Камчатний Микола Валерійович,
аспірант кафедри міжнародного права,
Національний юридичний університет
імені Ярослава Мудрого,
Україна, м. Харків
e-mail: n.kamchatniy@gmail.com
ORCID 0000-0002-0986-3211

doi: 10.21564/2414–990x.134.80112
УДК 341:004

ІСТОРІЯ МІЖНАРОДНО–ПРАВОВОГО РЕГУЛЮВАННЯ ПИТАНЬ, ПОВ'ЯЗАНИХ ІЗ ЗАСТОСУВАННЯМ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Досліджується генезис правового регулювання кібербезпеки у міжнародному праві, визначається місце цієї проблеми у відносинах між суб'єктами міжнародного права. Наведено приклади резонансних кібератак, що вчинялися на міжнародному рівні.

Ключові слова: кібербезпека; кіберпростір; кібератака; кіберзлочинність; міжнародна інформаційна безпека.

Камчатный Н. В., аспирант кафедры международного права, Национальный юридический университет имени Ярослава Мудрого, Украина, г. Харьков.
e-mail: n.kamchatniy@gmail.com ; ORCID 0000-0002-0986-3211

История международно-правового регулирования вопросов, связанных с использованием компьютерных технологий

Исследуется генезис правового регулирования кибербезопасности в международном праве, определяется место данной проблемы в отношениях между субъектами международного права. Приведено примеры резонансных кибератак, которые совершались на международном уровне.

Ключевые слова: кибербезопасность; киберпространство; кибератака; киберпреступность; международная информационная безопасность.

Вступ. Останнім часом залежність людства від нових технологій зростає з неймовірною швидкістю. На жаль, ця загалом прогресивна тенденція несе в собі і певні негативні наслідки. Станом на 2014 р. у світі вже 2,8 млрд людей мали доступ до мережі Інтернет, налічувалося близько 10 млрд пристроїв, що під'єднані до цієї всесвітньої мережі [1]. Спостерігається тенденція створення надзвичайно розгалуженої мережі під'єднаних до Інтернету речей,

що можуть функціонувати самостійно (так званий «Internet of Things»). Проте застосування таких технологій відкриває також і нові шляхи до зловживань з використанням мережі Інтернет, серед яких крадіжки, незаконний обіг заборонених товарів, надання незаконних послуг, диверсії, тероризм і навіть руйнування інфраструктури міст під час ведення війни. Це, безперечно, спонукає держави й міжнародні організації приділяти значно більшу увагу забезпеченню кібербезпеки, вимагає врегулювання цієї проблеми на міжнародному рівні.

Аналіз літературних даних і постановка завдання дослідження. Тематиці кібербезпеки присвятили свої роботи чимало вітчизняних учених, серед яких А. Пазюк, Д. Дубов, О. Мережко, Д. Шпенов, Р. Лук'янчук. Значно більшу увагу дослідженню питань кібербезпеки у міжнародному праві приділяють зарубіжні фахівці, серед яких М. Н. Шмітт, В. Хайнтшель фон Хайнег, В. Бутбі, Т. Вінгфілд, Б. Демейре, П. Маргуліс та інші.

З огляду на це ***метою*** нашої ***статті*** є визначення генезису міжнародно-правового регулювання кібербезпеки шляхом аналізу вчинених кібератак та їх наслідків, вивчення міжнародно-правового регулювання у сфері кіберпростору.

Виклад основного матеріалу. З розвитком технологій кіберпростір стає новим і не менш важливим, ніж наземний, повітряний, водний чи космічний простори, у якому держави змагаються за забезпечення власних національних інтересів. Одночасно він привертає увагу міжнародних терористичних груп, транснаціональних організованих злочинців.

У західній літературі одним із перших прикладів використання кібертехнологій задля впливу на іншу державу вважається використання у 1982 р. так званої «логічної бомби» [2]. Існує версія, що в цьому випадку був використаний «троянський» вірус, прихований у програмному забезпеченні, яке радянські шпигуни викрали у Канаді з метою забезпечення функціонування Транссибірського газопроводу. На той момент спеціалісти СРСР 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 Сполучених Штатів Америки. Під час випробувань тиску на певних ділянках газопроводу троянська програма була запущена і цим вплинула на максимальне збільшення тиску у системі, що не було відображено на спеціальних приладах з контролю покажчиків. У результаті у 1982 р. це призвело до надзвичайно потужного вибуху газу [3].

