***Білоусов Євген Миколайович***

*провідний науковий співробітник НДІ правового забезпечення інноваційного розвитку НАПрН України, професор кафедри права ЄС Національного юридичного університету імені Ярослава Мудрого, доктор юридичних наук, доцент*

***ЩОДО ПОНЯТТЯ «КІБЕРБЕЗПЕКА» В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ (ПОСТАНОВКА ПРОБЛЕМИ)***

У публікації зосереджено увагу на розгляді категорії «кібербезпека» в умовах воєнного стану. Підкреслено, що вищевказане поняття багатоаспектне, а тому досить проблематичною виявляється її формалізація, оскільки існує достатнє різноманіття наукових підходів щодо розуміння правової природи цієї категорії. Констатовано, що в сучасних умовах потребують уточнення та систематизації теоретико-методологічні засади забезпечення кібербезпеки (зокрема, понятійний апарат, рівні забезпечення кібербезпеки та її об’єктно-суб’єктний склад).

**Ключові слова:** кібербезпека, воєнний стан, правовий режим.

***Eugene Bilousov***

*Leading Researcher of Scientific Research Institute of Legal Support of Innovative Development of the National Academy of Sciences of Ukraine, Professor of the Department of EU Law, Yaroslav Mudryi National University of Law, 2nd PhD of Law, Associate Professor*

***ON THE CONCEPT OF "CYBER SECURITY" IN THE CONDITIONS OF THE LEGAL REGIME OF MARITIME (STATEMENT OF THE PROBLEM)***

The publication focuses on the category of "cybersecurity" in martial law. It is emphasized that the above concept is multifaceted, and therefore its formalization is quite problematic, as there is a sufficient variety of scientific approaches to understanding the legal nature of this category. It is stated that in modern conditions the theoretical and methodological principles of cybersecurity need to be clarified and systematized (in particular, the conceptual apparatus, levels of cybersecurity and its object-subject composition).

**Key words:** cybersecurity, martial law, legal regime.

Нові цивілізаційні виклики зумовлюють і пошук нових шляхів стримання військової агресії рф проти України, причому провідне місце в цьому повинна займати державна політика, спрямована на запобігання можливим руйнівним негативним наслідкам та проявам соціально-економічних, геополітичних ризиків для нашої держави та їх ефективного подолання. Кібербезпека в цьому контексті відіграє провідну роль через важливість та, як з’ясувалося, чи не найбільшу значущість для всієї системи національної безпеки саме в аспекті забезпечення функціонування національної економічної системи в умовах правового режиму воєнного стану.

Вважаємо, що для опрацювання дієвих механізмів забезпечення кібербезпеки країни необхідно вирішити низку проблем теоретико-методологічного характеру, серед яких чи не найважливішою є детермінація самої категорії «кібербезпека» та вироблення єдиного концептуального бачення її структури та змісту в умовах повномасштабної військової агресії рф проти України.

Слід зазначити, що будь-яке і соціально-економічне, і публічно-політичне явище потребує правового регулювання й така регламентація має постійно відбуватися, модернізуватися з метою охоплення засобами правового впливу тих чи інших процесів, які втілюють відповідні явища. Це твердження повною мірою стосується такої фундаментальної багатоаспектної категорії, як «кібербезпека», оскільки загрози та виклики національній безпеці України із площини теоретико-прогностичної набули цілком реальних якостей. В цих умовах питання функціонування системи забезпечення національної безпеки безпосередньо пов’язано із станом забезпечення кібербезпеки України, оскільки реалії сьогодення зумовлюють необхідність оперативного реагування з метою ефективного відбиття кіберзагроз, що проявляються через атаки окремих хакерів, хакерських угруповань, які фактично створюються та забезпечуються організаційно, фінансово й навіть методологічно державою-агресором. Саме тому, на нашу думку, існує нагальна потреба комплексного вирішення питань правового забезпечення кібербезпеки та модернізаціі наукових підходів до понятійно-категоріального апарату забезпечення кібербезпеки, що постають перед Україною в контексті її можливостей ефективно протистояти цим загрозам і викликам та з метою забезпечення збалансованого функціонування цієї системи.

