УДК 351.86

[https://doi.org/10.52058/2708-7530-2021-11\(17\)-57-69](https://doi.org/10.52058/2708-7530-2021-11(17)-57-69)

Геворкян Артем Юрійович кандидат економічних наук, доцент, в.о. директора Українського державного науково-дослідного інституту «Ресурс», вул. Малевича, 84, м. Київ-150, 03150, тел.: (050) 730-71-59, e-mail: bfpochta@gmail.com, <https://orcid.org/0000-0001-5043-1034>

МІЖНАРОДНИЙ ДОСВІД РЕГУЛЮВАННЯ СФЕРИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ЯК ФАКТОРУ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Анотація. Статтю присвячено дослідженню, систематизації та розробленню пропозицій щодо удосконалення напрямів міжнародного регулювання сфери інформаційно-комунікаційних технологій як фактору забезпечення національної та міжнародної безпеки. З'ясовано, що боротьба за володіння інформацією, досягнення і утримання інформаційної переваги зараз займає визначальне місце в геополітичній конкуренції світових держав. Країни, що вкладають значні фінансові, інтелектуальні та інші ресурси у розвиток інформаційного потенціалу, отримують цілу низку конкурентних переваг і можуть використовувати їх або як фактор сили на шкоду інтересам іншим учасникам міжнародних процесів, або як фактор для стримування міжнародної агресії та захисту своїх інтересів в глобальному інформаційному просторі.

Сформовано логічна схема виникнення проблем розвитку та регулювання інформаційно-комунікаційних технологій. Уточнено визначення категорії «глобальна інформаційна безпека», яке включає в собі переваги підходів американсько-європейського та членів Шанхайської організації співробітництва до цієї проблематики. Систематизовані сім основних напрямів створення ефективних механізмів міжнародного регулювання, надані їх теоретичні обґрунтування та можливості удосконалення у майбутньому.

Зроблено висновок, що подальша робота з питань забезпечення глобальної інформаційної безпеки буде спиратися на політичну волю сторін та їх готовності до конструктивного діалогу. Тому проведення змістовних теоретико-методичні та практичні дослідження в рамках кожного напрямку регулювання у сфері інформаційно-комунікаційних відносин, що становлять спільний інтерес світових країни, буде сприяти підвищенню рівня довіри між країнами і подальшому просуванню до універсальних домовленостей в області безпечного та правомірного використання глобального інформаційного простору.

Ключові слова: глобальний інформаційний простір, державне регулювання, інформаційна безпека, інформаційно-комунікаційні технології, інформаційна політика, механізм, національна безпека, публічне управління.

Gevorkyan Artem Yuriiovich Candidate of economic sciences, associate professor, acting director of the Ukrainian State Research Institute «Resource», 84, Malevich St., Kyiv-150, 03150, tel.: (050) 730-71-59, e-mail: bfpochta@gmail.com, <https://orcid.org/0000-0001-5043-1034>

INTERNATIONAL EXPERIENCE IN REGULATING THE SPHERE OF INFORMATION AND COMMUNICATION TECHNOLOGIES AS A FACTOR OF ENSURING NATIONAL SECURITY

Abstract. The article is devoted to the study, systematization and development of proposals for improving the directions of international regulation of the sphere of information and communication technologies as a factor of ensuring national and international security. It is found out that the struggle for information ownership, achievement and retention of Information Superiority now occupies a decisive place in the geopolitical competition of world powers. Countries that invest significant financial, intellectual and other resources in the development of Information potential gain a number of competitive advantages and can use them either as a factor of force to the detriment of the interests of other participants in international processes, or as a factor for deterring international aggression and protecting their interests in the global information space.

A logical scheme for the emergence of problems in the development and regulation of information and Communication Technologies is formed. The definition of the category "Global Information Security" has been clarified, which includes the advantages of the approaches of the American-European and members of the Shanghai Cooperation Organization to this issue. Seven main directions of creating effective mechanisms of international regulation are systematized, their theoretical justification and opportunities for improvement in the future are provided.