Однією з перших атак, безпосередньо спрямованих проти національної безпеки країни, була кібератака на Естонію у 2007 р. [4, с. 5–8]. Передумовою такого втручання вважається рішення уряду Естонії про переміщення пам'ятника радянським воїнам часів Другої світової війни з 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 та

інформаційні системи, сайти багатьох засобів масової інформації, громадських організацій. Хакерам вдалося навіть ненадовго вимкнути сервіс невідкладної допомоги, який функціонував завдяки мережі Інтернет [5, с. 110]. Відновлення повноцінного функціонування інформаційної інфраструктури потребувало певного часу та значних фінансових витрат. Хоча офіційного підтвердження участі російської влади у організації атак не було, багато хто з естонських представників влади наголошував саме на цій версії [6]. Усі технічні шляхи виводили експертів з інформаційно-комп'ютерних технологій саме на російські центри організації кібератак, які, до того ж, використовували для втручання «заражені» комп'ютери з понад 70 країн світу.

Уже за рік, у 2008 р., подібних посягань зазнали урядові сайти 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 та Великої Британії [5, с. 112]. Це був перший випадок у історії, коли наземна військова операція супроводжувалася скоординованою із нею кібератакою [7]. Хоча доказів того, що атаки були здійснені російськими військами чи координувалися російською владою, не існує, їх вигідність Росії під час військової операції є беззаперечною.

Однією з найбільш відомих на сьогодні кібератак вважається застосування кібернетичного вірусу «Stuxnet». Цей системний код був використаний у 2010 р. для атаки SCADA[1]-систем більш ніж однієї тисячі центрифуг зі збагачення урану виробництва компанії Siemens, розташованих у Натанзі (Іран) [8]. Атака вивела з ладу центрифуги, що унеможливило подальшу роботу компанії. При цьому вірус діяв так, що оператори центрифуг не помічали жодних відхилень під час роботи системи. У той же час шкідливий код змінював умови роботи обладнання, від чого процес ставав неконтрольованим, і центрифуги виходили з ладу фізично. Хоча офіційних підтверджень і визнання з боку держав того, що ця програма була створена за участю США та Ізраїлю, нема й досі, така версія широко обговорювалася.

Окрім того, чимало інших країн світу зазнавали більших чи менших атак на урядові та неурядові сайти, деякі об'єкти інфраструктури. Серед них як надзвичайно розвинені у кіберсфері країни, такі як США, Великобританія, Ізраїль, Південна Корея, Китай, так і країни зі значно нижчим рівнем розвитку кібертехнологій.

Усі ці випадки підтверджують зростання значення кіберпростору у міжнародних відносинах, необхідність правового регулювання між суб'єктами міжнародного права у ньому. Варто зазначити, що технології розвиваються значно

[1] SCADA (скорочення від англ. Supervisory Control And Data Acquisition) – умовний переклад як диспетчерське управління та збір даних. Це програмний пакет, призначений для розробки або забезпечення роботи у реальному часі систем збору, обробки, відображення і архівації інформації про об'єкт моніторингу або управління.

швидше, ніж норми, що регулюють їх використання. Це породжує необхідність правового закріплення питань щодо кіберпростору у національних законодавствах та міжнародного узгодження таких норм.

На жаль, на сьогодні існує досить вузький перелік міжнародно-правових актів, які б регулювали відносини суб'єктів міжнародного права у кіберпросторі. Слід зазначити, що досі не вироблено уніфікований понятійний апарат, тому в деяких країнах такі терміни, як «кіберпростір», «кібербезпека», «кібератака» та інші, що містять у своєму складі «кібер», трактуються у національному законодавстві по-різному.

Підвалини для подальшого співробітництва держав було закладено Резолюцією Генеральної Асамблеї (ГА) ООН 53/70 ще у 1998 р. Визнаючи і підкреслюючи швидкий розвиток технологій, а також те, що вони можуть бути застосовані у цивільній і військовій сферах, Генеральна Асамблея водночас наголосила, що ці технології можуть також використовуватись у цілях, несумісних із задачами забезпечення міжнародної стабільності та безпеки, і можуть негативно вплинути на безпеку держав. Своєю Резолюцією ГА ООН закликала держави-члени до співробітництва у розгляді існуючих загроз у сфері інформаційної безпеки; визначення основних понять, що стосуються інформаційної безпеки; а також до інформування Генерального Секретаря щодо доцільності розробки міжнародних принципів, які підвищать безпеку глобальних інформаційних телекомунікаційних систем та сприятимуть боротьбі з інформаційним тероризмом та криміналом [9]. Такий підхід спричинив тенденцію до висунення щорічних пропозицій з боку держав та підготовки Генеральною Асамблеєю резолюцій з питання досягнень у сфері інформатизації та телекомунікації у контексті міжнародної безпеки.

