УДК 338.2:351

Вороненко І.В., к.е.н., с.н.с.;
Тужик К.Л., к.е.н.,
Національний університет біоресурсів
і природокористування України

КОНЦЕПТУАЛЬНІ ЗАСАДИ ЩОДО РЕГУЛЮВАННЯ КІБЕРПРОСТОРУ. МІЖНАРОДНИЙ АСПЕКТ

В статті досліджено теоретичні аспекти формування кіберпростору, систематизовано основні положення міжнародних нормативно-правових норм, що регламентують функціонування та регулювання кіберпростору на міжнародному рівні. Здійснено аналіз рівня готовності щодо забезпечення результативного світового регулювання кіберпростором за допомогою глобального індексу кібербезпеки.

Ключові слова: *кіберпростір, кібербезпека, інформаційна безпека, інформаційний простір, захист інформації.*

Постановка проблеми. Трансформація інформаційного простору в Україні за останні роки суттєво скоротила темпи змін, що є неприпустимим, як в умовах підвищених зовнішніх та внутрішніх загроз для економіки України в умовах сьогодення, так і на шляху до євроінтеграції. Основним наслідком такої ситуації є низький інвестиційний клімат, темпи зростання кількісних, а головне якісних показників надання інформаційно-комунікаційних послуг, а також недостатня ефективність організаційно-економічного механізму державного регулювання даного сектору економіки.

Тому закономірним є виникнення проблеми побудови ефективної стратегії державного регулювання інформаційного простору як соціально-економічного чинника національної безпеки України, що сприятиме виведенню на якісно-новий рівень соціально-економічної безпеки в цілому, та, зокрема, кібербезпеки України, а також вирішенню низки нагальних завдань, що визначені у Концепції популяризації України у світі та просування інтересів України у світовому інформаційному просторі, затвердженої розпорядженням Кабінету Міністрів України від 7 червня 2017 р. № 383-р, Концепції розвитку електронного урядування в Україні, схваленої розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р, рішення Ради національної безпеки і оборони України «Про доктрину інформаційної безпеки України» від 29 грудня 2016 року, введеного в дію та затвердженого Указом Президента України від 25 лютого 2017 року № 47 [1-3], а саме: максимізації ефективності організаційно-економічного механізму державного регулювання інформаційного простору України, його сталий розвиток, національну безпеку України та, зокрема, кібербезпеку в відповідній сфері економічної діяльності, пришвидшення темпів на шляху євроінтеграції, популяризації України у світі та захисті й просуванні її інтересів.

Для пришвидшення даного процесу, що є особливо актуальним для України в умовах євроінтеграції, а також підвищених зовнішніх та внутрішніх загроз, виникає нагальна необхідність у дослідженні «кращої практики» усіх складових держаного регулювання інформаційного простору першочерговою складовою якого є аналіз зовнішнього середовища, а також положень міжнародного законодавства, що регламентують його функціонування та регулювання на міжнародному рівні. Наріжнем каменем на шляху забезпечення цього є формування ефективної системи безпеки кіберпростору, під яким в науковій літературі розуміється «інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії

© Вороненко І.В., Тужик К.Л., 2017

технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [4].

Аналіз останніх досліджень і публікацій. Результати дослідження наукових праць закордонних вчених дозволяють зробити висновок щодо їх суперечливого характеру та зосередженості лише на окремих складових державного регулювання інформаційного та кіберпростору. Так, окремі науковці в своїх працях висвітлюють лише загальні проблеми державного регулювання кіберпростору (Musiani F., Roberts A.S., Sharma A., Tesfachew T.). Частина дослідників зосередила свою увагу на проблемах нормативно-правого регулювання інформаційного простору (Ackerman J.M., Radu R., Sandoval-Ballesteros I.E., Shadiyev K. K., Tatham S. та ін.). Інші вчені досліджують інформаційні права людини (Coppel P., Mendel T.). Деякі вчені розглядають інформаційний простір з боку необхідності забезпечення інтелектуальної власності [Aplin T., Bently L., Cornish W., Llewelyn G.I., Sherman B.). Також серед іншого вчені намагаються в своїх працях вирішити проблеми впровадження технологічних змін в управління цією сферою (Pollitt C.); дослідити вплив інформаційних простору на громадську думку та рішення місцевої влади (Isaac-Henry K., Barnes C.), запропонувати ефективний механізм регулювання кіберпростору (Çeleb I., Jääger M., Tarazan S., Tufail T.).

