УДК 004.05+165.12(1-622НАТО+477)
DOI https://doi.org/10.32782/IT/2024-2-21

Михайло ШАРАПОВ
бакалавр з комп'ютерної інженерії, Національний авіаційний університет, пр. Любомира Гузара, 1, м. Київ, Україна 03058
***ORCID:** 0009-0007-8225-0677*

Бібліографічний опис статті: Шарапов, М. (2024). Визначення поняття «кібербезпека» в державах та інституціях держав-членів НАТО та Україні: порівняльний аналіз. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2, 160–166, doi: https://doi.org/10.32782/IT/2024-2-21

ВИЗНАЧЕННЯ ПОНЯТТЯ «КІБЕРБЕЗПЕКА» В ДЕРЖАВАХ ТА ІНСТИТУЦІЯХ ДЕРЖАВ-ЧЛЕНІВ НАТО ТА УКРАЇНІ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Актуальність *Стаття присвячена актуальному для Північно-Атлантичних та євроінтеграційних напрямків розвитку України питанню гармонізації основних понять кібербезпеки із відповідними світовими стандартами міжнародних організацій та держав-членів НАТО.*

Метою *даного дослідження є встановлення шляхом проведення порівняльного аналізу спільних та відмінних рис у вітчизняних та закордонних визначеннях поняття «кібербезпека».*

Методологія *дослідження спирається на використання методів аналізу, синтезу, семантичного та герменевтичного аналізу, порівняльно-змістовному методі, тощо. В статті аналізуються вітчизняні та закордонні підходи до формування визначення поняття «кібербезпека». Особлива увага приділяється розгляду цього поняття у стандартах міжнародних державних та недержавних професійних організаціях, у посібниках НАТО, тощо.*

Наукова новизна *дослідження полягає в аналізі новітніх (2020-2024 роки) стандартів, стратегій та методичних рекомендацій, розроблених в Україні та інституціях та організаціях держав – учасників блоку НАТО, порівнянні основних підходів до визначення поняття «кібербезпека» в них.*

Висновки*, що визначення, що застосовуються в нормативній базі держав-членів НАТО, провідних міжнародних організаціях та професійних союзах не є уніфікованими, акцент в них ставиться на захисній та технічній (інформаційно-комунікаційні системи) функціях; визначення, що пропонується в законодавстві України хоча й вносить свій вклад у різноманіття розбіжностей серед країн НАТО та країн-партнерів, але має ширший рівень встановлених задач та об'єктів, акцентується не тільки на захисній, але й превентивно-запобіжній функціях та, що на нашу думку є особливо значущим, ґрунтується на підході антропоцентризму; більшість існуючих визначень поняття кібербезпека можна розподілити на три великих умовних групи за ознакою предметної складової, визначеної у дефініціях: до першої групи увійдуть визначення, що акцентують увагу на кібербезпеці як особливому стані кіберпростору, до другої – розгляд кібербезпеки як набору методів технічного, правового та управлінського впливу, до третьої – акцентуація на діяльності уповноважених суб'єктів та професіоналів, метою якої є безпечний стан кіберпростору.*

Ключові слова: *поняття кібербезпеки, стратегії кібербезпеки держав-членів НАТО, стандарти міжнародних організацій з кібербезпеки, інформаційна безпека.*

Mykhaylo SHARAPOV
Bachelor of Computer Engineering, National Aviation University, 1, Lybomyra Huzara ave., Kyiv, Ukraine, 03058, mykhaylo.sharapov@gmail.com
***ORCID** 0009-0007-8225-0677*

To cite this article: Sharapov, M. (2024) Vyznachennia poniattia "kiberbezpeka" v derzhavakh ta instytutsiiakh derzhav-chleniv NATO ta Ukraini: porivnialnyi analiz [Definition of the concept of "cyber security" in the states and institutions of NATO member states and Ukraine: a comparative analysis]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2, 160–166, doi: https://doi.org/10.32782/IT/2024-2-21

