ми на 20 апреля 2016 г.) : совершено в г. Лаппеенранта 27 мая 2010 г. [Электронный ресурс]. – Режим доступа : http://docs.cntd.ru/document/902298924.

53. Terms of Lease in perpetuity of Tin Bigha Area : Signed at New Delhi on the 7-th of October 1982 [Електронний ресурс]. – Режим д оступу : http://www.clcbd.org/document/download/224.html.

54. Мирный договор с Финляндией : подписан в г. Париже 10 февраля 1947 г. // Внешняя политика Советского Союза 1947 г. – В 2-х кн. – Ч. І. : Док. и матер. Январь – июнь 1947 г. – Москва : Госуд. изд-во полит. лит., 1952. – С. 327–360.

55. Соглашение между Союзом Советских Социалистических Республик и Финляндской Республикой об отказе Советского Союза от прав на использование территории Порккала-Удд для военно-морской базы и выводе советских вооруженных сил с этой территории : совершено в г. Москве 19 сентября 1955 г. // Ведомости Верховного Совета СССР. – 1955. – № 20. – С. 548–550.

56. NATO Treaty : Signed in Washington DC, 4th April 1949 [Електронний ресурс]. – Режим доступу : http://avalon.law.yale.edu/20th_century/nato.asp.

УДК 341:004

МІЖНАРОДНО-ПРАВОВІ ПРОБЛЕМИ МІЛІТАРИЗАЦІЇ КІБЕРПРОСТОРУ

INTERNATIONAL LEGAL PROBLEMS OF CYBERSPACE MILITARIZATION

Федченко Д.І.,
студентка ІІІ курсу
Інститут прокуратури та кримінальної юстиції
Національного юридичного університету імені Ярослава Мудрого

Статтю присвячено дослідженню сутності актуального явища міжнародного права – кіберпростору. У статті проаналізовано наукові підходи до визначення цього поняття, встановлено його характерні ознаки. З огляду на стрімкий розвиток кіберпростору і похідних від нього явищ, надано характеристику кібервійни та кібербезпеки, досліджено проблеми, які виникають у зв'язку із практичним використанням цих понять, і запропоновано спосіб їх вирішення.

Ключові слова: кіберпростір, кібервійна, кібербезпека, кібератака, кіберзлочинність, інформатизація суспільства, інформаційна війна.

В статье исследуется суть актуального явления международного права – киберпространства. В статье проанализированы научные подходы к определению этого понятия, установлены его характерные качества. С учётом стремительного развития киберпространства и производных от него явлений предоставляется характеристика кибервойны и кибербезопасности, исследованы проблемы, возникающие в связи с практическим использованием этих понятий, и предложен способ их решения.

Ключевые слова: киберпространство, кибервойна, кибербезопасность, кибератака, киберпреступность, информатизация общества, информационная война.

The article is devoted to the study of the essence of the actual phenomenon of international law – cyberspace. The article examines the views of different scholars on the definition of this concept, as well as on its characteristic features. Given the rapid development of cyberspace and the phenomena derived from it, the characteristics of cyber warfare and cyber security were given, the problems that arise in connection with the practical use of these concepts were explored and a way of solving them was proposed.

In contemporary legal science, considerable attention is devoted to the study of cyberspace, but, unfortunately, there is no single approach to the definition of this concept. Therefore, there is a need for its consolidation in national legislation and international law. A phenomenon like cyberwar may have negative consequences for society and the state, so it is necessary to regulate it by a single normative act and create bodies that will function to provide cybersecurity.

The article explores the difference between the concepts of "cyberwar" and "information warfare". The article gives examples of cyberattacks to different countries of the world and follows the mechanism and the purpose of the activities of persons who carry out cyberattacks. The author compares the cyberwar and armed war, highlighting their common features and differences.

The article analyzes the need to stop the militarization of cyberspace, since its use for improper purposes may cause human casualties and compromise the existence of a state that is less developed in the field of information technology.

The article analyzes the influence of cyberspace on Ukraine.

Key words: cyberspace, cyberwar, cyberattack, information war, cybersecurity, cybercrime.

