» та «суб'єкт правовідносин»: питання розмежування. *Актуальні проблеми держави і права.* 2003. С. 91–95.

169. Скакун О. Ф. Теорія держави і права: навчальний посібник. Харків: Консул, 2009. 221 с.

170. Скакун О. Ф. Теорія держави і права: підручник. Харків: Еспада, 2009. 752 с.

171. Скакун О. Ф. Теорія права і держави: підручник. 3-те видання. Київ: Алерта; ЦУП, 2011. 524 с.

172. Скворцов С. С. Адміністративний договір як засіб управлінської діяльност:і автореф. дис. … канд.юрид.наук: 12.00.07. Харків: НУВС, 2005. 25 с.

173. Словник іншомовних слів / [за ред. О.С. Мельничука]. Київ, 1974. 776 с.

174. Сокольська Т. В. Якісна складова конкурентоспроможності продукції агросфери: дис ... канд. екон. наук. Біла Церква: б. в., 2009. 210 с.

175. Спасибо І. А. Щодо історії виникнення глобальної мережі інтернет. *Право та інновації*. 2014. № 3 (7). С. 15–25.

176. Старилов Ю. Н. Курс общего административного права в 3-х томах. Москва: Норма, 2002. 728 с.

177. Створення глобальної культури кібербезпеки: резолюція Генеральної Асамблеї ООН від 20.12.2002 №57/239. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement. (дата доступу – 13.03.2018).

178. Стефанчук Р. О. Цивільне право України: навчальний посібник. Київ: Наукова думка, 2004. 361 с.

179. Стефанюк В. С. Судовий адміністративний процес. Харків: Консум, 2003. 473 с.

180. Страчук О. В. Щодо поняття принципів права. *Часопис Київського університету права.* 2012. № 2. С. 40–43.

181. Сурилов А. В. Теория государства и права: учеб. пособие. Київ; Одесса: Выща шк., 1989. 439 с.

182. Сучасний тлумачний словник української мови: 100 000 слів / За заг. ред. д-ра філол. наук, проф. В. В. Дубічинського. Харків: ВД «ШКОЛА», 2009. 1008 с.

183. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. *Офіційний web-сайт Центру досліджень соціальних комунікацій НБУВ*. URL: http://nbuviap.gov.ua/index.php?option=com_content&view =article&id=2759:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam&catid=8&Itemid=350. (дата доступу – 22.02.2017).

184. Теорія держави і права: Академ. Курс: підручн. / За ред. О. В. Зайчука, Н. М. Оніщенко. Київ: Юринком-Інтер, 2006. 688 с.

185. Теорія держави і права: навч. посіб. для підгот. фахівців з інформ. безпеки / О. О. Тихомиров, М. М. Мікуліна, Ю. А. Іванов та ін.; за заг. ред. Л. М. Стрельбицької. Київ: Кондор-Видавництво, 2016. 332 с.

186. Теорія держави і права: навчальний посібник / А. М. Колодій, В. В. Копейчиков, С. Л. Лисенков. Київ: Юрінком Інтер, 2002. 368 с.

187. 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. Харків: Право, 2014. 368 с.

188. Теорія держави і права: підручник / кол. авт.; кер. авт. кол. канд. юрид. наук, проф. Ю. А. Ведєрніков. 2-е вид. перероб. і доп. Дніпропетровськ: Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2015. 468 с.

189. Теорія держави та права: [підручник): [за вимогами кредитно-модульної системи навчання] / Є. О. Гіда, Є. В. Білозьоров, А. М. Завальний та ін.: за заг. ред. Є. О. Гіди. Київ: ФОП О. С. Ліпкан, 2011. 576 с.

190. Теремецький В. І. Поняття адміністративно-правового регулювання у сфері оподаткування. *Держава та регіони*. Серія «Право». 2012. № 1 (35). С. 50–54.