DEFINITION OF THE CONCEPT OF "CYBER SECURITY" IN THE STATES AND INSTITUTIONS OF NATO MEMBER STATES AND UKRAINE: A COMPARATIVE ANALYSIS

Actuality*. The article is devoted to the issue of harmonization of the main concepts of cyber security with the relevant global standards of international organizations and NATO member states, which is relevant for the North Atlantic and European integration directions of Ukraine's development.*

The purpose *of this study is to establish, by conducting a comparative analysis, common and distinctive features in domestic and foreign definitions of the concept of "cyber security".*

The research methodology *is based on the use of methods of analysis, synthesis, semantic and hermeneutic analysis, comparative-content method, etc. The article analyzes domestic and foreign approaches to the formation of the definition of the concept of "cyber security". Special attention is paid to the consideration of this concept in the standards of international state and non-state professional organizations, in NATO guidelines, etc.*

The scientific novelty *of the research lies in the analysis of new (2020-2024) standards, strategies and methodological recommendations developed in Ukraine and the institutions and organizations of the NATO member countries, and in comparison of the basic approaches they use to define the "cyber security" concept.*

Conclusions. *The author comes to the conclusion that the definitions used in the normative base of NATO member states, leading international organizations and professional unions are not unified, the emphasis in them is on protective and technical (information and communication systems) functions; the definition proposed in the legislation of Ukraine, although it contributes to the diversity of disagreements among NATO countries and partner countries, but has a broader level of established tasks and objects, focuses not only on protective, but also preventive function, and that on our opinion is particularly significant, based on the approach of anthropocentrism; most of the existing definitions of the concept of cyber security can be divided into three large conditional groups based on the subject component referred to in the definitions: the first group includes definitions that focus on cyber security as a special state of cyberspace, the second includes consideration of cyber security as a set of technical, legal and management methods influence, to the third – emphasis on the activities of authorized subjects and professionals, the goal of which is the safe state of cyberspace.*

Key words: *the concept of cyber security, cyber security strategies of NATO member states, standards of international cyber security organizations, information security.*

Актуальність дослідження. Поняття «кібербезпека» останнім часом активно використовується у освітньому та науковому середовищі, але уніфікованого загальноприйнятого розуміння його змісту так і не існує. Потенційно це може спричинити значні проблеми в практичному контексті при формування стратегій міжнародного співробітництва як на рівні економічних суб'єктів так і держав. Однією із актуальних задач вітчизняних та світових науковців сьогодення є заповнення цієї лакуни. Аналіз існуючих підходів до визначення поняття «кібербезпека», визначення основних векторів еволюції цього поняття в умовах його стрімкого розвитку та впровадження у вітчизняні стандарти найкращих напрацювань в цій сфері українських та закордонних дослідників, практиків та уповноважених суб'єктів.

Аналіз останніх досліджень демонструє нам значну увагу до питання визначення кібербезпеки серед вітчизняних та закордонних науковців. Так, вже починаючи з 2000-х років семантичними та лексичними аналізам формулювання, змісту та природи цього явища присвячені праці Д. Рута, де аналізується грецьке походження поняття «кібер», методикам написання цього терміну тощо (Рут, 2015). Незвичний для вітчизняного наукового простору підхід проведення методологічних досліджень приватними консалтінговими компаніями демонструють А. Уолз, Дж. Перкінс та Дж. Вайсс, пропонуючи окремі формулювання для недержавних структур, зокрема, комерційного спрямування (Уолз, Перкінс, Вайсс, 2013). Оригінальний погляд на визначення кібербезпеки як міждисциплінарного феномену, з акцентом на захист прав, діяльність суб'єктів та казуальну природу нормативів пропонують Д. Крейген, Н. Дякун-Тібольт та Р. Пюрс (Крейген, Дякун-Тібольт, Пюрс, 2014).