Уже у 2000 р. та 2001 р. Генеральною Асамблеєю ООН було підготовлено Резолюції 55/63 та 56/121 відповідно. Обидві стосуються боротьби зі злочинним використанням інформаційних технологій. Цими Резолюціями державам, серед іншого, рекомендується обмінюватися інформацією, експертами задля більш ефективної боротьби зі злочинним використанням інформаційних технологій, забезпечувати співпрацю на рівні слідчих органів держав [10].

Своєю Резолюцією 57/239 2003 р. «Створення глобальної культури кібербезпеки» ГА ООН вкотре підкреслює важливість сучасних інформаційних телекомунікаційних систем для розвитку суспільства і водночас наголошує, що уряди, бізнес, громадські організації та індивідуальні особи-користувачі Інтернет мають бути обізнані щодо відповідних ризиків і також вживати заходів для підвищення безпеки. У зв'язку із цим Асамблея пропонує елементи для створення глобальної культури кібербезпеки [11].

Основним документом у цій сфері у рамках Ради Європи є ратифікована 49-ма державами Конвенція про кіберзлочинність 2001 р. (Будапештська конвенція про кіберзлочинність) [12]. Вона набула чинності для України 1 липня 2006 р. [13]. Це – перший міжнародний акт, направлений на захист населення та міжнародне співробітництво держав у сфері кіберзлочинності. Документ

визначає певний перелік термінів, що стосуються кіберзлочинності, діяння, що є порушеннями у комп'ютерній сфері, та відповідальність за них, деякі процедурні аспекти тощо. Підписанти Конвенції брали на себе зокрема такі зобов'язання:

– створювати внутрішнє законодавство з метою закріплення процедур, викладених у Договорі (таких, як пошук та захоплення, перехоплення комп'ютерних даних тощо);

– співпрацювати шляхом надання взаємної правової допомоги, навіть якщо нема іншої спеціальної угоди (наприклад, про екстрадицію, про доступ до комп'ютерних даних тощо);

– судово переслідувати кіберзлочини, вчинені на її території.

Додатковий протокол до Конвенції (Страсбург, 2003; набув чинності для України 1 квітня 2007 р.) розширює перелік кіберзлочинів за рахунок таких протиправних діянь, як: поширення расистського та ксенофобного матеріалу через комп'ютерні системи, погроза та образа з расистських і ксенофобних мотивів через комп'ютерну систему [14].

У 2012 р. у Женеві відбулася Всесвітня конференція електрозв'язку МСЕ[1]. Під час конференції ухвалено нову редакцію Регламенту Міжнародного союзу електрозв'язку, зміни до якого не вносилися двадцять чотири роки. Нова редакція Регламенту, серед багатьох інших, передбачає положення щодо безпеки електрозв'язку, обмеження спаму, сприяння розвитку пунктів обміну трафіком, заохочення конкуренції. Регламент містить застереження, яким його дія жодним чином не поширюється на регулювання змісту інформації (контенту). Ухвалення цієї редакції Регламенту вперше відбувалося не на консенсусній основі, а на тлі жорсткого політичного протистояння, з одного боку, прибічників посилення регуляторного впливу МСЕ на Інтернет (серед таких країн Російська Федерація, КНР та ін.), і противників розширення повноважень на регулювання Інтернету цим союзом (тобто МСЕ). Носіями останньої позиції були Сполучені Штати, Японія, Канада, держави-члени Європейського Союзу, які обстоювали принципи багатосторонньої участі усіх зацікавлених сторін (держав, громадянського суспільства і бізнесу) у процесі управління Інтернетом [15].

У рамках ЄС першим документом, що регулює кіберсферу, є Директива 95/46 / Європейського парламенту та Ради від 24 жовтня 1995 р. про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних. Відповідно до цієї Директиви держави-члени мають захищати основні права та свободи фізичних осіб, і, зокрема, їх право на недоторканність приватного життя щодо обробки персональних даних [16].

З метою забезпечення більш високого рівня кібербезпеки у Європейському Союзі Європейський парламент і Рада Європейського Союзу у 2004 р. створили Європейське агентство з мережевої та інформаційної безпеки. Статтею 2 Регламенту № 460/2004 передбачено, серед інших, такі цілі створення даного

[1] МСЕ – Міжнародний союз електрозв'язку (англ. International Telecommunication Union, ITU). Спеціалізована агенція Організації Об'єднаних Націй, яка відповідальна за інформаційні та комунікаційні технології.