Водночас, окремі питання щодо державного регулювання інформаційного простору України розглядаються в наукових працях вітчизняних вчених: Єсімова С.С., Мороза С.С. Питання інформаційної політики в Україні в контексті євроінтеграції розкрито в роботах Губерського Л., Камінського Є., Фурашева В.М., Яковенко М. Проте дані дослідження також носять несистемний характер та не надають чітких підходів та керівних механізмів щодо державного регулювання інформаційного простору України в умовах підвищених ризиків зовнішніх та внутрішніх загроз.

Мета дослідження полягає у систематизації положень міжнародних нормативно-правових норм, що регламентують функціонування та регулювання кіберпростору. Відповідна систематизація надасть змогу ідентифікувати, виокремити та розкрити понятійний апарат проблематики регулювання кіберпростору як складової інформаційного простору, визначити та оцінити його ключові складові.

Виклад основного матеріалу. Разом з технічним прогресом і досягненнями в області інформатизації ще на початку XXI століття на рівні Організації об'єднаних націй (ООН) відмічалось, що «кіберпростір», який включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, зберігання і обмін інформацією, додатки, послуги і системи, які відносяться до мережі прямо чи опосередковано – є джерелом не лише майбутнього розвитку суспільства, а й джерелом специфічних загроз [5]. Відтак міжнародна спільнота повинна протидіяти цим загрозам шляхом формування кібербезпеки.

Проведений аналіз нормативно-правових документів, що регламентують регулювання інформаційного та кіберпростору, дозволив дійти висновку, що вперше на міжнародному законодавчому рівні дану проблематику було закріплено у Резолюції Генеральної Асамблеї ООН A/RES/53/70 від 4 грудня 1998 року, в якій зазначено, що «поширення та використання інформаційних технологій і засобів зачіпає інтереси всієї міжнародної спільноти та що широка міжнародна взаємодія сприяє забезпеченню оптимальної ефективності; висловлює занепокоєння, що ці технології та засоби потенційно можуть бути використані в цілях, що несумісні з задачами забезпечення міжнародної стабільності та безпеки, та можуть негативно впливати на безпеку держав; усвідомлюючи необхідність попередження неправомірного використання та використання інформаційних ресурсів або технологій в злочинних або неправомірних цілях [7]. Зважаючи на зазначене, Генеральна Асамблея ООН :

– закликає держави-члени сприяти розгляду на багатосторонньому рівні наявних і потенційних загроз у сфері інформаційної безпеки;

– просить усі держави-члени інформувати Генерального секретаря щодо їх погляду на питання: загальної оцінки проблеми інформаційної безпеки; визначення основних понять, що відносяться до інформаційної безпеки, включно з несанкціонованим втручанням або

неправомірним використанням інформаційних і телекомунікаційних систем та інформаційних ресурсів;

– відмічає доцільність розроблення міжнародних принципів, що були б спрямовувані на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем та сприяли б боротьбі з інформаційним тероризмом та криміналом».

З огляду на поставлену проблематику, варто зазначити, що терміни «безпека у інформаційному просторі» та «безпека у кіберпросторі» або іншими словами «кібербезпека» є досить новим поняттями, які були запропоновані ІТ-професіоналами, консультантами, лобістами та політиками. Оксфордський англійський словник надає наступне визначення терміну «кібербезпека»: «стан захисту від злочинного або несанкціонованого використання електронних даних або заходи, прийняті для досягнення захисту» [8]. Розгорнуте визначення терміну «кібербезпека» міститься в Рекомендаціях Міжнародного союзу електрозв'язку (МСЕ) b-ITU-T X.1205 [9], сутність якого полягає в наборі засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, керівних принципів, підходів в управлінні ризиками, професійної підготовки, передових практик, страхувань і технологій, що можуть використовуватися для захисту кіберпростору, ресурсів організації і користувача.

