УДК 343.85
DOI https://doi.org/10.32841/2307-1745.2020.48-2.15

Яцик Т. П.,
кандидат юридичних наук, доцент, професор кафедри фінансових розслідувань Факультету підготовки, перепідготовки та підвищення кваліфікації працівників податкової міліції Університету державної фіскальної служби України

Бодунова О. М.,
кандидат юридичних наук, доцент кафедри кримінального права та кримінології Навчально-наукового інституту права Університету державної фіскальної служби України

ЩОДО РОЗМЕЖУВАННЯ ПОНЯТЬ «ІНФОРМАЦІЙНА БЕЗПЕКА» ТА «КІБЕРБЕЗПЕКА»

Анотація. У статті досліджено нормативно-правові акти та доктринальні джерела щодо визначення поняття та сутності інформаційної безпеки та кібербезпеки. Зазначено, що теоретичне розв'язання означеного протиріччя між інформаційно-психологічним та інформаційно-технічним аспектами інформаційної та кібербезпеки має важливу теоретичну і практичну значущість для сталого функціонування національної безпеки як цілісної і надійної системи і стає можливим за умов застосування системного підходу до забезпечення інформаційної безпеки України. З'ясовано, що Міжнародний телекомунікаційний союз у своїй Рекомендації дає таке визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. При цьому ресурси організації та користувача включають під'єднані комп'ютерні пристрої, персонал, інфраструктуру, додатки, послуги, системи телекомунікацій і всю сукупність переданої та/або збереженої інформації в кіберсередовищі, а мета кібербезпеки полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації або користувача, спрямованих проти відповідних загроз безпеки в кіберсередовищі. Загальні завдання забезпечення безпеки включають таке: доступність; цілісність, яка може включати автентичність і безвідмовність; конфіденційність. Зроблено висновок, що під кібербезпекою варто розуміти такий стан захищеності життєво важливих інтересів особи, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Ключові слова: кібербезпека, інформаційна безпека, інформаційний простір, інформаційне суспільство, кримінальні правопорушення.

Постановка проблеми. Для того щоб національна безпека України могла відповідати рівню провідних економічних держав, необхідні як послідовні дії з боку держави, спрямовані на підвищення ефективності й розвиток системи взаємодії учасників ІКТ-галузі та забезпечення безпеки критично важливих об'єктів інформаційної та кіберінфраструктур, так і приділення підприємствами та організаціями нашої держави більшої уваги до питань власної інформаційної й кібербезпеки.

Науково-технічна революція початку XXI століття спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (далі – ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (далі – ІТС), сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу [2].

Зважаючи на безперервний розвиток та постійну інформаційну боротьбу, що складає один з важливих елементів сучасної світової політики, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову інформаційної безпеки та кібербезпеки.

Аналіз останніх публікацій. Кримінологічні дослідження щодо поняття та сутності інформаційної безпеки та кібербезпеки проводилися такими вченими, як П. Д. Біленчук, Л. Д. Варунц, М. І. Малій, В. В. Марков, О.В. Таволжанський та інші.

Формулювання цілей (мети) статті. В основу дослідження покладено розгляд теоретичних положень щодо визначення поняття кібербезпеки та інформаційної безпеки, встановлення відмінностей та спільних рис.

Виклад основних результатів та їх обґрунтування. З ростом кількості комп'ютеризованих систем та автоматизованих інструментів все почало переходити в ІТ-поле. Спочатку інформаційна безпека означала мінімізацію кількості доступів до бухгалтерської інформації, різної документації, інформації про патенти тощо. Проте XXI століття зустріло нас ІТ-бумом: комп'ютер став з'являтися в кожному будинку, а інтернет з 2016 року резолюція ООН закріпила в правах людини «Право на доступ до інтернету».

З ростом девайсів, розумних речей, збільшенням трафіку, потоком даних, людина почала все більше переносити

в кіберсередовище: бухгалтерію, управління процесами, виконання робіт. З'явилася необхідність захисту інформації саме в діджитал кіберсередовищі.