191. Тихомиров О. О. Цивільно-правова відповідальність за інформаційні правопорушення: загальнотеоретичні аспекти. *Порівняльно-*

аналітичне право [Електронне науково-фахове видання]. 2015. № 2. С. 37–40. URL: http://www.pap.in.ua. (дата доступу – 23.03.2017).

192. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері: навч. посіб. Київ: Нац. акад. СБУ, 2015. 172 с.

193. У Великобританії створили реабілітаційний центр для кіберзлочинців. URL: http://ms.detector.media/web/cybersecurity/u_velikobritanii_stvorili_reabilitatsiyniy_tsentr_dlya_kiberzlochintsiv/. (дата доступу – 28.08.2018).

194. У Німеччині різко зросла кіберзлочинність. URL: https://www.dw.com/uk/у-німеччині-різко-зросла-кіберзлочинність/a-38555191. (дата доступу – 29.09.2017).

195. Удосконалення законодавства щодо протидії загрозам національній безпеці в інформаційній сфері необхідне для блокування російських кібератак СБУ. *Офіційний WEB-сайт Служби безпеки України.* URL: https://ssu.gov.ua/ua/news/1/category/2/view/5025#.1BtQx74C.dpbs. (дата доступу – 12.08.2018).

196. Фелик В. І. Адміністративно-правове забезпечення профілактичної діяльності Національної поліції України: монографія. Харків, 2016. 511 с.

197. Философский словарь / Под ред. И. Т. Фролова. 5-е изд. Москва: Политиздат, 1986. 590 с.

198. Философский словарь / Под ред. И. Т. Фролова. 7 изд., перераб. и доп. Москва: Республика, 2001. 719 с.

199. Философский словарь / Под ред. М. М. Розенталя. Москва: Политиздат, 1972. 496 с.

200. Фріс П. Л. Кримінально-правова політика України: автореферат. дис. д-ра юрид. наук: 12.00.08 / Національна академія внутрішніх справ України. - К., 2005. 38 с.

201. Фролов Ю. М. Суб'єкти адміністративного права: сутність та підстави класифікації. *Актуальні проблеми права: теорія і практика*. 2012. № 25. С. 549–557.

202. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162–169.

203. Харитонова О. І. Адміністративно-правові відносини: концептуальні засади та правова природа. Одеса, 2004. 328 с.

204. Хропанюк В. Н. Теория государства и права / Под ред. В. Г. Стрекозова. Москва: Интерстиль, 2000. 377 с.

205. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40–44. Ст. 356.

206. Чумак О. О. Адміністративно-правові засади діяльності державної виконавчої служби в Україні в умовах реформування органів виконавчої влади.: дис... докт. юрид. наук: 12.00.07 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2016. 483 с.

207. Шаповал В. Суб'єкти конституційного права України: Постановка проблем теоретичного визначення. *Право України*. 2000. № 8. С. 21.

208. Шатрава С. О. Юридична відповідальність як гарантія забезпечення законності діяльності судової міліції. *Форум права*. 2009. № 2. С. 423–429.

209. Шевченко О. А. Поняття принципу невідворотності кримінальної відповідальності. *Науковий вісник ДДУВС*. 2012. № 3. С. 460–468.

210. Шеломенцев В. П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2010. № 23. С. 342–348.

211. Шморгун Л. Г. Менеджмент організацій: навч. посіб. / Л. Г. Шморгун. Київ: Знання, 2010. 462 с.

212. Шульга А. М. Теория государства и права: пособие для подготовки к государственному (выпускному) экзамену. Харьков, 2000. 132 с.

213. Щодо Закону України «Про основні засади забезпечення кібербезпеки України». *Офіційний web-сайт kmp.ua (Аналітика)*. URL: http://kmp.ua/uk/analytics/infoletters/regarding-the-law-of-ukraine-on-the-basic-principles-of-cybersecurity-protection-of-ukraine/. (дата доступу – 22.01.2016).

214. Юркова Є. В. Межі адміністративно-правової охорони права інтелектуальної власності в Україні. *Форум права*. 2009. № 3. С. 710–714.