На сучасному етапі розвитку суспільства відбувається масове впровадження інформаційних технологій і їх здобутків у життєдіяльність всіх суб'єктів. Більшість людей, а отже, і держав, вже не можуть існувати та функціонувати без приєднання до мережі Інтернет. Спостерігається тенденція створення надзвичайно розгалуженої мережі під'єднаних до Інтернету речей, що можуть функціонувати самостійно (так званий "Internet of Things") [1, с. 199]. Як наслідок, поряд із загальновизнаними земним, повітряним, морським і космічним просторами виникає ще один, який потребує негайного правового врегулювання і на міжнародному, і на національних рівнях – кіберпростір. Відкритий кіберпростір розширює свободу та можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади й активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність і прозорість влади, сприяє запобіганню корупції. Водночас переваги сучасного кіберпростору обумовили виникнення нових загроз національній і міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп і осіб [2, с. 63]. Оскільки кіберпростір немає жодних меж, виникає нагальна потреба узгодити співробітництво, спрямоване на боротьбу з кіберзлочинністю на міжнародному рівні, адже повне нормативне регулювання даної сфери відсутнє, що призводить до низки проблем і суперечностей. Саме в цьому вбачається актуальність даної теми.

Кіберпростір і загрози, пов'язані з його виникненням, вже довгий час досліджують і міжнародні науковці, як-от: М. Шмітт, В. Хайнтшель фон Хайнег, В. Бутбі, Т. Вінгфілд, Б. Демейре, П. Маргуліс, Дж. Карр, М. Лібіцкі, Х. Лін, М. Магомедов, Т. Рід, Е. Філіол, Г. Шинкарецька й інші, і вітчизняні вчені, серед яких: Д. Дубов, А. Войцехів-

ський, О. Мережко, Ю. Разметаєва, В. Бурячок, О. Грицун, І. Забара, Є. Скулиш, М. Камчатний. Однак, зважаючи на різноманітність наукових поглядів на досліджуване явище, досі не розроблено єдиного підходу до термінологічного визначення поняття «кіберпростір» і похідних від нього («кібербезпека», «кібервійна» тощо), виокремлення характерних рис, з'ясування сутності цих явищ, обґрунтування засобів боротьби із загрозами, які виникають. Провідні фахівці сходяться лише у визнанні необхідності ухвалення єдиного універсального акта, який би врегулював відносини між державами в цій сфері.

Тому **метою статті** є формування узагальненого визначення понять «кіберпростір» і «кібербезпека», наведення характеристики загроз, які виникають у даній сфері, та проблем, пов'язаних із запобіганням таким загрозам, формулювання можливих шляхів їх вирішення на міжнародному рівні.

Кожного року держави створюють нові спеціалізовані органи й ухвалюють акти національного законодавства, які покликані гарантувати кібербезпеку, нормальне функціонування всіх систем, приєднаних до мережі Інтернет, регулювати власну діяльність у кіберпросторі, захищати своє інформаційне середовище. Це свідчить про визнання державами реальної наявності небезпеки від неправомірних діянь у кіберпросторі.

Підтвердженням мілітаризації кіберпростору, що зростає, є дослідження, проведене Джеймсом А. Льюїсом і Катріною Тімлін у межах Інституту Організації Об'єднаних Націй (далі – ООН) з питань роззброєння (далі – ЮНІДІР) щодо оцінки національних доктрин держав у сфері кібербезпеки та кібервійни. У дослідженні держави розподілено на дві категорії: держави, що відносять питання інформаційної безпеки до військової доктрини, та держави, що стоять на позиції розгляду питань інформаційної безпеки з погляду цивільного підходу. Варто звернути увагу на те, що вищезазначене дослідження проводилось двічі – у 2011 та 2012 рр. Відповідно до дослідження 2011 р., 68 із 193 держав-членів ООН мають національні доктрини інформаційної безпеки. Серед них 32 держави включили поняття кібервійни до своїх національних стратегій, а питання інформаційної безпеки віднесено до компетенції воєнних відомств, тоді як у 36 державах питання інформаційної безпеки віднесено до відання цивільних відомств і організацій. Проте дослідження, проведене 2012 р., засвідчило надзвичайно швидке зростання національних доктрин інформаційної безпеки серед держав-членів ООН. Так, станом на 2012 р. їх кількість зросла до 114, серед яких 47 доктрин відносять питання інформаційної безпеки до військового аспекту, а 67 мають виключно цивільні програми. На особливу увагу заслуговує той факт, що відповідно до проведеного дослідження кількість держав, які створили чи планують створити спеціальні військові формування з питань кібербезпеки, зросла за рік із 12 до 27 [3, с. 113]. Це свідчить про зростання впливу кіберпростору і кіберзагроз на внутрішню та зовнішню політику держав.

