УДК 342.9: 004.056.5
DOI https://doi.org/10.24144/2788-6018.2024.05.73

ДО ПРОБЛЕМИ ВИЗНАЧЕННЯ ТА РОЗМЕЖУВАННЯ ДЕФІНІЦІЙ «ІНФОРМАЦІЙНА БЕЗПЕКА» І «КІБЕРБЕЗПЕКА»

Гончаренко Г.А.,
доктор юридичних наук, доцент,
професор спеціальної кафедри № 1
Центру захисту національної державності,
Навчально-науковий інститут державної безпеки
Національної академії Служби безпеки України
ORCID: 0000-0003-2483-8097

Гончаренко Г.А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека».

Стаття присвячена проблемі визначення та порівняння дефініцій, зокрема в контексті інформаційної та кібербезпеки. Основний акцент зроблено на аналізі існуючих наукових підходів до визначення цих понять, з метою виявлення спільних та відмінних рис між ними. Досліджені різні трактування термінів у вітчизняній та міжнародній науковій літературі, звертаючи увагу на їхній розвиток у зв'язку з сучасними викликами в інформаційному просторі.

Враховуючи наявні як в науці так і в практичній площині різні підходи до визначення термінів «інформаційна безпека» та «кібербезпека», в цьому дослідженні проводиться порівняння вітчизняних і міжнародних визначень, аналіз законодавчої та наукової літератури з урахуванням впливу нових технологій на формування сучасних дефініцій у сфері інформаційної безпеки. Основна увага приділяється методологічним підходам до побудови дефініцій, їх точності, зрозумілості та застосовності в різних контекстах. Акцент робиться на необхідності узгодження термінології, яка б адекватно відображала сучасні виклики та ризики, з якими стикається держава у сфері інформаційної та кібербезпеки. Також підкреслено важливість чіткого розмежування понять для ефективного правового регулювання та практичного застосування, акцентується увага на необхідності уніфікації термінології та розробці стандартів для побудови чітких і однозначних дефініцій, звертається увага на важливість міждисциплінарного підходу в процесі створення дефініцій, що дозволяє врахувати специфіку різних наукових напрямів.

Новизна роботи полягає в комплексному підході до аналізу дефініцій, що дає можливість не лише виявити ключові відмінності та подібності між різними трактуваннями, але й запропонувати рекомендації щодо їхнього вдосконалення. Проаналізувавши приклади з різних галузей, демонструючи, як неоднозначні або некоректні визначення можуть призводити до непорозумінь і помилок в наукових дослідженнях та практичному застосуванні, автор пропонує власну методику оцінки якості саме цих дефініцій, яка може бути використана для покращення наукової комунікації та підвищення точності термінології, в статті вперше публікується авторське бачення визначень дефініцій «інформаційна безпека» та «кібербезпека», враховуючи безпекову складову та міждисциплінарний характер. Це робить статтю важливим внеском у наукову дискусію щодо розвитку термінології у сфері інформаційної та кібербезпеки.

Основними аспектами статті є **а**наліз різних підходів до визначення інформаційної та кібербезпеки, порівняння дефініцій національних і міжнародних дослідників, пропозиція нових, інтегрованих підходів до розуміння цих понять та обговорення практичних аспектів застосування цих дефініцій у сфері національної безпеки.

Ключові слова: інформаційна безпека, кібербезпека, визначення поняття інформаційної безпеки, визначення поняття кібербезпеки, порівняння дефініцій «інформаційна безпека» і «кібербезпека».

Goncharenko G. To the problem of defining and distinguishing the definitions of «information security» and «cyber security».

The article is devoted to the problem of definition and comparison of definitions, in particular in the context of information and cyber security. The main emphasis is placed on the analysis of existing scientific approaches to the definition of these concepts, with the aim of identifying common and distinctive features between them. Different interpretations of terms in domestic and international scientific literature are studied, paying attention to their development in connection with modern challenges in the information space.

Taking into account the different approaches to the definition of the terms «information security» and «cyber security» available both in science and in practice, this study compares domestic and international definitions, analyzes legislative and scientific literature, taking into account the impact of new technologies on the formation of modern definitions in the field information security. The main attention is paid to methodological approaches to the construction of definitions, their accuracy, comprehensibility and applicability in different contexts. Emphasis is placed on the need to agree on a terminology that would adequately reflect the modern challenges and risks that the state faces in the field of information and cyber security. The importance of a clear demarcation of concepts for effective legal regulation and practical application is also emphasized, emphasis is placed on the need to unify terminology and the development of standards for the construction of clear and unambiguous definitions, attention is drawn to the importance of an interdisciplinary approach in the process of creating definitions, which allows taking into account the specifics of various scientific areas.