Праці вітчизняних дослідників, які приділяють увагу поняттю кібербезпеки умовно можна поділити на підходи спеціалістів у комп'ютерних науках, які більше зосереджують увагу на операційних процесах, методах та механізмах (Марченко, 2023), стратегіях та станах систем (Баранов, 2014), розмежуванню поняття із поняттям інформаційної безпеки (Фурашев, 2012), тощо. Другою групою є дослідники, що визначають поняття кібербезпеки у полі публічного управління та правовому контексті. В.П. Шеломенцев зосереджується на правових підставах цього явища (Шеломенцев, 2012), І. Діордіца аналізує це поняття у Стратегії національної безпеки України (Діордіца, 2016), Є.В. Кубанов – його формування у понятійно-категоріальному апараті системи публічного управління (Кубанов, 2018).

Аналіз цих досліджень демонструє нам, що попри величезну увагу до поняття кібербезпека у науковців, в умовах проголошеного Україною курсу європейської та північноатлантичної інтеграції виникає потреба в порівняльному аналізі визначення поняття «кібербезпека» у вітчизняній науці та практиці та його застосування та розуміння в інституціях та державних структурах держав-членів НАТО та ЄС, міжнародних стандартизаційних підходах тощо.

Метою даного дослідження є встановлення шляхом проведення порівняльного аналізу

спільних та відмінних рис у вітчизняних та закордонних визначеннях поняття «кібербезпека». Вважаємо, що для досягнення поставленої мети необхідно виконати наступні **задачі**: визначити ступінь уніфікації існуючих дефініцій поняття «кібербезпека»; порівняти визначення цього поняття, що запропоновано у законодавстві України з існуючими варіантами у стандартах НАТО та його держав-членів, міжнародних стандартизаційних організаціях тощо; встановити спільні риси у існуючих підходах до розуміння цього поняття та класифікувати їх.

Об'єктом дослідження є понятійний апарат інформаційної безпеки та кібербезпеки, а **предметом** дослідження є поняття «кібербезпека», що застосовується в державах та інституціях держав-членів НАТО та Україні.

Виклад основного матеріалу дослідження. Розвиток поняття «кібербезпеки» тісно пов'язаний не тільки із науковими, але й освітніми процесами. В освітньо-науковому просторі України спеціальність «Кібербезпека» є новою, а її впровадження є прямим результатом інтеграції вітчизняної науки до світових систем та процесів. У вітчизняних класифікаторах ми можемо побачити її формування на базі вже існуючих стандартів спеціальностей «Інформаційна безпека держави» та «Системи захисту інформації» (Наказ МОН, 2021; Проект стандарту, 2024; Постанова Кабінету Міністрів, 2015). Такий підхід в цілому відповідає й загальносвітовій практиці.

У західних джерелах термін «кібербезпека» почав замінювати собою терміни «комп'ютерна безпека» та «інформаційна безпека» у 10-ті роки XXI століття (Шатц, Біхруш, Уолл, 2017). Вже у 2013 році американські дослідники А. Уолз, Дж. Перкінс та Дж. Вайсс наголосили, що «… використання терміну Кібербезпека як синоніму інформаційної безпеки чи IT безпеки вводить в оману споживачів та спеціалістів з безпеки…» (Уолз, Перкінс, Вайсс, 2013) та наголосили на потребі їх чіткого розмежування. Подальші роки наукових досліджень та практичних реалізацій політики кібербезпеки підтвердили далекоглядність цієї тези і на сьогодні інститут кібербезпеки розглядається як повноцінний самостійний феномен, хоча й тісно пов'язаний із попередніми концептами інформаційної безпеки та комп'ютерної безпеки.

Аналіз визначень від провідних міжнародних інституцій, фахових асоціацій, дослідників та національних стратегій країн НАТО демонструє розбіжності у визначенні цього поняття.

Зокрема, у багатьох випадках чітке визначення поняттю «кібербезпека» не дається, натомість наводиться простий перелік опису функцій чи об'єктів та завдань. В Міжнародній стандартній класифікації освіти категорія «кібербезпека» взагалі не застосовується (Міжнародна стандартна класифікація освіти, 2013).