Спроби нормативного регулювання кіберпростору розпочалися з 1998 р. Кожного року Генеральна Асамблея готує резолюції «Досягнення в сфері інформатизації і телекомунікацій у контексті міжнародної безпеки». Ці документи сприяють підвищенню уваги держав до необхідності врегулювання відносин між ними в кіберпросторі. Окрему увагу питанням кібербезпеки приділяє й ООН. У липні 2000 р. в Японії президенти восьми провідних країн світу підписали Хартію глобального інформаційного суспільства (також відому як Окінавська хартія – *Д. Ф.*) з метою розвитку світової економіки та переходу до нового етапу розвитку суспільства. У Хартії підкреслюється: «Інформаційно-комунікаційні технології є одними з найбільш важливих чинників, що впливають на формування суспільства двадцять першого століття. Їх революційна дія стосується способу життя людей, їхньої освіти і роботи, а також взаємодії уряду і самого суспільства» [4, с. 794]. 20 грудня 2002 р. резолюцією 57/239 Генеральної Асамблеї були ухвалені «Елементи для створення глобальної культури кібербезпеки». Як зазначається в документі, «глобальна культура кібербезпеки буде вимагати від усіх учасників врахування 9 основних взаємодоповнюючих елементів: обізнаність, відповідальність, реагування, етика, демократія, оцінка ризику, проектування та впровадження засобів забезпечення безпеки, управління забезпеченням безпеки, переоцінка». Також у 2012 р. Всесвітньою асамблеєю зі стандартизації електрозв'язку Міжнародного союзу електрозв'язку була ухвалена Резолюція 50 «Кібербезпека», якою, серед іншого, було підкреслено, що всім зацікавленим сторонам необхідно разом працювати над розробленням стандартів і принципів для захисту від кібератак і полегшення виявлення джерел атак. Крім того, варто сприяти глобальним узгодженим і сумісним процесам обміну інформацією, що стосується реагування на інциденти. Також у 2012 р. ООН було підготовлено Доповідь групи урядових експертів із досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки. Група серед іншого погодилася, що заходи по зміцненню довіри, як-от контакти на високому рівні і своєчасний обмін інформацією, можуть підвищити довіру і впевненість серед усіх країн і сприяти зниженню ризику виникнення конфлікту завдяки підвищенню передбачуваності й усуненню хибних уявлень. Важливим є те, що за результатами Доповіді було підтверджено, що на кіберпростір поширюється дія міжнародного права, зокрема й Статуту ООН [5, с. 321].

Серед органів, які здійснюють регулювання кіберпростору, варто зазначити такі: в Європейському Союзі (далі – ЄС) функціонує Агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), у Сполучених Штатах Америки (далі – США) кібербезпекою займається Агентство національної безпеки, у НАТО створений Комітет із кібернетичної оборони (The Cyber Defence Committee), а також Спільний центр із кібернетичної оборони (Cooperative Cyber Defence Centre of Excellence), Спеціалізований центр з оборони у сфері кібербезпеки НАТО (CCDCOE), Міжнародний альянс із забезпечення кібербезпеки (ICSPA), Інтерпол (INTERPOL), Міжнародне багатостороннє товариство проти кіберзагроз (IMPACT) та ін. Саме вони мають здійснювати регулювання діяльності у кіберпросторі.

Держави та міжнародні установи вживають термін «кіберпростір», але офіційного нормативного його тлумачення не надано. У науковій розробці існує безліч підходів до його визначення.