Аналіз досліджень, присвячених визначенню сутності понятійного апарату «кіберпростір» та «кібербезпека» дозволив визначити основні сфери кібербезпеки, що зображено на рис. 1 [8].

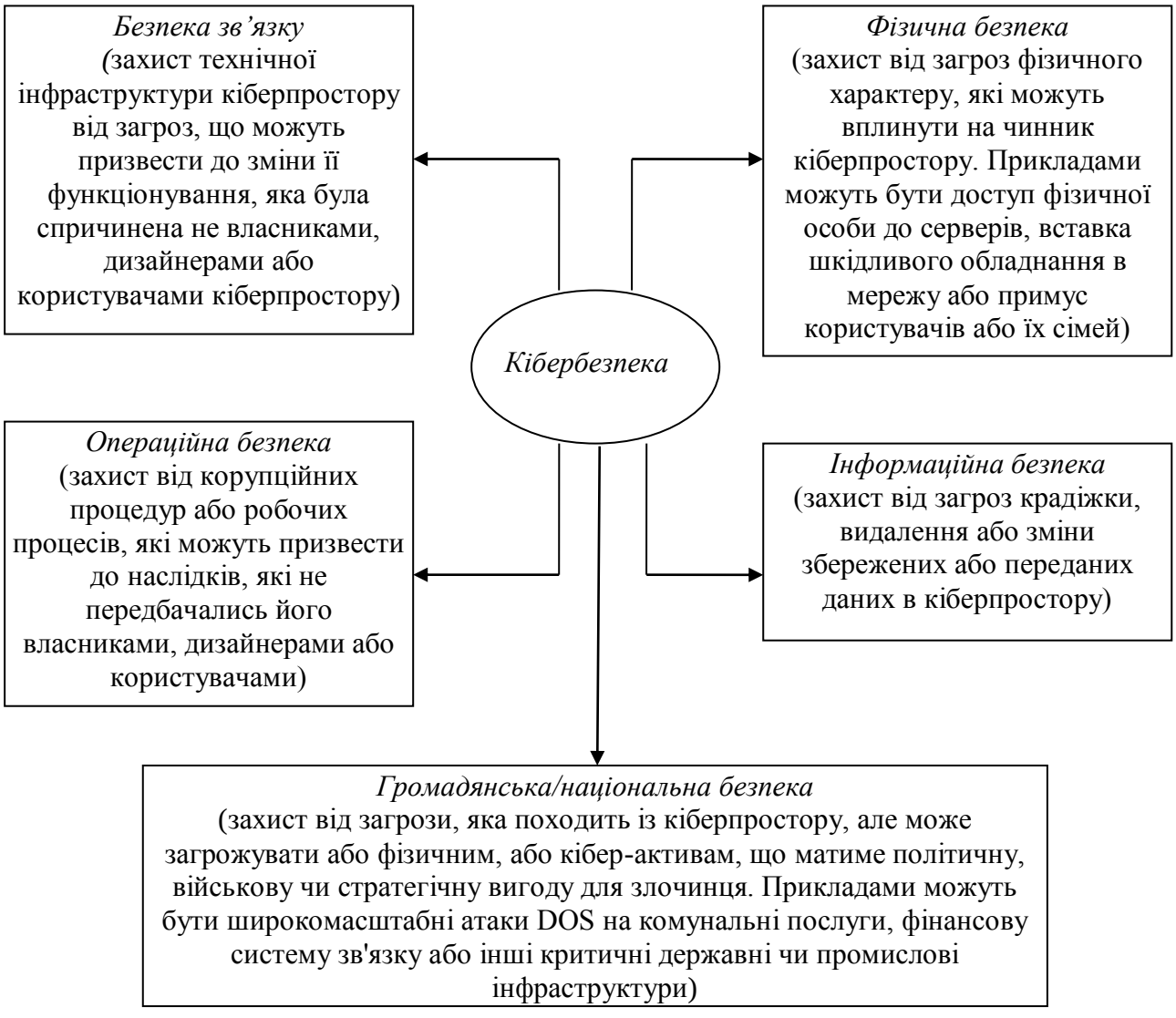

Рис. 1. Основні сфери кібербезпеки

В 2000 році на зустрічі «Групи восьми» на Окинаві була прийнята Хартія глобального інформаційного суспільства. В ній були запропоновані основні принципи та цілі створення глобального інформаційного суспільства: «забезпечення сталого економічного розвитку, покращення суспільного благополуччя, стимулювання соціальної узгодженості, ствердження демократії, транспарентного та відповідального управління, прав людини розвитку культурного різноманіття і забезпечення міжнародного миру і стабільності» [10]. Крім того в документі, було визнано існування загрози кіберзлочинності та відмічена необхідність взаємоузгоджених методів та протидій такій злочинності силами міжнародної спільноти.

Вневдовзі після підписання Окинавської хартії, резолюцією Генеральної Асамблеї ООН 56/183 2001 року було прийнято рішення щодо проведення спільно з Міжнародним союзом електрозв'язку (МСЕ) Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства [11]. Здійснення відповідного заходу передбачалося у два етапи: в 2003 році в Женеві і в 2005 році в Тунісі [12]. За результатами зустрічі було прийнято низку міжнародних документів, що стали фундаментом побудови глобальної інформаційної інфраструктури, зокрема: «Декларація принципів побудови інформаційного суспільства: глобальні виклики в новому тисячолітті», «План дій» [13], «Туніський обов'язок» [14] і «Туніська програма для інформаційного суспільства» [15]. Основними завданнями, що поставлені в документах, є використання потенціалу інформаційних і телекомунікаційних технологій для досягнення цілей розвитку ООН, сформульованих в «Декларації тисячоліття» [16].