It is concluded that further work on ensuring global information security will be based on the political will of the parties and their readiness for constructive dialogue. Therefore, conducting meaningful theoretical, methodological and practical research within each area of regulation in the field of information and communication relations, which are of common interest to world countries, will help to increase the level of trust between countries and further move towards universal agreements in the field of safe and legitimate use of the global information space.

Keywords: global information space, state regulation, information security, information and communication technologies, information policy, mechanism, national security, public administration.

Постановка проблеми. Комплексний розвиток інформаційно-комунікаційних технологій у останні роки постає як каталізатор численних соціально-економічних, культурних і політичних процесів на національному та глобальному рівнях. Еволюційні процеси у соціально-економічних,

техніко-технологічних та інших сферах життєдіяльності держави та суспільства призвела до того, що на зміну індустріальній епосі прийшла постіндустріальна-інформаційна епоха, в якій головну роль відіграють нові інноваційні технології і різноспрямовані інформаційні потоки [1]. Закономірним підсумком цього еволюційного процесу є істотна трансформація як суспільства, так й держави, що спричинило виникнення:

- суспільства нового типу – глобального інформаційного суспільства;
- нового типу економіки – інформаційна або інноваційна економіка;
- нової форми управління державою – електронного уряду,

Всі ці трансформаційні зрушення надають можливість прискорення процесів обміну та отримання інформації, істотно змінюють ритм і стиль життя громадянського суспільства та інших суб'єктів інформаційно-комунікаційних відносин. Отже, на сьогоднішній день рівень розвитку сектору інформаційно-комунікаційних технологій визначає роль держави у світовій економіці та її політичну вагу на міжнародній арені. Тому боротьба за володіння інформацією, досягнення і утримання інформаційної переваги зараз займає визначальне місце в геополітичній конкуренції світових держав. Країни, що вкладають значні фінансові, інтелектуальні та інші ресурси у розвиток інформаційного потенціалу, отримують цілу низку конкурентних переваг і можуть використовувати їх або як фактор сили на шкоду інтересам іншим учасникам міжнародних процесів, або як фактор для стримування міжнародної агресії та захисту своїх інтересів в глобальному інформаційному просторі.

Такі характеристики глобального інформаційного простору, як транскордонність, відкритість, доступність і відносна анонімність обумовлюють привабливість інформаційної інфраструктури з точки зору можливості здійснення неправомірних дій у злочинних і терористичних цілях [2], що є прямою загрозою для національної безпеки країни. Таким чином, протидія даним видам загроз стає важливою складовою комплексу заходів щодо забезпечення інформаційної безпеки як на національному, так і на глобальному рівні.

У зв'язку з цим особливої актуальності набувають дослідження питань міжнародного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення та зміцнення національної безпеки окремих країн, а також подолання викликів і небезпек, які виникають у глобальному інформаційному просторі.

Аналіз останніх досліджень і публікацій. Проблематика регулювання сфери інформаційно-комунікаційних технологій та її взаємозв'язок з національною та світовою безпекою є предметом науково-прикладних досліджень багатьох вітчизняних та зарубіжних вчених, зокрема: Дороніна І.М., Бекстрема Р., Бреннана С., Мюллера М., Аванесової Н.Е., Шмідт М., Голдсміт Дж., Сінгер П., Кох Г. та інші. Цими вченими були проведені

змістовні дослідження та отримані важливі науково-теоретичні та практичні результати, зокрема в обґрунтуванні окремих напрямів регулювання сфери інформаційно-комунікаційних технологій на міжнародному рівні. Однак, проблема систематизації усіх цих напрямів, а також їх удосконалення ще залишаються не повністю вирішеними та потребують подальших досліджень

Мета статті – дослідження, систематизація та пропозиції щодо удосконалення напрямів міжнародного регулювання сфери інформаційно-комунікаційних технологій як фактору забезпечення національної та міжнародної безпеки.

