УДК 341:004

КАМЧАТНИЙ М. В.,
аспірант кафедри міжнародного права
Національного юридичного університету імені Ярослава Мудрого

ОСНОВНІ ОЗНАКИ ПОНЯТТЯ «КІБЕРВІЙНА» В СУЧАСНОМУ МІЖНАРОДНОМУ ПРАВІ

Анотація. Статтю присвячено дослідженню визначення одного з основних проблемних понять у сучасному міжнародному праві – «кібервійна». У статті досліджено сучасні ознаки поняття «кібервійна», що запропоновані вітчизняними та закордонними дослідниками. Автор вперше в українській доктрині порівнює різні концепції цього поняття й виділяє їхні основні спільні ознаки.

Ключові слова: кібервійна, інформаційна війна, кіберпростір, кібератака, міжнародна інформаційна безпека.

Постановка проблеми. На сьогодні розвиток технологій досяг такого рівня, що замість первинної мети – полегшення комунікації, пришвидшення інформаційних та виробничих процесів – створюється нова загроза для користувачів таких технологій. Цей розвиток, беззаперечно, відбивається і на зовнішній політиці держав. Людство вже зробило наступний крок на шляху використання кіберпростору – тепер його використовують і у воєнних цілях. Умовно ще вчора протиправними діями із використанням Інтернету були крадіжки персональних даних, шахрайство, промисловий шпіонаж. На сьогодні ж можливості використання Мережі, як і масштаби її розповсюдження світом, значно підвищилися. Уже абсолютно реальними є такі поняття, як шпигунство із використанням Інтернету, кібернетичний тероризм і навіть кібервійна.

Актуальність порушеної проблеми міжнародно-правового визначення кібервійни підтверджується численними потужними атаками на інформаційні інфраструктури держав (кібератаки на Естонію в 2007 році, на Грузію в 2008-му), створенням відповідних національних військових формувань, відповідальних за ведення кібервійни (такі органи утворені в США, Великобританії, Німеччині, Нідерландах, Бразилії, Сінгапурі, Індії, Австралії та інших державах). Проте універсального визначення поняття «кібервійна», або, як її також інколи називають, «інформаційна» або «мережева війна», у міжнародному співтоваристві досі не було сформульовано. Поруч із ним виникають питання щодо розуміння термінів «кібератака», «кібероперація», «кіберконфлікт», «кіберзагроза», «кіберзброя» тощо.

Слід зазначити, що розвинуті країни світу постійно посилюють свої матеріально-технічні та організаційні можливості для використання кіберпростору у військово-політичних цілях. Активно утворюються відповідні військові підрозділи. Так, Сполучені Штати Америки посилили свою увагу на кібервійні в 2010 році, коли Кіберкомандування США об'єднало можливості кіберармії, ВПС, ВМС і морської піхоти під одним дахом. На реалізацію цього проекту було виділено мільярди доларів. Два роки тому Пентагон оголосив про значне розширення своїх можливостей у кіберсфері, збільшивши штат з 1 800 працівників у 2014 році до 6 000 у 2016 році. Уже цього року командування США заявило про використання вперше з часу його створення спеціального підрозділу – Кіберкомандування (U.S. Cyber Command) – з метою вчинення мережевих атак проти Ісламської держави [1]. Китай також заявив про наміри розвивати свої кібернетичні потужності [2]. Відомо, що Росія, Ізраїль та Великобританія теж мають досить потужні системи для організації та вчинення кібератак і забезпечення кібероборони.

Інститут ООН із питань роззброєння (ЮНІДІР) у 2013 році вказав на зростаючу останніми роками тенденцію прийняття країнами власних національних доктрин з питань кібербезпеки. Згідно з дослідженням, проведеним Дж. А. Льюїсом та К. Тімлін у 2012 році, 114 держав вже підготували доктрини, з них 47 відносять питання інформаційної безпеки до військового аспекту, інші 67 мають суто цивільний характер [3].

Мета статті – дати загальнотеоретичне визначення поняття та основних ознак кібервійни; визначити основні ознаки поняття «кібервійна», що є спільними для сучасної вітчизняної та зарубіжної доктрини міжнародного права.