У 2007 году МСЕ, яка є провідною установою ООН з питань інформаційно-комунікаційних технологій та глобальним координатором для урядів і приватного сектора в галузі розвитку мереж і послуг, найважливіша роль якого після Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства та Повноважної конференції МСЕ 2006 року полягає в зміцненні довіри і безпеки при використанні інформаційно-комунікаційних технологій, оголосила щодо початку Глобальної програми кібербезпеки (ГПК) як основи міжнародного співробітництва в області кібербезпеки за участю багатьох зацікавлених сторін, що спрямована на досягнення синергії з існуючими й майбутніми ініціативами і партнерами [17].

До найважливіших ініціатив в сфері кібербезпеки під егідою ГПК відносяться: програма в галузі національної групи CIRT (Група реагування на комп'ютерні інциденти); створення регіональних центрів кібербезпеки, які покликані стати каталізаторами розширення регіональної співпраці, координації та спільної діяльності для вирішення проблеми зростаючих кіберзагроз; проект«Підвищення кібербезпеки в найменш розвинених країнах»; Глобальний індекс кібербезпеки (ГІК) – показник рівня розвитку кібербезпеки кожної держави, який спрямований на забезпечення правильної мотивації країн до нарощування своїх зусиль в області кібербезпеки.

В 2012 році МСЕ в Дубаї було скликано Всесвітню конференцію з міжнародних телекомунікацій (WCIT-12) з метою перегляду Міжнародних правил електрозв'язку (ITR) та прийняття документу, який би відповідав новим викликам 21 століття, попередня версія яких була затверджена ще у 1998 році [18]. На доповнення, було прийнято рішення щодо початку процесу інтернаціоналізації управління Інтернетом для забезпечення стабільності, безпеки та безперебійності функціонування глобального інформаційного простору.

Остання на сьогодні резолюція Генеральної Ассамблеї ООН з даної проблематики була прийнята наприкінці 2014 року, в якій серед іншого [19].