Виклад основного матеріалу. На сучасному етапі розвитку інформаційно-комунікаційні технології приносять в усі сфери життєдіяльності та функціонування суспільства. суб'єктів господарювання і держави та роблять значний вплив на цивілізаційний розвиток і глобальні процеси у економіці, соціальній та культурній сфері, а також в сфері забезпечення національної безпеки країни. Тому, можна стверджувати, що інформаційно-комунікаційні технології складають основу швидкого розвитку інформаційного суспільства та глобального інформаційного простору як в цілому, так й окремих її сфер та аспектів.

Зараз основний провідник інформаційно-комунікаційних технологій – глобальна мережа Інтернет охоплює близько 4,5 мільярдів людей [3]. При цьому активно розвивається «Інтернет речей», який пов'язує не тільки звичайних користувачів, а й мережи, комп'ютерні пристрої, побутові прилади та інші об'єкти інформаційно-комунікаційної інфраструктури. Це спричиняє основну проблему розвитку та регулювання інформаційно-комунікаційних технологій, яку сформулював Бекстром Р. Представимо її у виді логічної схеми на рис. 1 [4].

Рис. 1. Логічна схема виникнення проблем розвитку та регулювання інформаційно-комунікаційних технологій

Джерело: систематизовано на основі [4]

Важливо відзначити, що науково та технологічно розвинені країни одночасно є й більш уразливими в глобальному інформаційному просторі. Також в умовах широкої мережевої інтеграції зростає взаємозв'язок і взаємозалежність інформаційних просторів різних країн світу, в тому числі й агресивно налаштованих або з недосконалим законодавством в сфері застосування інформаційно-комунікаційних технологій. З вищенаведеного виходить, що питання реагування на виклики та протидії ризикам, загрозам і небезпекам в інформаційно-комунікаційній сфері мають як національний, так й глобальний вимір.

Але, слід зауважити, що міжнародне співтовариство з питань раціонального застосування та безпечного користування інформаційно-комунікаційних технологій досі не прийшло до єдиного тлумачення та розуміння ключових термінів в цій області, а також величини та структури впливу цього процесу на національну безпеку окремих країн і глобального інформаційного простору. Досліджуючи наукові публікації та літературу іноземних вчених з цього питання можна виділити два основних підходи до визначення інформаційної безпеки – широкий і вузький [5].

В рамках широкого підходу поняття інформаційної безпеки включає в себе як інформаційно-технічні, так й інформаційно-психологічні аспекти. Цього підходу дотримуються країни-члени Шанхайської організації співробітництва, а також ряду інших держав, які визначають інформаційну безпеку як стан захищеності особистості, суспільства і держави та їх інтересів від загроз, деструктивних та інших негативних впливів в глобальному інформаційному просторі [6-7].

В іншого боку, США, Великобританія та країни Євросоюзу у своїй концепції розвитку дотримуються більш вузького підходу до визначення терміну «інформаційна безпека», який обмежується технологічними аспектами і по суті є захистом інформації, інформаційних систем і мереж від несанкціонованого доступу, використання, розкриття, пошкодження, внесення змін або знищення з метою забезпечення цілісності, конфіденційності та доступності [8]. Таким чином, питання інформаційної безпеки з точки зору цих країн не включають регулювання контенту і його управління. Натомість вони вважають пріоритетом забезпечення кібербезпеки, тобто безпеки глобального інформаційного простору в рамках системи, що охоплює взаємопов'язані мережі інформаційно-комунікаційної інфраструктури і розміщені в них дані, в тому числі Інтернет, телекомунікаційні мережі, автоматизовані системи управління тощо.