Аналіз літературних даних. Свої праці цій проблематиці присвячували такі українські вчені: В. Бурячок, А. Войціховський, О. Грицун, Д. Дубов, І. Забара, О. Мережко, Ю. Размєтаєва, Є. Скулиш. Серед закордонних вчених свої роботи присвятили Ч. Дунлап, Р. Кларк, Н. Ладарєв, М. Лібіцкі, Х. Лін, М. Магомедов, Л. Мурав'єц, Б. Рабоін, Т. Рід, В.В. Теняєв, Е. Філіол, С. Хілдрет, Г. Шинкарецька, М. Шмідт та ін.

Виклад основного матеріалу. У сучасному міжнародному праві поняття «кібервійна» перебуває лише в процесі становлення. На універсальному і регіональному рівнях здійснено тільки певні кроки на шляху до узгодження міждержавних позицій щодо її змісту. У межах ООН вперше визначення кібервійни було надано в резолюції Ради Безпеки № 1113 (2011) від 05.03.2011. Відповідно до неї кібервійною вважається використання комп'ютерів або цифрових засобів із боку уряду або з явним знанням чи схваленням цим урядом проти іншої держави або приватної власності в іншій державі, включаючи навмисний доступ, перехоплення даних або пошкодження цифрової та керованої цифровим методом управління інфраструктури. А також виробництво та поширення пристроїв, які можуть бути використані для підриву внутрішньої активності [4].

У міжнародному договірному праві поняття «кібервійна» ще не було застосовано. Разом із тим змістовно близький до нього термін «інформаційна війна» вже був закріплений в регіональному міжнародному договорі, а саме в Переліку основних понять, що є додатком до Угоди між урядами держав – членів Шанхайської організації співробітництва в галузі забезпечення міжнародної інформаційної безпеки 2009 р. «Інформаційна війна» – це протиборство між двома або більше державами в інформаційному просторі з метою нанесення збитку інформаційним системам, процесам і ресурсам, критично важливим і іншим структурам, підриву політичної, економічної і соціальної систем, масованої психологічної обробки населення для дестабілізації суспільства та держави, а також примусу держави до прийняття рішень в інтересах протиборчої сторони [5].

У документах НАТО поняття «кібервійна» прямо не визначено. Проте в аналізі та рекомендаціях до Нової стратегічної концепції Альянсу групою експертів з її розроблення визнається той факт, що в кіберпросторі можуть бути вчинені атаки на держави – члени Альянсу. А тому, зважаючи на поширення залежності країн – членів НАТО від телекомунікаційних технологій, а також на збільшення кількості вчинюваних атак на інформаційну інфраструктуру, організація має цілком серйозно підійти до питання класифікації кібервійни як дії, що підпадає під статтю 5 Вашингтонського договору. Підкреслюється, що НАТО повинна оновити свій підхід до оборони території Альянсу з урахуванням сучасних можливостей для здійснення нападів на держави [6].

На двосторонньому рівні на шляху до взаєморозуміння питань, пов'язаних із використанням приставки «кібер» у поняттях, що стосуються міжнародного права, одними з перших спробу узгодити власну термінологію у кіберсфері зробили США та РФ. У 2011 та 2014 році було видано два збірники ключових термінів англійською та російською мовами. Відповідно до останньої редакції кібервійною є найвищий ступінь кіберконфлікту між державами, під час якого держави вчиняють кібератаки проти кіберінфраструктур супротивника як частини військової кампанії. Кібервійна може бути оголошена формально однією (всіма) конфліктуючими сторонами, або не бути оголошеною формально й існувати *de facto* [7, с. 32]. Варто також підкреслити, що в зазначеному збірнику також є й інший термін – «бойові дії у кіберпросторі» (англ. cyber warfare). Цей термін визначається як кібератаки, що проводяться державами (групами держав, організованими політичними групами) проти кіберінфраструктур і є частиною військової кампанії.

Водночас безпосередньо в США до укладання російсько-американського збірника кібервійна визначалася як масово координований цифровий напад на уряд однієї країни урядом іншої або великими групами громадян. Це дія з боку держави з метою проникнути в комп'ютери або мережі іншої країни задля заподіяння шкоди або порушення їхньої діяльності [8]. Міністерство оборони США у свою чергу в цьому контексті визначає кі-

бероперації як використання кібернетичних можливостей, де основною метою є досягнення військових цілей або настання певних наслідків через кіберпростір. Комп'ютерна мережева атака визначається як дії, вчинені на основі використання комп'ютерних мереж, з метою зірвати, заблокувати, зіпсувати або знищити інформацію, що знаходиться в комп'ютерах і комп'ютерних мережах [9].