Якщо розглядати кіберпростір як словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений і працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі й обробки інформації) [6, с. 216].

З філософського погляду, кіберпростір – це сфера віртуального буття людини, де діють інші закони, інші звичаї, де людина перетворюється на громадянина іншої держави, стає «кібернавтом» [7, 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.

Деякі держави все ж пропонують власне визначення згаданого поняття. Наприклад, у США кіберпростір – це сфера, яка характеризується можливістю використання електронних й електромагнітних засобів для запам'ятовування, модифікування й обміну даними в мережевих системах і пов'язаній із ними фізичній інфра-

структурі; у Великобританії кіберпростіром називають всі форми мережевої цифрової активності, що містять контент і дії, здійснювані через цифрові мережі; у Німеччині кіберпростір – це вся інформаційна інфраструктура, яка доступна через Інтернет поза будь-якими територіальними кордонами. За офіційними документами Євросоюзу, кіберпростір – це віртуальний простір, в якому циркулюють електронні дані світових персональних комп'ютерів [2, с. 62].

В Україні взагалі відсутнє єдине поняття кіберпростору. С. Гнатюк у результаті багатокритеріального аналізу запропонував таке узагальнене визначення: кіберпростір – це віртуальний простір, що отриманий у результаті взаємодії користувачів, програмного й апаратного забезпечення, мережевих технологій (зокрема й Інтернету) для підтримки й управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства [8, с. 119].

Підсумовуючи вищезазначене, доцільно запропонувати ще одне узагальнене визначення: кіберпростір – це категорія міжнародного права, яка визначає специфічну сферу, що не обмежена жодними кордонами та використовується державами, іншими суб'єктами для досягнення відповідних цілей або настання певних наслідків, шляхом застосування кібернетичних можливостей, новітніх інформаційних технологій.

Виникнення мережі Інтернет і подальше формування кіберпростору було спрямоване виключно на досягнення мирних цілей і задоволення мирних потреб, але існування позитивного явища закономірно спричиняє наявність негативного. Кіберпростір характеризується масштабністю, і як позитивні наслідки його існування, так і негативні, можуть сягати від загрози порушення права на приватність однієї особи до порушення права на життя, діяльності інфраструктури, існування держави загалом.

Розвиток і вдосконалення інформаційних технологій розширює можливості кіберзлочинів, зокрема і для здійснення фізичних вбивств, бо у сфері охорони здоров'я, де багато пристроїв мають вихід у мережу, злочинці можуть безконтактно здійснювати вбивства, наприклад, відключивши кардіостимулятор або апарат штучної вентиляції легенів, змінивши призначену дозу ліків. Безумовно, у майбутньому зросте небезпека шахрайств, пов'язаних із кредитними картами, можливими атаками на енергосистеми, що забезпечують електроенергією військові об'єкти, систему управління безпілотними літальними апаратами тощо.

Серед перших прикладів запровадження кібертехнологій для впливу на іншу державу можна назвати використання 1982 р. так званої логічної бомби. Існує версія, що тоді був використаний троянський вірус, прихований у програмному забезпеченні, яке радянські шпигуни викрали в Канаді з метою забезпечення функціонування Транссибірського газопроводу. На той момент спеціалісти Союзу Радянських Соціалістичних Республік не мали власного програмного забезпечення для управління системами газопроводу і не могли розпізнати прихований у викраденій програмі змінений код. Відомо, що ця програма була створена і використана під час холодної війни спеціальними службами США. Під час випробувань тиску на певних ділянках газопроводу троянська програма була запущена і цим вплинула на максимальне збільшення тиску в системі, що не було відображено на спеціальних приладах із контролю покажчиків. У результаті, у 1982 р. це призвело до надзвичайно потужного вибуху газу [1, с. 200].