Виходячи з вищенаведеного, можна надати уточнене визначення категорії «глобальна інформаційна безпека», яке включала би в собі переваги двох підходів, – це комплексна система захисту інформаційного суспільства, держави та інших суб'єктів інформаційно-комунікаційних технологій, основною метою якої є оперативне реагування на сталі та нові виклики внутрішнього і зовнішнього середовища, зменшування ризиків, нівелювання

загроз і небезпеки що породжує глобальний інформаційний простір, а також безпека мережі інформаційно-комунікаційної інфраструктури і розміщених в них відкритих або конфіденційних даних (відомостей).

На сьогоднішній день, незважаючи на існуючу відмінність в підходах ключових країн щодо регулювання глобального інформаційного простору, намітилися позитивні зрушення в їх позиціях, що виражається у включеності в багатосторонній переговорний процес з широкого кола питань забезпечення міжнародної безпеки у сфері інформаційно-комунікаційних технологій. У ході дослідження проблематики цього питання, можна дійти висновку, що необхідна систематизація основних напрямів, які становлять спільний інтерес для світових країн у глобальному інформаційному просторі, що сприятиме поетапному просуванню до створення ефективних механізмів міжнародного регулювання у сфері застосування та користування інформаційно-комунікаційними технологіями (рис. 2).

Рис. 2. Основні напрями створення ефективних механізмів міжнародного регулювання

Джерело: систематизовано автором на основі [9-19]

Отже, можна зробити висновок, що зараз однією із найважливішою задачею, яка стоїть перед міжнародним співтовариством в сфері регулювання глобальної системи інформаційно-комунікаційних технологій, є розробка міжнародно-правових рамок для забезпечення заходів щодо впровадження та ефективного функціонування механізмів міжнародної інформаційної безпеки як основи для зміцнення національної безпеки країн у світовому інформаційному просторі (рис. 2). Для вирішення цієї проблеми у світовій практиці домінуючими є два підходи, сутність яких розкрито у табл. 1.

Таблиця 1

Підходи для забезпечення заходів щодо впровадження та ефективного функціонування механізмів міжнародної інформаційної безпеки

Американсько-європейський підхід	Комплексний підхід
Сутність підходу	
<p>Для забезпечення кібербезпеки на глобальному рівні не застосовується розробка і прийняття нових норм і принципів. Натомість базову основу режиму забезпечення кібербезпеки формують резолюції Генеральної Асамблеї ООН про боротьбу зі злочинним використанням інформаційно-комунікаційних технологій [9], резолюції Ради Безпеки ООН, положення яких спрямовані на протидію тероризму [10], а також положення Конвенції Ради Європи про кіберзлочинність [11]. У свою чергу, Статут ООН та прийняті принципи міжнародного права забезпечують необхідну базу для регулювання дій країн при використанні інформаційно-комунікаційних технологій у військово-політичних цілях тим самим зміцнюючи національну безпеку більш уразливих в цій сфері держав [12].</p>	<p>Доводить необхідність у розробці нової Конвенції ООН про забезпечення міжнародної інформаційної безпеки як головного механізму регулювання розвитку глобального інформаційного простору [13]. Ця конвенція повинна охоплювати увесь перелік викликів та загроз глобальної інформаційної безпеки, зокрема:</p> <ul style="list-style-type: none"> – дії в інформаційно-комунікаційному просторі з метою підризу політичних, соціально-економічних систем країни; – психологічна обробка населення, яка породжує дестабілізацію інформаційного суспільства; – маніпулювання інформаційними потоками в інформаційному просторі інших держав тощо.
Практична спрямованість підходу	
<p>Отже, в американському підході особливу увагу приділяється розробці глобальних механізмів забезпечення кібербезпеки на усіх рівнях використання інформаційно-комунікаційних технологій.</p>	<p>Таким чином основним практичним завданням Конвенції про забезпечення міжнародної інформаційної безпеки повинно стати вирішення широкого спектру питань щодо забезпечення інформаційної безпеки, який не буде обмежуватися лише аспектами кібербезпеки.</p>

Джерело: систематизовано автором на основі [9-13]