The novelty of the work lies in a comprehensive approach to the analysis of definitions, which makes it possible not only to identify key differences and similarities between different interpretations, but also to offer recommendations for their improvement. Having analyzed examples from various fields, demonstrating how ambiguous or incorrect definitions can lead to misunderstandings and errors in scientific research and practical application, the author offers his own methodology for assessing the quality of these definitions, which can be used to improve scientific communication and increase the accuracy of terminology, in the author's vision of the definitions of «information security» and «cyber security» is published for the first time in the article, taking into account the security component and interdisciplinary nature. This makes the article an important contribution to the scientific debate on the development of terminology in the field of information and cyber security.

The main aspects of the article are the analysis of different approaches to the definition of information and cyber security, the comparison of definitions by national and international researchers, the proposal of new, integrated approaches to understanding these concepts, and the discussion of practical aspects of the application of these definitions in the field of national security.

Key words: information security, cyber security, definition of the concept of information security, definition of the concept of cyber security, comparison of the definitions of «information security» and «cyber security».

Постановка проблеми. У сучасному світі питання інформаційної безпеки та кібербезпеки набувають все більшої актуальності. Хоча ці терміни часто використовуються взаємозамінно, вони мають різні аспекти і завдання. Дослідники вказують на суттєві відмінності між цими поняттями, що важливо для розуміння їхнього значення та застосування.

В загальному розумінні, інформаційна безпека охоплює захист інформації незалежно від формату її зберігання чи передачі і забезпечує конфіденційність, цілісність і доступність інформаційних ресурсів (це поняття включає не лише захист даних від несанкціонованого доступу, але і їхнє правильне використання, збереження та управління ними). Кібербезпека ж, в свою чергу, зосереджена на захисті комп'ютерних систем, мереж і програм від цифрових атак і охоплює захист інформаційних систем від злому, вірусів, шкідливого програмного забезпечення та інших форм кіберзагроз. Проте, змістовне наповнення цих понять досі є предметом не лише наукових, а й в практичній площині дискусій, що актуалізує необхідність узгодження термінології, яка б адекватно відображала сучасні виклики та ризики, з якими стикається держава у сфері інформаційної та кібербезпеки.

Для ефективного правового регулювання та практичного застосування наголошуємо на важливості чіткого розмежування цих понять, необхідності уніфікації термінології та розробці стандартів для побудови чітких і однозначних дефініцій.

Стан опрацювання проблеми. Проблеми визначення дефініцій, зокрема в контексті інформаційної та кібербезпеки були предметом досліджень низки вітчизняних вчених, таких як Липкан В.А., Цимбалюк В.С., Горбенко О.І., Морозов С.П., Ткаченко І.В., Семенюк Н.М., Мельник А.О., Захарова О.В., Черненко Г.В. та інших. Проте, не сформована одностайна позиція українських вчених щодо визначень, іноді маючи суттєві відмінності, яка не враховує сучасні виклики і загрози в інформаційній сфері. Все зазначене актуалізує потребу дослідити наявні і сформувати уніфіковане бачення, яке зможе мати міждисциплінарний спектр застосування, дослідити різні трактування термінів у вітчизняній та міжнародній науковій літературі, звертаючи увагу на їхній розвиток у зв'язку з сучасними викликами в інформаційному просторі.

Метою статті є аналіз проблем визначення та розмежування понять «інформаційна безпека» та «кібербезпека», узгодження термінології, яка б адекватно відображала сучасні виклики та ризики, з якими стикається держава у сфері інформаційної та кібербезпеки, а також систематизація підходів до їхнього розуміння і використання в контексті національної безпеки України.

Виклад основного матеріалу. Дослідницькі центри Гарвардського університету (зокрема, Гарвардської школи Кеннеді) активно працюють над тим, щоб розширити розуміння безпеки, включивши в нього проблеми кібернетичної та інших напрямків цифрової безпеки, включаючи питання змісту і визначення понять інформаційної безпеки та кібербезпеки. Серед дослідників, які грунтовно займаються цією проблематикою, можна виділити Мартіна Лібрікта/Martin Libicki, Брюса Шнайєра/Bruce Schneier та Майкла Сулмейєра/Michael Sulmeyer.