– закликається сприяти розгляду на багатосторонньому рівні існуючих та потенційних загроз у сфері інформаційної безпеки, а також можливих стратегій з розгляду загроз, що виникають у цій сфері, виходячи з необхідності зберегти вільний потік інформації;

– проситься продовжувати інформувати щодо точки зору і оцінки з наступних питань: загальної оцінки проблем інформаційної безпеки; зусиллях, що вживаються на національному рівні для зміцнення інформаційної безпеки та сприяння міжнародному співробітництву в цій галузі; змісту концепцій, які були б спрямовані на зміцнення безпеки

глобальних інформаційних та телекомунікаційних систем; можливих заходах, які могли б бути прийняті міжнародним співтовариством для зміцнення інформаційної безпеки на глобальному рівні.

В травні 2015 року МСЕ здійснив публікацію першого ГІК, розрахованого за даними 2014 року, який спрямований на створення для країн правильної мотивації, щоб інтенсифікувати їх зусилля в сфері кібербезпеки, кінцева мета якого полягає у допомозі розвитку глобальної культури кібербезпеки і її інтеграції в найважливіші інформаційні та комунікаційні технології [20]. Варто зазначити, що ГІК являє собою складений індекс, який об'єднує 25 показників та оцінює рівень зобов'язань в п'яти сферах: правові заходи, технічні заходи, організаційні заходи, розвиток потенціалу та міжнародне співробітництво. Такий підхід дозволяє оцінити ефективність та успішність не конкретних заходів, а в цілому існуючих і діючих національних структур, що відповідають за кібербезпеку.

Наступний звіт щодо ГІК був опублікований МСЕ через 3 роки (у 2017 році за даними 2016 року) [21], за результатами якого зроблено висновок щодо вцілому поліпшення та зміцнення програми кібербезпеки в різних країнах у всіх регіонах порівняно з 2014 роком (рис. 2) [20, 21].

