

ПОНЯТТЯ ТА ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ ЯК ОБ'ЄКТА АДМІНІСТРАТИВНО-ПРАВОВОЇ ОХОРОНИ

БУХАРЄВ Владислав Вікторович - здобувач Університету сучасних знань

УДК: 342.95 (477)

У статті, ґрунтуючись на аналізі наукових поглядів учених, розглянуто поняття та визначено особливості кібербезпеки як об'єкта адміністративно-правової охорони.

Наголошується, що адміністративно-правова охорона – це системне явище адміністративного права, сутність якого полягає у діяльності публічних органів, спрямованої на забезпечення прав громадян або підтримання відповідного легального режиму в тій чи іншій сфері суспільного буття. Водночас, адміністративно-правова охорона 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.

Відзначається, що визначення поняття та особливостей кіберпростору є принципово важливим аспектом нашого дослідження, адже на цьому ґрунтується бачення кібербезпеки. Зазначено, що кібербезпека – це певний стан кіберпростору, який характеризується фактичною відсутністю правопорушень, однак, представлений термін має децю більший зміст.

Обґрунтовується, що нормативне визначення поняття «кібербезпеки» є позитивним фактором для правових системи нашої держави. Обстоюється позиція, що кібербезпеку більш доцільно було б розглядати як стан захищеності діяльності людей та держави, власності, інформації цих суб'єктів у кіберпросторі,

із використанням спеціальних електронних приладів, від протиправних посягань.

Наголошується на тому, що на даний час в Україні сформовано специфічну нормативно-правову основу даної проблематики. Більше того, на даний час немає одноманітності поглядів учених з приводу даного питання. З іншого боку, проблематика характеризується великою кількістю особливостей як негативного, так і позитивного забарвлення.

Ключові слова: кібербезпека, забезпечення кібербезпеки, адміністративно-правова охорона, поняття, особливості.

Постановка проблеми

Починаючи з моменту надбання Україною незалежності, вектор державного розвитку було спрямовано на технологічний прогрес та імплементацію у людське життя інформаційних технологій, які на сьогодні 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 всі органи влади, що існують в Україні, провадять ті чи інші функції з використанням новітніх технологій, що фактично спричинило перенесення процесу обміну, обробки та пошуку інформації в електронний простір. Наряду з цим, «цифрова» революція також має низку негативних аспектів, одним з яких є низький рівень кібербезпеки. Ця проблематика неодноразо-

во підіймалася у роботах науковців різних галузей знань. Не є виключенням правова сфера, оскільки саме у її межах було розроблено головні механізми охорони кібербезпеки. Вивчення даного питання є пріоритетним напрямком роботи для правників у галузі адміністративного, кримінального та цивільного права, адже кібербезпека у вигляді об'єкта правової охорони безпосередньо входить у поле інтересів держави.

Стан дослідження

Багато теоретичних питань забезпечення кібербезпеки було у полі зору чималої кількості науковців, зокрема їм приділяли увагу Л.О. Макаренко, Ю.А. Ведерніков, С.С. Скворцов, В.С. Стефанюк, О.Ю. Прокopenko, В.В. Марков, К.І. Бриль, О.О. Мандюк, С.С. Алексеев, О.В. Логінов, Р.О. Стефанчук, А.М. Куліш, О.М. Музичук, А.І. Педешко, О.О. Тихомиров, О.К. Тугарова, І.В. Європіна та багато інших. Однак, незважаючи на чималу кількість наукових праць, поняття та особливості кібербезпеки як об'єкта адміністративно-правової охорони практично залишилось поза увагою вчених.

Саме тому **метою** статті є визначення особливостей кібербезпеки як об'єкта адміністративно-правової охорони.

Виклад основного матеріалу

Наразі існує велика кількість наукових поглядів на проблематику визначення адміністративно-правової охорони. Наявність різних концептуальних підходів щодо питання особливостей зазначеного механізму юридичного забезпечення окремих об'єктів обумовлена фактичною відсутністю його дефініції у законодавчих актах. Галунько В.В. 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 [1, с.242 – 247].

Доволі цікавою є думка Харитонова О.І., який зосереджує увагу на те, що явище адміністративно-правової охорони є окремим правовим інститутом. 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. У 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 [2, 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, спрямованої 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 встановлену, засновану на правових принципах діяльність держави, в особі окремих органів влади, спрямовану на підтримку об'єктів права: інтелектуальної та промислової власності, надр та вод, окремих правомочностей та законних інтересів громадян тощо. Підсумовуючи всі приведені вище відомості, ми можемо стверджувати, що адміністративно-правова охорона сама по собі є доволі цікавим явищем. Однак, метою статті є розгляд інституту адміні-

стративного забезпечення конкретного об'єкту – кібербезпеки. Останнє явище також підлягає самостійному аналізу, так як воно характеризується великою кількістю особливостей.

Як і в ситуації з вищенаведеним у дослідженні поняттям адміністративно-правової охорони, термін кібербезпека на даний час активно обговорюється у науковій літературі. Це дає нам змогу звернутися до напрацювань учених, які розглядали цей об'єкт та його особливості. Як ми розуміємо, 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, у 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 [3, 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 [4, 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.

На думку Діордіца І.В., кібербезпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства

та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [5, с.110]. Схожої думки дотримується Баранов О.А., який зазначає, що кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [6, с.38]. На нашу думку останні погляди не зовсім точно відображають сутність досліджуваного явища, адже не зрозуміло, про які саме важливі інтереси людини і громадянина та системи йдеться мова.