Посібник Центру Якості Взаємодії з Кіберзахисту CCDCOE NATO з написання національних стратегій із кібербезпеки загального визначення також не дає. У посібнику зазначається, що у стратегіях деяких країн НАТО явна дефініція кібербезпеки взагалі відсутня, а у низки країн застосовується власне формулювання. Центр не дає рекомендованого визначення для національних стратегій, а для цілей роботи із методичними рекомендаціями пропонує широке та узагальнююче «кібербезпека – це бажаний стан, за якого інформаційно-комунікаційні системи надійно захищені у кіберпросторі» (Посібник, 2013).

Міжнародна Організація Стандартизації (ISO) та Міжнародна Електротехнічна Комісія (IEC), що розробили низку стандартів ISO/IEC серії 27K, у текстах стандартів оперують поняттям «інформаційна безпека». Згадка про кібербезпеку у серії 27K з'являється у Технічній Специфікації ISO/IEC 27100 (2020), яка є стандартом у стадії розробки. Вона зазначає, що кібербезпека – широке поняття яке застосовується у світі по різному. Стандартного визначення у специфікації не запропоновано (МОС/МЕК, 2020). Такий підхід на нашу думку обумовлений тим, що зазначене поняття нещодавно увійшло у науковий обіг і є відкритим для дискусій та подальшої формальної стандартизації.

Застосування методу семантичного аналізу дефініцій (Шатц, Біхруш, Уолл, 2017) демонструє нам, що найближчім до того, що використовується у 7 з 11 досліджених країн НАТО є визначення, запропоноване Міжнародним Телекомунікаційним Союзом: «…Кібербезпека – це набір інструментів, політик, концепцій безпеки, заходів безпеки, інструкцій, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можна використовувати для захисту кіберсередовища, організації та активів користувачів. Активи організації та користувача включають підключені обчислювальні пристрої, персонал, інфраструктуру, програми, служби, телекомунікаційні системи та всю інформацію, що передається та/або зберігається в кіберсередовищі. Кібербезпека прагне забезпечити досягнення та підтримку властивостей безпеки організації та активів користувача проти відповідних ризиків безпеки в кіберсередовищі. Загальні цілі безпеки включають доступність; цілісність,

яка може включати автентичність і неспростовність; конфіденційність…» (Міжнародний Телекомунікаційний Союз, 2009).

В свою чергу Національний інститут стандартів та технологій США розглядає феномен кібербезпеки крізь призму запобігання кіберзагрозам, тобто, використовуючи методику «від зворотного»: «… запобігання шкоді, захист та відновлення комп'ютерних електронно-комунікаційних систем та послуг, дротового зв'язку та електронних комунікацій, включаючи інформацію, що міститься у них, з метою забезпечення її доступності, цілісності, автентичності, конфіденційності та неспростовності…» (Національний інститут стандартів та технологій, 2015)

Міжнародна професійна асоціація з аудиту та контролю інформаційних систем ISACA акцентує увагу на захисній природі цього явища «… захист інформаційних активів через боротьбу із загрозами для інформації що обробляється, зберігається та передається крізь інформаційні системи, що використовують інтернет…» (Міжнародна професійна асоціація, 2016) Такий підхід на нашу думку є штучним звуженням поняття кібербезпеки, адже фактично ототожнює його із поняттям «інформаційна безпека» (до того ж концентруючись переважно на інформаційній безпеці у мережі Інтернет) залишаючи поза увагою комп'ютерну безпеку та безпеку електронно-комунікаційних систем.

Законодавство України визначає кібербезпеку – 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» (Указ Президента України, 28.12.2021; Указ Президента України, 26.08.2021; Закон України, 05.10.2017). Вітчизняна наукова доктрина також акцентує увагу на захисті інформації та ефективних стратегіях захисту кіберпростору як основній складовій кібербезпеки (Марченко, 2023), що є абсолютно обґрунтованим в умовах складних викликів, що стоять перед нашою державою сьогодні.