215. Явич Л. С. О принципе научности в работе советского государственного аппарата. *Правоведение*. 1978. № 2. С. 64.

216. Як це робила Польща: досвід боротьби з кіберзагрозами. *Електронне видання «Економічна правда».* URL: https://www.epravda.com.ua/columns/2017/10/12/630044/. (дата доступу – 19.09.2017).

217. Якість і безпека: сучасні реалії: матеріали наук.-практ. конф., 02-03 берез. 2017 р. / Вінниц. нац. техн. ун-т, Вінниц. нац. аграр. ун-т, Вінниц. мед. коледж ім. Данили Заболотного. Вінниця: ВНТУ, 2017. 91 с.

218. Bundesministerium des Innern. Cyber–Sicherheitsstrategie für Deutschland. Februar 2011. URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicatio nFile

219. Computer-related crime. Recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems / Strasbourg. Council of Europe, Pub. And Documentation Service. Croton N.Y.: Manhattan Pub. Co. 1990. 114 p.

220. Cyberbezpieczeństwo / Ministerstwo Cyfryzacji Official website. URL: https://www.gov.pl/cyfryzacja/cyberbezpieczenstwo

221. Cybersecurity in Japan / Published: January 2018. URL: https://gettingthedealthrough.com/area/72/jurisdiction/36/cybersecurity-japan/

222. How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par With the Rest of the World. URL: https://www.cfr.org/blog/how-japans-new-cybersecurity-strategy-will-bring-country-par-rest-world.

223. Marshall J. H. Office of Legal Education Executive Office for United States Attorneys / J. H. Marshall, M. W. Balle. 2010. 213 p.

224. Rosenbach Markel. Nationales Cyber–Abwehrzentrum. Spiegel OnlineNetzwelt, 21 März 2011. URL: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,747140,00.html

225. Watson Farley & Williams, "Briefing: The New German IT Security Act," February 2016, http://www.wfw.com/wpcontent/ uploads/2016/02/WFW-Briefing-GermanyIT-Security-Feb-2016-EN-15-Feb.pdf

ДОДАТКИ

Додаток 1

Список публікацій здобувача:

Статті у наукових фахових виданнях:

6. Бухарєв В. В. Адміністративно-правові форми забезпечення кібербезпеки в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2015. Вип. 33. Ч. 2. С. 61–66.

7. Бухарєв В. В. Види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2016. Вип. 6-2. Т. 2. С. 188–192.

8. Бухарєв В. В. Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2017. Вип. 43. Т. 3. С. 128–133.

9. Бухарєв В. В. Напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. *Наше право*. 2018. № 2. С. 52–57.

10. Бухарєв В. В. Поняття та особливості кібербезпеки як об’єкту адміністративно-правової охорони. *Європейські перспективи.* 2018. № 3. С. 11–16.

Статті у зарубіжних періодичних наукових виданнях:

3. Бухарєв В. В. Напрямки удосконалення взаємодії суб’єктів забезпечення кібербезпеки України. *Верховенство права*. 2018. № 3. С.71–76.

4. Бухарев В. В. Историко-правовой анализ развития законодательства в сфере обеспечения кибербезопасности. *Legea si viata*. 2018. № 11/2. С. 23–26.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

4. Бухарєв В. В. Адміністративно-правові методи забезпечення кібербезпеки в Україні. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи*: Міжнародна науково-практична конференція, м. Київ, 13-14 березня 2015 р. – К.: Центр правових наукових досліджень, 2015. С. 59–62.

5. Бухарєв В. В. Нормотворчість як адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток сучасного права в умовах глобальної нестабільності*: Матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 9-10 вересня 2016 р.) – Одеса: ГО «Причорноморська фундація права», 2016. С. 78–79.

6. Бухарєв В. В. Адміністративний договір як важлива адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток державності та права в Україні: реалії та перспективи*: Матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 вересня 2018 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2018. С. 59–62.

