АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.9
DOI https://doi.org/10.32844/2618-1258.2019.3-1.11

АРТЕМЕНКО Я.В.

ЩОДО ПОНЯТТЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

У статті здійснено оцінку конструкції для позначення та змісту поняття «національна система кібербезпеки» з урахуванням всіх складників, необхідних для досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. З'ясовано, що сьогодні основними суб'єктами кібербезпеки визначені винятково державні інституції. Включення до їх числа недержавних інституцій дозволить у національному секторі кібербезпеки як сукупності суб'єктів її забезпечення виділити державний та приватний блоки. Визначено, що національною системою кібербезпеки України доцільно позначати сукупність елементів, розвиток яких забезпечить досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. З огляду на сформовану міжнародними експертами матрицю кібербезпеки доцільними складниками національної системи кібербезпеки України можна визначити: нормативно-правову базу; суб'єктів забезпечення кібербезпеки, об'єднаних в сектори, які взаємодіють на засадах державно-приватного партнерства та координуються єдиним центром; інструменти їх діяльності; об'єкти забезпечення кібербезпеки; освіту у сфері кібербезпеки. Іншими словами, національну систему кібербезпеки України доцільно розуміти як поєднання нормативного, інституційного, інструментального та освітнього компонентів (блоків, складників). Зроблено висновок, що національна система забезпечення кібербезпеки України повинна являти собою сукупність об'єктів та суб'єктів, зв'язки між якими та з зовнішніми щодо вказаної системи елементами у вигляді окремих заходів, здійснюваних за рахунок охоплених компетенцією кожного форм та методів діяльності, виникають, змінюються та припиняються задля досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Суб'єктами національної системи забезпечення кібербезпеки в Україні повинні бути: держава в особі конкретних органів, установ чи організацій; громадянське суспільство у вигляді окремих громадян, громадських організацій, суб'єктів самоврядної влади; приватний сектор у вигляді представників бізнесу.

Ключові слова: *національна система кібербезпеки, забезпечення кібербезпеки, кіберпростір, суб'єкти забезпечення кібербезпеки.*

In the article is evaluated the design for the designation and content of the concept of "national cybersecurity system" taking into account all the components necessary to achieve the state of protection of vital interests of the individual and the citizen, society and the state while using cyberspace. It has been found that public institutions are excluded by the main cybersecurity entities. The inclusion of non-governmental institutions in the national sector will allow the national and private sectors to be singled out in the national cybersecurity sector. It is determined that the national system of cybersecurity of Ukraine is advisable to designate a set of elements, the development of which will ensure the achievement of the state of protection of vital interests of the individual and the citizen, society and the state during the use of cyberspace. Considering the cyber security matrix formed by international experts, the relevant components of the

© АРТЕМЕНКО Я.В. – аспірант (Міжрегіональна академія управління персоналом)

national cybersecurity system of Ukraine can be determined: the regulatory framework; cybersecurity entities integrated into sectors that operate on a public-private partnership and are coordinated by a single center; tools of their activity; cybersecurity facilities; cybersecurity education. In other words, it is advisable to understand the national cybersecurity system of Ukraine through a combination of regulatory, institutional, instrumental and educational components (blocks, components). It is concluded that the national system of cybersecurity of Ukraine should represent a set of objects and entities, the links between which and with the elements external to the specified system in the form of separate measures carried out at the expense of the scope of competence of each form and method of activity, arise, are modified and terminated to achieve a state of protection of the vital interests of the individual and the citizen, society and the state while using cyberspace. The subjects of the national cybersecurity system in Ukraine should be: the state, represented by specific bodies, institutions or organizations; civil society in the form of individual citizens, non-governmental organizations, subjects of self-government; the private sector as business representatives.

