УДК 351.746:007

Володимир Стець
аспірант кафедри державознавства і права
ОРІДУНАДУ при Президентові України

ТЕОРЕТИКО-ПРАВОВІ ПРОБЛЕМИ ВИЗНАЧЕННЯ СУТНОСТІ КІБЕРБЕЗПЕКИ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В статті розглядаються проблемні питання щодо визначення місця кібербезпеки в структурі національної безпеки України та її співвідношення з інформаційною безпекою. Проаналізовані деякі підходи до визначення сутності кібербезпеки з врахуванням останніх змін у законодавстві. Виявлені певні протиріччя в діючому законодавстві щодо вказаних питань, запропонована авторська дефініція кібербезпеки та узагальнено підхід до розуміння співвідношення кібербезпеки та інших складових національної безпеки. Розв'язання цих проблем безпосередньо впливає на розподіл функцій і повноважень органів публічного управління кібербезпекою та сприяє підвищенню ефективності забезпечення кібербезпеки України.
***Ключові слова**: кібербезпека; інформаційна безпека; національна безпека.*

Volodymyr Stets
PhD Student of the Law and Legislative Process Department,
ORIPA NAPA under the President of Ukraine

THEORETICAL AND LEGAL PROBLEMS IN DEFINING THE ESSENCE OF CYBERSECURITY AS A COMPONENT OF INFORMATION SECURITY

The article is devoted to the theoretical and legal analysis of scientific approaches and legislation of Ukraine on defining the essence of cybersecurity as a component of information security. The solution of this complex problem is important, firstly, for the optimal distribution of functions between the public authorities in the sphere of national security and, secondly for the creation of an effective organizational and legal model in ensuring cybersecurity of Ukraine.
However, at present there are no common definitions of the concept of cybersecurity and its place in the national security structure. That leads to contradictions in the provision of current legislation of Ukraine in the sphere of national security. The legal aspect of this problem, taking into account recent changes in Ukrainian legislation, remains insufficiently investigated. The purpose of the article is to clarify the essence of the legal definition of such concept as «cybersecurity», its place in the structure of national security and its correlation with information security.
In order to achieve the purpose of the article the author analyzes the basic theoretical approaches to defining the essence of cybersecurity as a component of information security, the definition of the concept of «cybersecurity» in the current regulatory acts of Ukrainian legislation and strategic documents of separate countries of the world.
The results of the analysis lead to conclusion that most of the definitions relate to the security of computer systems, telecommunication networks, and information. Besides, the expediency of applying the phrase «security state» in the definition of cybersecurity has been proved. Taking into account the shortcomings of the definition of cybersecurity in the Law of Ukraine «On Basic Principles of Ensuring Cybersecurity of Ukraine» the author offers his own version of definition, free from excess signs and characteristics of cybersecurity.
The dominating point of view among the scholars is the recognition of cybersecurity as a component of information security. The author has proved the need to consolidate this fact in special legislation in the sphere of national security.
In general, it can be considered that cybersecurity covers only that part of information sphere where information and telecommunication systems are used for information processing. The mostly right approach is that cybersecurity is an important independent sphere of national security and at the same time it is an integral part of other security spheres, in particular, of information sphere, to the extent when other types of national security depend on the realization of cyber threats.
***Key words**: cybersecurity; information security; national security.*

Постановка проблеми

Стрімке зростання потоків інформації в сучасному світі викликає гостру необхідність в забезпеченні безпеки, в першу чергу, критично важливої інформації для людини, суспільства та держави, в тому числі тієї, що створюється, зберігається, обробляється та розповсюджується у кіберпросторі.

Ключовим поняттям, що характеризує досягнення цієї мети в кіберпросторі, є «кібербезпека». Точне та коректне визначення цього поняття є дуже важливим, оскільки воно відображає розуміння сутності безпеки в кіберпросторі та її місце в структурі національної безпеки, що впливає на оптимальний розподіл функцій між публічними органами, які здійснюють управління у сфері забезпечення національної безпеки, та в концентрованому вигляді вказує на організаційно-правову модель забезпечення кібербезпеки в конкретній країні.

Виділення невирішених раніше частин загальної проблеми

На сьогодні відсутнє загальноприйняте визначення кібербезпеки, що означає відсутність загальноприйнятого розуміння сутності цього поняття. Це ускладнює вирішення питання щодо співвідношення кібербезпеки та інформаційної безпеки. Дослідники цієї проблематики про-

понують різноманітні підходи до вирішення зазначеної проблеми, наукові дискусії тривають й досі. Проте правовий аспект цієї проблеми з урахуванням останніх змін у вітчизняному законодавстві залишається не дослідженим.