Загалом наявність різних наукових підходів в різний період часу (але з моменту набуття Україною незалежності) до вирішення проблеми забезпечення кібербезпеки держави дає розуміння важливості цього питання, його наріжності та визначальності для різних сфер наукового пізнання. Це, у свою чергу, розкриває необхідність подальших наукових досліджень категорії «кібербезпека» як окремого загальносуспільного феномену, що впливає на соціально-економічний та публічно-політичний розвиток держави.

Сучасний етап розвитку наукової думки (від 2014 р. і до сьогодні) пов’язаний головним чином із переглядом механізмів, пріоритетів та напрямів державної політики у сфері забезпечення кібербезпеки; диференціацією складових системи кібербезпеки держави та розробленням нового інструментарію з метою її належного функціонування. Геополітичне, соціально-економічне становище України об’єктивує необхідність більш активного втручання держави в процеси забезпечення кібербезпеки, а також консолідації внутрішніх ресурсів та елементів інституційного забезпечення державної політики в цій сфері. Важливим в контексті наукового опрацювання змісту цієї категорії та з’ясування її місця в структурі системи забезпечення національної безпеки було і залишається вирішення питання щодо сприйняття на рівні національної правової доктрини положень «реалістичної» та «ліберальної» концепцій кібербезпеки. «Реалістична» концепція містить положення щодо контролю над поширенням інформації та технологій, розробки засобів ведення кібервійни, моніторинг рівня кібербезпеки потенційних супротивників, збільшення рівня безпеки інформаційних систем усередині держави. Концепція «ліберального» підходу передбачає укладання міжнародних угод з питань кібербезпеки, побудову взаємовідносин держав у кіберпросторі на основі взаємної довіри. Окремим напрямом наукових досліджень є звернення до категорії «кібербезпека» в контексті її взаємозв’язку із категорією «національна безпека». Як слушно зауважує Р. Лук’янчук, до 2014 року кібербезпека не визнавалася самостійною складовою національної безпеки, а вважалася винятково складовою інформаційної безпеки. Гібридна війна, розпочата проти України, зумовила перегляд системи державного управління кібербезпекою, у зв’язку з чим було внесено корективи до основних засад державної політики забезпечення національної безпеки [1]. Тобто, досліджуючи загальнотеоретичні засади національної безпеки держави, вчений доводить, що місце кібербезпеки в ній не може визначатися як певна сукупність координат, а є, імовірніше, рамковим станом усієї системи національної безпеки, але в досліджуваній сфері. Слід зазначити, що дослідження різноманіття трактувань сутності категорії «кібербезпека держави» [2,3,4,5] свідчить про те, що в науковому середовищі наразі немає консенсусу щодо цієї дефініції, тому вважається цілком обґрунтованим зробити висновок, що підходи до визначення поняття «кібербезпека» мають спиратися на її основні сутнісні характеристики (інтереси суб’єктів, стійкість (стабільність) функціонування системи, багаторівнева структура об’єктів), які повинні мати єдиний системний сенс.

Можна також стверджувати, що відмінності в підходах до формулювання досліджуваного поняття пов’язані із тим, що різні за сферою наукових інтересів дослідники вкладають у сутність цієї категорії абсолютно різні фундаментальні положення. Так, якщо цю категорію розглядати з погляду суто економіки, то необхідно за вихідну якість кібербезпеки брати її вплив (як потенційний, так і реальний) на рівноважний стан функціонування національної економіки, але якщо це визначення трактувати в контексті політичних наук, то перманентним є відносність критеріїв стабільності економічного стану різних країн. Баланс при цьому може не зберігатися, але ступінь стабільності або запас міцності національної економіки як результат впливу на неї кібератак є визначальним.