Висновки. Таким чином, проаналізувавши низку визначень поняття «кібербезпека» у стандартах, стратегіях та наукових працях вітчизняних та закордонних дослідників, спостерігаємо що

– визначення, що застосовуються в нормативній базі держав-членів НАТО, провідних міжнародних організаціях та професійних союзах не є уніфікованими, акцент в них ставиться на захисній та технічній (інформаційно-комунікаційні системи) функціях;

– визначення, що пропонується в законодавстві України хоча й вносить свій вклад у різноманіття розбіжностей серед країн НАТО та країн-партнерів, але має ширший рівень встановлених задач та об'єктів, акцентується не тільки на захисній, але й превентивно-запобіжній функціях та, що на нашу думку є особливо значущим, ґрунтується на підході антропоцентризму;

– більшість існуючих визначень поняття кібербезпека можна розподілити на три великих умовних групи за ознакою предметної складової, визначеної у дефініціях: до першої групи увійдуть визначення, що акцентують увагу на кібербезпеці як особливому стані кіберпростору, до другої – розгляд кібербезпеки як набору методів технічного, правового та управлінського впливу, до третьої – акцентуація на діяльності уповноважених суб'єктів та професіоналів, метою якої є безпечний стан кіберпростору.

Перспективи подальших досліджень полягають у подальшому уточненні та уніфікації поняття «кібербезпека», що, на нашу думку, буде відбуватися як в українському, так і в закордонному науковому просторі. Таке подолання термінологічних розбіжностей відіграє значну роль у підвищенні операційної сумісності між Україною та державами-членами НАТО у галузі кібербезпеки, зокрема й з розробки, удосконалення та створення нових стандартів кібербезпеки. Кібербезпека як явище, є з одного боку новим, а з іншого – таким, що постійно та стрімко розвивається, а отже стандартизація цього феномену буде поглиблюватися та поширюватися, охоплюючи все більшу предметну область.

ЛІТЕРАТУРА:

1. Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти: наказ Міністерство освіти і науки України. 18.03.2021. № 332.

2. Проект стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для третього (доктор філософії) рівня вищої освіти. Міністерство освіти і науки України. https://mon.gov.ua/storage/app/media/gromadske-obgovorennya/2023/12/14/Zvit-ho-proyekt.stand.VO-125-Kiberbezpeka.ta.zakhyst.informatsiyi.na.tretomu.rivni.VO.14.12.2023.pdf (дата звернення: 08.05.2024).

3. Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: постанова Кабінету Міністрів України. 29.04.2015 р. № 266 (в редакції постанови Кабінету Міністрів України від 7.07.2021 р. № 762). URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#n11 (дата звернення: 08.05.2024).

4. Schatz D., Bashroush R., Wall J. Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, 2017. № 12 (2). URL: https://commons.erau.edu/jdfsl/vol12/iss2/8/ (дата звернення: 08.05.2024).

5. ISCED-F (Міжнародна стандартна класифікація освіти – Галузі, МСКО-Г) 2013. URL: https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-fields-of-education-and-training-2013-detailed-field-descriptions-2015-en.pdf (дата звернення: 08.05.2024).

6. National Cyber Security Strategy Guidelines. NATO CCDCOE. 2013 URL: https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/ (дата звернення: 08.05.2024).

7. ITU. Series X: Data networks, open system communications and security. Overview of cybersecurity. Recommendation ITU-T X.1205 https://www.itu.int/rec/T-REC-X.1205-200804-I (дата звернення: 08.05.2024).

8. Стратегія інформаційної безпеки: Указ Президента України. 28.12. 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 08.05.2024).

9. Стратегія кібербезпеки України: Указ Президента України. 26.08.2021 р. № 447/2021 URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 20.05.2024).

10. Закон України Про основні засади забезпечення кібербезпеки України. 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.05.2024).

11. Rout D. Developing a Common Understanding of Cybersecurity. *ISACA Journal*, 2015. V. 6. URL: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity (дата звернення: 20.05.2024).