Згідно з порівняльним звітом Швейцарського Департаменту зовнішніх справ у австрійській стратегії кібербезпеки кібервійни належать до актів війни всередині і навколо віртуального простору за допомогою засобів, переважно пов'язаних з інформаційними технологіями. У більш широкому сенсі це передбачає підтримку військових сил у традиційних оперативних просторах, тобто наземному, морському, повітряному та космічному просторах із залученням заходів, вчинених у віртуальному просторі. Загалом цей термін також стосується високотехнологічної війни у вік інформації, заснованої на значній комп'ютеризації, впровадженні електроніки та мереж майже у всіх військових секторах. Також у звіті вказується, що, наприклад, у Бельгії кібервійна визначається як використання кібернетичних можливостей у достатніх масштабах та протягом певного періоду часу і при високій швидкості з метою досягнення певних цілей або ефектів у або через кіберпростір. Такі дії розглядаються як загроза національним інтересам держави цілей [10].

Загалом можна констатувати, що на цей час розвиток міжнародно-правового регулювання ведення кібервійн іде в напрямі формування відповідних міжнародно-правових звичаїв. Про це, зокрема, пише Г.Г. Шинкарецька: «Вочевидь, ми є свідками звичаєво-правового розвитку цієї галузі права» [11, с. 3]. Можемо припустити, що цей шлях нормоутворення, безсумнівно, буде складним і специфічним, оскільки нові «кіберзвичаї» будуть формуватися в межах таких галузей міжнародного права – права міжнародної безпеки, права міжнародно-правої відповідальності, МГП, права розв'язання міжнародних спорів, міжнародного кримінального права, які самі здебільшого мають міжнародне звичаєво-правове вираження. З цього, наприклад, виходить М. Шмітт (M. Schmitt), коли намагається тлумачити норму про заборону застосування сили в контексті нових міжнародних кібервідносин [12, с. 572, 573]. Аналогічним чином робить М.Ш. Магомедов, але при цьому він вказує на необхідність формування відповідної міжнародної договірної бази, оскільки тільки вона може забезпечити належний рівень ефективності застосування міжнародного гуманітарного права щодо використання нападів на комп'ютерні системи у зв'язку зі специфікою цього засобу ведення [13, с. 479].

З такою позицією слід погодитися. Разом із тим зазначимо, що оскільки укладання універсальних міжнародних договорів у найближчі роки є малоймовірним, за допомогою міжнародно-правових звичаїв можна забезпечити комплексне та деталізоване регулювання відповідних правовідносин, що само по собі вже мало місце в регулюванні деяких питань права

міжнародної безпеки та міжнародного економічного права, про що йдеться в роботах українського дослідника Ю.В. Щокіна [14, с. 288–301; 15]. На сучасному етапі велика підготовка до цього здійснюється науковцями. Отже, зараз найбільш активний пошук змістовних характеристик поняття «кібервійна» йде в доктрині міжнародного права.

Попри різноманітність думок, можна виділити певні ознаки поняття «кібервійна», властиві багатьом визначенням. Так, в Оксфордському словнику вона визначається як використання комп'ютерних технологій з метою зірвати діяльність держави або організації, особливо навмисні напади на інформаційні системи для стратегічних або військових цілей [16].

М. Шмітт вже у 2002 році запропонував своє визначення інформаційної війни (кібервійни) як виду інформаційних операцій, тобто заходів, спрямованих на здійснення впливу на інформацію та 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 у 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» [17].

На думку Б. Рабоіна (B. Raboin), кібервійна, незалежно від використаного її специфічного визначення, символізує використані державами озброєння, які функціонують в межах кібернетичного простору для спричинення проблемного і деструктивного впливу на реальний світ [18, с. 609].

Е. Філіол (E. Filiol) вказує, що кібервійна є кібернетичним виміром збройного конфлікту. Згідно з його визначенням, кібервійна – це технічний вимір інформаційної війни; використання кібернетичних можливостей для проведення агресивних операцій у кіберпросторі проти військових цілей, проти держави або її населення; типова війна, де щонайменше один із компонентів у її реалізації, мотивації та інструментах (зброї в найширшому значенні цього слова), базується в комп'ютерному або цифровому полі [19, с. 80].