Мета

Метою статті є уточнення сутності нормативно-правового визначення поняття «кібербезпека», її місця в структурі національної безпеки та співвідношення з інформаційною безпекою.

Аналіз останніх досліджень і публікацій

Різні аспекти зазначеної проблематики розглядались в працях науковців О.А. Баранова, В.Л. Бурячка, В.М. Бутузова, Т.Н. Ворожцової, Д. В. Дубова, С.В. Мельніка, В.М.Панченко, Н.А.Ткачук, В.Б.Толубко, С.В.Толюпи, А.В. Тонконогова, В.П. Шеломенцева та ін.

Виклад основного матеріалу

На сьогодні існує багато різних наукових підходів і офіційних дефініцій щодо визначення поняття «кібербезпека», що відображають сутність кібербезпеки з різних сторін та під різними кутами зору.

Вітчизняні науковці пропонували такі підходи до визначення кібербезпеки (вибірково, оскільки розгляд всіх наявних підходів потребує значно більшого обсягу статті).

Д .В. Дубов сприймає кібербезпеку як стан захищеності інтересів людини і громадянина, суспільства та держави в кіберпросторі [6]. Практично так само вважає В. М. Бутузов, він визначає кібербезпеку як стан захищеності життєво важливих прав та інтересів людини, суспільства, держави в кіберпросторі від внутрішніх і зовнішніх протиправних посягань та загроз таких посягань [4].

О. А. Баранов розглядав кібербезпеку як такий стан захищеності інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди. Також він зробив висновки щодо кваліфікуючих ознак належності до проблематики кібербезпеки: 1) обов'язкова умова використання комп'ютерних систем і телекомунікаційних мереж (основна); 2) проблематика кібербезпеки має відношення до забезпечення суб'єктів інформаційних відносин достовірною, своєчасною та повною інформацією, а також до недопущення порушення її цілісності та конфіденційності; 3) з проблемою кібербезпеки пов'язана проблема нейтралізації негативних інформаційних впливів на технологічному рівні; 4) до кібербезпеки відноситься проблема забезпечення безпеки соціальних та соціотехнічних систем, що використовують комп'ютерні системи та телекомунікаційні мережі; 5) базова мета забезпечення кібербезпеки – це забезпечення стану захищеності життєво важливих інтересів людини, суспільства і держави [2].

В. М. Панченко вважає, що поняття «кібербезпека» означає безпеку об'єктів, які пов'язані з комп'ютерними технологіями, насамперед цифровими мережами (такими, що забезпечують зв'язок між обчислювальними пристроями – комп'ютерами, смартфонами, комунікаторами тощо); що вона є складовою безпеки інформаційної [10].

Згідно з підходом Т. Н. Ворожцової кібербезпека – це інформаційна безпека комп'ютерів та мереж, тобто сукупність технологій, процесів, методів, призначених для захисту комп'ютерного обладнання, інформації, програм, послуг від небажаного або несанкціонованого доступу [5].

Колектив авторів (В. Л. Бурячок та ін.) запропонував своє визначення через «стан захищеності кіберпростору держави в цілому чи окремих об'єктів її інфраструктури» [3]. Варто зауважити, що відносно самого кіберпростору, що є базовим поняттям в кібербезпековій тематиці, існує багато різних підходів щодо тлумачення його сутності та не має загальновизнаної дефініції.

Деякі з наведених підходів отримали певне відображення в офіційних дефініціях в українському законодавстві. Так, у Стратегії кібербезпеки України кібербезпека визначається як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [17].

У Законі України «Про основні засади забезпечення кібербезпеки України» закріплена дещо інша дефініція: кібербезпека – захищеність 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 [15]. Необхідно підкреслити, що згідно із Законом України «Про національну безпеку України» Стратегія кібербезпеки України є основою для підготовки державних програм та нормативно-правових актів у сфері забезпечення кібербезпеки України [14]. Проте законодавець в Законі закріпив іншу дефініцію поняття «кібербезпека», ніж у Стратегії та до сих пір це протиріччя не усунено [15, 17].

До самого визначення кібербезпеки в Законі є певні зауваження щодо переліку об'єктів захисту та доцільності включення характеристик захищеності (сталий розвиток інформаційного суспільства та ін.) [15]. Крім того, законодавець пішов шляхом фактичного ототожнення двох понять як синонімів – кібербезпека та захищеність. Але дефініція самого поняття «захищеність» у вказаних законах відсутня.