Також треб зробити особливий наголос на тому, що характерні особливості інформаційно-комунікаційних технологій породжують цілу низку питань щодо можливості застосування розроблених в «доінформаційну (доцифрову)» епоху міжнародних стандартів, підходів, принципів й норм стосовно глобального інформаційного простору. З цим твердженням погоджуються й відомі західні дослідники в сфері міжнародного права Шмідт М. та Голдсміт Дж., які відзначають, що загальні положення Статуту ООН в цілому орієнтовані на обмеження використання країнами військової сили і здебільшого не враховують такі неприпустимі методи ведення державного протиборства в глобальному інформаційному просторі, як кібершпionaж або неправомірне використання продуктів інтелектуальної власності, що може бути причиною завдання більш значних матеріальних, соціально-культурних, «безпекових» та інших збитків країнам навіть порівняно з традиційними військовими атаками [14-15]. Тобто, можна зробити висновок про необхідність розробки спеціальних норм для кіберпростору з метою ліквідації можливих правових невідповідностей між законодавством різних країн, а також стратегічними напрямками їх національної безпеки.

Наступним важливим елементом у системі міжнародного регулювання сфері інформаційно-комунікаційних технологій є розробка ефективних заходів щодо зміцнення довіри в глобальному інформаційному просторі (рис. 2). На практиці це можливо здійснити тільки шляхом впровадження моделей двостороннього (між державами-лідерами в інформаційно-комунікаційній сфері) та багатостороннього співробітництва (між розвиненими державами та країнами, які розвиваються) з метою протидії ризикам, загрозам і небезпекам в глобальному інформаційному просторі. В цьому ж аспекті є також важливим продовження розпочатої в рамках Організації з безпеки і співробітництва в Європі роботи над переліком заходів щодо забезпечення безпеки в інформаційному полі [16].

Третім напрямом створення ефективних механізмів міжнародного регулювання є комплексна розробка та впровадження правил відповідальної поведінки для усіх суб'єктів сфери інформаційно-комунікаційних технологій (рис. 2). Такий напрям пояснюється тим, що на сьогоднішній день всі основні країни-лідери у глобальному інформаційному просторі визнали потребу в правилах відповідальної поведінки в інформаційній сфері для забезпечення власної національної та світової інформаційної безпеки у довгостроковому періоді. Тому, прийняття та удосконалення даної концепції залежить просування світових держав у напрямі розробки загальноприйнятих визначень і підходів до розуміння безпеки в сфері інформаційно-комунікаційних технологій.

Забезпечення безпеки критичної інфраструктури є одним з основних завдань національної безпеки усіх без винятку світових країн (рис. 2). Тому співробітництво в цієї області можна віднести до сфери спільних інтересів, а отже, на глобальному рівні постійно вводяться обмеження на проведення

хакерських та інших кібератак проти об'єктів критичної, а особливо цивільної інфраструктури. Тому набуває доцільності складення офіційного списку таких «недоторканих об'єктів» з обов'язковим закладанням списку цих об'єктів в правила поведінки держав та в угоди між ними.

Ще одним важливим напрямом регулювання справедливо вважається розробка, впровадження та вдосконалення механізмів використання кіберзброї розвинутими в цій сфері державами (рис. 2). Це зумовлено тим, що його використання з метою здійснення ворожих дій, актів агресії або створення загроз міжнародному миру і безпеці викликає деструктивні наслідки та може призвести до порушення рівноваги у безпеці в сфері інформаційно-комунікаційних технологій. Треба зазначити, що вищенаведена ідея про формування режимів обмеження використання кіберзброї та ведення явних або скритих кібервійн, знаходить підтримку у політиків і експертів країн-лідерів у цій сфері [17-18]. Такий стан справ можна вважати позитивним сигналом і в стратегічній перспективі дана проблема може бути вирішена шляхом як двосторонніх, так і багатосторонніх переговорів з питань міжнародної інформаційної безпеки між основними країнами (США, Євросоюз, Китай, Росія Японія тощо).