Відповідно до огляду Міжнародного інституту політики Лоуі, саме визначення «кібервійна» оспорюється; вказується, що кібервійна передбачає використання комп'ютерної техніки, насамперед мережі Інтернеті, щоб зірвати або погіршувати діяльність противника. Кібервійни тісно пов'язані з іншими аспектами кібербезпеки, такими як кіберзлочинность, кібертероризм і кібершпигунство, і ці категорії інколи важко відрізнити. Але кібервійна, як правило, практикується військовими і силами безпеки держав, чия мета полягає в тому, щоб погіршити військовий потенціал су-

противника з кінцевою метою примушувати противника в необхідних політичних цілях. Кібервійна також містить розроблення та реалізацію стратегій безпеки для захисту від подібних заходів [20].

С. Хілдрет (S. Hildreth) зазначає, що термін «кібервійна» може бути використаний для опису різних аспектів захисту і нападу на інформаційні та комп'ютерні мережі у віртуальному просторі, а також позбавлення супротивника здатності робити те ж саме [21]. Іншим визначенням кібервійни, представленим К. Коулманом, є таке: це конфлікт, який використовує ворожі, незаконні операції або напади на комп'ютери та мережі у спробі порушити зв'язок та інші частини інфраструктури як механізму, метою якого є завдати економічної шкоди або розхитати захист [22].

Дж. Карр (J. Carr) описує кібервійну як мистецтво та науку боротьби без бою або перемогу супротивників без проливання їхньої крові [23]. Таким чином, автор вказує, що акти, вчинені під час кібервійни, не мають спричиняти жертв у реальному світі.

Д. Дубов, розкриваючи значення терміну «кібервійна», вказує, що під ним розуміються або систематичні напади на інформаційну інфраструктуру, або сукупність кібератак на інформаційні мережі (об'єкти критичної інфраструктури) держави [24, с. 14].

На думку О. Мережка, кібервійну точніше було б визначити як застосування комп'ютерних технологій та Інтернету однією державою або за її безпосередньої підтримки проти іншої держави, спрямоване проти її безпеки й оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї іншої держави [25].

Ю. Размєтаєва зазначає, що кібервійна може бути визначена як протистояння у кіберпросторі, яке ведеться за допомогою комп'ютерних технологій з метою завдати шкоди супротивнику. Кібервійна ведеться переважно державними суб'єктами за участі приватних і може супроводжувати збройний чи інший конфлікт між ними [26].

Г.Г. Шинкарецька зазначає, що в російській доктрині міжнародного права внутрішнє визначення поняття, яке б відповідало англійським cyber attacks і cyber war, перебуває лише у стадії становлення. Вона пропонує такі терміни: «кібератака», «кібернетичний напад», «комп'ютерна війна» і, власне, «кібернетична війна». Водночас дослідниця вважає, що поняття «кібервійна» за змістом відповідає поняттю «інформаційна війна», під якою слід розуміти «саме воєнні дії, що спрямовані проти інформаційних систем, а не війну інформацій у журналістському сенсі» [11, с. 2]. Разом із тим інші російські дослідники, В.В. Теняєв і Н.П. Ладарєв, поняття «кібервійна» застосовують як загальноприйняте. Вони визначають його таким чином: «Кібервійна (англ. cyber-warfare) – комп'ютерне протистояння у просторі Інтернет, спрямоване перш за все на дестабілізацію комп'ютерних систем і доступу до Інтернету державних закладів, фінансових і ділових центрів і утворення безладдя і хаосу у житті країн, які спираються на Інтернет у повсякденному житті» [27, с.46].