Проте поняття «кібербезпека» є ширшим, ніж захищеність, а захищеність є головнимм чинником формування кібербезпеки. Якщо звернутися до найбільш поширеного розуміння безпеки взагалі, то це стан, коли загрози відсутні і немає небезпеки. Загрози можна класифікувати за різними критеріями, наприклад, за ступенем уразливості об'єкта. Зрозуміло, що для захисту від більш уразливих загроз потрібно забезпечити більшу захищеність й навпаки (з метою економії ресурсів), тобто підвищення та зниження рівня захисту повинно здійснюватися відповідно рівню загроз. У разі виконання цієї вимоги безпека об'єкта захисту буде забезпечена у будь-якому випадку та об'єкт захисту буде знаходиться у єдиному стані _ безпеки. За умови невиконання вимоги щодо адекватності рівня захищеності рівню загроз, об'єкт захисту буде знаходитися у стані небезпеки, але деяка захищеність від загроз нижчого

рівня у нього буде (випадки злочинної бездіяльності, непереборної сили та ін. не розглядаємо).

Таким чином, залежно від ступеня адекватності рівня захищеності рівню потенційних загроз об'єкт захисту може перебувати або в стані наявності кібербезпеки, або в стані відсутності кібербезпеки (навіть за певної захищеності об'єкту). Тобто, в такому розумінні кібербезпека є якісною характеристикою поточного стану об'єкта захисту. Відповідно, у випадку зростання рівня загроз, система управління кібербезпекою повинна своєчасно та адекватно відреагувати для забезпечення кібербезпеки об'єктів захисту в нових умовах. Тобто, у визначенні кібербезпеки все ж доцільно використовувати «стан захищеності», а не просто «захищеність», яка відображає процес забезпечення кібербезпеки.

Якщо звернутися до міжнародного досвіду, то можна зробити висновок, що на сьогодні єдине визначення кібербезпеки на міжнародному рівні відсутнє. Наприклад, в стратегічних документах окремих країн закріплені такі визначення [1,7]:

- сукупність організаційних, правових, технічних та освітніх заходів, які спрямовані на забезпечення безперервного функціонування кіберпростору (Політика захисту кіберпростору Республіки Польща);
- бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму (Стратегія кібербезпеки Німеччини);
- заходи з попередження шкоди від збоїв в роботі ІКТ та в її усуненні (Національна стратегія кібербезпеки Королівства Нідерланди);
- бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, що зберігаються або обробляються даною системою (Стратегія безпеки та оборони інформаційних систем Франції);
- це такий сприятливий стан, за якого надійно захищено кіберпростір і забезпечено належне його функціонування (Стратегія кібербезпеки Фінляндії 2013 року).

В наведених прикладах сутність поняття «кібербезпека» передається через ключове слово «заходи» або «стан». Використання в дефініції слова «заходи» означає, що у країні акцент робиться на організаційну сторону забезпечення кібербезпеки. Використання слова «стан», як виділив О.А.Баранов, вказує на головну мету всього процесу забезпечення кібербезпеки. Аналіз різних визначень говорить про те, що усі вони формулюються навколо комп'ютерних систем, телекомунікаційних мереж та інформації, що циркулює в них.

Таким чином, з урахуванням вищевикладеного, можна запропонувати такий варіант визначення поняття «кібербезпека»: «Кібербезпека – це стан об'єктів захисту, за якого їх життєво важливі інтереси та/або характеристики у кіберпросторі мають рівень захищеності, що є адекватним потенційним та реальним загрозам». У цьому визначенні під адекватністю рівня захищеності реальним та потенційним загрозам потрібно розуміти таку організацію системи кіберзахисту, яка гарантує своєчасну нейтралізацію загроз з прийнятними наслідками. Кіберпростір розглядається як складова інформаційного простору. Крім того, таке визначення відповідає принципу пропорційності та адекватності заходів кіберзахисту, який закріплений у ст.7 «Принципи забезпечення кібербезпеки» Закону України [15].

Іншою важливою проблемою у побудові національної системи кібербезпеки є визначення місця кібербезпеки у структурі національної безпеки та її співвідношення з інформаційною безпекою. Ця проблема дуже складна, оскільки інформаційно-телекомунікаційні технології масштабно застосовуються практично в усіх без винятку сферах суспільного життя.

