УДК 340+35.078.3
DOI https://doi.org/10.32840/pdu.2021.2.4

В. С. Павленко
orcid.org/0000-0002-8860-7696
провідний науковий співробітник
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України

СУТНІСТЬ КІБЕРБЕЗПЕКИ У ТЕОРІЇ ІНФОРМАЦІЙНОГО ПРАВА

Статтю присвячено дослідженню сутності категорії «кібербезпека» у теорії інформаційного права, її ознак і складників і з'ясуванню її ролі у сфері правового регулювання суспільних інформаційних відносин в Україні. Методологія дослідження феномену кібербезпеки загалом базується на положеннях загальнонаукового діалектичного методу. Для повного та ґрунтовного розкриття теми у статті використовуються формально-юридичний і формально-логічний методи наукового пізнання. Обґрунтовується, що державна політика України у сфері національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки тощо. У межах національного сегменту кіберпростору держави, в т. ч. з метою захисту прав, свобод і законних інтересів людини та громадянина у сфері кібербезпеки, національна кібербезпекова політика як фундамент забезпечення інформаційної безпеки держави виступає результатом досягнення інших соціально-економічних цілей суспільства і держави у найбільш важливих сферах життєдіяльності. Аргументується, що важливим інструментом забезпечення національної кібербезпеки виступає встановлення та зміцнення національних, регіональних і міжнародних партнерських відносин у сфері кібербезпеки, забезпечення захисту від кібератак, пом'якшення їх наслідків, розслідування останніх, відновлення після заподіяної ними шкоди, в т. ч. шляхом проведення спільних навчальних програм із застосуванням або створенням відповідних інформаційних мереж зв'язку чи екстреного обміну інформацією про такі загрози. Отже, за сучасних умов кібербезпека виступає домінантним об'єктом правового регулювання і потребує доктринального дослідження як явище, що пронизує майже всі правові відносини в державі. Акцентується увага на тому, що на шляху забезпечення кібербезпеки постає таке явище, як кібероборона як сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в державі та кіберпросторі та спрямовані на забезпечення захисту її суверенітету й обороноздатності, запобігання виникненню збройного конфлікту та можливості для відсічі збройній агресії. У чинному національному законодавстві відсутнє легальне закріплення терміна «кібербезпека», що вкрай негативно позначається на правозастосовній практиці, оскільки його закріплення дасть більш глибоке уявлення про кібербезпеку у практиці його застосування. Доведено, що кібербезпека у широкому розумінні є станом захищеності інформаційного середовища, що гарантує дотримання прав і законних інтересів особистості, суспільства і держави в інформаційній сфері. Запропоновано поняття кібербезпеки закріпити в Законі України «Про національну безпеку України». До основних елементів кібербезпеки віднесено такі, як: безпека додатків, інформація або безпека даних, безпека мережі, відновлення після кібератак, планування кіберзахисту, операційна безпека, хмарна безпека, критична безпека інфраструктури, фізична безпека, навчання кінцевих користувачів. Перспективами подальших наукових пошуків правових засад кібербезпеки стане розроблення теоретичного підходу до принципів забезпечення кібербезпеки держави та визначення норм про кібербезпеку в системі права України, а також розробка теорії кіберзлочинності та юридичної відповідальності за кіберзлочини.

Ключові слова: *кібербезпека, інформаційне право, інформаційна безпека, кіберпростір, інформаційне суспільство, кіберзахист, кібероборона.*