Наведені визначення терміну «кібервійна» мають багато спільного, але разом із тим порушують низку дискусійних питань. Зокрема, які ознаки має мати певне втручання чи акт, здійснений у кіберсфері, для того, щоб бути названим кібервійною? Які саме дії в кіберпросторі можна визначити як кібервійну? Очевидним є той факт, що будь-яке подібне втручання має бути здійснене саме з використанням інформаційно-комп'ютерних технологій (ІКТ). На практиці це втручання вже визначають як кібератаки та розподіляють їх залежно від спрямованості, що може слугувати надалі основою для класифікації. Так, це можуть бути шпигунські дії в кіберпросторі, певні маніпуляції щодо критичної інфраструктури, атаки, що завдають фінансових збитків державі, які мають бути націлені на військові чи цивільні об'єкти, мати на меті певний інформаційний вплив на населення країни або знищувати інформаційну мережу. З іншого боку, Т. Рід (T. Rid) стверджує, що досі ми не бачили кібервійн, а на сьогодні існують лише кібератаки. Зразки втручань, що мали місце останніми роками, мали на меті переважно шпіонаж, комп'ютерну злочинність, підривну діяльність, хактивізм [28].

Наступним важливим моментом є те, що такий акт має бути здійснений державою або від імені держави. Хоча на сьогодні є чітке розуміння того факту, що вчинені кібератаки досить складно відслідкувати, а відтак постає питання атрибуції такої атаки державі, що її вчинила. Особливо це складно зробити в разі застосування так званої «логічної бомби», тобто такої загрози для об'єкта кіберсфери, яка може проявитися не одразу, а протягом декількох місяців або навіть років з моменту потрапляння в систему.

Окремим аспектом є інтенсивність вчинюваної кібератаки, бо, якщо це є точкове ураження якогось об'єкту інфраструктури, то про кібервійну говорити вже не буде можливим. Залежно від кількості вчинених одночасно кібератак або від кількості уражених, знищених або виведених з ладу об'єктів, постає питання визначення негативних наслідків для держави, що зазнала втручання. Більш того, окрім інтенсивності, кібервійна повинна мати таку ознаку, як тривалість вчинюваних атак.

Питання про застосовність до регулювання кібервійн норм чинного міжнародного права потребує окремих досліджень і загалом перебуває за межами предмета цієї статті. Звісно, слід категорично не погодитися з тими авторами, які повністю відкидають можливості сучасного міжнародного права в регулюванні відносин у кібепросторі. Ми вважаємо, що проблеми більшою мірою спричинені можливостями нового, ширшого тлумачення і застосування чинних норм. Можна цілком погодитися із Г.Г. Шинкарецькою, яка, досліджуючи можливості чинного МГП щодо регулювання кібератак, зазначила: «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» [29, с. 241].

На цей час актуальним є нове тлумачення тих норм, які визначають міжнародно-правові основи застосування сили (пп. 4 і 7 ст. 2 Статуту

ООН; резолюції 3314 (XXIX) «Визначення агресії» Генеральної Асамблеї ООН від 14 грудня 1974 р.), права на самооборону (ст. 51 Статуту ООН), правил ведення війни (jus in bello) та ін.

Висновок. Попри відсутність нормативного закріплення та чіткого єдиного понятійного апарату, що регулював би відносини на міжнародному рівні у кіберсфері, держави визнають, що норми міжнародного права можуть бути застосовані під час вчинення кібератак на інші держави. До моменту створення універсального міжнародного акту, яким би було врегульовано усі питання щодо використання кіберпростору, визнання його новим простором є стримувальним фактором, що зупиняє держави від неконтрольованих атак та кібервтручань. Це вкотре підкреслює нагальну необхідність спершу виробити понятєвий апарат, який має бути узгоджений між суб'єктами міжнародного права, а також напрацювати міжнародно-правові норми, які б чітко визначали меж прав і відповідальності держав у глобальному інформаційному просторі.

Термін «кібервійна» має досить різні тлумачення, проте слід зазначити, що спільними для багатьох дослідників є такі ознаки:

– кібервійна може вестися лише із застосуванням інформаційно-комп'ютерних технологій;

– для визначення однієї або сукупності кібератак як кібервійни вони мають досягати певного рівня потужності та інтенсивності;

– атаки під час кібервійни націлені на дані, які підлягають комп'ютерному обробленню чи пересиланню за допомогою комп'ютера;

– у зв'язку з високою складністю організації та ведення кібервійни вона можлива лише за активної участі збройних сил держави, оскільки потребує координації дій. Саме тому в багатьох розвинених країнах у межах оборонних відомств створюються структури з реагування на концентровані кібератаки та навіть ведення кібервійн;