А. В. Тонконогов вважає, що кібербезпека, як і кіберпростір, має дві змістові складові – інформаційну і технічну, завдяки чому кардинально розширюється сфера її дії. Основні положення його поглядів можна коротко викласти наступним чином. Кібербезпека завдяки своїй технічній складовій не входить повністю до складу інформаційної безпеки, існує паралельно з нею, є частиною інформаційно-психологічної складової інформаційної безпеки, і водночас є одним з важливих видів національної безпеки держави, що є станом захищеності від внутрішніх та зовнішніх загроз віртуальної реальності в кіберпросторі [12].

Н. Ткачук вважає, що кібербезпека тісно пов'язана з іншими елементами системи національної безпеки, оскільки загрози, які надходять з кіберпростору, можуть бути реалізовані в інформаційному, військовому, екологічному та ін. сегментах національної безпеки держави [11].

С. В. Мельник стверджує, що поняття «кібербезпека» з технологічної точки зору і завдань забезпечення національної безпеки є безумовно складовою частиною поняття «інформаційна безпека», оскільки розглядаються ті ж самі загрози, методи, засоби і заходи захисту, реалізація яких (атаки) обмежується тільки технологіями кіберпростору. У цьому разі ті ж самі технологічні особливості є підставою і для розгляду кібербезпеки як окремої категорії, що належить, насамперед, до завдань забезпечення громадської та міжнародної безпеки. Також він відзначає, що у межах галузевих досліджень інформаційна безпека традиційно розглядається як невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки [9].

В цілому можна зробити висновок, що домінуючою точкою зору серед науковців є визнання кібербезпеки складовою інформаційної безпеки. Проте, в процесі здійснення державного управління органи влади повинні керуватися положеннями, які закріплені в законодавстві України. Тому аналіз сучасної офіційної позиції щодо цих питань має науково-практичний інтерес.

Вихідними пунктами є положення Конституції України [8], де наведені без визначень такі види безпеки: безпека людини; екологічна безпека; економічна безпека; інформаційна безпека; державна безпека; безпека України; безпека судді та членів його сім'ї; громадська безпека; національна безпека. Таким чином, в цьому переліку кібербезпека відсутня.

З аналізу діючого законодавства України можна зробити висновок, що протягом останніх шести років спостерігається певна еволюція поглядів на місце кібербезпеки в структурі національної безпеки.

В Стратегії розвитку інформаційного суспільства (2013 рік) [18] в розділі «Інформаційна безпека» та в Рекомендаціях парламентських слухань на тему «Законодавче забезпечення розвитку інформаційного суспільства в Україні» від 3 липня 2014 року [16] вказано на кібербезпеку як на частину інформаційної безпеки.

Проте в Стратегії національної безпеки (2015 рік) [19] загрози інформаційній безпеці та загрози кібербезпеці рознесені в різні пункти розділу 3. Крім того, з положення щодо концентрації зусиль у ході реформи Служби безпеки України також випливає, що інформаційна та кібернетична безпеки є різними видами національної безпеки.

В Стратегії кібербезпеки України (2016 рік) [17] вказано на невідкладність створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України. З тексту Стратегії випливає, що розробники Стратегії розрізняють кібербезпеку та інформаційну безпеку, але вважають, що кіберпростір є в економічній, науково-технічній, інформаційній сферах, сфері державного управління, оборонно-промисловому і транспортному комплексах, інфраструктурі електронних комунікацій, секторі безпеки і оборони України.

В Доктрині інформаційної безпеки України (2017 рік) [13] немає ніяких вказівок на те, що кібербезпека є складовою інформаційної безпеки, хоча Стратегія кібербезпеки України [17] в Доктрині згадується.

В ч.1 ст.5 Закону України «Про основні засади забезпечення кібербезпеки України» (прийнятий у 2017 році, набрав чинності у 2018 році) [15] прямо вказано, що сфера кібербезпеки є складовою національної безпеки України. При цьому Служба безпеки України забезпечує реагування на кіберінциденти у сфері державної безпеки, а до об'єктів кібербезпеки віднесені «національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави», тобто можна дійти до висновку, що кібербезпека фактично ототожнюється з національною безпекою.

Нарешті 21 червня 2018 року був прийнятий Закон України «Про національну безпеку України» [14], в якому в ч.4 ст.3 наданий перелік з 7 складових національної безпеки: воєнна, зовнішньополітична, державна, економічна, інформаційна, екологічна, кібернетична безпеки. По тексту Закону України [14] немає ніяких положень про те, що кібербезпека є частиною будь-яких інших складових національної безпеки.