В законодавстві України «кібербезпека» визначається як складова національної безпеки, оскільки являє собою стан «захищеності 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» [6]. Аналіз змісту досліджуваної норми дозволяє нам стверджувати, що саме «реалістичний» підхід до визначення поняття «кібербезпека» було реалізовано законодавцем України, при цьому складові елементи концепції «ліберального» підходу також знайшли своє нормативне закріплення в тексті цього Закону, оскільки функціонування національної системи кібербезпеки забезпечується шляхом: 1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО; 2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО [6]. Вважаємо, що запропоноване в законодавстві України поняття «кібербезпека» в цілому є термінологічно узгодженим із низкою інших понять даного нормативно-правого акту, є таким, що сприяє найбільш точному, стислому і інформативному викладу змісту цієї норми; дозволяє покращити ситуацію правової визначеності у правовідносинах із забезпечення функціонування системи кібербезпеки України; запропоноване визначення «кібербезпека» передбачає досягнення і збереження властивостей безпеки і інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, їх спрямованість проти потенційних кіберзагроз. Разом із тим, при розгляді варіанта військової агресії, в якій сторони змушені постійно відповідати на реальні загрози та виклики стосовно один одного, стає зрозумілим, що кібервійна є одним із чинників, який здатен безпосередньо впливати на результати такого протистояння (у ситуації повномасштабної військової агресії рф проти України – це додаткові, а інколи – й вирішальні можливості отримати військову перевагу та перемогу для нашої держави).

Таким чином, з огляду на вищезазначене, можемо стверджувати що поняття «кібербезпека» багатоаспектне, а тому досить проблематичною виявляється її формалізація, оскільки існує достатнє різноманіття наукових підходів щодо розуміння правової природи цієї категорії. Окремого вирішення потребує низка проблем, виявлених у процесі аналізу наукового доробку як вітчизняних, так і зарубіжних учених із питань забезпечення кібербезпеки на рівні держави, а саме:

* По-перше, потребують уточнення та систематизації теоретико-методологічні засади забезпечення кібербезпеки, де, окрім понятійного апарату, слід чітко розмежовувати рівні забезпечення кібербезпеки та її об’єктно-суб’єктний склад.
* По-друге, потребує постійного моніторингу законодавство в сфері забезпечення кібербезпеки в умовах повномасштабної військової агресії рф проти України.
* По-третє, потребують актуалізації наукові пошуки з проблеми визначення місця України в глобальній та регіональних системах забезпечення кібербезпеки з урахуванням наслідків військової агресії та в контексті того цивілізаційного вибору, який було зроблено нашою державою.

**ЛІТЕРАТУРА**

1. Лук’янчук Р. В. Державне управління у сфері забезпечення кібербезпеки України: дис. … канд. юрид. наук, 25.00.01. Київ. 2017. URL: http://instzak.rada.gov.ua/uploads/documents/31444.pdf.
2. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2. С. 54-62
3. Логінова Н. І. Правові основи кібербезпеки в Україні. *Правові та інституційні механізми забезпечення розвитку держави та прав в умовах євроінтеграції*: матеріали міжнар. наук.-практ. конференції. Одеса: 2016. Т. 1. С. 575-577
4. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова системи забезпечення національної безпеки України. *Підприємництво, господарство і право.* 2017. № 5. С. 174-180.
5. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи. Одеса : Фенікс, 2020. 404 с.
6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19.

**REFERENCES**

1. Lukianchuk R. V. (2017). State Administration in the field of cybersecurity of Ukraine. *Candidate’s thesis*. Kyiv. Retrieved from http://instzak.rada.gov.ua/uploads/documents/31444.pdf [in Ukrainian].

2. Baranov, O. A. (2014). About interpretation and definition of the concept of «cybersecurity». *Pravova informatyka, 2*, 54–62 [in Ukrainian].

3. Lohinova, N. I. (2016). Legal Fundamentals of Cybersecurity in Ukraine. *Pravovi ta instytutsiini mekhanizmy zabezpechennia rozvytku derzhavy ta prav v umovakh yevrointehratsii: materialy mizhnar. nauk.-prakt. Konferentsii*, Vol. 1 (pp. 575–577). Odesa [in Ukrainian].

4. Lipkan, V. & Diorditsa, I. (2017). National cybersecurity system as a component of the national security system of Ukraine. *Pidpryiemnytstvo, hospodarstvo i parvo, 5*, 174–180 [in Ukrainian].

5. Tarasiuk, A. V. (2020). Cybersecurity of Ukraine at the present stage of state formation: theoretical and legal basis. Odesa : Feniks [in Ukrainian].

6. Law of Ukraine On the Basic Principles of Cyber Security of Ukraine № 2163-VIII (2017, October 5). Retrieved from http://zakon3.rada.gov.ua/laws/show/2163-19 [in Ukrainian].