Постановка проблеми. Державна політика України у сфері національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки тощо. У межах національного сегменту кіберпростору держави, в т. ч. з метою захисту прав, свобод і законних інтересів людини та громадянина у сфері кібербезпеки, національна кібербезпекова політика як фундамент забезпечення інформаційної безпеки держави виступає результатом досягнення інших соціально-економічних цілей суспільства і держави у найбільш важливих сферах життєдіяльності. Важливим інструментом забезпечення національної кібербезпеки виступає встановлення та зміцнення національних, регіональних і міжнародних партнерських відносин у сфері кібербезпеки, забезпечення захисту від кібератак, пом'якшення їхніх наслідків, розслідування останніх, відновлення після заподіяної ними шкоди, у т. ч. шляхом проведення спільних навчальних програм із застосуванням або створенням відповідних інформаційних мереж зв'язку чи екстреного обміну інформацією про такі загрози. Отже, за сучасних умов кібербезпека виступає домінантним об'єктом правового регулювання і потребує детального аналізу як явище, що пронизує всі найважливіші правові відносини у державі.

Аналіз останніх досліджень і публікацій. Науково-теоретичний фундамент інформаційного права, зокрема теорії кібербезпеки, закладали вітчизняні та зарубіжні вчені, серед яких: І.В. Арістова [1], І.Л. Бачило [2], В.В. Волинець [3], В.І. Гурковський [4], І.В. Діордіца [5; 6], І.А. Кисарець [7], В.А. Ліпкан [8], А.І. Марущак [9], В.Я. Настюк [10], Г.П. Несвіт [11], С.В. Петров [12], Ю.В. Романчук [13], І.М. Сопілко [14], К.Г. Татарникова [15], В.С. Цимбалюк [16], О.В. Шепета [17] та ін., однак сьогодні сутність кібербезпеки як юридичної категорії у теорії інформаційного права не була досліджена всебічно.

Мета статті полягає у розробці науково-теоретичних засад поняття «кібербезпеки» як правової категорії у теорії вітчизняного інформаційного права.

Методику наукового пошуку становлять: діалектичний, формально-логічний, формально-юридичний метод, розроблені юриспруденцією прийоми та методи тлумачення права (мовний, логічний, систематичний), а також лінгвістичні методи (компонентний, контекстуальний).

Виклад основного матеріалу. Транскордонний характер кіберпростору, його залежність від складних інформаційних технологій, активне використання майданчиків і сервісів кіберпростору усіма верствами населення визначають нові можливості, але і розвивають нові загрози, зокрема для: а) нанесення шкоди правам, інтересам і життєдіяльності особистості, організації, державних органів; б) проведення кібератак проти інформаційних ресурсів із боку кіберзлочинців і кібертерористів; в) використання кіберзброї у рамках спеціальних операцій і кібервоєн, у т. ч. таких, що супроводжують традиційні бойові дії.

Захист інформації сьогодні – це насамперед захист цінностей. Сучасне суспільство живе в інформаційному середовищі, де створення, використання та поширення інформації виступає важливою економічною, політичною та культурною діяльністю. Сучасне суспільство фактично переходить від споживання та надання економічних послуг до економічної інформації, яка робить акцент на інформаційну діяльність, базується на інформаційних технологіях, таких як комп'ютери, мобільні пристрої та Інтернет. Відносини, що виникають у кіберпросторі, дедалі частіше стають об'єктом незаконного посягання. Інформація, яка знаходиться у кіберпросторі, може бути використана і піддатися атаці, що ведеться з далекої відстані. Загрози у кіберпросторі численні й досить різноманітні, як і сам кіберпростір. Вони закладені у самій природі мережі: їх взаємопов'язаність, масштабність, швидкість і складність сприйняття того, що відбувається – все це характеризує випадки кібератак.

Постає питання, чи не існує безумовного захисту від кібератак, які відбуваються не тільки з-за кордону, а й за межами фізичного простору, у цифровому кіберпросторі? За останні роки різко зросла кількість кібератак, що здійснюються за допомогою шкідливого програмного забезпечення. Велика частина цих

атак проводилася щодо фінансового сектора, їх метою були комп'ютери фінансових установ. Інші види кіберзлочинів, особливо порушення законодавства про інтелектуальну власність, особливо привабливі для кіберзлочинців, котрі діють у таких сферах, як піратство у галузі програмного забезпечення, порушення авторських прав тощо.