Додаток 2

Акти впроваджень

«ЗАТВЕРДЖУЮ»
Відповідальний секретар
Кримінологічної асоціації України
доктор юридичних наук, професор

О. М. Литвинов
5 січня 2018 року

А К Т

впровадження результатів дисертаційного дослідження здобувача наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право (081 – Право) Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» у наукову діяльність Кримінологічної асоціації України

Комісія у складі:

1. Ященка А. М. – доктора юридичних наук, доцента, члена Кримінологічної асоціації України

2. Шевелева К. Є. – кандидата юридичних наук, доцента, члена Кримінологічної асоціації України

3. Цвіркун Н. Ю. – кандидата юридичних наук, доцента члена Кримінологічної асоціації України.

цим актом засвідчує, що результати дисертаційного дослідження Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України», використовуються у наукових дослідженнях Кримінологічної асоціації України.

Зокрема при: 1) вивченні об'єктивних і суб'єктивних факторів, які впливають на рівень, структуру, динаміку, характер порушень законодавства у сфері кібербезпеки України; 2) соціально-кримінологічному дослідженні видів порушень законодавства у сфері кібербезпеки України для визначення способів їх профілактики; 3) вивченні особи правопорушника, дослідження механізму вчинення конкретного проступку, класифікації видів і типів особи правопорушника; 4) розробці наукових рекомендацій щодо усунення чи

нейтралізації явищ, які спричиняють порушення законодавства у сфері кібербезпеки України; 5) розробці заходів, пов'язаних із виявленням осіб, від яких можна очікувати вчинення порушень законодавства у сфері кібербезпеки України, вивчення цих осіб і вжиття дієвих профілактичних заходів упливу на них; 6) визначенні основних напрямків і заходів протидії порушенням законодавства у сфері кібербезпеки, удосконаленні правового регулювання профілактичної діяльності; 7) наданні консультативно-дорадчої допомоги щодо супроводження правотворчого процесу правоохоронних органів; 8) розробці пропозицій та рекомендацій щодо удосконалення національного адміністративного законодавства, яке регулює забезпечення кібербезпеки України.

Впровадження результатів дисертаційного дослідження Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» в наукову діяльність Кримінологічної асоціації України забезпечило розширення науково-методичного інструментарію експертно-кримінологічного дослідження нормативно-правових актів і їх проектів з питань правоохоронної діяльності.

Члени комісії _____ **(А. М. Ященко)**

_____ **(К. Є. Шевелев)**

_____ **(Н. Ю. Цвіркун)**

5 січня 2018 року

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
вул. Кірпи, 2а, м. Київ, 03035
Тел. 228-10-31
E-mail: sipl@.i.ua
www.sipl.com.ua

SCIENTIFIC INSTITUTE OF PUBLIC LAW
2a Kyrpu Str., Kyiv, 03035
Tel. 228-10-31
E-mail: sipl@.i.ua
www.sipl.com.ua

16.01.2020 № 5/1/2-72 На № _____ від _____

ДОВІДКА

про використання результатів дисертації здобувача наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» під час внесення змін і доповнень до законодавства, що регламентує правоохоронну діяльність

Повідомляємо спеціалізованій вченій раді, що результати дисертації Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» спрямовані на визначення особливостей кібербезпеки як об'єкта адміністративно-правової охорони, встановлення видів об'єктів кібербезпеки та кіберзахисту, окреслення систему суб'єктів забезпечення кібербезпеки України та особливостей їх адміністративно-правового статусу, систематизацію адміністративно-правових форм та методів забезпечення кібербезпеки України, узагальнення зарубіжного досвіду забезпечення кібербезпеки використовуються Науково-дослідним інститутом публічного права під час розробки пропозицій та рекомендацій щодо удосконалення національного законодавства та розроблення нових нормативно-правових актів, які регулюють забезпечення кібербезпеки України в межах реалізації теми наукового дослідження. «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації №0115U005495).

