УДК 342.9:004.056

Веселова Лілія Юріївна,
кандидат юридичних наук, доцент кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ, вул. Успенська, 1, м. Одеса, 65014; 0937118904; e-mail: cvet-Liliya@ukr.net, https//orcid.org/ 0000-0001-6665-0426.

ТЕРМІНОЛОГІЧНИЙ КОНСЕНСУС У ФОРМУВАННІ АДМІНІСТРАТИВНО-ПРАВОВОЇ ПАРАДИГМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Анотація. У статті розглянуто проблеми щодо формулювання основних понять та визначення недоліків понятійного апарату у сфері забезпечення кібернетичної безпеки. Говориться, що у сучасних умовах суспільного розвитку на передній план виходить кібернетична безпека та її забезпечення не лише шляхом упровадження відповідної державної політики на основі прийнятих доктрин, стратегій, концепцій і програм, а й створенням дієвого механізму адміністративно-правового забезпечення кібернетичної безпеки в Україні. Під час проведення дослідження щодо термінологічного консенсусу у формування адміністративно-правової парадигми кібернетичної безпеки аналізуються напрацювання американських науковців та експертів щодо розуміння та визначення таких понять як «кібернетичний простір», «кібернетична безпека», «система кібернетичної безпеки». У статті не залишаються осторонь і вітчизняні науковці щодо їх розуміння понятійного апарату у сфері забезпечення кібернетичної безпеки. Проводиться аналіз міжнародних стандартів щодо наявності в них вищезазначених дефініцій. Під час дослідження зазначається, що адміністративно-правове регулювання та забезпечення кібербезпеки в Україні є новим і доволі динамічним напрямом сучасних знань, який потребує подальшого вивчення. Узагальнюючи запропоновані визначення, які розглядаються у статті, систему забезпечення кібернетичної безпеки запропоновано розглядати як узгоджену діяльність, на основі застосування спеціальних інструментів та методів, уповноважених нормами міжнародного та національного права спеціальних суб'єктів забезпечення кібербезпеки, з метою охорони суспільних відносин у сфері використання інформаційних та телекомунікаційних технологій, прогнозування кібернетичних загроз та захисту кіберпростору. У висновку йде мова, що усі перераховані положення під час наукового дослідження щодо термінологічного консенсусу у формування адміністративно-правової парадигми кібернетичної безпеки мають важливий методологічний зміст щодо розуміння проблем кібернетичної безпеки і не лише в контексті інших видів безпеки. У свою чергу, складнощі з визначенням поняття кіберпростору обу-

мовлюють проблеми щодо розуміння кібернетичної безпеки та кібернетичної війни (війни в кіберпросторі).

Ключові слова: кібернетичний простір, інформаційні системи, адміністративно-правове регулювання, національна безпека.

Veselova Liliia Yuriivna,
Candidate of Law, Associate Professor of the Department of Administrative of the Odessa State Police the University of Internal Affairs, Odessa, Ukraine, st. Uspenskaya, 1, Odesa, 65014; 0937118904; e-mail: cvet-Liliya@ukr.net, https//orcid.org/ 0000-0001-6665-0426