Держави несуть юридичну, організаційну та політичну відповідальність за забезпечення кібербезпеки. Оскільки кібербезпека і захист важливої інформації й інфраструктури лежать в основі безпеки та процвітання держав, керівництво забезпеченням безпеки має ініціюватися найвищими рівнями державної влади. Уряду слід визначити сфери відповідальності та підзвітності, забезпечити контроль і безперервність всіх необхідних дій. На рівні держави цей підхід передбачає спільну відповідальність, що вимагає скоординованих дій, пов'язаних із попередженням, реагуванням і ліквідацією наслідків із боку всіх міністерств і урядових установ, а також приватного сектору та громадян на загрозі у сфері кібербезпеки. На регіональному і міжнародному рівні цей підхід означає координацію і співробітництво з усіма основними партнерами. І саме уряди держав повинні забезпечити механізм підготовки висококваліфікованих кадрів у сфері кібербезпеки, здатних очолити та скоординувати цю роботу.

Насамперед інформація виступає об'єктом інформаційного права – правової галузі, яка є сукупністю юридичних норм, що визначають поведінку суб'єктів (громадян, юридичних осіб публічного і приватного права тощо) в інформаційній сфері. Як і будь-якій галузі, інформаційне право володіє власним термінологічним апаратом, у складі якого самостійне місце посідає категорія «кібербезпека». Сучасні тенденції розвитку інформаційного права свідчать про динамічний розвиток і видозміну підходів до його правових категорій, появу нових, вдосконалення наявних.

Аналіз змісту терміна «кібербезпека» як феномену у праві необхідно розпочати зі з'ясування сутності юридичних категорій взагалі. Так, незважаючи на роботи вчених, досі відсутнє єдине визначення поняття «юридичний термін», немає однозначного підходу до виділення вимог, які повинні пред'являтися до юридичної термінології в законодавчому тексті. Наявні дослідження проблем формування і функціонування юридичної терміносистеми мають переважно спектральний характер, у них не акцентовано увагу на інформаційно-термінологічному полі. У сучасній нормотворчості актуальними залишаються такі проблеми, як відповідність терміна змісту, що вкладається в це поняття, вживання оціночних понять, мовні похибки в тексті закону. До кінця не досліджені особливості використання дефініцій у текстах інформаційно-правових нормативних актів, недостатньо уваги приділяється аналізу їх змісту.

На переконання М.Л. Давидової, процес формування юридичних термінів у галузі цифрових технологій проходить кілька етапів: 1) формування термінології інформаційно-технологічної сфери (значною мірою за рахунок запозичень із англійської мови); 2) включення її у мову стратегічних документів; 3) вироблення на їх основі власне юридичних термінів, котрі закріплюються у текстах нормативно-правових актів. Аналізуючи прогалини у сфері нормування відносин в інформаційній царині, дослідниця презюмує характерні риси сучасного стану нормотворчої техніки, а саме: 1) декларативність тексту, використання великої кількості публіцистичних оборотів свідчать про популізм, прагнення зробити текст більш зрозумілим, барвистим або наочнішим. Такі прийоми є недоречними в офіційному документі, можуть побічно вказувати на недолік його змістовної частини, спробу компенсувати раціональний вплив емоційним; 2) відсутність усталеної наукової термінології, що фіксує наявність правових відносин у сфері цифрових технологій. Через об'єктивні причини значна частина термінології запозичується з англійської мови. Такі терміни часто мають метафоричний характер, що дає стимул вітчизняним нормотворцям до винаходу власної термінології, внаслідок чого знижується авторитет нормативного тексту [18, с. 57].