Найбільш змістовним ми вважаємо визначення Корченко О.Г., 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 кібергруп розгортаються навколо інформаційного ресурсу, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем [7, 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 [8, с.41]. Іншою особливістю даного визначення є те, що воно подано з урахуванням 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 стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [9]. Ми вважаємо, що наведене поняття хоча і є лаконічним, однак не відображає усю сутність явища кібербезпеки. Безперечно, нормативне визначення поняття є позитивним фактором для правових систем нашої держави. Однак, на нашу думку, з урахуванням поглядів різних учених кібербезпеку більш доцільно було б роз-

глядати як стан захищеності діяльності людей та держави, власності, інформації цих суб'єктів у кіберпросторі, із використанням спеціальних електронних приладів, від протиправних посягань.

Отже, вище ми розібралися із особливостями адміністративно-правової охорони та кібербезпеки, шляхом аналізу специфіки цих явищ, але науковому розгляду підлягає питання їх співвідношення. Консолідуючи приведені у статті відомості, адміністративно-правову охорону кібербезпеки можна визначити, як діяльність відповідних державних органів, що здійснюється на засадах імперативності та ієрархічності, направлену на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб'єктів у кіберпросторі. Головною особливістю адміністративного забезпечення 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 найбільш пагубні наслідки для суб'єктів, які порушують легальний стан певного об'єкту, 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 недо-

пущення виникнення подібних ситуацій та інших негативних факторів.

Варто відзначити, що стаття 8 Закону України «Про основи національної безпеки України» визначає основні напрями державної політики з питань забезпечення національної безпеки та, зокрема, кібербезпеки, а саме: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [10].

Дані напрямки забезпечення кібербезпеки реалізуються у роботі різних органів державної влади, що також має певний нормативно-правовий вираз. Так, у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах», а саме в статті 10 цього акту розкривається роль державних органів у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. У Законі зазначено, що спеціальний центральний орган виконавчої влади за 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 загрози [11].

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 [12]. 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 напрями розвитку сучасних електронних банківських технологій, 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 [12]. Важливість кібербезпеки у діяльності НБУ

за даних умов обумовлюються тим, що всі вказані типи електронних систем, несуть у собі великий об'єм даних, які за негативних обставин можуть бути використані не за їх цільовим призначенням. До того ж, головним завданням 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 [12]. У 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 також одним із головних обов'язків Національного банку України сьогодні.

Висновок

Проаналізувавши інститут адміністративно-правової охорони кібербезпеки, ми визначили його поняття, відповідно до якого він являє собою діяльність окремих державних органів, що здійснюється на засадах імперативності та ієрархічності, направлену на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб'єктів у кіберпросторі. Слід наголосити на тому, що на даний час в Україні хоча і сформовано специфічну нормативно-правову основу даної проблематики, однак не всі питання протидії цьому негативному явищу вирішено у законодавстві. Більше того, на даний час відсутня єдність поглядів вчених з приводу забезпечення кібербезпеки, тож окреслена проблематика вимагає подальшого вивчення.

Література

1. Адміністративне право України : навчальний посібник у 4-х томах / В.В. Галунько // Херсон : ХМТ, 2011. Т. 334 с
2. Харитонова О.І. Адміністративно-правові відносини : концептуальні засади та правова природа / О.І. Харитонова // Одеса. 2004. 328 с.
3. Коваленко Н.В. Про правовий режим кібербезпеки в Україні / Н.В. Коваленко

ко // Актуальні проблеми вітчизняної юриспруденції. 2016. №3. С.96 – 100.

4. Інформаційна а кібербезпека : соціотехнічний аспект : підручник /- В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко,- С.В. Толюпа // К.:ДУТ. 2015. 288с.

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

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

7. 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.

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

9. Про основні засади забезпечення кібербезпеки України / Закон України від 05.10.2017 № 2163-VIII [Електронний ресурс] Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2163-19>

10. Про основи національної безпеки України : закон від 19.06.2003 №964 – IV // Відомості Верховної Ради України. 2003. №39. ст.351.

11. Про захист інформації в інформаційно-телекомунікаційних системах : закон від 05.07.1994 №80/94 – ВР // Відомості Верховної Ради України. 1994. №31. ст.286.

12. Про Національний банк України: закон від 11.10.2017 №679 – XIV // Відомості Верховної Ради України. 1999. №29. ст.238.

SUMMARY

In the article, based on the analysis of scientific views of scientists, the concept and defined the features of cybersecurity as an object of administrative and legal protection.

It is noted that administrative-legal protection is a systemic phenomenon of administrative law, the essence of which is the activity of public bodies, aimed at ensuring the rights of citizens or maintaining the corresponding legal regime in one or another sphere of social life. At the same time, administrative-legal protection is transformed into a legal institute when it is applied to specific objects. This is explained by the fact that under such conditions administrative-legal protection ceases to be an abstract phenomenon and acquires a concrete mechanism of implementation, which is determined by a separate group of legal norms.

It is noted that the definition of the concept and features of cyberspace is a fundamentally important aspect of our study, because this is based on the vision of cybersecurity. It is noted that cybersecurity is a certain state of the cyberspace, which is characterized by the actual absence of offenses, however, the presented term has a somewhat higher meaning.

It is substantiated that the normative definition of the concept of “cybersecurity” is a positive factor for the legal system of our state. The position is that cybersecurity would be more appropriate to consider as a state of protection of the activities of people and the state, property, information of these subjects in cyberspace, using special electronic devices, from unlawful encroachments.

It is emphasized that in the present time in Ukraine a specific legal and regulatory framework for this issue has been formed. Moreover, there is currently no monotony of scientists’ views on this issue. On the other hand, the problem is characterized by a large number of features, both negative and positive color.

Key words: cybersecurity, providing of cyber security, administrative-legal protection, notions, peculiarities.