LEGAL ASSIGNMENT OF CYBER SECURITY TERMS

L. Veselova,
Odesa State University of Internal Affairs, Ukraine
e-mail: cvet-Liliya@ukr.net

Abstract. The article analyzes the regulatory framework in cybersecurity. The problem of fixing cybersecurity terms is being raised. Summarizing the proposed definitions in the regulations and research of scientists, the author of the article on cybersecurity offers to understand the holistic system of ensuring the protection of vital interests of citizens, society and the state, as well as minimizing the likelihood of real and potential cyber threats, their consequences and society also ensuring the sustainable development of the individual, society and the state. It is said that all of the provisions in the article have important methodological content on understanding cyber security issues and not only in the context of other types of security. In turn, the difficulty in defining the concept of cyberspace causes the following problems in understanding cybersecurity and cyberwar (cyberspace wars). At the same time, with the modern technological development of the cybersphere, the methodological principles of administrative and legal support for cybersecurity require further improvement. As a result, it is noted that the national cybersecurity system depends not only on the successful work and interaction of the subjects in the specified field, including it depends on the quality filling of regulatory legal acts with a single terminology, without gaps and ambiguities that lead to inadequate legal responses . Therefore, cybersecurity is a systemic and purposeful phenomenon that provides protection, resilience and the ability to develop cyberspace entities.

Keywords: cybernetic space, telecommunication technologies, information security, regulatory framework.

Постановка проблеми. Однією з головних вимог щодо якості нормативно-правової бази будь-якої сфери є дотримання єдності термінології та її несуперечливості. Також важливою складовою є відповідність нормативно-правової бази міжнародним понятійним стандартам. Нажаль в законодавчих текстах у сфері кібербезпеки наявні прогалини, які потребують аналізу з метою їх подальшого опрацювання та вдосконалення.

Мета. Через аналіз нормативно-правової бази, напрацювання науковців комплексно висвітлити проблеми щодо юридичного закріплення термінів у сфері кібербезпеки.

Виклад основного матеріалу. Концептуально проблематика забезпечення кібербезпеки витікає із юридичного закріплення термінів, що описують цю сферу. Не останньою чергою ця проблема є наслідком недосконалого чинного законодавства, а також до певної міри – своєрідною традицією штучного розширення предмету інформаційної безпеки на максимальну кількість сфер [1, с. 119].

У Стратегії забезпечення кібернетичної безпеки уряду Австралії (Cyber security strategy, 2009) зазначено, що кібербезпека – це забезпечення доступності, цілісності та конфіденційності інформаційних та телекомунікаційних технологій Австралії, а також захист людей, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання ІКТ для цілей сексуальної експлуатації [2].

Канадська Стратегія щодо забезпечення кібернетичної безпеки (Canada's Cyber Security Strategy, 2010), закріплює поняття кібербезпеки як захист киберсистем від шкідливого неправильного використання та від інших деструктивних атак. А виходячи зі змісту складного визначення кібератаки, кібербезпека є захистом від цих атак [3]. Крім того, канадська Стратегія визначає основною метою забезпечення кібербезпеки – це найсучасніше використання кібернетичного простору, під яким розуміють стратегічний актив, а також необхідність, передбачення і протистояння кіберзагрозам, що виникають. У Стратегії Франції щодо забезпечення кібернетичної безпеки (Information systems defence and security, 2011) під забезпеченням кібербезпеки пропонують розуміти бажаний стан інформаційної системи, за якого вона може протистояти подіям у кіберпросторі, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними [4]. Стратегія кібербезпеки Німеччини (Cyber Security Strategy for Germany) визначає кібербезпеку як деяку сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків [5]. У Нідерланській національній стратегії кібернетичної безпеки (Holland, DeN Haag: National Coordinator for Security and Counterterrorism, 2013) під кібербезпекою визначають сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз [6]. Національна стратегія кібербезпеки Турецької Республіки 2013 р. визначає, що під кібернетичною безпекою слід розуміти захист інформаційних систем, що входять до складу кіберпростору,

від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам [7].