Шостим напрямом міжнародного регулювання сфери інформаційно-комунікаційних технологій є усестороння взаємодія з ідентифікації джерел деструктивних дій в інформаційно-комунікаційній мережі (рис. 2). Його важливість обумовлено складністю встановлення джерела інформаційної атаки і мотивів його здійснення. Практичним впровадженням цього напрямку може бути представлено як самостійні домовленості, так й бути складовою частиною документа з глобальної інформаційної безпеки.

На національному рівні провідні країни світу ведуть активні роботи у цьому напрямку, які виражається у впровадженні механізмів ідентифікації в інформаційно-комунікаційній мережі в сферах здійснення комерційних, фінансових та інших операцій, де присутній значний ризик втрати даних (відомостей) внаслідок крадіжок або «зливу», а також є вірогідність заподіяння протиправних дій щодо звичайних користувачів. Але, в останні роки спостерігається стала тенденція до зростання глобальної кіберзлочинності, що обумовлює доцільність введенню системи ідентифікації користувачів й на міжнародному рівні. Така ініціатива буде відповідати національним інтересам усіх світових держав та сприятиме зміцненню безпеки в інформаційно-комунікаційній мережі, а також в значній мірі допоможе у роботі міжнародних служб з інформаційної безпеки.

Останнім, але не менш важливим напрямом міжнародного регулювання є вироблення та постійний моніторинг домовленостей щодо чітких правил і меж ведення діяльності зі збору інформації в кіберпросторі, а також здійснення доступу до даних в інформаційно-комунікаційних мережах (рис. 2). Провідні країни світу сьогодні визнають необхідність щодо проведення швидкого та

ефективного розслідування злочинів у кіберпросторі, при цьому визначаючи форми покарання за протиправні дії у вигляді ефективних механізмів міжнародного співробітництва, чого можна досягнути тільки шляхом гармонізації національних законодавств та стратегій національної безпеки. Але зараз країнам ще не в повній мірі вдається подолати розбіжності у розумінні та вирішенні цієї проблеми. В той час слід зазначити, що у поточному вигляді Будапештська конвенція вже не відповідає всім наявним та потенційним викликам, які породжує кіберзлочинність [19; 20]. Тому основною пропозицією щодо вирішення означеної проблеми має стати внесення відповідних змін до цієї Конвенції, які би враховували інтереси усіх без винятку зацікавлених в мирному використанні кіберпростору країн шляхом розробки комплексного, науково-обґрунтованого документу про протидію кіберзлочинності.

Таким чином, проведені дослідження показали, що існує значна кількість різноспрямованих напрямків міжнародного співробітництва у регулювання сфери інформаційно-комунікаційних відносин, які вже функціонують в останні роки або проходять процес постійного удосконалення. Отже, можна зробити висновок, що подальша робота з питань забезпечення глобальної інформаційної безпеки буде спиратися на політичну волю сторін та їх готовності до конструктивного діалогу. Тому проведення змістовних теоретико-методичні та практичні дослідження в рамках кожного напрямку регулювання у сфері інформаційно-комунікаційних відносин, що становлять спільний інтерес світових країни, буде сприяти підвищенню рівня довіри між країнами і подальшому просуванню до універсальних домовленостей в області безпечного та правомірного використання глобального інформаційного простору.

Висновки. Проведені у статі змістовні теоретико-методичні та практичні дослідження щодо проблеми міжнародного регулювання сфери інформаційно-комунікаційних технологій та їх взаємозв'язок з формування і зміцненням національної та міжнародної безпеки дозволили зробити наступні висновки та припущення:

- уточнено визначення категорії «глобальна інформаційна безпека», зокрема – це комплексна система захисту інформаційного суспільства, держави та інших суб'єктів інформаційно-комунікаційних технологій, основною метою якої є оперативне реагування на сталі та нові виклики внутрішнього і зовнішнього середовища, зменшування ризиків, нівелювання загроз і небезпеки що породжує глобальний інформаційний простір, а також безпека мережі інформаційно-комунікаційної інфраструктури і розміщених в них відкритих або конфіденційних даних (відомостей);

- систематизовані основні напрями створення ефективних механізмів міжнародного регулювання, надані їх теоретичні обґрунтування та можливі варіанти удосконалення;

- зроблено висновок, що подальша робота з питань забезпечення

глобальної інформаційної безпеки буде спиратися на політичну волю країн-лідерів у сфері інформаційно-комунікаційних технологій та їх готовності до конструктивного діалогу.