Мартін Лібрікт визначає інформаційну безпеку як комплекс заходів, які охоплюють захист конфіденційності, цілісності та доступності інформації. Він наголошує на важливості управління ризиками та захисту інформаційних систем від несанкціонованого доступу, а також на необхідності політики безпеки, яка враховує як технічні, так і організаційні аспекти, а кібербезпеку розглядає як захист комп'ютерних систем та мереж від атак, які можуть призвести до порушення їхньої цілісності, доступності або конфіденційності. Він також підкреслює важливість розробки стратегій, які враховують можливі кіберзагрози та їхній вплив на національну безпеку [1]. Будучи експертом з кібербезпеки та криптографії Брюс Шнайєр, визначає кібербезпеку як галузь, що охоплює захист комп'ютерних систем, мереж та програмного забезпечення від атак і кіберзагроз. Його визначення включає як технічні, так і стратегічні аспекти захисту інформаційних систем, підкреслюючи важливість інноваційних технологій та міжнародної співпраці в цій сфері. Майкл Сулмейєр розглядає кібербезпеку як сферу, що охоплює заходи для запобігання та реагування на кіберзагрози, які можуть бути спрямовані на критичну інфраструктуру держави. Він підкреслює важливість міжнародної співпраці та розробки політик для захисту від кіберконфліктів [2]. Ці визначення відображають як технологічний, так і стратегічний підходи до забезпечення безпеки в інформаційному та кіберпросторах.

Над проблемою визначення дефініцій «інформаційна безпека» та «кібербезпека», розмірковували й цілий ряд вітчизняних вчених, які напрацювали вагомий науковий доробок, який варто продемонструвати наочно, показати різноманіття думок з цього приводу. Так, Вадим Липкан розкривав інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави в інформаційній сфері, який забезпечує запобігання нанесенню шкоди через несанкціоноване використання, розповсюдження та викривлення інформації, а кібербезпеку як сукупність заходів, спрямованих на захист кіберпростору від зовнішніх та внутрішніх загроз, забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів у цифровому середовищі [3].

Натомість вчений Віктор Цимбалюк інформаційну безпеку розглядає як комплексну систему правових, організаційних та технічних заходів, спрямованих на забезпечення захисту інформації та інформаційної інфраструктури від загроз природного та антропогенного характеру, а кібербезпеку як стан захищеності інформаційних систем та мереж від кіберзагроз, що забезпечується через застосування спеціальних технологій, процесів та практик управління ризиками в цифровому середовищі [4].

У своєму науковому виданні «Інформаційна та кібербезпека: концептуальні засади та практичні аспекти [5]» вчений Олексндр Горбенко під поняттям «інформаційна безпека» розуміє стан інформаційного середовища, за якого забезпечується стійкість до зовнішніх та внутрішніх загроз, гарантовано права та свободи громадян в інформаційній сфері, а також захищені національні інтереси держави, а під поняттям «кібербезпека» – здатність систем та мереж протидіяти кіберзагрозам, забезпечуючи безперебійну роботу інформаційно-комунікаційних технологій та захист даних від несанкціонованого доступу і модифікації.

Цікавою є позиція вченого Сергія Морозова, викладена в монографії «Стратегії забезпечення інформаційної та кібербезпеки держави [6]», де під інформаційною безпекою вбачається певна система заходів та механізмів, спрямованих на захист інформаційних ресурсів та забезпечення інформаційної суверенності держави в умовах глобалізації та інформаційних війн, а «кібербезпека» як процес захисту кіберпростору від різноманітних загроз, включаючи захист персональних даних, державних інформаційних систем та критичної інфраструктури від кібератак.

Вчений Ігор Ткаченко пов'язав дефініцію «інформаційна безпека» з дотримання правових норм і визначає її як стан захищеності інформаційних ресурсів, при якому забезпечується їх цілісність, конфіденційність та доступність, а також дотримання правових норм в інформаційній сфері, а «кібербезпеку» визначив як процес управління ризиками в цифровому середовищі, що включає виявлення, аналіз та нейтралізацію кіберзагроз для забезпечення стійкого функціонування інформаційних систем [7].

Визначення інформаційної безпеки вчена Наталія Семенюк досить логічно поєднала з загрозами, бо мова йде про безпеку, надавши їй таке визначення як стан, при якому забезпечується захист інформації від випадкових або навмисних загроз, що можуть призвести до нанесення шкоди суб'єктам інформаційних відносин, а кібербезпеку показала як комплекс дій та процедур, які гарантують безпечне використання

кіберпростору, запобігаючи несанкціонованому доступу, розкриттю та знищенню цифрової інформації [8].