Оскільки в двох основних законах [15,14] у цій сфері відсутні положення щодо кібербезпеки як складової інформаційної безпеки, можна стверджувати, що законодавством не встановлено включення кібербезпеки до сфери інформаційної безпеки і що вона розглядається як самостійна складова національної безпеки. Одночасно не встановлені й чіткі критерії розмежування розглянутих складових національної безпеки, з деяких положень можна зробити висновок, що кібербезпека все ж таки присутня в інших складових національної безпеки. Таким чином, законодавство у сфері національної безпеки потребує удосконалення та приведення у відповідність з теоретичними розробками наукових дослідників у сферах інформаційної безпеки і кібербезпеки, тому доречно в основоположних нормативно-правових актах чітко вказати, що кібербезпека – це складова частина інформаційної безпеки.

Висновки

Аналіз існуючих підходів до визначення поняття «кібербезпека» в наукових працях та в діючому законодавстві показує, що більшість визначень стосується безпеки комп'ютерних систем, телекомунікаційних мереж та інформації в них. Крім того, доведено доцільність застосування в дефініції кібербезпеки словосполучення «стан захищеності» замість просто захищеності. З урахуванням недоліків дефініції «кібербезпека» в Законі України «Про основні засади забезпечення кібербезпеки України» запропонований авторський варіант визначення, вільний від надлишкових ознак та характеристик кібербезпеки.

Домінуючою точкою зору серед науковців щодо співвідношення кібербезпеки та інформаційної безпеки є визнання кібербезпеки складовою інформаційної безпеки. Проте, діюче законодавство щодо цього питання суперечливе, в ньому відсутні чіткі положення про кібербезпеку як складову інформаційної безпеки, водночас деякі положення вказують на присутність кібербезпеки в інших складових національної безпеки. Це заважає правильному розумінню її місця в структурі національної безпеки.

В цілому можна вважати, що кібернетична безпека охоплює тільки ту частину інформаційної сфери, де для обробки інформації застосовуються інформаційно-телекомунікаційні системи. Найбільш вірним виявляється підхід, відповідно до якого кібербезпека є важливою самостійною сферою національної безпеки та водночас вона є складовою інших сфер безпеки, зокрема інформаційної, в тій мірі, в якій стан інших видів національної безпеки залежить від реалізації кіберзагроз.

Література.

1. Акульшина В. Кібербезпека Фінляндії: правовий та інституційний механізми. Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 158–165.

2. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. № 2 (42). С. 54–62.

3. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

4. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КІТ, 2010. 408 с.

5. Ворожцова Т. Н. Разработка онтологии кибербезопасности в энергетике. Information Technology and Security. 2013. № 1 (3). С. 19–25.

6. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

7. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf.

8. Конституція України : Закон від 28 черв. 1996 р. № 254. Відом. Верхов. Ради України. 1996. № 30. Ст. 141.

9. Мельник С.В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з

кібербезпеки. Інформаційні технології і засоби навчання. 2016. Том 55. №5. С. 87–197.

10. Панченко В. М. Співвідношення понять: інформаційна та кібернетична безпека. Інформаційна безпека людини, суспільства, держави. 2013. № 2(12). С. 20–23.

11. Ткачук Н. Кібербезпека у контексті актуальних змін до стратегічних документів у сфері національної безпеки та оборони України. Вісник прокуратури. 2016. № 3. С. 56–64

12. Тонконогов А. В. Кибернетическая безопасность: понятие и сущность феномена. Право и кибербезопасность. 2013. № 2. С. 36–43.

13. Про Доктрину інформаційної безпеки України: Указ Президента України від 25 лютого 2017 р. № 47/2017. Уряд. кур'єр. 2017. № 38.

14. Про національну безпеку України: Закон України від 21 черв. 2018 р. № 2469. Відом. Верхов. Ради України. 2018. № 31. Ст. 241.

15. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-19. Відом. Верхов. Ради України. 2017. № 45. Ст. 403.

16. Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні»: Постанова Верховної Ради України від 3 липня 2014 року № 1565-VII. Відом. Верхов. Ради України. 2014. № 33. Ст. 1163.

17. Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 берез. 2016 р. № 96/2016. Офіц. вісн. України. 2016. № 23. Ст.899.

18. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15 трав. 2013 р. № 386. Уряд. кур'єр. 2013. № 105.

19. Стратегія національної безпеки України: Указ Президента України від 26 трав. 2015 р. № 287. Офіц. вісн. України. 2015. № 43. Ст. 14.