Key words: *national cybersecurity system, cybersecurity, cyberspace, cybersecurity entities.*

Вступ. Для створення умов безпечного функціонування кіберпростору його використання в інтересах особи, суспільства і держави як мети Стратегії кібербезпеки України першим з поставлених завдань було створення національної системи кібербезпеки [1]. І створення такої системи було вкрай необхідним, зважаючи на ряд реалізованих кіберзагроз у вигляді кібератак (розповсюдження в Україні "WannaCry" як шкідливого програмного забезпечення, за допомогою якого вимагають кошти за дешифровку зашифрованих через вказану програму даних на персональних комп'ютерах; злам енергетичних підприємств України «Прикрапаттяобленерго» у грудні 2015 року; відключення від електроенергії Київської ГАЕС з іншими об'єктами інфраструктури Києва у грудні 2016 року; кібератака 2017 року через програму для звітності та документообігу M.E.doc. з інфікацією більше 12 000 серверів та робочих станцій; кібератаки на сайти Міністерства Інфраструктури України, Міжнародний одеський аеропорт та Київський метрополітен у жовтні 2017 року тощо).

Проблеми забезпечення кібербезпеки неодноразово ставали приводом досліджень науковців, серед яких О.О. Астахов, І.В. Діордіца, С.В. Демедюк, О.В. Глазов, І.Ф. Корж, В.А. Ліпкан, В.М. Пасічник, М.М. Присяжнюк, Є.Б. Смірнов, О.В. Топчій, В.І. Ткаченко, Є.І. Цифра та інші.

З прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2] в законодавстві України з'являється категорія «національна система кібербезпеки». При цьому в законі закріплено і тлумачення вказаної конструкції, яке потребує оцінки та критики задля вдосконалення та відповідності сучасним кібервикликам.

Постановка завдання. Метою статті є оцінка конструкції для позначення та змісту поняття «національна система кібербезпеки» з урахуванням всіх складників досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Результати дослідження. В Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2] визначено поняття «національна система кібербезпеки», яка згідно ч. 1 ст. 8 вказаного Закону 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 [2]. Як нам видається, доцільним є аналіз як самої використаної конструкції для позначення поняття, так і її трактування законодавцем.

По-перше, вважаємо, що конструкція «національна система кібербезпеки» потребує уточнення щодо країни, в якій така система буде функціонувати. Зокрема, в назві статті. Тим більше, що науковцями пропонується також окремо використовувати термін «система кібернетичної безпеки Міністерства оборони України та Збройних сил України» [3, с. 175]. Що ж до використання таких понять, як «національна» та «система», то їх використання ми вважаємо доцільним, оскільки відповідні категорії вказують на правовий статус, рамки регулювання та функціонування

кожного з елементів відповідної структури, які діють у взаємодії під час використання урегульованих відносно одне одного повноважень. В.А. Ліпкан та І.В. Діордіца, досліджуючи національну систему кібербезпеки як складника частини системи забезпечення національної безпеки України, наголошують на необхідності етимологічного тлумачення використаного понятійно-категорійного ряду. «Національний» – стосується нації, національності, пов'язаний з їхньою суспільно-політичною діяльністю; властивий певній нації, національності; державний, який належить даній країні або стосується її народу. «Система» – порядок, зумовлений правильним, планомірним розташуванням і взаємним зв'язком частин чого-небудь; сукупність яких-небудь елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням [3, с. 175–176].

Виходячи з діяльнісного підходу до трактування поняття національної системи кібербезпеки, коли закріплене у ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2] передбачає визначення системою не тільки суб'єктів, але і здійснювані ними заходи, звертаємо увагу на обрану для позначення явища правової дійсності конструкцію. Зокрема, названий зв'язок виводить на перший план питання співвідношення понять «система кібербезпеки» та «система забезпечення кібербезпеки».

Виходячи з того, що поняття кібербезпека є складником національної безпеки, то вже напрацьовані матеріали щодо тлумачення понять нацбезпекознавства слід враховувати під час визначення ознак, поняття та структури національної системи кібербезпеки України. В.А. Ліпкан звертає увагу на доцільність розмежування понять «система національної безпеки» і «система забезпечення національної безпеки» [4, с. 60]. І така концепція заслуговує на увагу і під час дослідження кібербезпеки.

В Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2] кібербезпека визначається як захищеність, а отже, певний стан, результат. І це відповідає розумінню поняття безпеки у філософії як такого стану захищеності буття, цінностей та інтересів суб'єкта (об'єкта) безпеки від загроз та небезпек, за якого забезпечуються оптимальні умови його життєдіяльності, розвитку та самореалізації [5]. Концепція розуміння поняття «безпека» як цінності сьогодні вважається класичною у наукових школах США та провідних країн Європи. Безпека у цьому розумінні означає збалансований стан функціонування соціальної системи (людини, держави, світового співтовариства), антропогенних, природних систем тощо, за якого людина завдяки знанням про навколишнє природне середовище і тенденції його розвитку своїми діями спроможна своєчасно виявити та мінімізувати вплив існуючих та потенційних загроз або уникнути їх, що своєю чергою дає їй можливість зберігати систему своїх цінностей і забезпечувати подальший їх розвиток [6, с. 12]. Наприклад, бажаним станом інформаційної системи кібербезпека визначається у стратегії Франції [7, с. 64]. Однак для законодавства України постає питання, що вказаний підхід до тлумачення поняття кібербезпеки як стану не стикується зі змістом поняття «система кібербезпеки», коли під ним розуміють суб'єктів та їх діяльність.

Хоча існує визначення змісту поняття національної безпеки як певної сукупності суб'єктів. Наприклад, В.І. Ткаченко, Є.Б. Смірнов та О.О. Астахов вважають, що «поняття національної безпеки являє собою складну систему, яка об'єднується суб'єктами – особистістю, суспільством, державою, що знаходяться у тісному взаємозв'язку, діяльність яких спрямовується єдиними цілями» [8, с. 3]. Водночас в чинному законодавстві України поняття кібербезпеки тлумачиться як захищеність, а от поняття національної системи кібербезпеки непослідовно з цієї точки зору охоплює суб'єктів та заходи.

Як ми вважаємо, діяльнісний підхід під час тлумачення поняття та розкриття його змісту передбачає використання терміну чи конструкції для позначення явища в динаміці. З цієї позиції, якщо система кібербезпеки – це діяльність, то і кібербезпека повинна бути визначена діяльністю. Наприклад, у німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, у результаті реалізації яких досягається мінімізація ризиків. У канадській стратегії під кібербезпекою можна розуміти захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак. Кібербезпека як захист інформаційних систем розуміється у Туреччині. За Національною стратегією кібербезпеки Нідерландів 2013 р. кібербезпека – це сукупність зусиль щодо запобігання шкоди [7, с. 64]. Водночас в законодавстві України застосовано інший підхід.

Зокрема, в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2], під поняттям кібербезпеки розуміють захищеність таких об'єктів, як громадяни (їх права і свободи), суспільство (його духовні та матеріальні цінності), держава (її конституційний устрій, суверенітет і територіальна цілісність) [9, с. 44] через захищеність

їх національних інтересів. А тому, як нам видається, система забезпечення кібербезпеки є доцільною для використання конструкцією для позначення взаємодії суб'єктів з метою досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Ураховуючи той факт, що система кібербезпеки є багатокомпонентною, як слушно вказує В.А. Ліпкан, «постає потреба в існуванні спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування та розвитку самої системи кібербезпеки, тобто у забезпеченні життєздатності її системоутворюючих елементів, зокрема національних інтересів людини, суспільства держави. Такою системою і є система забезпечення кібербезпеки [4, с. 58]. Про систему забезпечення безпеки стверджують О.В. Глазов [9, с. 44] та С.В. Демедюк [10, с. 147], відмежовуючи стан захищеності від діяльності по його досягненню. На наш погляд, обсяг поняття, закріпленого у ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2], вказує на доцільність використання конструкції національна система забезпечення кібербезпеки України для характеристики описаного у положеннях статті явища.

Забезпечення кібербезпеки, як вважають експерти BSA (Business Software Allience – міжнародна торговельна асоціація, створена у 1988 році виробниками програмного забезпечення), досягається через п'ять напрямів, сформованих у матрицю кібербезпеки (EU Cybersecurity Dashboard), розроблену для країн – членів Євросоюзу задля вирішення питання достатньої оснащеності державних і приватних стейкголдерів для того, щоб запобігати, мінімізувати та належним чином реагувати на кіберінциденти та кіберзагрози. Матриця кібербезпеки охоплює п'ять компонентів:

− наявність та якість нормативно-правової бази;
− операційні можливості;
− державно-приватне партнерство;
− наявність окремих планів для окремих секторів;
− освіта [11, с. 17].