TERMINOLOGICAL CONSENSUS IN THE FORMATION OF ADMINISTRATIVE-LEGAL PARADIGM OF CYBERNETIC SECURITY

Abstract. The article deals with the problems of formulating the basic concepts and identifying the shortcomings of the conceptual apparatus in the field of cyber security. It is said that in the current conditions of social development, cyber security and its security come to the fore not only by introducing appropriate state policy on the basis of adopted doctrines, strategies, concepts and programs, but also by creating an effective mechanism of administrative and legal support for cyber security in Ukraine. The study on terminological consensus in the formation of the administrative and legal paradigm of cyber security analyzes the experience of American scientists and experts in understanding and defining such concepts as "cyber space", "cyber security", "cyber security". The article does not leave aside the domestic scientists on their understanding of the conceptual apparatus in the field of cyber security. International standards are analyzed for the above definitions. During the research it is noted that the administrative and legal regulation and provision of cybersecurity in Ukraine is a new and rather dynamic trend of modern knowledge that needs further study. Summarizing the proposed definitions discussed in the article, the cyber security system is proposed to be considered as a concerted activity, based on the application of special instruments and methods authorized by the norms of international and national law of special cybersecurity entities to safeguard public relations in the field of information and use of information and telecommunication technologies, cyber threats prediction and cyberspace protection. The conclusion is that all of the above provisions in the scientific research on terminological consensus in the formation of the administrative-legal paradigm of cyber security have important methodological content on understanding cyber security issues, and not only in the context of other types of security. In turn, the difficulty in defining the concept of cyberspace causes problems in understanding cyber security and cyber war (cyberspace war).

Keywords: cybernetic space, information systems, administrative and legal regulation, national security.

Постановка проблеми. Необхідною умовою розвитку суспільства є наявність низки відповідних факторів, серед яких провідним є рівень безпеки [1, с. 192-204]. З огляду на зазначене у сучасних умовах суспільного розвитку на передній план виходить кібернетична безпека та її забезпечення не лише шляхом упровадження відповідної державної політики на основі прийнятих доктрин, стратегій, концепцій і програм, а й створенням дієвого механізму адміністративно-правового забезпечення кібернетичної безпеки в Україні.

Розвиток інформаційного суспільства, який супроводжується впровадженням у повсякденному житті комп'ютерної техніки, інформаційних й телекомунікаційних технологій, потребує адекватного правового регулювання у цій сфері, так як поряд із позитивними аспектами технічного прогресу, мають місце негативні прояви, які поширюються та завдають збитків, порушують права свободи громадян тощо. Саме тому нагальною є потреба формування ефективної правової системи забезпечення кібернетичної безпеки як на міжнародному, так і на національному рівнях. Тобто відносини у кібернетичному просторі потребують достатнього правового регулювання. Як зазначають українські фахівці, особливо актуальною визначена проблема постає відносно забезпечення національної безпеки та суспільно небезпечних діянь, які повинні набути статусу правопорушень у кіберсфері та тягнути за собою юридичну відповідальність [2].

З огляду на зазначене, проблеми адміністративно-правового забезпечення кібербезпеки визначається певними чинниками: розвитком світових і національних комп'ютерних мереж і нових технологій, що забезпечують доступ до інформаційних ресурсів; перекладом інформаційних ресурсів на електронні носії і концентрацією їх в інформаційних системах; підвищенням «ціни» створюваної і накопиченої інформації, що слугує реальним ресурсом соціально-культурного і особового розвитку; розробкою і вдосконаленням інформаційних технологій, які можуть ефективно використовуватися кримінальними структурами [3, с. 135].

Аналіз основних досліджень і публікацій. На думку С. Демедюка, відсутність належного адміністративно-правового регулювання забезпечення та організації кібербезпеки в Україні є одним з найважливіших чинників розвитку і зростання кіберзлочинності [4]. Попри те, що останніми роками тематика кібербезпеки в Україні все частіше артикулюється на найвищому державницькому рівні, адміністративно-правове регулювання забезпечення та організації кібербезпеки, реальні заходи в цій сфері все ще залишаються багато в чому фрагментарними та несистемними. Адміністративно-правове регулювання та забезпечення кібербезпеки в Україні є новим і доволі динамічним напрямом сучасних знань. Питанням щодо визначення кібернетичної безпеки займалися такі вітчизняні науковці як О. Манжай, С. Мельник, А. Погорецький та багато інших, серед зарубіжних дослідників – Памела Вулей, Деніел Куел, Дж. Ліпман, Дж. Льюіс тощо. Однак, на сьогодні в цій сфері немає ані «надійної аксіоматики», ані чітко сформульованої термінології та

загальноприйнятих понять, категорій, принципів тощо, що потребує подальшої розробки [4].