12. Walls A., Perkins E., Weiss J. Definition: Cybersecurity. *Gartner,* 2013. 7 June. URL: https://www.gartner.com/en/documents/2510116 (дата звернення: 20.05.2024).

13. Craigen D., Diakun-Thibault N., Purse, R. Defining Cybersecurity. *Technology Innovation Management Review*, 2014. № 4(10). P. 13–21.

14. Марченко О. Кібербезпека та захист інформації: аналіз впливу ризиків та загроз із використанням сучасних ефективних стратегій кіберзахисту. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2023. № 3. С. 50–59. doi: https://doi.org/10.32782/IT/2023-3-6

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

16. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*, 2012. № 2. С. 162-169.

17. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*, 2012. № 1. С. 312-320.

18. Діордіца І. Поняття та зміст національної системи кібербезпеки. *Jurnalul Juridic National: Teorie si Practica*, 2016. Decembrie. P. 37-42.

19. Кубанов Е.В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. *Аспекти публічного управління*, 2018. вип. 6, вип. 8, Вересень. С. 49-55. doi:10.15421/151846.

20. ISO/IEC TS 27100:2020. Технічна специфікація. URL: https://www.iso.org/obp/ui#iso:std:iso-iec:ts:27100:ed-1:v1:en (дата звернення: 20.05.2024).

21. Cybersecurity. *NIST glossary*. URL:https://csrc.nist.gov/glossary/term/cybersecurity (дата звернення: 20.05.2024).

22. Cybersecurity. Fundamentals Glossary. *ISACA*. URL: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/cybersecurity_fundamentals_glossary.pdf?la=en&hash=B74D338B90ED9CEA1B4E05AABF40139EF692C866 (дата звернення: 20.05.2024).

REFERECES:

1. Pro zatverdzhennia standartu vyshchoi osvity za spetsialnistiu 125 “Kiberbezpeka” dlia druhoho (mahisterskoho) rivnia vyshchoi osvity: nakaz Ministerstvo osvity i nauky Ukrainy. [On the approval of the standard of higher education in specialty 125 “Cybersecurity” for the second (master’s) level of higher education: order of the Ministry of Education and Science of Ukraine] 18.03.2021. № 332 [in Ukrainian]

2. Proekt standartu vyshchoi osvity za spetsialnistiu 125 “Kiberbezpeka” dlia tretoho (doktor filosofii) rivnia vyshchoi osvity. Ministerstvo osvity i nauky Ukrainy. [The project of the standard of higher education in the specialty 125 “Cyber security” for the third (doctor of philosophy) level of higher education. Ministry of Education and Science of Ukraine] Retrieved from: https://mon.gov.ua/storage/app/media/gromadske-obgovorennya/2023/12/14/Zvit-ho-proyekt.stand.VO-125-Kiberbezpeka.ta.zakhyst.informatsiyi.na.tretomu.rivni.VO.14.12.2023.pdf [in Ukrainian]

3. Perelik haluzei znan i spetsialnostei, za yakymy zdiisniuietsia pidhotovka zdobuvachiv vyshchoi osvity: postanova Kabinetu Ministriv Ukrainy vid 29.04. 2015 r. № 266 (v redaktsii postanovy Kabinetu Ministriv Ukrainy vid 7.09.2021 r. № 762). [List of fields of knowledge and specialties for which higher education applicants are trained: resolution of the Cabinet of Ministers of Ukraine dated 04.29. No. 266 of 2015 (as amended by Resolution No. 762 of the Cabinet of Ministers of Ukraine of 7.09.2021).] Retrieved from: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#n11 [in Ukrainian].

4. Schatz, D., Bashroush, R., Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, 12 (2). Retrieved from: https://commons.erau.edu/jdfsl/vol12/iss2/8/ [in English].

5. ISCED-F (Mizhnarodna standartna klasyfikatsiia osvity – Haluzi, MSKO-H) (2013). [International standard classification of education – Sectors, MSKO-G] Retrieved from: https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-fields-of-education-and-training-2013-detailed-field-descriptions-2015-en.pdf [in English].