– сучасна кібервійна може передувати або супроводжувати розвиток збройного конфлікту. Вона може бути вчинена в координації з наземними, повітряними чи морськими операціями;

– суб'єктами ведення кібервійни можуть бути лише ті суб'єкти міжнародного права, які мають значний вплив на формування сучасних публічних міжнародних правовідносин, а саме держави, міжнародні міжурядові та деякі неурядові організації;

– кібервійна завжди потребує залучення значних матеріальних і технічних ресурсів, а також високого рівня їх організації з боку суб'єкта, що веде кібервійну;

– такі війни мають спричиняти вимірювальні наслідки;

– шкода, завдана актами кібервійни, має досягти певного високого рівня суспільної небезпеки;

– метою кібервійни є досягнення певних політичних цілей.

Слід зазначити, що існують також й інші характеристики, застосовні до терміну «кібервійна», проте вони є не такими широковживаними.

На жаль, в українському законодавстві немає чіткого визначення терміну «кібервійна», а також ознак, яким вона має відповідати. Отже, порушена проблематика потребує подальшого вивчення.

Література:

1. Sanger E.D. U.S. Cyberattacks Target ISIS in a New Line of Combat. April 24, 2016 / D.E. Sanger [Електронний ресурс]. – Режим доступу : http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=2.
2. China Military Seeks to Bring Cyber Warfare Units Under One Roof, Bloomberg News. [Електронний ресурс]. – Режим доступу : https://www.bloomberg.com/news/articles/2015-10-22/china-military-chiefs-seek-to-unify-cyber-warfare-operations.
3. The Cyber Index. International Security Trends and Realities. UNIDIR /2013/3, United Nations Institute for Disarmament Research, Geneva, Switzerland. [Електронний ресурс]. – Режим доступу : http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.
4. UN Security Council, Resolution 1113 (2011), 5 March 2011.
5. Угода між урядами держав-членів Шанхайської організації співробітництва в області забезпечення міжнародної інформаційної безпеки, [Електронний ресурс]. – Режим доступу : http://base.spinform.ru/show_doc.fwx?rgn=28340.
6. НАТО в 2020 году: Гарантированная безопасность, динамичное взаимодействие, Анализ и рекомендации группы экспертов по новой Стратегической Концепции НАТО [Електронний ресурс]. – Режим доступу : http://www.nato.int/cps/ru/natohq/official_texts_63654.htm?selectedLocale=en.
7. Rauscher K. The Russia – U.S. Bilateral on Cybersecurity – Critical Terminology Foundations Issue 1 / K. Rauscher, V. Yaschenko. – EastWest Institute, Information Security Institute of Moscow State University. – 48 p.
8. Definition of cyber warfare [Електронний ресурс]. – Режим доступу : http://definitions.uslegal.com/c/cyber-warfare.
9. Joint Chiefs of Staff, Joint Publication 1-02 / Dictionary of Military and Associated Terms (JP 3-0), Department of Defense, Washington D.C., 8 November 2010 (As Amended Through 15 October 2011).
10. Maurer T. Compilation of Existing Cybersecurity and Information Security Related Definitions. Report, October 2014 / T. Maurer & R. Morgus. – 62 p.
11. Шинкарецкая Г.Г. Информационные технологии, война и гражданское население / Г.Г. Шинкарецкая. – 8 с. – Електронний ресурс]. – Режим доступу : http://www.igpran.ru/public/articles/ShinkareckayaGG.pdf.
12. Schmitt M.N. Cyber Operations and the Jus Ad Bellum Revisited / Michael N. Schmitt // Villanova Law Review. – Vol. 56, Issue 3. – 2001. – P. 569–605.
13. Магомедов М.Ш. Нападение на компьютерные сети и МГП: пробелы и возможные пути их устранения / М.Ш. Магомедов // Рос. ежегод. конф. междунар. права, 2009. Спецвыпуск. – СПб. : Социально-коммерческая фирма «РОССИЯ-НЕВА», 2010. – С. 470–490.
14. Щокін Ю.В. Міжнародно-правовий звичай: проблеми теорії і практики : [монографія] / Ю.В. Щокін. – Х. : Право, 2012. – 456 с.