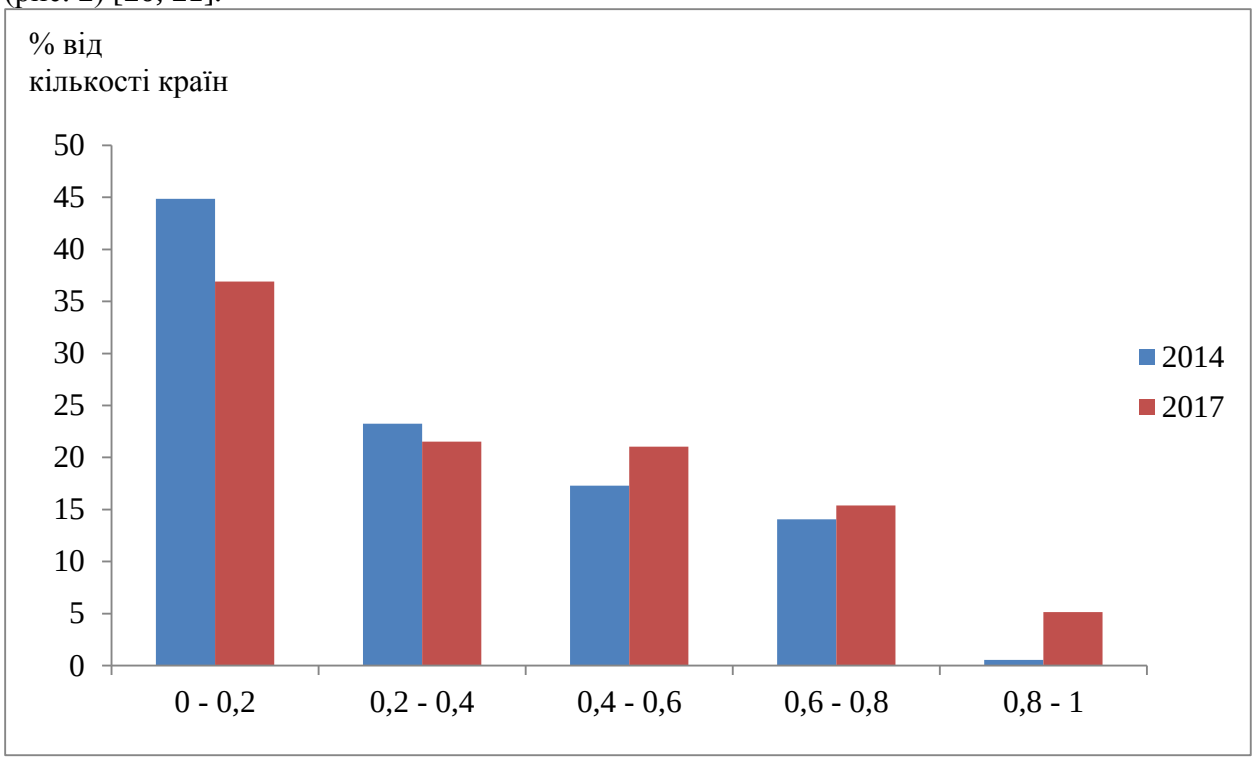

Рис. 2. Порівняняння Глобального індексу кібербезпеки за даними 2014 та 2016 років

Авторами даної роботи з метою розподілу всієї сукупності країн-членів МСЕ, а їх налічується 193, на якісно однорідні типи було здійснено інтервальне групування країн за рівнем ГІК: величина інтервалу значення ГІК $i = 0.11$, кількість груп $k = 8$. Результати групування країн за рівнем ГІК за даними 2016 року наведено на рис. 3.

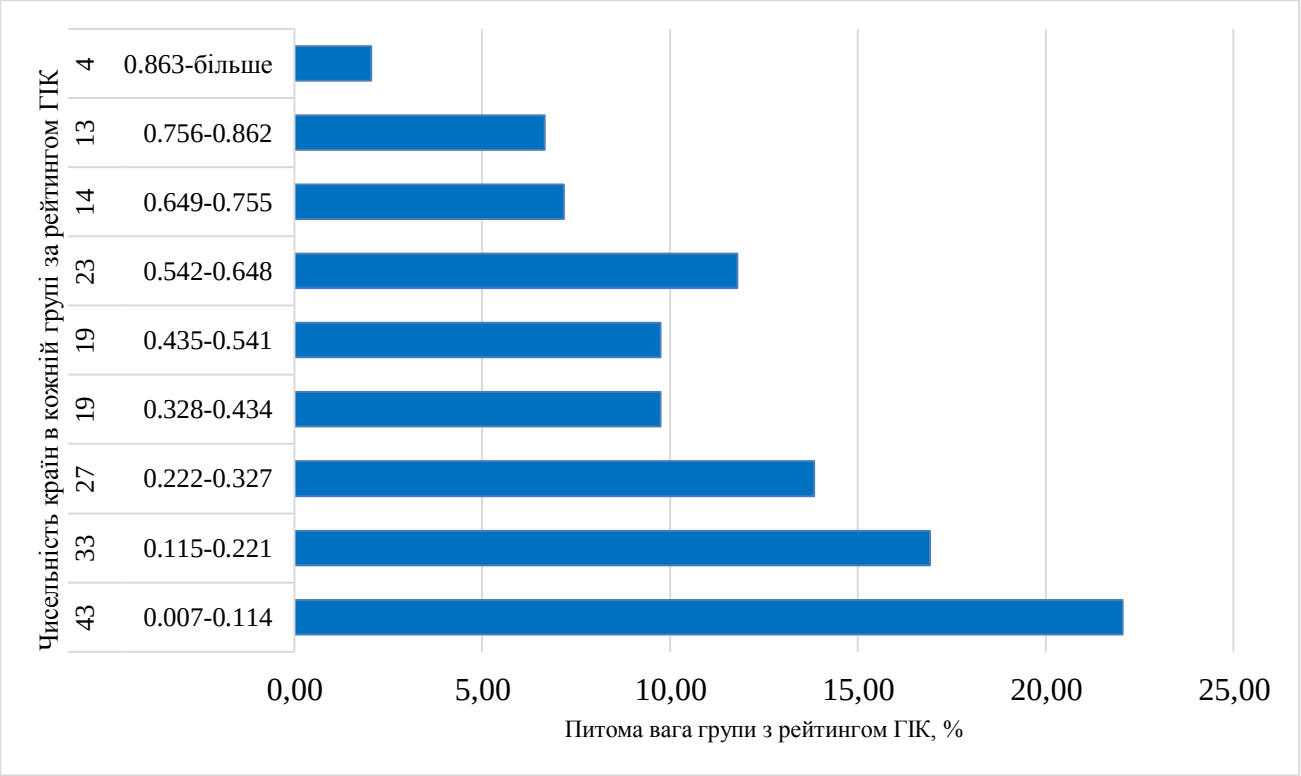

Рис. 3. Групування країн за рівнем Глобального індексу кібербезпеки, 2016 р.