6. National Cyber Security Strategy Guidelines. NATO CCDCOE. (2013) Retrieved from https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/ [in English].

7. ITU. Series X: Data networks, open system communications and security. Overview of cybersecurity. Recommendation ITU-T X.1205. Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I [in English].

8. Stratehiia informatsiinoi bezpeky: Ukaz Prezydenta Ukrainy. [Information security strategy: Decree of the President of Ukraine.[28.12. 2021 p. № 685/2021. Retrieved from https://www.president.gov.ua/documents/6852021-41069 [in Ukrainian].

9. Stratehiya kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy. [Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine]. 26.08.2021. № 447/2021. Retrieved from https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].

10. Zakon Ukrayiny Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny. [Law of Ukraine On the Basic Principles of Ensuring Cyber Security of Ukraine] 05.10.2017. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

11. Rout, D. (2015). Developing a Common Understanding of Cybersecurity. *ISACA Journal*, V. 6. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity [in English].

12. Walls, A., Perkins, E., Weiss, J. (2013). Definition: Cybersecurity. *Gartner,* 7 June. Retrieved from https://www.gartner.com/en/documents/2510116 [in English].

13. Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21. [in English].

14. Marchenko, O. (2023). Kiberbezpeka ta zakhyst informatsiyi: analiz vplyvu ryzykiv ta zahroz iz vykorystannyam suchasnykh efektyvnykh stratehiy kiberzakhystu. [Cybersecurity and information protection: analysis of the impact of risks and threats using modern effective cyber protection strategies]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 50–59. doi: https://doi.org/10.32782/IT/2023-3-6 [in Ukrainian]

15. Baranov, O. A. (2014). Pro tlumachennya ta vyznachennya ponyattya “kiberbezpeka”. [On the interpretation and definition of the concept of “cyber security”] *Pravova informatika – Legal Informatic*, 2 (42), 54–62 [in Ukrainian].

16. Furashev, V.M. (2012). Kiberprostir ta informatsiynyy prostir, kiberbezpeka ta informatsiyna bezpeka: sutnist', vyznachennya, vidminnosti [Cyberspace and information space, cyber security and information security: essence, definition, differences]. *Informatsiya i pravo – Information and Law*, 2, 162–169 [in Ukrainian].

17. Shelomentsev, V. P. (2012). Pravove zabezpechennya systemy kibernetychnoyi bezpeky Ukrayiny ta osnovni napryamy yiyi udoskonalennya [Legal support of the cyber security system of Ukraine and the main directions of its improvement]. *Borot'ba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka – Fight against organized crime and corruption (theory and practice)*, 1, 312–320 [in Ukrainian].

18. Diorditsa, I. (2016). Ponyattya ta zmist natsional'noyi systemy kiberbezpeky [The concept and content of the national cyber security system]. *Jurnalul Juridic National: Teorie si Practica*, Decembrie, 37–42 [in Ukrainian].

19. Kubanov, E. V. (2018). Teoretychni pidkhody do ponyatiyno-katehorial'noho aparatu kiberbezpeky v systemi publichnoho upravlinnya [Theoretical approaches to the conceptual and categorical apparatus of cyber security in the system of public administration]. *Aspekty publichnoho upravlinnya – Aspects of public administration*, 6 (8), 49–55. doi:10.15421/151846 [in Ukrainian].

20. ISO/IEC TS 27100:2020. Technical specification. Retrieved from https://www.iso.org/obp/ui#iso:std:iso-iec:ts:27100:ed-1:v1:en [in English].

21. Cybersecurity. *NIST glossary*. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity [in English].

22. Cybersecurity. Fundamentals Glossary. *ISACA*. Retrieved from https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/cybersecurity_fundamentals_glossary.pdf?la=en&hash=B74D338B90ED9CEA1B4E05AABF40139EF692C866 [in English].