Наступним прикладом використання кіберпростору з неправомірною метою є кібератака, безпосередньо спрямована проти національної безпеки Естонії 2007 р. Передумовою такого втручання вважається рішення уряду Естонії про переміщення пам'ятника радянським воїнам часів Другої світової війни із центру Таллінна на його околиці. Це рішення спровокувало хвилю атак на численні інтернет-сайти Естонії. У результаті втручання хакерів протягом декількох тижнів були неспроможні функціонувати в нормальному режимі урядові, банківські сайти й інформаційні системи, сайти багатьох засобів масової інформації, громадських організацій. Хакерам вдалося навіть ненадовго вимкнути сервіс невідкладної допомоги, який функціонував завдяки мережі Інтернет. Відновлення повноцінного функціонування інформаційної інфраструктури потребувало певного часу та значних фінансових витрат.

Наступного року подібна ситуація сталася в Грузії. Спочатку було атаковано офіційний сайт президента Грузії, а 8 серпня, одночасно з розгортанням військового протистояння між Росією та Грузією, були атаковані інші офіційні сайти влади країни. Втручань зазнали також сайти фінансових установ, засобів масової інформації, навчальних закладів на території Грузії, а також сайти посольств США і Великої Британії. Це був один із перших випадків, коли наземна збройна операція супроводжувалася кібероперацією. Водночас варто зазначити, що порушення роботи згаданих сайтів не було метою хакерів, маючи можливість атакувати системи SCADA, вони цього не зробили, тому ціллю використання інформаційних технологій був саме вплив на державу для того, щоб примусити її вчинити відповідні дії, а не руйнування важливих сфер її діяльності.

Наслідки використання кіберпростору в неправомірних цілях можуть бути настільки масштабними і руйнівними, що науковці починають говорити про існування такої загрози, як кібервійна. Зараз існує багато поглядів щодо сутності поняття «кібервійна». Наприклад, М. Шмітт вже 2002 р. запропонував своє визначення інформаційної війни (кібервійни) як виду інформаційних операцій, тобто заходів, спрямованих на здійснення впливу на інформацію й інформаційні системи супротивника з метою захисту власної інформації та інформаційних систем. До таких операцій він відносить будь-які заходи, спрямовані на виявлення, зміну, знищення чи передачу даних, що зберігаються в комп'ютері, підлягають комп'ютерному обробленню чи пересиланню за допомогою комп'ютера. Вони можуть відбутися в мирний час, під час кризи або на стратегічному, оперативному й тактичному рівнях збройного конфлікту. Також до таких операцій можна віднести психологічні операції, воєнні хитрощі, електронну війну та фізичний напад на комп'ютерні мережі. У вужчому розумінні інформаційна війна, на його думку, складається з «інформаційних операцій, що проводяться під час виникнення кризи чи конфлікту з метою досягнення чи сприяння досягненню конкретних цілей щодо конкретного супротивника» [9, с. 16].

Б. Рабоін визначає кібервійну як деструктивний вплив у межах кіберпростору на реальний світ. О. Мережко до характерних рис додає здатність кібервійни загрожувати суверенітету. Д. Дубов зазначає, що кібервійна буде вважатися такою виключно якщо буде завдано певної сукупності кібератак. Дж. Карр стверджує, що кібервійна не повинна спричиняти реальних фізичних наслідків, тобто це «боротьба без крові». Е. Філіол вважає, що для кібервійни обов'язковою є наявність комп'ютера, а науковці Міжнародного інституту Лоуі зазначають важливість не пристрою, а зв'язку з мережею Інтернет.

Підсумовуючи вищенаведене, варто зазначити, що кібервійна – це специфічний вид боротьби між відповідними суб'єктами в кіберпросторі з використанням новітніх інформаційних технологій, що втілюються в цифрових засобах і пристроях, приєднаних до мережі Інтернет, що здатна спричинити істотні наслідки для життєдіяльності людини та функціонування й існування держави.

За практичного використання поняття «кібервійна» виникає низка проблем. Передусім, чи можна застосову-

вати норми міжнародного законодавства, що стосуються ведення збройних війн до кібервійни? У Резолюції 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 р. зазначено: «Агресією є застосування збройних сил державою проти суверенітету, територіальної недоторканності чи політичної незалежності іншої держави, або в будь-який інший спосіб, несумісний зі Статутом Організації Об'єднаних Націй, як це встановлено в цьому визначенні» (ст. 1). У Резолюції також подано список дій, що в будь-якому разі будуть кваліфіковані як «акти війни» (ст. 3), і майже всі вони передбачають фізичний контакт двох держав, найчастіше – із застосуванням кінетичної зброї.