Міжнародний телекомунікаційний союз визначає кібербезпеку як набір інструментів, політик, концепцій безпеки, заходи

безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, передовий досвід, гарантії та технології, які можуть бути використані, щоб захистити кіберсередовище, організацію й активи користувачів. Організація й активи користувачів включають підключені обчислювальні пристрої, персонал, інфраструктуру, додатки, послуги, телекомунікаційні системи та всі передані та/або збережені дані у кіберсередовищі [19]. Таке визначення лише побічно відображає характерні ознаки поняття кібербезпеки як категорії в інформаційному праві, однак у чинному національному законодавстві відсутнє легальне закріплення терміну «кібербезпека», що вкрай негативно позначається на правозастосовній практиці, оскільки закріплення цього терміна дасть більш глибоке уявлення про кібербезпеку у практиці його застосування.

Іноді кібербезпеку також визначають крізь призму діяльності, спрямованої на захист систем, мереж і комп'ютерних програм від цифрових атак. Метою таких кібератак зазвичай є отримання доступу до конфіденційної інформації, її зміна або знищення, вимагання грошей у користувачів або порушення нормального бізнес-процесу підприємства. На шляху забезпечення кібербезпеки постає таке явище, як кібероборона. Остання визначається як сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються у державі та кіберпросторі та спрямовані на забезпечення захисту її суверенітету й обороноздатності, запобігання виникненню збройного конфлікту та відсіч збройній агресії. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки й оборони створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз [20, с. 366]. Кібероборона має стати одним із пріоритетних напрямів державної політики у сфері оборони.

Висновки. Кібербезпека у широкому розумінні є станом захищеності інформаційного середовища, що гарантує дотримання прав і законних інтересів особистості, суспільства та держави в інформаційній сфері. Поняття кібербезпеки доцільно закріпити в Законі України «Про національну безпеку України». До основних елементів кібербезпеки належать: безпека додатків, інформація або безпека даних, безпека мережі, відновлення після кібератак, планування кіберзахисту, операційна безпека, хмарна безпека, критична безпека інфраструктури, фізична безпека, підготовка кінцевих користувачів. Перспективами подальших наукових пошуків правових засад кібербезпеки стане розроблення теоретичного підходу до принципів забезпечення кібербезпеки держави та визначення норм про кібербезпеку в системі права України, а також розробка теорії кіберзлочинності та юридичної відповідальності за кіберзлочини.

Список використаної літератури:

1. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : дис. ... докт. юрид. наук : 12.00.07. Харків, 2002. 408 с.
2. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право : учебник / под ред. Б.Н. Топорнина. Санкт-Петербург : Юридический центр Пресс, 2001. 787 с.
3. Волинець В.В. Проблеми правового забезпечення інформаційної функції держави у сучасній Україні. *Юридична Україна.* 2012. № 10. С. 4–10.
4. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : дис. ... канд. юрид. наук з держ. упр. : 25.00.02. Київ, 2004. 225 с.
5. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України : дис. ... докт. юрид. наук : 12.00.07. Запоріжжя, 2018. 521 с.
6. Діордіца І.В. Кібербезпекова політика України: стан та пріоритетні напрями реалізації : монографія. Запоріжжя : Видавничий дім «Гельветика», 2018. 548 с.
7. Кисарець І.А. Політико-культурна парадигма державної інформаційної політики : дис. ... канд. політ. наук : 23.00.03. Київ, 2008. 195 с.
8. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення : монографія. Київ : Текст, 2003. 180 с.

9. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності : навчальний посібник. Київ : Скіф; КНТ, 2008. 344 с.
10. Настюк В.Я. Адміністративно-правові режими у сфері національної безпеки та протидії тероризму : монографія. Київ, 2008. 245 с.
11. Несвіт Г.П. Інформаційна політика держави як чинник реформування суспільства : дис. ... канд. політ. наук : 23.00.02. Одеса, 2001. 193 с.
12. Петров С.В. Адміністративно-правове забезпечення реалізації права громадян на інформацію : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2013. 196 с.
13. Романчук Ю.В. Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти : автореф. дис. ... канд. політ. наук : 23.00.04. Київ, 2009. 20 с.
14. Сопілко І.М. Інформаційні правовідносини за участю органів державної влади України : монографія. Київ : Леся, 2013. 220 с.
15. Татарникова К.Г. Кодифікація законодавства України про інформацію : дис. ... канд. юрид. наук : 12.00.07. Київ, 2014. 212 с.
16. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : монографія. Київ : Освіта України, 2010. 388 с.
17. Шепета О.В. Адміністративно-правові засади технічного захисту інформації : монографія. Київ : О.С. Ліпкан, 2012. 296 с.
18. Давыдова М.Л. Формирование и нормализация юридической терминологии в сфере цифровых технологий. *Вестник ВолГУ.* 2020. Т. 19. № 4. С. 52–63.
19. Understanding the concept of cyber security. Policy competition and economic analysis department. URL: https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/682-understanding-the-concept-of-cyber-security/file (last accede: 21.04.2021).
20. Фараон С.І. Дефініційні проблеми термінології у сфері кібербезпеки і кіберборони та шляхи їх вирішення. *Актуальні проблеми управління інформаційною безпекою держави :* зб. тез наук. доп. наук.-практ. конф. (м. Київ, 4 квіт. 2019 р.). Київ : Нац. акад. СБУ, 2019. С. 365–368.

Pavlenko V. The essence of cyber security in the theory of information law

The article deals with the study of the essence of the category "cybersecurity" in the theory of information law, its features and components and to clarify its role in the legal regulation of public information relations in Ukraine. The methodology of studying the phenomenon of cybersecurity in general is based on the provisions of the general scientific dialectical method. At the same time, formal and legal and formal-logical methods of scientific cognition are used in the article for full and thorough disclosure of the topic. The article substantiates that the state policy of Ukraine in the field of national security and defense is aimed at ensuring military, foreign policy, state, economic, information, environmental security, cyber security, etc. Within the national segment of the state cyberspace, in order to protect the rights, freedoms and legitimate interests of man and citizen in the field of cybersecurity, national cybersecurity policy as a foundation for information security of the state is the result of other socio-economic goals. It is argued that an important tool for national cybersecurity is the establishment and strengthening of national, regional and international partnerships in the field of cybersecurity, protection against cyberattacks, mitigation, investigation of the latter, recovery from damage, including through joint training programs with the use or creation of appropriate information communication networks or emergency exchange of information about such threats. Thus, in modern conditions, cybersecurity is the dominant object of legal regulation and requires doctrinal research as a phenomenon that permeates almost all legal relations in the state. Emphasis is placed on the fact that cybersecurity is a phenomenon such as cyber defense as a set of political, economic, social, military, scientific, scientific and technical, informational, legal, organizational and other activities carried out in the state and cyberspace which are aimed at ensuring the protection of its sovereignty and defense capabilities, prevention of armed conflict and opportunities to repel armed aggression. It is emphasized that in the current national legislation there is no legal enshrinement of the term "cybersecurity", which has a very negative impact on law enforcement practice, as the enshrinement of such a term will give a deeper idea of cybersecurity in practice. It is proved that cybersecurity in a broad sense is a state of security of the information environment, which guarantees the rights and legitimate interests of the individual, society and the state in the information sphere. It is proposed to enshrine the concept of cybersecurity in the Law of Ukraine "On National Security of Ukraine". The main elements of cyber security include

the following: application security, information or data security, network security, recovery after cyberattacks, cyber security planning, operational security, cloud security, critical infrastructure security, physical security, end-user training. Prospects for further scientific research on the legal basis of cybersecurity will be the development of a theoretical approach to the principles of cybersecurity and the definition of cybersecurity in the legal system of Ukraine, as well as the theory of cybercrime and legal liability for cybercrime.

Key words: *cybersecurity, information law, information security, cyberspace, information society, cyber defense, cyber defense.*