З огляду на запропоновані компоненти доцільним видається визначення елементів національних систем кібербезпеки: 1) нормативно-правова база (нормативний компонент); 2) суб'єкти забезпечення кібербезпеки (інституційний складник), 3) інструменти їх діяльності (діяльнісний компонент); 4) освіта у сфері кібербезпеки, яку відносять до числа найперспективніших напрямів державно-приватної взаємодії у сфері кібербезпеки [12, с. 103]. Формування, розвиток та вдосконалення вказаних компонентів національних систем кібербезпеки і буде запорукою забезпечення захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Система ж забезпечення кібербезпеки має іншу структуру.

Системою забезпечення національної безпеки, яка у кіберпросторі називається кібербезпекою, В.А. Ліпкан пропонує визначати систему теоретико-методологічних, нормативно-правових, інформаційно-аналітичних, організаційно-управлінських, розвідувальних, контррозвідувальних, оперативно-розшукових, кадрових, науково-технічних, ресурсних та інших заходів, спрямованих на забезпечення процесу управління загрозами за небезпеками, за якого державними і недержавними інституціями гарантується прогресивний розвиток українських національних інтересів, джерел духовного і внутрішнього добробуту народу України, ефективне функціонування самої системи забезпечення національної безпеки України [4, с. 60]. Однак, як нам видається, обмеження обсягу поняття національної системи забезпечення кібербезпеки лише заходами значно і безпідставно звужує зміст поняття.

Аналіз змісту поняття національної системи кібербезпеки, яке закріплено у ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2], дає підстави для здійснення узагальнення наданих компонентів і вказує на обмеження сутності категорії заходами та суб'єктами. Водночас система кібернетичної безпеки, як справедливо вказують В.А. Ліпкан та І.В. Діордіца, повинна розглядається як сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [3, с. 175–176]. Підтримуючи наведену позицію щодо змісту категорії національної системи забезпечення кібербезпеки, зауважимо, що, на наш погляд, опущення категорій методів та форм діяльності в процесі визначення поняття національної системи забезпечення кібербезпеки України під час вказівки на заходи, які здійснюються суб'єктами, видається недоцільним. Форми діяльності суб'єктів національної системи забезпечення кібербезпеки вказують на її зовнішній прояв, являючи собою сталі поєднання доступних для застосування суб'єктом

кібербезпеки методів на визначених підставах та з певними наслідками. Методи ж вказують на доступні для застосування та використання суб'єктами забезпечення кібрбезпеки способи, засоби і прийоми забезпечення кібербезпеки.

Яким чином вирішити означену проблему обсягу категорії національної системи забезпечення кібербезпеки? Можливими для впровадження концепціями формування обсягу поняття «національна система забезпечення кібербезпеки» нам видаються два варіанти формування термінології Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [2] та на цій основі розширення категоріально-понятійного апарату науки адміністративного права України.

Перший варіант – це спрощене трактування поняття національної системи забезпечення кібербезпеки як «сукупність суб'єктів забезпечення кібернетичної безпеки, властивих конкретній нації чи державі, які взаємодіють з метою забезпечення відсутності небезпеки для індивіда, суспільства і країни загалом» [3, с. 175]. В запропонованому варіанті, як вважає І.В. Діордіца, поняття надається у вузькому значенні, охоплюючи сукупність органічно об'єднаних спільними цілями суб'єктів, які здійснюють свою діяльність у кіберпросторі з метою реалізації національних інтересів [13, с. 110]. Але в запропонованому варіанті обсягу категорії національна система кібербезпеки, базуючись на аналізі термінології Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII [2], доцільним можна визначити використання терміну «сектор», а не система. Однак в такому разі змістом категорії «національний сектор кібербезпеки» повинно бути охоплено і громадян та громадські об'єднання, які добровільно беруть участь у забезпеченні кібербезпеки. Науковці застерігають, що «прерогатива державних органів щодо забезпечення кібербезпеки не має всеохоплюючого характеру через те, що згодом такий механізм може перетворити державу на монопольного суб'єкта цієї діяльності і звідси стати індикатором формування тоталітарної держави», – доходить висновку В.А. Ліпкан [4, с. 58]. Сьогодні основними суб'єктами кібербезпеки визначені винятково державні інституції. Включення до їх числа недержавних інституцій дозволить у національному секторі кібербезпеки як сукупності суб'єктів її забезпечення виділити державний та приватний блоки.