Логічно виникає таке питання: чи можна вважати кіберзброю зброєю у звичайному розумінні (як пристрій, що виготовлений для завдання шкоди)? Міжнародний суд ООН під час розгляду питання законності погрози та використання ядерної зброї у своєму консультативному висновку зазначив, що заборона поширюється на застосування сили, незалежно від того, яка зброя застосовувалась. Враховуючи такий підхід Міжнародного суду ООН, операції в кіберпросторі потраплятимуть під заборону ст. 2 (4) Статуту ООН, якщо їх застосування призведе до наслідків, які можна прирівняти до наслідків від застосування кінетичної, хімічної, біологічної чи ядерної зброї. Беззаперечно, до таких операцій відносяться ті їх види, що спрямовані на нанесення травм, призводять до втрати життя чи руйнування об'єктіві нфраструктури, незалежно від того, чи завдають вони фізичного руйнування, функціональної шкоди, чи поєднують обидва випадки [4, с. 116].

Щодо інформаційної зброї, то, на думку Д. Брауна, йдеться про певний комплекс інструментів, які не просто співіснують, але з певною метою поєднані: «Отже, кажучи про ідентифікацію інформаційної зброї, маємо на увазі три компоненти: код, комп'ютерну систему й оператора. Кожен із цих компонентів має підпадати під міжнародне законодавство, яке регулює збройні конфлікти. Відповідно, застосування цієї зброї має стримуватися принципами воєнної необхідності, пропорційності, гуманності, лицарства, а цілі для неї мають бути легітимними» [10, с. 151].

Серед інших проблем врегулювання кібервійн також визначають високий рівень латентності, неможливість встановити територію-нападника, а отже, особу, суб'єктів кібервійни, адже для збройної війни – це солдати або комбатанти, а для кібервійни цей аспект залишається дискусійним, неможливість передбачити кібернапад у майбутньому, різниця в шкоді, яка завдається, оцінка важливості кібератак для визначення відповідальності, переростання кібервійни в реальний збройний конфлікт, який призведе до більш масштабних наслідків. Усі вони потребують негайного вирішення та нормативного врегулювання.

Також варто розмежовувати поняття «кібервійна» й «інформаційна війна». Інформаційна війна охоплює більше сфер і засобів її ведення, має більш різноманітні наслідки. Сьогодні єдиним конвенційним визначенням поняття «інформаційна війна» є визначення, закріплене в Угоді між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері міжнародної інформаційної безпеки та двох додатках до неї. Згідно з Додатком 1 до вищезазначеної конвенції, «інформаційна війна» – це «протистояння між двома чи більше державами в інформаційному просторі з метою завдання збитків інформаційним системам, процесам і ресурсам, критично важливим та іншим структурам, підриву політичної, економічної та соціальної систем, масового психологічного впливу на населення для дестабілізації суспільства та держави, а також для того, щоб змусити державу приймати рішення в інтересах ворогуючої сторони» [11].

Поряд із явищами кіберпростору та кібервійни виникає необхідність гарантування кібербезпеки. Кібербезпека – це здатність захистити інформаційні системи від протиправного впливу для забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам; сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі інформаційно-комунікаційних технологій (далі – ІКТ) або неправильного їхнього використання, а також із відновлення ІКТ після реалізації цих загроз тощо. Засади гарантування кібербезпеки виражаються в національних стратегіях кібербезпеки багатьох держав, оскільки вони визнають важливість даної сфери на сучасному етапі розвитку, а також у Конвенції про кіберзлочинність, ухваленій 23 листопада 2001 р. і ратифікованій Україною 7 вересня 2005 р.