15. Щёкин Ю.В. Влияние рекомендательных резолюций Генеральной Ассамблеи ООН на формирование норм международного обычного права / Ю.В. Щёкин // Проблеми законності : Респ. міжвідом. наук. зб. / Відп. ред. В.Я. Тацій. – Х.: Нац. юрид. акад. України, 2007. – Вип. 90. – С. 191–199.
16. Definition of cyberwar in English [Електронний ресурс]. – Режим доступу: https://en.oxforddictionaries.com/definition/cyberwar.
17. Schmitt N.M. Wired warfare: Computer network attack and jus in bello / M.N. Schmitt. IRRC. – June 2002. – Vol. 84, No 846. – P. 335-336.
18. Raboin B. Corresponding Evolution: International Law and the Emergence of Cyber Warfare / B. Raboin // Journal of the National Association of Administrative Law Judiciary. – Fall 2011. – P. 81–99.
19. Ventre D. Information Warfare / D. Ventre. – USA : John Wiley & Sons, Inc., 2016. – 352 p.
20. Defence & Security. Cyber Warfare / Lowy Institute for International Policy [Електронний ресурс]. – Режим доступу : https://www.lowyinstitute.org/issues/cyber-warfare.
21. Hildreth S.A. Cyberwarfare / S.A. Hildreth // Congressional Research Service Report for Congress. – No. RL30735, 19 June 2001.
22. Coleman K. The Cyber Arms Race Has Begun / K. Coleman. – CSO Online, 28 January 2008.
23. Carr J. Inside Cyber Warfare / J. Carr. – USA, O'Reilly, 2010.
24. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван – К. : НІСД, 2011. – 30 с.
25. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві / О. Мережко [Електронний ресурс]. – Режим доступу : http://www.justinian.com.ua/article.php?id=3233.
26. Размєтаєва Ю.С. Кібервійна: загальнотеоретичні аспекти / Ю.С. Размєтаєва // Вісник АМСУ. Серія: Право. – 2015. – № 1 (14).
27. Теняев В.В. Предпосылки мировой кибервойны / В.В. Теняев, Н.П. Ладарев // Актуальні питання розслідування кіберзлочинів : матеріали Міжнар. наук.-практ. конф. (м. Харків, 10 груд. 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – С. 46–48.
28. Rid T. NATO Review Magazine. Cyberwar – does it exist? / T. Rid // NATO [Електронний ресурс]. – Режим доступу : http://www.nato.int/docu/review/2013/Cyber/Cyberwar-does-it-exist/EN/index.htm.
29. Шинкарецкая Г.Г. Враждебное воздействие на компьютерные системы государства и международное право / Г.Г. Шинкарецкая // Рос. ежегод. конф. междунар. права. – СПб. : Социально-коммерческая фирма «РОССИЯ-НЕВА», 2014. – С. 235–250.

Камчатный Н. В. Основные признаки понятия «кибервойна» в современном международном праве

Аннотация. Статья посвящена исследованию определений одного из основных проблемных понятий в современном международном праве – «кибервойна». В статье исследованы современные признаки понятия «кибервойна», предложенные отечественными и зарубежными исследователями. Автор впервые в украинской доктрине сравнивает различные концепции этого понятия и выделяет их основные общие признаки.

Ключевые слова: кибервойна, информационная война, киберпространство, кибератака, международная информационная безопасность.

Kamchatniy M. The main features of the concept of "cyberwar" in contemporary international law

Summary. The article presents a study determining one of the basic problematic concepts in contemporary international law – the term "cyberwar". The author explores the concepts that were proposed by Ukrainian and foreign researchers in the field of international law. The relevance and the need to bring the understanding of the term to a common point as well as the need of bringing in line of the term with international law is proved. The lack of international instruments regulating the conduction of such an activities as cyberwar, or somehow limiting mentioned acts is shown. For the first time in Ukrainian doctrine different approaches to the concept of "cyberwar" were analyzed and compared. The main common features of the term were proposed by the author. It is indicated that there is no definition of the term "cyberwar" in Ukrainian legislation. The main features of acts which distinguish cyberwar from cyber interventions or pointed cyberattacks are indicated. The importance of continuing of the study of this concept both in Ukrainian and foreign science of international law, the need to settle the features and fixing a new concept in international legal regulations.

Key words: cyberwar, information warfare, cyberspace, cyberattacks, international information security.