Повертаючись до об'єму категорії «національна система забезпечення кібербезпеки», іншим варіантом тлумачення поняття є комплексний підхід до визначення змісту категорії, який передбачає врахування всіх аспектів забезпечення кібербезпеки національною системою, суб'єкти якої не зможуть діяти без чіткого визначення форм та методів їх діяльності як частини компетенції кожного зі структурних елементів.

Висновки. Національною системою кібербезпеки України пропонуємо позначати сукупність елементів, розвиток яких забезпечить досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. З огляду на сформовану міжнародними експертами матрицю кібербезпеки доцільними складниками національної системи кібербезпеки України можна визначити 1) нормативно-правову базу; 2) суб'єктів забезпечення кібербезпеки, об'єднаних в сектори, які взаємодіють на засадах державно-приватного партнерства та координуються єдиним центром; 3) інструменти їх діяльності; 4) об'єкти забезпечення кібербезпеки; 5) освіту у сфері кібербезпеки. Іншими словами, національну систему кібербезпеки України доцільно розуміти поєднанням нормативного, інституційного, інструментального та освітнього компонентів (блоків, складників).

Національна система забезпечення кібербезпеки України повинна являти собою сукупність об'єктів та суб'єктів, зв'язки між якими та з зовнішніми щодо вказаної системи елементами у вигляді окремих заходів, здійснюваних за рахунок охоплених компетенцією кожного форм та методів діяльності, виникають, змінюються та припиняються задля досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Суб'єктами національної системи забезпечення кібербезпеки в Україні повинні бути: 1) держава в особі конкретних органів, установ чи організацій; 2) громадянське суспільство у вигляді окремих громадян, громадських організацій, суб'єктів самоврядної влади; 3) приватний сектор у вигляді представників бізнесу. І вже державу в особі її агентів можна вважати окремим сектором забезпечення кібербезпеки, до якого можна включити тих суб'єктів, якими сьогодні представлено склад національної системи кібербезпеки як основних: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України № 96/2016 від 15.03.2016. *Офіційний вісник України*. 2016 р. № 23. С. 69.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Офіційний вісник України*. 2017 р. № 91. С. 31.

3. Ліпкан В.А., Діордіца І.В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право.* 2017. № 5. С. 174–180.

4. Ліпкан В.А. Поняття системи забезпечення національної безпеки України. *Право і Безпека*. 2003. Т. 2, № 4. С. 57–60.

5. Пасічник В.М. Філософська категорія безпеки як основа нової парадигми державного управління національною безпекою. *Демократичне врядування*. 2011. Вип. 7. URL: http://nbuv.gov.ua/UJRN/DeVr_2011_7_7.

6. Корж І.Ф. Філософія поняття безпека. Реформування національної безпеки: історія, сучасність, перспективи : матеріали підсумкової науково-практичної конференції (19 травня 2016 року). Київ : Інститут УДО КНУ імені Тараса Шевченка, 2017. 116 с. С. 11–12.

7. Присяжнюк М.М. Особливості забезпечення кібербезпеки / М.М. Присяжнюк, Є.І. Цифра. *Реєстрація, зберігання і обробка даних*. 2017. Т. 19, № 2. С. 61–68.

8. Ткаченко В.І. Шляхи формування системи забезпечення національної безпеки / В.І. Ткаченко, Є.Б. Смірнов, О.О. Астахов. *Збірник наукових праць Харківського університету Повітряних Сил.* 2015. Вип. 2. С. 3–8.

9. Глазов О.В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Наукові праці [Чорноморського державного університету імені Петра Могили]*. Сер. : Політологія. 2011. Т. 155, Вип. 143. С. 42–46.

10. Демедюк С.В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис*. 2015. № 2. С. 144–147.

11. Кольцов М. Приходько О. Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні: аналітичні матеріали проекту ГО «Лабораторія законодавчих ініціатив» у рамках Програми USAID «РАДА: підзвітність, відповідальність, демократичне парламентське представництво». URL: https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka.pdf.

12. Топчій О. В. Сучасний стан нормативно-правового регулювання підготовки фахівців із кібербезпеки в Україні. *Jurnalul Juŗidic national: Teorie şi Practica.* № 5 (33). Chişinău, 2018. С. 100–104.

13. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право.* 2017. № 7. С. 109–116.

14. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018 р. № 31. С. 5.