Література:

1. Геворкян А.Ю. Удосконалення напрямів державного управління та регулювання у сфері інформаційної політики для зміцнення економічної безпеки території. Publishing House “Baltija Publishing”, 2021. С. 97-101.
2. Доронін І.М. Національна безпека України в інформаційну епоху: правові аспекти: моногр. Київ: ТОВ Видавничий дім «АртЕк», 2019. 434 с.
3. Internet World Stats. Usage and Population. – URL: <http://www.internetworldstats.com/top20.htm> (дата звернення: 10.10.2021).
4. Beckstrom, R. Speech at the London Conference on Cyberspace. 2011. URL: <https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf> (дата звернення: 10.10.2021).
5. Brennen S., Susan W. Cyberthreats and The Decline of The Nation-state. Abingdon, Oxon: Routledge, 2014. 175 p.
6. Mueller M. Networks and States: The Global Politics of Internet Governance. Cambridge, Mass: MIT Press, 2010. 313 p.
7. Аванесова Н.Е., Мордовцев О. С., Сергієнко Ю. І. Теоретико-методичні засади ідентифікації та взаємозв'язку впливу дестабілізуючих факторів на економічну безпеку промислового підприємства. Бізнес Інформ. 2020. №9. С. 20–28. URL: <https://doi.org/10.32983/2222-4459-2020-9-20-28> (дата звернення 05.01.2021).
8. DOD Dictionary of Military and Associated Terms, 2021. 366 p., URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-05-02-174746-340> (дата звернення: 10.10.2021).
9. General Assembly of the United Nations. URL: <https://www.un.org/en/ga/> (дата звернення: 10.10.2021).
10. UN Security Council. URL: <https://www.un.org/en/> (дата звернення: 10.10.2021).
11. Convention on Cybercrime. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (дата звернення: 10.10.2021).
12. United Nations Charter. URL: <https://www.un.org/en/about-us/un-charter/full-text> (дата звернення: 10.10.2021).
13. United Nations. URL: <https://www.un.org/en/> (дата звернення: 10.10.2021).
14. Schmitt M. Cyberspace and International Law: The Penumbra Mist of Uncertainty. Harvard Law Review. – URL: <https://harvardlawreview.org/2013/04/cyberspace-and-international-law-the-penumbra-mist-of-uncertainty/> (дата звернення: 10.10.2021).
15. Goldsmith J. How Cyber Changes the Laws of War. The European Journal of International Law. 2013. Vol. 24(1). pp. 133-138.
16. Organization for Security and Co-operation in Europe. URL: <https://www.osce.org/> (дата звернення: 10.10.2021).
17. Singer P.W. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford, Oxford University Press, 2014. URL: http://book.itep.ru/depositary/cyberwar/P.W.Singer_Allan_Friedman_Cybersecurity_and_Cyberwar_What_Everyone_Needs_to_Know_2014_Oxford_University_Press.pdf (дата звернення: 10.10.2021).
18. Koh H. Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace. URL: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers (дата звернення: 10.10.2021).

19. Convention on cybercrime. Budapest, 23.XI.2001. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (дата звернення: 10.10.2021).

20. Кухарєва О.О. Тенденції зовнішньоекономічної безпеки України // Бізнес-навігатор. – Випуск 3 (64) (2021). – С. 75-79.