Розглядаючи ці визначеня через призму державного управління, А.О. Мельник у науково-практичному виданні «Кібербезпека в державному управлінні: теорія та практика» [9] визначає інформаційну безпеку як стан, при якому інформаційні ресурси захищені від внутрішніх та зовнішніх загроз, а також забезпечено належне функціонування інформаційної інфраструктури в інтересах громадян та держави, а кібербезпеку як комплекс політик, процедур та технологій, які забезпечують захист електронних даних та систем від несанкціонованого доступу, пошкодження або втрати, спричинених кіберінцидентами.

Досліджуючи різницю між дефініціями «інформаційна безпека» і «кібербезпека» зазначимо їх взаємопов'язаність, але вони є окремими поняттями, кожне з яких має свій акцент та охоплення в контексті захисту інформаційних ресурсів.

Інформаційна безпека охоплює захист усіх видів інформації, незалежно від того, в якій формі вона існує – електронній, паперовій, вербальній тощо. Це включає захист конфіденційності, цілісності та доступності інформації, а також захист від загроз, які можуть поставити під загрозу ці аспекти [10]. Інформаційна безпека охоплює більш широкий спектр заходів і підходів, включаючи політику, процеси та людський фактор. Кібербезпека, з іншого боку, є складовою інформаційної безпеки.

Кібербезпека спеціалізується на захисті комп'ютерних систем, мереж та програмного забезпечення від цифрових загроз й включає в себе технічні засоби захисту, такі як фаєрволи, антивірусне програмне забезпечення, системи виявлення вторгнень, а також заходи, що запобігають кібератакам, кіберзлочинам та іншим зловмисним діям у кіберпросторі [11].

Тож, інформаційна безпека та кібербезпека це, безсумнівно, тісно пов'язані, поняття, але вони мають свої особливості, на які подивимося у контексті забезпечення захисту даних.

Так, інформаційна безпека охоплюючи всі аспекти захисту інформації, незалежно від її форми (електронна, друкована, усна тощо), та включаючи засоби і методи захисту інформаційних ресурсів від загроз, що можуть бути як внутрішніми, так і зовнішніми, включає в себе такі три ключові компоненти: (а) конфіденційність, забезпечення того, що інформація доступна тільки тим, хто має на це право; (б) цілісність, забезпечення того, що інформація є точною і повною, а будь-які зміни вносяться лише авторизованими особами; (в) доступність, забезпечення своєчасного та надійного доступу до інформації для тих, хто має на це право.

З іншого боку, кібербезпека, яку можна вважати підмножиною інформаційної безпеки, стосується виключно захисту комп'ютерних систем, мереж та програмного забезпечення від кіберзагроз, таких як хакерські атаки, віруси, фішинг та інші форми кібератак і виділимо також три основні аспекти кібербезпеки: (а) захист мережевої інфраструктури, захист від атак, які можуть спричинити збій у роботі мережі; (б) захист даних, захист даних від несанкціонованого доступу та крадіжок; (в) реагування на інциденти, здатність ефективно реагувати на інциденти, що можуть загрожувати безпеці систем.

Підсумуємо, що інформаційна безпека стосується загальної концепції захисту інформації в будь-якому вигляді, тоді як кібербезпека спеціалізується на захисті інформаційних систем та цифрових активів.

Повернемося до чинної нормативно-парової бази, яка встановлює правові основи діяльності у сфері кібербезпеки, визначає повноваження органів державної влади та відповідальність суб'єктів, що діють в кіберпросторі та на законодавчому рівні в пункт 5 частини першої статті 1 Законі України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [12] закріпила поняття «кібербезпека» як 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.

Поняття «інформаційна безпека України» закріплено в Стратегії інформаційної безпеки, затвердженій Указом Президента України від 28 грудня 2021 року № 685/2021 [13] і розкриває це поняття як складову частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Інформаційна безпека в юридичному контексті спрямована на комплексний захист інфор-

маційних ресурсів, включаючи як фізичні, так і цифрові аспекти. В цілому, законодавство України, що регулює інформаційну безпеку, зазвичай фокусується на захисті конфіденційності, цілісності та доступності інформації, а також на забезпеченні відповідності стандартам і вимогам безпеки.

Кібербезпека в юридичному контексті спрямована на захист комп'ютерних систем і мереж від кіберзагроз, таких як атаки хакерів, віруси та інше шкідливе програмне забезпечення. Юридичні норми, що регулюють кібербезпеку, зосереджені на забезпеченні безпеки цифрових інфраструктур і протидії кіберзлочинності.