Комплексне дослідження адміністративно-правового регулювання у сфері кібернетичної безпеки передбачає, насамперед, проведення глибокого аналізу щодо формулювання основних понять. Недоліки понятійного апарату у сфері адміністративно-правового регулювання забезпечення та організації кібербезпеки не дозволяють: визначити ознаки та об'єктивно оцінити основні загрози у національному сегменті кіберпростору; визначити найбільш ефективні заходи забезпечення кібербезпеки; чітко сформулювати завдання та функції суб'єктів кібербезпеки тощо [5].

Мета статті. Аналіз проблеми формулювання основних понять та визначення недоліків понятійного апарату у сфері забезпечення кібернетичної безпеки.

Виклад основного матеріалу. На думку І. Діордіци, системою забезпечення кібербезпеки варто розуміти сукупність організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на створення умов для реалізації національних інтересів у кіберпросторі, а також сил, засобів і методів, які використовуються для досягнення даної цілі відповідно до законодавства [6]. У вузькому сенсі система забезпечення кібербезпеки – це сукупність органічно об'єднаних спільними цілями суб'єктів, які здійснюють свою діяльність у кіберпросторі з метою реалізації національних інтересів. Кожна держава індивідуально визначає сфери, які вона відносить до кібернетичної безпеки, перелік об'єктів і суб'єктів її забезпечення, виходячи зі тих стратегічних цілей і завдань, які стоять перед державою на національному та міжнародному рівнях, та її практичних можливостей реалізації національних інтересів [7, с. 110].

За своїм змістом та тлумаченням достатньо обґрунтованим є підхід до визначених формулювань. Поряд з цим, особливістю думки автора є все ж акцент на національних аспектах, що уникає використання міжнародного підґрунтя, тлумачень норм міжнародного права.

Кібернетична безпека також розглядається як певна система, тобто сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [8, с. 303]. Або, система кібернетичної безпеки – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з метою забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Розвиток національної системи кібербезпеки має супроводжуватись відповідними корективами у процесі реформування сфери національної безпеки, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором [9, с. 176].

Узагальнюючи запропоновані визначення, систему забезпечення кі-

бернетичної безпеки можемо сформулювати як узгоджена діяльність, на основі застосування спеціальних інструментів та методів, уповноважених нормами міжнародного та національного права спеціальних суб'єктів забезпечення кібербезпеки, з метою охорони суспільних відносин у сфері використання інформаційних та телекомунікаційних технологій, прогнозування кібернетичних загроз та захисту кіберпростору.

Безумовно, ключовою проблемою у формуванні тезаурусу сфери кібербезпеки є визначення поняття кіберпростір [10, с. 69]. Переважна більшість експертів кібернетичної безпеки пов'язують визначення поняття та проблематику кібербезпеки саме через кібернетичного простору, під яким розуміють сукупність комп'ютерних, телекомунікаційних та Інтернет систем або як середовище, яке створює інтегративну основу всіх кіберявищ [4].

Зазначене поняття використовується достатньо часто, і в наукових дослідження існує безліч підходів до його визначення. З точки зору поєднання слів «кібернетичний» та «простір», кіберпростір – це простір (територія), який створений та працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки інформації) [11, с. 216]. З філософської точки зору, кіберпростір – це сфера віртуального буття людини, де діють інші закони, інші звичаї, де людина перетворюється на громадянина іншої держави, стає «кібернавтом» [12, с. 144].

Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі [13, с. 654] .

В різних країнах зазначене поняття визначається дещо по іншому, зокрема [14, с. 62]: США: кіберпростір – це сфера, яка характеризується можливістю використання електронних і електромагнітних засобів для запам'ятовування, модифікування та обміну даними в мережевих системах і пов'язану з ними фізичну інфраструктуру; Великобританія: кіберпростір – це всі форми мережевої цифрової активності, що включають у себе контент і дії, здійснювані через цифрові мережі; Німеччина: кіберпростір – це вся інформаційна інфраструктура, яка доступна через Інтернет поза будь-якими територіальними кордонами; Євросоюз: кіберпростір – це віртуальний простір, у якому циркулюють електронні дані світових персональних комп'ютерів.