Україна також діє в межах кіберпростору, тому постійно перебуває під загрозою кібератак. Так в Україні хакерам вдалося атакувати десятки об'єктів критичної інфраструктури. Все почалося з того, що в травні 2014 р. вони ледь не зірвали процес підведення підсумків президентських виборів. Вночі були атаковані сервери Центральної виборчої комісії з метою видалення даних про перебіг виборчого процесу. Наприкінці 2015 та 2016 рр. зловмисники провели декілька операцій, під час яких у деяких регіонах країни тисячі споживачів залишилися без електроенергії, виходили з ладу електронні системи Укрзалізниці, на грані знищення опинилися дані Держказначейства якраз перед плануванням соціальних виплат і пенсій тощо. Все зазначене свідчить про необхідність детального врегулювання кіберпростору національним законодавством, а також створення дієвої системи спеціалізованих органів, здатних гарантувати кібербезпеку. Зараз ці питання в Україні регулюються Конвенцією про кіберзлочинність, Указом президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про стратегію кібербезпеки України»», р. XVI Кримінального кодексу України «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» та деякими іншими актами, які все одно не забезпечують комплексного регулювання даної сфери.

Отже, кіберпростір являє собою важливе середовище, в якому певною мірою існує людина та держава. Його значення на даний момент важко переоцінити, воно влучно описується висловом Г. Раттрея, з яким неможливо не погодитися: «Розвиток військово-повітряних сил у першій половині XX ст. означав, що атака проти стратегічних центрів може бути здійснена впродовж години. Поява балістичних ракет з ядерними боєголовками скоротила цей термін до кількох хвилин. Актуалізація кіберпростору скоротила його до секунд» [10, с. 144]. Тобто в еру інформаційних технологій кіберпростором охоплюються майже всі сфери життєдіяльності відповідних суб'єктів. Оскільки його використання може відбуватися не лише із правомірною метою, нагальною є необхідність вирішення питання щодо застосування чинних норм права до нового явища – кібервійни. Варто погодитися з думкою Г. Шинкарецької, яка зауважує: «Ніде в документах міжнародного гуманітарного права немає положень про те, що його застосування може залежати від типу воєнних операцій або від специфічних засобів і методів ведення війн» [9, с. 18], оскільки відсутність конкретних норм щодо кібервійни не має стати причиною для уникнення відповідальності за ці неправомірні дії. Через існування реальної загрози у вигляді кібервійни, одним із провідних напрямів подальшої діяльності міжнародної спільноти має стати гарантування кібербезпеки для всіх держав світу. Вирішити це питання можна лише шляхом ухвалення єдиного універсального акта, в якому мають бути визначені всі сторони кіберпростору.

ЛІТЕРАТУРА

1. Камчатний М. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій / М. Камчатний // Проблеми законності. – 2016. – С. 199–207.
2. Присяжнюк М., Цифра Є. Особливості забезпечення кібербезпеки / М. Присяжнюк, Є. Цифра // Експертні системи та підтримка прийняття рішень. – 2017. – С. 61–68.
3. Грицун О. Правовий аналіз використання кіберпростору у воєнних цілях / О. Грицун // Актуальні проблеми міжнародних відносин. – 2015. – Вип. 124 (1). – С. 112–121.
4. Лук'янчикова В. Кіберпростір : загрози для міжнародних відносин та глобальної безпеки / В. Лук'янчикова // Гілея: науковий вісник. – 2013. – № 72. – С. 793–796.
5. Камчатний М. Нормативно-правове закріплення питань кібербезпеки у міжнародному праві / М. Камчатний // Актуальні проблеми сучасного міжнародного права : зб. наук. ст. за матеріалами І Харк. міжнар.-прав. читань, присвяч. пам'яті проф. М. Яновського і В. Семенова, Харків, 27 листопада 2015 р. : у 2-х ч. – Харків, 2015. – Ч. 1. – С. 320–323.
6. Манжай О. Використання кіберпростору в оперативно-розшуковій діяльності / О. Манжай // Право і Безпека. – 2009. – № 4. – С. 215–219.
7. Владленова І. Кіберзлочинність як виклик інформаційному суспільству / І. Владленова, Е. Кальницький // Гілея : науковий вісник : зб. наук. пр. – К., 2013. – Вип. 77. – С. 142–146.
8. Гнатюк С. Кібертероризм : історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк // Безпека інформації. – 2013. – Т. 19. – № 2. – С. 118–129.
9. Камчатний М. Основні ознаки поняття «кібервійна» в сучасному міжнарожному праві / М. Камчатний // Альманах міжнародного права. – 2017. – Вип. 15. – С. 12–22.
10. Дубов Д. Кіберпростір як новий вимір геополітичного суперництва : [моногр.] / Д. Дубов. – К. : НІСД, 2014. – 328 с.
11. Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 р. [Електронний ресурс]. – Режим доступу : http://base.spinform.ru/show_doc.fwx?rgn=28340.