Також в рамках цього дослідження, і на рівні науковому і на рівні нормативному наявну різницю між інформаційною безпекою та кібербезпекою можна наочно показати, взявши такі критерії порівняння як «цілі та методи» (1), умовно «обсяг захисту» (2) та «аспекти загроз» (3):

(1) інформаційна безпека включає управлінські та технічні заходи для забезпечення конфіденційності, цілісності і доступності інформації, а кібербезпека зосереджена на технічних рішеннях, таких як виявлення і запобігання атак, криптографія, захист від вірусів та інших шкідливих програм;

(2) інформаційна безпека охоплює всі аспекти захисту інформації, включаючи як цифрові, так і фізичні аспекти, а кібербезпека орієнтована виключно на захист цифрових систем і мереж;

(3) інформаційна безпека розглядає загрози як з боку внутрішніх, так і зовнішніх джерел, зокрема людських помилок і зловмисних дій, а кібербезпека переважно концентрується на зовнішніх загрозах, таких як хакери та кіберзлочинці.

На підставі дослідженого, враховуючи іноземний, український науковий, практичний аспект бачення та нормативно-правове закріплення, надамо власне визначення дефініцій.

Так, вважаємо, що інформаційна безпека – це стан захищеності інформаційного середовища, що забезпечує конфіденційність, цілісність та доступність інформації незалежно від її форми (цифрової, паперової, усної). Інформаційна безпека охоплює широкий спектр заходів, включаючи технічні, організаційні та правові, які спрямовані на захист інформаційних ресурсів від внутрішніх і зовнішніх загроз, таких як несанкціонований доступ, викривлення інформації, а також навмисне або випадкове порушення її цілісності. Особлива увага приділяється управлінню ризиками та створенню політик, що спрямовані на збереження інформаційної безпеки на всіх рівнях.

А під поняттям «кібербезпека» розуміємо підсистему інформаційної безпеки, яка зосереджена на захисті комп'ютерних систем, мереж і програмного забезпечення від цифрових загроз. Кібербезпека передбачає впровадження технічних і організаційних заходів для запобігання кіберзагрозам, таких як хакерські атаки, віруси, шкідливе програмне забезпечення, фішинг, а також вжиття дій для швидкого реагування та відновлення після інцидентів. Основними аспектами кібербезпеки є захист мережевої інфраструктури, захист даних і оперативне реагування на кіберінциденти.

Висновки. Зміст понять «інформаційна безпека» та «кібербезпека» вказує на їхню взаємопов'язаність, проте кожне з них має свої специфічні акценти. Інформаційна безпека охоплює всі аспекти захисту інформації, незалежно від її форми, тоді як кібербезпека спеціалізується на захисті цифрових систем і ресурсів у кіберпросторі. Важливість цих понять зростає в умовах сучасних інформаційних загроз, що потребує ефективних стратегій і систем захисту на національному та міжнародному рівнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Harvard University Information Security. URL: https://privsec.harvard.edu (дата звернення: 02.09.2024).
2. Harvard Kennedy School. URL: https://www.hks.harvard.edu/faculty-research/policy-topics/science-technology-data/security (дата звернення: 02.09.2024).
3. Липкан В.А. Основи національної безпеки України. Київ: Правова єдність. 2010. 352 с.
4. Цимбалюк В.С. Кібербезпека в системі національної безпеки України: теоретико-правовий аспект. Львів: Світ. 2015. 290 с.
5. Горбенко О.І. Інформаційна та кібербезпека: концептуальні засади та практичні аспекти. Харків: видавництво «Фоліо». 2017. 320 с.
6. Морозов С.П. Стратегії забезпечення інформаційної та кібербезпеки держави. Дніпро: Акцент. 2018. 268 с.
7. Ткаченко І.В. Кібербезпека та захист інформаційних систем. Вінниця: видавництво «Нова книга». 2015. 298 с.
8. Семенюк Н.М. Інформаційна безпека в умовах сучасних викликів: теорія та практика. Київ: Наукова думка. 2019. 375 с.
9. Мельник А.О. Кібербезпека в державному управлінні: теорія та практика. Полтава: Полтавський літопис, 2016. 285 с.
10. Захарова О.В. Інформаційна безпека: підручник. Київ: видавництво «Ліра-К». 2021. 312 с.

11. Черненко Г.В. Кібербезпека: сучасні загрози та захист. Харків: Харківський національний університет імені В.Н. Каразіна. 2020. 268 с.
12. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.09.2024).
13. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення: 02.09.2024).