Що стосується поняття інформаційної безпеки, то теоретичне вирішення проблеми забезпечення інформаційної безпеки в Україні здійснюється, переважно за двома основними напрямами. В дослідженнях за першим напрямом акцентується увага на технологічній, правовій і організаційній захищеності телекомунікаційних систем та інформаційних ресурсів держави як основного об'єкту забезпечення інформаційної безпеки, а поняття інформаційної безпеки пов'язується, переважно, зі захистом даних. У дослідженнях за другим напрямом, спираючись на гуманітарні аспекти негативних наслідків впливу інформації та інформаційних технологій на суспільство, колективну та індивідуальну свідомість, автори роблять наголос на необхідності протидії інформаційним загрозам, у контексті їх негативного впливу на свідомість, пропонуючи розв'язання проблеми захисту інформаційного простору в ідеологічному, психологічному і правовому ключі. У межах другого напряму відокремлюють, як об'єкт захисту, національну свідомість та життєвоважливі інформаційні інтереси людини і суспільства, що захищаються також нормами національного права. Тобто, у межах загального об'єкту забезпечення інформаційної безпеки – інтересів людини, суспільства і держави, в одному випадку, пропонується розглядати інформаційні ресурси і телекомунікаційні системи держави, в іншому, – індивідуальну, суспільну, національну свідомість та інтереси громадян [3, с. 24].

Варто відмітити, що теоретичне розв'язання означеного протиріччя між інформаційно-психологічним та інформаційно-технічним аспектами інформаційної та кібербезпеки має важливу теоретичну і практичну значущість для сталого функціонування національної безпеки як цілісної і надійної системи і стає можливим за умов застосування системного підходу до забезпечення інформаційної безпеки України [4; 6].

В. М. Фурашев розуміє інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою, насамперед, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням [11].

І. Р. Боднар національну безпеку України в інформаційній сфері розглядає як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки. Тому в процесі визначення характеру ризиків слід брати до уваги наступні елементи:

– концептуальне засади політичної безпеки, її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави;

– визначення об'єктів та цілей;

– визначення прийнятних з погляду забезпечення інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки, а також оцінки ризиків та управління ризиками;

– визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб'єктів включно зі звітністю про події, які несуть потенційні загрози [1].

У зв'язку з цим, у поле зору науковців потрапило поняття «кібербезпека», які спочатку ототожнювали з поняттям «інформаційна безпека». Кібербезпека – це новий виток інформаційної безпеки, який спрямований саме на діджитал середовище. Кібербезпека має на увазі не тільки захист інформації, а й захист всієї системи в інформаційному полі, в ІТ-полі (поле комп'ютерних технологій) в цілому [5].

Варто зазначити, що кібербезпека включає в себе захист інформації, але не обмежується лише нею. Це захист від вірусів, хакерських атак, підробки даних, які можуть не тільки видалити/вкрасти дані, але і вплинути на роботу і продуктивність співробітників, використовувати інформацію проти людини або структури, а також зупинити виробництво. Кібербезпека сьогодні відповідає за три чинники: системи, процеси, люди. Так, 29 серпня 2019 року на Всесвітній конференції по штучному інтелекту в Шанхаї Джек Ма і Ілон Маск обговорювали все що хвилює людство в останні роки: «Ми вже кіборги. Люди настільки інтегровані з телефоном і комп'ютером, що навіть не усвідомлюють цього. Коли ми забуваємо десь мобільний, то здається, ніби втратили частину тіла».

В українському законопроєкті запропоновано свій варіант визначення кібербезпеки, під якою розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави в кіберпросторі [8]. При цьому в законопроєкті кіберпростір – середа, яка виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Дане визначення має дуже низький методологічний потенціал і не дозволяє конкретизувати особливості кібербезпеки. Більше того, абсолютно необгрунтовано до кібербезпеки віднесені проблеми функціонування інформаційних систем в загальному сенсі, внаслідок чого до проблематики кібербезпеки можуть бути віднесені телебачення і радіо, а також навіть бібліотеки та архіви.

З урахуванням того, що проблема кібербезпеки носить глобальний характер, досить цікавою видається позиція міжнародних організацій. Так, Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй Рекомендації дає таке визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача [9]. При цьому ресурси організації та користувача включають під'єднані комп'ютерні пристрої, персонал, інфраструктуру, додатки, послуги, системи телекомунікацій і всю сукупність переданої та/або збереженої інформації в кіберсередовищі, а мета кібербезпеки полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації або користувача, спрямованих проти відповідних загроз безпеки в кіберсередовищі. Загальні завдання забезпечення безпеки включають таке: доступність; цілісність, яка може включати автентичність і безвідмовність; конфіденційність [9].