З рисунку 2 видно, що багато країн мають однаковий рейтинг, що вказує на однаковий рівень готовності до забезпечення кібербезпеки, незважаючи на це найбільша кількість країн – 43, що складає понад 22 відсотка припадає на групу з найнижчим значенням ГІК (0.007 – 0.114), тобто заходи з кібербезпеки в цих країнах практично на застосовуються, а найменшу частку, а саме – 4, що у відсотках складає 2,1 займають країни, показник ГІК яких є найвищим – 0.863 і більше. Вищевикладене обумовляє нагальну необхідність інтенсифікації заходів щодо забезпечення кібербезпеки на найвищому рівні.

Висновки. Аналіз міжнародних документів щодо регулювання кіберпростору дозволив систематизувати вимоги щодо інформаційної та кібербезпеки. В результаті структурно-функціонального аналізу документів, що стосуються регулювання кіберпростору, авторами ідентифіковано найбільш вживані з них поняття, а саме: «кібепростір», «безпека зв'язку», «кібербезпека», «інформаційна безпека», «фізична безпека», «операційна безпека» та «громадянська/національна безпека». Здійснено аналіз рівня готовності щодо забезпечення результативного світового регулювання кіберпростором за допомогою ГІК, який свідчить що лише 17 країн світу зі 193 країн-членів МСЕ (менш ніж 9 відсотків від загальної кількості) є стійкими до кіберзагроз.

Отримані результати контент-аналізу проблематики регулювання кіберпростору регулювання дозволять в подальшому виявити недоліки нормативно-правового забезпечення регулювання кіберпростору в Україні та розробити пропозиції щодо його удосконалення, що в свою чергу сприятиме виведенню на якісно-новий рівень соціально-економічної безпеки в цілому, та, зокрема, кібербезпеки України в умовах підвищених зовнішніх та внутрішніх загроз.

Список використаної літератури

1. Концепція популяризації України у світі та просування інтересів України у світовому інформаційному просторі, затверджена розпорядженням Кабінету Міністрів

України від 7 червня 2017 р. № 383-р. Режим доступу: http://zakon2.rada.gov.ua/laws/show/739-2016-%D1%80.

2. Концепція розвитку електронного урядування в Україні, схвалена розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. Режим доступу: http://zakon2.rada.gov.ua/laws/show/649-2017-%D1%80.

3. Рішення Ради національної безпеки і оборони України «Про доктрину інформаційної безпеки України» від 29 грудня 2016 року, введене в дію та затверджене Указом Президента України від 25 лютого 2017 року № 47. Режим доступу: http://zakon2.rada.gov.ua/laws/show/47/2017.

4. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності / О. В. Манжай // Право і Безпека. – 2009. – № 4. – С. 215-219. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Pib_2009_4_50.pdf.

5. Radiocommunication Sector (ITU-R) – ITU Terms and Definitions [Електронний ресурс] // International telecommunication union. – 2017. – Режим доступу до ресурсу: https://www.itu.int/net/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en#lang=en.

6. Musiani F. Governance by algorithms / F. Musiani // Internet Policy Review. – 2013. – № 2 (3). P. 1-8.

7. Резолюция, принятая Генеральной Ассамблеей ООН A/RES/53/70 от 04.01.1999 "Достижения в сфере информатизации и телекоммуникации в контексте международной безопастности: резолюция" [Електронний ресурс] // ООН. – 1999. — Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement.