У свою чергу, Мельник С.В. кіберпростір визначає як простір, сформований інформаційно-комунікаційними системами, в якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних [15]. Американський дослідник Дж. Ліпман сформулював дві основні складові щодо характеристики кіберпростору: визначення кіберпростору та воєнні дії у кіберпросторі [16, с. 74]. Ним також запропоновано визначення кібербезпеки щодо воєнної сфери США: забезпечення для США свободи

дій, контроль доступу та визначення місцезнаходження противника у кіберпросторі [16, с. 73]. Дж. Ліпман зазначав, що важливим є розуміння того, чим є кіберпростір (і чим він не є), а також того, що означає боротьба у кіберпросторі [16, с. 74]. При цьому акцентовано увагу на певних змінах у сприйнятті кіберпростору військовими експертами [16] та перехід до визначення не через фізичні властивості, а впроваджуючи теоретичні поняття віртуального світу. У той же час американка Памела Вуллей з Інституту технологій повітряних сил США, запропонувала визначати кіберпростір як створене людиною цифрове довкілля, що використовується для миттєвого, безкордонного, глобального, без організаційних, культурних, національних чи політичних кордонів збору, зберігання й передачі даних та інформації між електронним обладнанням [17, с. 8]. У доповіді «Безпека кіберпростору для 44-го Президента», підготовленій за загальним керівництвом Дж. Льюїса поняття кіберпростір визначено дещо більше, ніж просто мережа інтернет, що включає всі мережеві форми та цифрову діяльність [18, с. 11]. Водночас автори акцентують увагу, наводячи приклади численних проникнень хакерів в інформаційні системи, на особливостях загроз від кібератак, наслідки від яких очікувалися переважно фізичного характеру (відкриття шлюзів, авіакатастрофи), натомість вони мають яскраво виражений інформаційний характер [18, с. 12]. Крім того, у документі зазначено, що головні загрози критичній інфраструктурі походять передусім від військових і розвідувальних служб інших держав, оскільки саме вони підготовлені необхідним чином, мають необхідні ресурси та ставлять перед собою чіткі цілі [18, с. 13]. Група авторів окремого дослідження «Кібермогутність і національна безпека» (*Cyberpower and National Security*) акцентують увагу на достатньо широких можливостях визначення феномену кібер. Зокрема, Деніел Куел, розглядаючи термінологію у зазначеному дослідженні, навів близько 30 визначень кіберпростору та в остаточному варіанті запропонував наступне: кіберпростір – операційний домен, обмежений використанням електроніки та електромагнітним спектром для створення, збереження, зміни, обміну та використання інформації у взаємопов'язаних та інтернетизованих інформаційних системах та пов'язаній з ними інфраструктурі [19, с. 4]. Резюмуючи досвід американських науковців та експертів, варто зазначити на прагматизмі у визначеннях ключових понять: найважливіший урок, який ми винесли із цього багатоманіття, це те, що визначення мають допомагати формувати політики чи робити аналіз, а не обмежувати їх [19, с. 4]. Саме використовуючи такий концептуальний підхід, доречним є використання базового поняття у якості шаблону, доповнюючи його щоразу додатковими характеристиками, які сприятимуть динаміці його розвитку. Зокрема, розширюючи поняття кібербезпека, пропонується включити не лише технічні питання, а й людський чинник – ворожі інсайдерські дії чи людські помилки, а також проблеми владних відносин на національному та міжнародному рівнях [10, с.71-72].

Не залишаються осторонь і вітчизняні науковці щодо визначення поняття кіберпростору. О. Манжай

зазначає, що це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [20, с. 145]. Професор А. Погорецький пропонує розуміти під кіберпростором штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо) [21, с. 80].

Цікавою є думка [10, с. 72] з приводу того, що у західних дослідженнях при визначенні поняття кіберпростір нерозв'язаною та нерозтлумаченою залишилась друга частина терміну – «простір». Поряд з цим, вітчизняні науковці «простір» розуміють достатньо широко й описують його у якості певної частини буття людини.