Українські дослідники пропонують своє бачення терміна кібербезпеки. Так, деякі з них вважають, що в контексті нормативно-правового розуміння національної та інформаційної

безпеки кібербезпека може визначатися як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно- телекомунікаційних систем [7, с. 43–48]. Цим визначенням автори визначають в якості об'єкта загроз – національні інтереси у сфері функціонування інформаційно-телекомунікаційних систем, що значно звужує поле можливих життєво важливих інтересів людини і громадянина, суспільства і держави. Крім того, пропозиція використовувати в якості критерію захищеності життєво важливих інтересів людини і громадянина, суспільства і держави критерій «стабільний розвиток суспільства» не дозволяє сформувати методологічну основу для оцінки рівня такої захищеності, оскільки важко дати кількісні оцінки «стабільного розвитку».

В. Н. Фурашев визначає кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [10, с. 167].

Висновки та перспективи подальших досліджень. На основі зіставлення результатів аналізу проблем визначення терміна «кібербезпека» та «інформаційна безпека» можемо зробити висновок про те, що кібербезпека – це окремий напрям інформаційної безпеки, поява якого обумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж.

Погоджуючись з науковцями, відмітимо, що під кібербезпекою варто розуміти такий стан захищеності життєво важливих інтересів особи, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Література:

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75. https://core.ac.uk/download/pdf/141443493.pdf (дата звернення: 12.01.2020).
2. Бурячок В.Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник /; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf (дата звернення: 12.01.2020).
3. Горлинський В.В. Філософія безпеки і сталого людського розвитку: ціннісний вимір: монографія. Київ, Україна : Парапан, 2011. 231 с.
4. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. *Підприємство, господарство і право. Інформаційне право* 7/2018. URL: https:// phd.znu.edu.ua/page//aref/07_2018/Diorditsa_aref.pdf (дата звернення: 12.01.2020).
5. Інформаційна безпека і кібербезпека – в чому різниця? URL: https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/ (дата звернення: 12.01.2020).
6. Кожедуб Ю. Організаційна парадигма забезпечення інформаційної безпеки. *Information Technology and Security*. Vol. 6, iss. 1(10). pp. 26–36. July-December 2018. doi: 10.20535/2411-1031.2018.6.1.153133
7. Мельник С. В., Тихомиров О. О., Лєнков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки : зб. матер. наук.-практ. конф. *«Актуальні проблеми управління інформаційною безпекою держави»*, (Київ, 22 березня 2011 р.). К. : Вид-во НА СБ України, 2011. Ч. 2. С. 43–48.
8. Про внесення змін до Закону України «Про основи національної безпеки України»: проект Закону України щодо кібернетичної безпеки України від 07.03.13 р. № 2483. URL: //www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998 (дата звернення: 12.01.2020).
9. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. Женева : МСЭ, 2009. С. 55. URL: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru (дата звернення: 12.01.2020).
10. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.
11. Фурашев В. М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика*. 2012. № 2(34). С. 51–59. http://ippi.org.ua/sites/default/files/12fvmbbi.pdf (дата звернення: 12.01.2020).

Yatsyk T. P., Bodunova O. M. Concerning the definition of the concepts of "information security" and cyber security

Summary. The article examines the regulations and doctrinal sources for defining the concept and essence of information security and cybersecurity. It is noted that the theoretical solution of this contradiction between information-psychological and information-technical aspects of information and cybersecurity has important theoretical and practical significance for the sustainable functioning of national security as a holistic and reliable system and becomes possible with a systematic approach to information security of Ukraine.The International Telecommunication Union found in its Recommendation that cybersecurity is a set of tools, strategies, security principles, security guarantees, guidelines, risk management approaches, actions, training, hands-on experience, insurance, and technology that can be used to protect the cyber environment, organizational and user resources. The resources of the organization and the user include connected computer devices, personnel, infrastructure, applications, services, telecommunications systems and the whole set of transmitted and / or stored information in the cyber environment, and the purpose of cybersecurity is to try to achieve and maintain security properties of organizational resources or the user against appropriate security threats in the cyber environment. Common security objectives include: accessibility; integrity, which may include authenticity and reliability; confidentiality. It is concluded that cybersecurity should be understood as a state of protection of vital interests of the individual, society and the state in the use of computer systems and / or telecommunications networks, which minimizes harm to them due to: incompleteness, timeliness and unreliability of information used; negative information impact; negative consequences of the functioning of information technologies; unauthorized dissemination, use and violation of the integrity, confidentiality and availability of information.

Key words: cybersecurity, information security, information space, information society, criminal offenses.