УДК 341.1/8

ЩОДО ВІДПОВІДАЛЬНОСТІ ДЕРЖАВ У МІЖНАРОДНОМУ ПРАВІ

OF THE RESPONSIBILITY OF STATES IN THE INTERNATIONAL LAW

Шинкарчук М.Б.,
студент IV курсу
Інститут прокуратури та кримінальної юстиції
Національного юридичного університету імені Ярослава Мудрого

У статті розкриті фундаментальні ідеї інституту міжнародно-правової відповідальності. Аналізуються функції цього інституту, а також основні цілі, поставлені перед ним. Визначені проблеми, пов'язані з реалізацією міжнародно-правової відповідальності, а також значення їх вирішення для міжнародної спільноти і підтримання миру. У цьому процесі виділяється важлива проблема сучасного міжнародного права, яка має унікальне значення і полягає в неоднаковому розумінні умов і сутності реалізації відповідальності держав за міжнародно-правові правопорушення. Її особливість у тому, що рівень розвитку системи міжнародного права певною мірою залежить від чіткого розуміння правових меж взаємовідносин держав. Розвиток вивчення окремих проблем інституту розглядається крізь призму важливого значення та все більшої деталізації в умовах сучасного реформування міжнародних відносин.

Метою статті є дослідження фундаментальних понять, пов'язаних з інститутом міжнародно-правової відповідальності, та аналіз проблематики, пов'язаної з механізмом застосування відповідальності.

Ключові слова: міжнародно-правова відповідальність, цілі інституту міжнародно-правової відповідальності, функції та принципи міжнародно-правової відповідальності, міжнародні правопорушення, проблеми відповідальності в міжнародному праві.

В статье раскрываются фундаментальные идеи института международно-правовой ответственности. Анализируются функции этого института, а также основные цели, поставленные перед ним. Определены проблемы, связанные с реализацией международно-правовой ответственности, а также значение их решения для международного сообщества и поддержания мира. В этом процессе выделяется важная проблема современного международного права, которая имеет уникальное значение и заключается в неодинаковом понимании условий и сущности реализации ответственности государств за международно-правовые правонарушения. Анализируется уровень развития системы международного права в определенной степени и зависимость от четкого понимания правовых границ взаимоотношений государств. Развитие изучения отдельных проблем института рассматривается через призму важного значения и все большей детализации в условиях современного реформирования международных отношений.

Целью статьи является исследование фундаментальных понятий, связанных с институтом международно-правовой ответственности и анализ проблематики, связанной с механизмом применения ответственности.

Ключевые слова: международно-правовая ответственность, цели института международно-правовой ответственности, функции и принципы международно-правовой ответственности, международные правонарушения, проблемы ответственности в международном праве.

The article reveals fundamental ideas of the institute of the international legal responsibility. There is detailed analysis of regulation, which is provided by modern worldwide associations and connected with delimitation of rights of countries which are involved into international conflict to avoid misunderstanding of behavior models. These includes review of functions and aims of the international responsibility that helps to control level of violations which can be made by different governments on the world stage. Besides most important aims of this principle are determined so that it shows the way how it can be improved or developed to create more helpful influence on each country and disagreements between some of them.

According to the science sphere of the international law there is great variety of disputable questions in the understanding of such aspect as responsibility, following by huge amount of works connected with solutions of such situation in the world.

The purpose of the article is the analyses of worldwide attitude toward such terms as “international legal responsibility” and “international offenses” and providing formulation of these terms in the system of international law.