References:

1. Gevorkyan A. (2021) Udoskonalennia napriamiv derzhavnoho upravlinnia ta rehuliuвання u sferi informatsiinoi polityky dlia zmitsnennia ekonomichnoi bezpeky terytorii [Improving the directions of Public Administration and regulation in the field of information policy to strengthen the economic security of the territory]. *Publishing House "Baltija Publishing"*, 97-101 [in Ukrainian].
2. Doronin I.M. (2019). *Natsionalna bezpeka Ukrainy v informatsiinu epokhu: pravovi aspekty* [National security of Ukraine in the Information Age: legal aspects]. Kiev, TOV Vydavnychiy dim «ArtEk», 2019. 434 [in Ukrainian].
3. *Internet World Stats. Usage and Population*. – URL: <http://www.internetworldstats.com/top20.htm> (available: 10.10.2021) [in English].
4. Beckstrom, R. *Speech at the London Conference on Cyberspace*. 2011. URL: <https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf> (available: 10.10.2021) [in English].
5. Brennen S., Susan W. *Cyberthreats and The Decline of The Nation-state*. Abingdon, Oxon: Routledge, 2014. 175 p [in English].
6. Mueller M. *Networks and States: The Global Politics of Internet Governance*. Cambridge, Mass: MIT Press, 2010. 313 p [in English].
7. Avanesova N., Mordovtsev O., Sergienko Yu. (2020) Teoretyko-metodychni zasady identyfikatsii ta vzaïmozv'язku vplyvu destabilizuiuchykh faktoriv na ekonomichnu bezpeku promyslovoho pidpriemstva. [Theoretical and methodological foundations of identification and interrelation of the influence of destabilizing factors on the economic security of an industrial enterprise]. *Biznes Inform [Business Inform]*. 9. 20–28. URL: <https://doi.org/10.32983/2222-4459-2020-9-20-28> (available 05.01.2021) [in Ukrainian].
8. *DOD Dictionary of Military and Associated Terms*, 2021. 366 p., URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-05-02-174746-340> (available: 10.10.2021) [in English].
9. *General Assembly of the United Nations*. URL: <https://www.un.org/en/ga/> (available: 10.10.2021) [in English].
10. *UN Security Council*. URL: <https://www.un.org/en/> (available: 10.10.2021) [in English].
11. *Convention on Cybercrime*. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (available: 10.10.2021) [in English].
12. *United Nations Charter*. URL: <https://www.un.org/en/about-us/un-charter/full-text> (available: 10.10.2021) [in English].
13. *United Nations*. URL: <https://www.un.org/en/> (available: 10.10.2021).
14. Schmitt M. Cyberspace and International Law: The Penumbra Mist of Uncertainty. *Harvard Law Review*. – URL: <https://harvardlawreview.org/2013/04/cyberspace-and-international-law-the-penumbral-mist-of-uncertainty/> (available: 10.10.2021) [in English].
15. Goldsmith J. How Cyber Changes the Laws of War. *The European Journal of International Law*. 2013. Vol. 24(1). pp. 133-138 [in English].
16. *Organization for Security and Co-operation in Europe*. URL: <https://www.osce.org/> (available: 10.10.2021) [in English].
17. Singer P.W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford/

Oxford University Press, 2014. URL: http://book.itep.ru/depositary/cyberwar/P.W.Singer_Allan_Friedman_Cybersecurity_and_Cyberwar_What_Everyone_Needs_to_Know_2014_Oxford_University_Press.pdf (available: 10.10.2021) [in English].

18. Koh H. *Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace*. URL: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers (available: 10.10.2021) [in English].

19. *Convention on cybercrime. Budapest, 23.XI.2001*. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (available: 10.10.2021) [in English].

20. Kuhareva, O.O. (2021). Tendencii zovnishn'oekonomichnoï bezpeki Ukraïni [Trends in foreign economic security of Ukraine]. *Biznes-navigator – Business Navigator*, 3 (64) (2021), 75-79 [in Ukrainian].