Висновки. Таким чином, усі перераховані положення мають важливий методологічний зміст щодо розуміння проблем кібернетичної безпеки і не лише в контексті інших видів безпеки. У свою чергу, складнощі з визначенням поняття кіберпростору обумовлюють проблеми щодо розуміння кібернетичної безпеки та кібернетичної війни (війни в кіберпросторі).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Айзикович А.С. и др. Краткий словарь по социологии: словарь. Москва: Политиздат, 1988. 477 с.

2. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права.* 2011. № 4. С. 27-30. URL: http:/Avww. nbuv. gov. ua/e-journals/FP/2011 -4/11 bvmprk.pdf.

3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика.* 2014. № 2 (42). С. 132-138.

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

5. Кравцова М.О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії. URL: www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security

6. Поняття та зміст системи забезпечення кібербезпеки. URL: http://goal-int.org

7. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право.* 2017. № 10. С. 110–116.

8. Шеломенцев В.П. Сутність організаційного за безпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 2(28). С. 299–309.

9. Ліпкан В.А., Ліпкан О.С. Національна і міжнародна безпека у визначеннях та поняттях. 2-ге вид., доп. і перероб. Київ: Текст, 2008. 400 с.

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

11. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і Безпека.* 2009. № 4. С. 215–219.

12. Владленова І.В., Кальницький Е.А. Кіберзлочинність як виклик інформаційному суспільству. *Гілея: науковий вісник*. 2013. Вип. 77. С. 142–146.

13. Федченко Д.І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *«Молодий вчений»*. 2018. № 5 (57), травень. С. 653-658.

14. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. *Експертні системи та підтримка прийняття рішень*. 2017. С. 61–68.

15. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. URL: http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011_30/ Zbirnik_30_28.pdf

16. Liepman M. J., Jr. Cyberspace: The Third Domain. URL: https://www. hsdl.org/?view&doc=89385&coll=public

17. Woolley P. Defining Cyberspace as a United States Air Force Mis s ion. URL: http:// www.d tic.mil/cgi-bin/GetTRDoc?AD=ADA453972& Locat ion=U 2&doc =GetTRDoc.pdf

18. Securing Cyberspace for the 44th Presidency / ed. by A.J.Lewis. URL:http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

19. Cyberpower and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. Washington, D.C.: Potomac Books, 2009. 642 p.

20. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. Науковий журнал. 2009. № 4. С. 142–149.

21. Погорецький М., Шеломенцев В. Поняття кіберпростору як середовища вчинення злочинів. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2. С. 77–81.

REFERENCES:

1. Ajzikovich A.S. i dr. (1988) Kratkij slovar' po sociologii [A Brief Dictionary of Sociology]. Moskva: Politizdat [in Russian].

2. Babakin V.M. (2011) Osoblyvosti mizhnarodnoho spivrobitnytstva pry rozsliduvanni kiberzlochyniv [Special features of the international competition for the provision of technical services]. *Forum prava – Forum right, 4, 27-30*. URL: http:/ Avww. nbuv. gov. ua/e-journals/FP/2011 -4/11 bvmprk.pdf [in Ukrainian].

3. Baranov O.A. (2014) Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka» [About interpreting and defining «cybersecurity»]. *Pravova informatyka – Legal Informatics, 2 (42), 132-138* [in Ukrainian].

4. Demediuk S.V. (2015) Okremi pytannia administratyvno-pravovoho ta orhanizatsiinoho zabezpechennia kiberbezpeky [Some issues of administrative and legal support for cybersecurity]. *Pivdennoukrainskyi pravnychyi chasopys – South Ukrainian Law Journal, 2, 144-147* [in Ukrainian].

5. Kravtsova M.O. Faktory determinatsii kiberzlochynnosti v suchasnii kryminolohichnii teorii [Determinants of cybercrime determination in modern criminological theory]. URL:www. infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security [in Ukrainian].