Комплексне дослідження адміністративно-правового регулювання у сфері кібербезпеки передбачає, насамперед, проведення глибокого аналізу щодо формулювання основних понять. Недоліки понятійного апарату у сфері адміністративно-правового регулювання забезпечення та організації кібербезпеки не дозволяють: визначити ознаки та об'єктивно оцінити основні загрози у національному сегменті кіберпростору; визначити найбільш ефективні заходи забезпечення кібербезпеки; чітко сформулювати завдання та функції суб'єктів кібербезпеки тощо [8].

На думку І. Діордіци, системою забезпечення кібербезпеки варто розуміти сукупність організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на створення умов для реалізації національних інтересів у кіберпросторі, а також сил, засобів і методів, які використовуються для досягнення даної цілі відповідно до законодавства [9]. У вузькому сенсі система забезпечення кібербезпеки – це сукупність органічно об'єднаних спільними цілями суб'єктів, які здійснюють свою діяльність у кіберпросторі з метою реалізації національних інтересів. Кожна держава індивідуально визначає сфери, які вона відносить до кібернетичної безпеки, перелік об'єктів і суб'єктів її забезпечення, виходячи зі тих стратегічних цілей і завдань, які стоять перед державою на національному та міжнародному рівнях, та її практичних можливостей реалізації національних інтересів [10, с. 110]. За своїм змістом та тлумаченням достатньо обґрунтованим є підхід до визначених формулювань. Поряд з цим, особливістю думки автора є все ж акцент на національних аспектах, що уникає використання міжнародного підґрунтя, тлумачень норм міжнародного права.

Кібербезпека також розглядається як певна система, тобто сукупність спеціальних суб'єктів забезпечення кібербезпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [11, с. 303].

Узагальнюючи запропоновані визначення, під кібербезпекою пропонуємо розуміти цілісну систему забезпечення стану захищеності життєво важливих інтересів громадян, суспільства та держави, а також мінімізації ймовірності реальних і потенційних кіберзагроз, їх наслідків та підвищення стійкості суспільства у кіберпросторі, а також забезпечення сталого розвитку особистості, суспільства та держави.

Безумовно, ключовою проблемою у формуванні тезаурусу сфери кібербезпеки є визначення поняття кіберпростір [12, с. 69]. Зазначене поняття використовується достатньо часто, і в наукових дослідження існує безліч підходів до його визначення. З точки зору поєднання слів «кібернетичний» та «простір», кіберпростір – це простір (територія), який створений та працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки інформації) [13, с. 216]. З філософської точки зору, кіберпростір – це сфера віртуального буття людини, де діють інші закони, інші звичаї, де людина перетворюється на громадянина іншої держави, стає «кібернавтом» [14, с. 144].

Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі [15, с. 654] .

В різних країнах зазначене поняття визначається дещо по іншому, зокрема [16, с. 62]:

США: кіберпростір – це сфера, яка характеризується можливістю використання електронних і електромагнітних засобів для запам'ятовування, модифікування та обміну даними в мережевих системах і пов'язану з ними фізичну інфраструктуру;

Великобританія: кіберпростір – це всі форми мережевої цифрової активності, що включають у себе контент і дії, здійснювані через цифрові мережі;

Німеччина: кіберпростір – це вся інформаційна інфраструктура, яка доступна через Інтернет поза будь-якими територіальними кордонами;

Євросоюз: кіберпростір – це віртуальний простір, у якому циркулюють електронні дані світових персональних комп'ютерів.

Американські експерти щодо кібербезпеки у воєнній сфері [17; 18], визначають поняття кіберпростір, базуючись на закріпленому у Національній військовій стратегії для операцій у кіберпросторі (2006 рік) – це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язана з ними фізична інфраструктура [19, с. 9]. На думку експертів [12, с. 69] саме це визначення було покладено і в основу розроблення документа Стратегічне бачення Кіберкомандування повітряних сил (2008 рік) [20] та Стратегії національної безпеки США (2010 рік), в якому, зокрема, зазначається, що військові повинні й надалі мати можливість захищати інтереси США у всіх основних сферах – землі, повітрі, воді, космосі та кіберпросторі [21, с. 22].