8. Визначення кібербезпеки – прогалини та дублювання у стандартизації [Електронний ресурс] / [С. Бруксон, С. Цадзов, Р. Екмаєр та ін.] // Heraklion: ENISA. – 2016. – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

9. База даних рекомендацій МСЕ-Т [Електронний ресурс] // МСЄ. – 2017. – Режим доступу до ресурсу: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136.

10. Окинавская Хартия Глобального Информационного Общества [Електронний ресурс] // Институт Развития Информационного Общества. – 2000. – Режим доступу до ресурсу: http://www.iis.ru/library/okinawa/charter.ru.html.

11. Резолюция, принятая Генеральной Ассамблеей ООН 56/183 "Всемирная встреча на высшем уровне по вопросам информационного общества" [Електронний ресурс] // ООН. – 2002. – Режим доступу до ресурсу: http://www.ifap.ru/ofdocs/un/56183.pdf.

12. Світовий Саммiт Інформаційного Суспільства [Електронний ресурс] // Женева-Туніс. – 2003–2005. – Режим доступу до ресурсу: http://www.itu.int/net/wsis/documents/index2.html.

13. ВВУИО План действий WSIS-03/GENEVA/DOC/5-R [Електронний ресурс] // ООН. – 2003 – Режим доступу до ресурсу: http://www.un.org/russian/conferen/wsis/plan.pdf.

14. Туніський обов'язок [Електронний ресурс] // ООН. – 2005. – Режим доступу до ресурсу: http://www.itu.int/net/wsis/docs2/tunis/off/7-ru.pdf.

15. ВВУИО Тунисская Программа для Информационного Общества WSIS-05/TUNIS/DOC/6 (Rev.1)-R [Електронний ресурс] // ООН. – 2005. – Режим доступу: http://www.un.org/russian/conferen/wsis/agenda.pdf.

16. Декларація тисячоліття Організації Об'єднаних Націй [Електронний ресурс] // ООН. – 2000. – Режим доступу до ресурсу: http://zakon3.rada.gov.ua/laws/show/995_621.

17. В поисках кибердоверия [Електронний ресурс] / [Хамадун И. Туре] // МСЭ. – 2014. – Режим доступу до ресурсу: http://zakon3.rada.gov.ua/laws/show/995_621.

18. Всесвітня конференція з міжнародних телекомунікацій [Електронний ресурс] // МСЄ-Дубаї. – 2012. – Режим доступу до ресурсу: http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.

19. Резолюция, принятая Генеральной Ассамблеей ООН A/69/435 от 02.12.2014 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" [Електронний ресурс] // ООН. – 2014. – Режим доступу до ресурсу: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/69/28&referer=/english/&Lang=R.

20. Глобальный индекс кибербезопасности и профили по киберблагополучию [Електронний ресурс] / [Хамадун И. Туре] // МСЭ. – 2015. – Режим доступу до ресурсу: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-R.pdf.

21. Глобальный индекс кибербезопасности – 2017. [Електронний ресурс] // МСЭ. – 2017. – Режим доступу до ресурсу: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx.

Вороненко Ирина Викторовна, Тужик Екатерина Леонидовна. Концептуальные основы регулирования киберпространства. Международный аспект. *Исследованы теоретические аспекты формирования киберпространства, систематизированы основные положения международных нормативно-правовых норм, регламентирующих функционирование и регулирование киберпространства на международном уровне. Осуществлен анализ уровня готовности по обеспечению результативного мирового регулирования киберпространством с помощью глобального индекса кибербезопасности.*

Ключевые слова: *киберпространство, кибербезопасность, информационная безопасность, информационное пространство, защита информации.*

Voronenko Iryna, Tuzhyk Kateryna. Regulating Cyberspace Conceptual Bases. International aspects. *This study analyzes theoretical aspects of the cyberspace formation, systematizes the main provisions of international regulations of the functioning and regulation of cyberspace at the international level. The analysis of the level of preparedness for ensuring effective world regulation of cyberspace with the help of the Global Cybersecurity Index is carried out.*

Keywords: *cyberspace, cybersecurity, information security, information space, information security.*