6. Poniattia ta zmist systemy zabezpechennia kiberbezpeky [The concept and content of the cybersecurity system]. *URL: http://goal-int.org* [in Ukrainian].

7. Diorditsa I.V. (2017) Systema zabezpechennia kiberbezpeky: sutnist ta pryznachennia [Cybersecurity system: essence and purpose]. *Pidpryiemnytstvo, hospodarstvo i pravo – Entrepreneurship, economy and law, 10, 110-116* [in Ukrainian].

8. Shelomentsev V.P. (2012) Sutnist orhanizatsiinoho za bezpechennia systemy kibernetychnoi bezpeky Ukrainy ta napriamy yoho udoskonalennia [The essence of organizational security of the cyber security system of Ukraine and directions of its improvement]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka) – Combating Organized Crime and Corruption (Theory and Practice), 2(28), 299-309* [in Ukrainian].

9. Lipkan V.A., Lipkan O.S. (2008) Natsionalna i mizhnarodna bezpeka u vyznachenniakh ta poniattiakh [National and international security in definitions and concepts]. (2-he vyd)., dop. i pererob. Kyiv: Tekst [in Ukrainian].

10. Dubov D.V. (2014) Kiberprostir yak novyi vymir heopolitychnoho supernytstva [Cyberspace as a new dimension of geopolitical rivalry]. Kyiv: NISD [in Ukrainian].

11. Manzhai O.V. (2009) Vykorystannia kiberprostoru v operatyvno-rozshukovii diialnosti [The use of cyberspace in search operations]. *Pravo i Bezpeka – Law and Security, 4, 215-219* [in Ukrainian].

12. Vladlenova I.V., Kalnytskyi E.A. (2013) Kiberzlochynnist yak vyklyk informatsiinomu suspilstvu [Cybercrime as a challenge to the information society]. *Hileia: naukovyi visnyk – Gilea: a scientific bulletin, 77, 142-146* [in Ukrainian].

13. Fedchenko D.I. (2018) Cystema zabezpechennia kiberbezpeky: problemy formuvannia ta efektyvnoi diialnosti [Cybersecurity system: problems of formation and effective activity]. *«Molodyi vchenyi» – «Young Scientist», 5(57), 653-658* [in Ukrainian].

14. Prysiazhniuk M.M., Tsyfra Ye.I. (2017) Osoblyvosti zabezpechennia kiberbezpeky [Features of providing cybersecurity]. *Ekspertni systemy ta pidtrymka pryiniattia rishen – Expert systems and decision support, 61-68* [in Ukrainian].

15. Melnyk S.V., Tykhomyrov O.O., Lienkov O.S. Do problemy formuvannia poniatiino-terminolohichnoho aparatu kiberbezpeky [The problem of the formation of the conceptual terminological apparatus of cybersecurity]. URL: http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011_30/Zbirnik_30_28.pdf [in Ukrainian].

16. Liepman M. J., Jr. Cyberspace: The Third Domain. URL: https://www. hsdl.org/?view&doc=89385&coll=public

17. Woolley P. Defining Cyberspace as a United States Air Force Mis s ion. URL: http:// www.d tic.mil/cgi-bin/GetTRDoc?AD=ADA453972& Locat ion=U 2& doc =GetTRDoc.pdf

18. Securing Cyberspace for the 44th Presidency / ed. by A.J.Lewis. URL:http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

19. Cyberpower and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. Washington, D.C.: Potomac Books, 2009. 642 p.

20. Manzhai O. V. (2009) Vykorystannia kiberprostoru v operatyvno-rozshukovii diialnosti [The use of cyberspace in search operations]. *Pravo i bezpeka. Naukovyi zhurnal – Law and security. Scientific journal, 4, 142-149* [in Ukrainian].

21. Pohoretskyi M., Shelomentsev V. (2009) Poniattia kiberprostoru yak seredovyshcha vchynennia zlochyniv [The concept of cyberspace as a crime medium]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy – Information security of the person, society, state, 2, 77-81* [in Ukrainian].