Військові експерти США у контексті стратегічного бачення кібербезпеку пропонують розуміти як своєрідну сукупність категорій: «використання кіберпростору» (атаки в кіберпросторі та збільшення власних сил), «контроль кіберпростору» (оборонні дії в кіберпросторі й атакуючі контрдії в кіберпросторі) та «налаштування кіберпростору» (глобальні спостережні операції в кіберпросторі, операції з управління та контролю за мережами та безпекою, операції з цивільної підтримки в кіберпросторі) [20, с. 11].

У той же час офіційними документами в США: Огляд політики щодо кібепростору (2009) та Директива Президента з національної безпеки 54 / Директива Президента з внутрішньої безпеки 23 (2008) (*National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – NSPD*-54/*HSPD*-23), кіберпростір визначено як взаємозалежні мережі, комп'ютерні системи, *IT*-інфраструктури, що включають інтернет, телекомунікаційні мережі, комп'ютерні процесори та контролери у критично важливих сферах [22, с. 1].

У доповіді «Безпека кіберпростору для 44-го Президента», підготовленій за загальним керівництвом Дж. Льюїса поняття кіберпростір визначено дещо більше, ніж просто мережа інтернет, що включає всі мережеві форми та цифрову діяльність [23, с. 11]. Група авторів окремого дослідження «Кібермогутність і національна безпека» (*Cyberpower and National Security*) акцентують увагу на достатньо широких можливостях визначення феномену кібер. Зокрема, Деніел Куел, розглядаючи термінологію у зазначеному дослідженні, навів близько 30 визначень кіберпростору та в остаточному варіанті запропонував наступне: кіберпростір – операційний домен, обмежений використанням електроніки та електромагнітним спектром для створення, збереження, зміни, обміну та використання інформації у взаємопов'язаних та інтернетизованих інформаційних системах та пов'язаній з ними інфраструктурі [24, с. 4].

Резюмуючи досвід американських науковців та експертів, варто зазначити на прагматизмі у визначеннях ключових понять: найважливіший урок, який ми винесли із цього багатоманіття, це те, що визначення мають допомагати формувати політики чи робити аналіз, а не обмежувати їх [24, с. 4]. Саме використовуючи такий концептуальний підхід, доречним є використання базового поняття у якості шаблону, доповнюючи його щоразу додатковими характеристиками, які сприятимуть динаміці його розвитку. Зокрема, розширюючи поняття кібербезпека, пропонується включити не лише технічні питання, а й людський чинник – ворожі інсайдерські дії чи людські помилки, а також проблеми владних відносин на національному та міжнародному рівнях [12, с.71-72].

Не залишаються осторонь і вітчизняні науковці щодо визначення поняття кіберпростору. О. Манжай зазначає, що це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [25, с. 145]. А професор А. Погорецький пропонує розуміти під кіберпростором штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо) [26, с. 80].

Цікавою є думка [12, с. 72] з приводу того, що у західних дослідженнях при визначенні поняття кіберпростір нерозв'язаною та нерозтлумаченою залишилась друга частина терміну – «простір». Поряд з цим, вітчизняні науковці «простір» розуміють достатньо широко й описують його у якості певної частини буття людини.

Усі перераховані положення мають важливий методологічний зміст щодо розуміння проблем кібернетичної безпеки і не лише в контексті інших видів безпеки. У свою чергу, складнощі з визначенням поняття кіберпростору обумовлюють наступні проблеми щодо розуміння кібербезпеки та кібервійни (війни в кіберпросторі). Поряд з тим, за умов сучасного технологічного розвитку кіберсфери, методологічні засади адміністративно-правового забезпечення кібербезпеки потребують подальшого вдосконалення.