Директор Інституту **Галунько В.В.**

«ЗАТВЕРДЖУЮ»
Декан факультету № 4
Харківського національного
університету внутрішніх справ,
кандидат юридичних наук, старший
науковий співробітник, підполковник
поліції

В.В. Марков

«26» січня 2018 року

А К Т

про впровадження результатів дисертаційного дослідження Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України», поданого на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 12.00.07 – адміністративне право та процес; фінансове право; інформаційне право у практичну діяльність Навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору Харківського національного університету внутрішніх справ

Комісія в складі:

Макаренка П.В. – заступника декана з навчально-методичної роботи факультету № 4 Харківського національного університету внутрішніх справ, кандидата психологічних наук, доцента;

Гнусова Ю. В. – завідувача кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ, кандидата технічних наук, доцента;

Струкова В. М. – завідувача кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ, кандидата технічних наук, доцента

цим актом засвідчує, що результати дисертаційного дослідження Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України», поданого на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 12.00.07 – адміністративне право та процес; фінансове право; інформаційне право використовуються у практичній діяльності Навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору Харківського національного університету внутрішніх справ.

Зокрема при: 1) визначенні особливостей кібербезпеки як об'єкта адміністративно-правової охорони; 2) встановленні системи суб'єктів забезпечення кібербезпеки України та особливостей їх адміністративно-правового статусу; 3) окресленні особливостей юридичної відповідальності за порушення законодавства у сфері кібербезпеки України.

Впровадження результатів дисертаційного дослідження Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» у практичну діяльність Навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору Харківського національного університету внутрішніх справ забезпечило розширення науково-методичного інструментарію під час опрацювання зарубіжного досвіду забезпечення кібербезпеки та визначенні можливості його використання в Україні.

Пропозиції дисертанта щодо розвитку форм та методів забезпечення кібербезпеки України, правових засад забезпечення кібербезпеки України взято за основу для підготовки відповідних методичних рекомендацій.

Результати дисертаційного дослідження Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» мають необхідний теоретичний рівень та практичну спрямованість, сприятимуть підвищенню якості правового регулювання діяльності суб'єктів забезпечення кібербезпеки України.

Члени комісії

П.В. Макаренко

Ю.В. Гнусов

В.М. Струков

Міністерство освіти і науки України

Сумський державний університет

ЗАТВЕРДЖУЮ

Перший проректор

Сумського державного університету

_____ В.Д. Карпуша

«_10_» ___вересня_ 2018 р.

АКТ

про впровадження в освітній процес результатів дисертаційного дослідження здобувача Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право

Комісія у складі:

Голова – завідуючий кафедри АГПФЕБ, д.ю.н., доцент Гаруст Ю.В.

Члени комісії – к.ю.н., доцент, доцент кафедри АГПФЕБ Логвиненко М.І.

– к.ю.н., доцент, доцент кафедри АГПФЕБ Рєзнік О.М.

Комісія склала цей акт з приводу розгляду результатів дисертаційного дослідження здобувача Бухарєва Владислава Вікторовича «Адміністративно-правові засади забезпечення кібербезпеки України» і їх використання в освітньому процесі з дисциплін «Адміністративне право», «Судові та правоохоронні органи», кафедри адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету.

Висновок: комісія вважає, що результати проведеного дослідження здобувачем Бухарєвим Владиславом Вікторовичем «Адміністративно-правові засади забезпечення кібербезпеки України» отримані на основі ґрунтовного аналізу та вивчення сутності та особливостей адміністративно-правових засад забезпечення кібербезпеки в Україні, мають комплексний характер та використовуються під час проведення лекцій, семінарських і практичних занять

кафедри адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету зі студентами при вивченні дисциплін «Адміністративне право», «Судові та правоохоронні органи».

Акт виконаний у 2-х примірниках.

Голова комісії Ю.В. Гаруст

Члени комісії М.І. Логвиненко

О.М. Рєзнік