Висновки. У підсумку необхідно зазначити, що національна система кібербезпеки залежить не тільки від успішної роботи та взаємодії суб'єктів в означеній сфері, в тому числі вона залежить від якісного наповнення нормативно-правових актів з єдиною термінологією, без прогалин та неоднозначностей, які призводять до неадекватного реагування правозастосовника. Тож, кібербезпека є системним й цілеспрямованим явищем, яке забезпечує захист, стійкість та спроможність до розвитку суб'єктів кіберпростору.

References:

1. Dubov D.V. (2013) Stratehichni aspekty kiberbezpeky Ukrainy [Strategic aspects of cybersecurity in Ukraine]. *Stratehichni priorytety [Strategic priorities]*. № 29. P. 119-126 (In Ukrainian).

2. Cyber security strategy: Commonwealth of Australia: AustraliaN Government, 2009. URL://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber %20Security%20Strategy%20-%20for%20website.pdf.

3. Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. Her Majesty the QueeN iN Right of Canada, 2010. 14 c. URL: www.publicsafety.gc.ca/cnt/rsrcs/ pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

4. Information systems defence and security: France's strategy. – French Network and InformatioN Security Agency. 2011. C. 23.URL: https://www.gouvernement.fr/sites%20/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf.

5. Cyber Security Strategy for Germany. – Berlin : Federal Ministry of the Interior. 2011. 15 p. URL: //www.cio.bund.de/SharedDocs/Publikationen/DE/ Strategische-Themen/css_engl_ download.pdf?.

6. Natsyonalnaia stratehyia kyberbezopasnosty (NCSS). Ot ponymanyia k vozmozhnosty [National Cyber Security Strategy (NCSS). From understanding to opportunity] / ofits. tekst : Holland, DeN Haag: National Coordinator for Security and Counterterrorism, Retrieved from https://www.enisa.europa.eu/activities/ Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2 Engelseversie (In Ukrainian).

7. National Cyber Security Strategy and 2013-2014 Action Plan: Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. P. 47. URL: //www.ccdcoe. org/strategies/TUR_Cyb erSecurity .pdf.

8. Kravtsova M.O. Faktory determinatsii kiberzlochynnosti v suchasnii kryminolohichnii teorii [Determinants of cybercrime determination in modern criminological theory] Retrieved from https:// www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security (In Ukrainian).

9. Poniattia ta zmist systemy zabezpechennia kiberbezpeky [The concept and content of the cybersecurity system] Retrieved from http://goal-int.org (In Ukrainian).

10. Diorditsa I.V. (2017) Systema zabezpechennia kiberbezpeky: sutnist ta pryznachennia [Cybersecurity system: essence and purpose]. *Pidpryiemnytstvo, hospodarstvo i pravo* [*Entrepreneurship, economy and law*]. № 10. P. 110–116 (In Ukrainian).

11. Shelomentsev V.P. (2012) Sutnist orhanizatsiinoho za bezpechennia systemy kibernetychnoi bezpeky Ukrainy ta napriamy yoho udoskonalennia [The essence of organizational for security of the cyber security system of Ukraine and directions of its improvement]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)* [*Combating Organized Crime and Corruption (Theory and Practice)*]. . № 2(28). P. 299–309 (In Ukrainian).

12. Dubov D.V. (2014) Kiberprostir yak novyi vymir heopolitychnoho supernytstva [Cyberspace as a new dimension of geopolitical rivalry]. Kyiv: NISD. 328 p. (In Ukrainian).

13. Manzhai O.V. (2009) Vykorystannia kiberprostoru v operatyvno-rozshukovii diialnosti [The use of cyberspace in search operations]. *Pravo i Bezpeka* [*Law and Security*]. № 4. P. 215–219 (In Ukrainian).

14. Vladlenova I.V., Kalnytskyi E.A. (2013) Kiberzlochynnist yak vyklyk informatsiinomu suspilstvu [Cybercrime as a challenge to the information society]. *Hileia: naukovyi visnyk* [*Gilea: a scientific bulletin*]. Vol. 77. P. 142–146 (In Ukrainian).

15. Fedchenko D.I. (20180 Cystema zabezpechennia kiberbezpeky: problemy formuvannia ta efektyvnoi diialnosti [Cybersecurity system: problems of formation and effective activity]. *«Molodyi vchenyi»* [*"Young Scientist"*]. № 5 (57), P. 653-658 (In Ukrainian).

16. Prysiazhniuk M.M., Tsyfra Ye.I. (2017) Osoblyvosti zabezpechennia kiberbezpeky [Features of providing cybersecurity]. *Ekspertni systemy ta pidtrymka pryiniattia rishen* [*Expert systems and decision support*]. P. 61–68 (In Ukrainian).

17. Fahrenkrug T. D. Cyberspace Defined. URL: http://www.au.af.mil /au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm.

18. Cyber Atlantic 2011. URL: http://www.enisa.europa.eu/activities/ Resilience-and-CIIP/cybercrisis-cooperation/cyber-atlantic/cyber-atlantic-2011.

19. National Military Strategy for Cyberspace Operations. URL: http://www.dod.gov/pubs/foi/ ojcs/07-F-2105doc1.pdf.

20. Air Force Cyber Command Strategic Vision. URL: http://www.dtic.mil/cgi–bin/GetTRDoc?AD=ADA479060&Location= U2&doc=GetTRDoc.pdf.

21. Cyber Cooperation Added To U.S.-Australia Treaty. URL: http://www.officialwire.com/main.php?action=posted_news&rid=44771.

22. Cyberspace Policy Review. URL: http://www.whitehouse.gov /assets/documents/Cyberspace_Policy_Review_final.pdf.

23. Securing Cyberspace for the 44th Presidency / ed. by A.J.Lewis. URL:http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

24. Cyberpower and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. Washington, D.C.: Potomac Books, 2009. 642 p.

25. Manzhai O. V. (2009) Vykorystannia kiberprostoru v operatyvno-rozshukovii diialnosti [The use of cyberspace in search operations]. *Pravo i bezpeka. Naukovyi zhurnal* [Law and security. Scientific journal]. № 4. P. 142–149 (In Ukrainian).

26. Pohoretskyi M., Shelomentsev V. (2009) Poniattia kiberprostoru yak seredovyshcha vchynennia zlochyniv [The concept of cyberspace as a crime medium]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy* [Information security of the person, society, state]. № 2. P. 77–81 (In Ukrainian).

Юридическое зкрепление терминов в области кибербезопасности

Веселова Лилия Юрьевна, e-mail: cvet-Liliya@ukr.net
Одесский государственный университет внутренних дел, г. Одесса, Украина

Аннотация. В статье анализируется нормативно-правовая база в сфере кибербезопасности. Раскрывается проблема по юридическому закреплению определений в сфере кибербезопасности. Обобщая предложенные определения в нормативно-правовых актах и исследованиях ученых, автор статьи под кибербезопасностью предлагает понимать целостную систему обеспечения состояния защищенности жизненно важных интересов граждан, общества и государства, а также минимизации вероятности реальных и потенциальных киберугроз, их последствий и повышения устойчивости общества в киберпространстве, а также обеспечение устойчивого развития личности, общества и государства. Говорится, что все перечисленные положения имеют важный методологический смысл в понимании проблем кибернетической безопасности и не только в контексте других видов безопасности. В свою очередь, сложности с определением понятия киберпространства обусловливают следующие проблемы в понимании кибербезопасности и кибервойны (войны в киберпространстве). Вместе с тем, в условиях современного технологического развития киберсферы, методологические основы административно-правового обеспечения кибербезопасности требуют дальнейшего совершенствования. В итоге отмечается, что национальная система кибербезопасности зависит не только от успешной работы и взаимодействия субъектов в указанной сфере, в том числе она зависит от качественного наполнения нормативно-правовых актов с одной терминологией, без коллизий и неоднозначностей, которые приводят к неадекватному реагированию правоприменителей. Поэтому, кибербезопасность является системным и целенаправленным явлением, которое обеспечивает защиту, устойчивость и способность к развитию субъектов киберпространства.

Ключевые слова: кибернетическое пространство, телекоммуникационные технологии, информационная безопасность, нормативно-правовая база.