агентства: розширити можливості Співтовариства щодо реагування на проблеми інформаційної безпеки; надавати допомогу і рекомендації Комісії та державам-членам з питань, пов'язаних із мережевою та інформаційною безпекою; надавати допомогу Комісії у технічній підготовчій роботі з оновлення і розробки законодавства Співтовариства у сфері мережевої та інформаційної безпеки [17].

У 2016 р. підписано документ, що продемонстрував собою прагнення європейських держав до співробітництва у кіберсфері. Ним стала Директива ЄС з мережевої та інформаційної безпеки (EU Network and Information Security (NIS) Directive) [18]. Її метою є досягнення високого загального рівня безпеки мережевих та інформаційних систем у рамках Союзу. Так, для досягнення цієї мети, поряд з іншим, Директива зобов'язує держави-члени: ухвалити відповідні національні стратегії; створювати групи зі співробітництва з метою підтримки і сприяння стратегічній співпраці та обміну інформацією між державами-членами; створювати групи реагування на комп'ютерні інциденти з метою розвитку довіри між державами-членами та швидкого й ефективного оперативного співробітництва; встановлювати вимоги безпеки для операторів цифрових послуг тощо.

Після атак у 2007 р. на кіберпростір Естонії 2008 р. у НАТО остаточно ухвалили рішення про створення Центру з підвищення кваліфікації зі спільної кібероборони – CCD COE (Cooperative Cyber Defence Centre of Excellence). Центр сфокусувався на координації кіберзахисту та створенні політики для надання допомоги союзникам під час нападів [5, с. 110]. Рішенням Північноатлантичної Ради CCD COE була створена як Міжнародна військова організація [19].

На її базі у 2013 р. групою експертів з міжнародного права, за загальною редакцією М. Н. Шмітта, підготовлено так званий Tallinn Manual on the International Law Applicable to Cyber Warfare (Талліннський посібник з ведення війни або Талліннський посібник з міжнародного права, застосовного до кібервійни) [20]. Посібник приділяє особливу увагу праву на війну (jus ad bellum) – міжнародно-правовим нормам, які регулюють застосування сили державами як інструменту своєї національної політики і jus in bello, яке називають правом збройних конфліктів або міжнародним гуманітарним правом. Талліннський посібник – це не офіційний документ, проте він є втіленням наукових думок групи незалежних експертів, котрі діють виключно від свого імені.

Відповідно до зростаючої ролі кіберпростору багато держав створюють власні національні законодавчі норми та стратегії кібербезпеки. Так, нині 27 країн-членів НАТО, Європейський Союз, 12 країн Європи, що не є членами НАТО, а також 38 країн із інших частин світу мають власні національні стратегії кібербезпеки [21]. Серед них і Україна, де у 2016 р. Указом Президента України №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України» було затверджено національну стратегію кібербезпеки [22]. Раніше, у 2009 р., штаб-квартира НАТО ухвалила стратегічний документ «Рамки співробітництва у питаннях

кібернетичного захисту між НАТО та державами-партнерами». Цим актом було закладено підґрунтя для налагодження співробітництва у сфері кібербезпеки між країнами-учасниками, зокрема й Україною [23].

Висновки. Нерідко комп'ютерні технології використовуються з метою завдання шкоди об'єктам військової та цивільної інфраструктури, негативного впливу на процеси виробництва, збоїв у системі функціонування національних Інтернет-ресурсів тощо. Питання кібербезпеки дедалі гостріше стає проблемою не лише національного рівня, а тому вимагає розширення міжнародно-правового співробітництва між суб'єктами міжнародного права задля збереження миру і недопущення розв'язання кібернетичних війн, які можуть супроводжуватися і кінетичними.

Безперечно, наукові пошуки у цій сфері потребують подальших зусиль.

References:

1. The Internet Organised Crime Threat Assessment (iOCTA), European Police Office (2014). www.europol.europa.eu. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf.

2. Thomas, Reed. (2005). At the Abyss: An Insider's History of the Cold War. Published in the United States. New York: Presidio press.

3. Byres, Eric J., Eng, P. (2009). Cyber Security And The Pipeline Control System. Lantzville, BC, Canada.

4. William, C. Major. (2009). Ashmore. Impact of Alleged Russian Cyber Attacks. School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas.

5. Schreier, Fred. (2015). On Cyberwarfare. DCAF HORIZON. Working paper No. 7.

6. Tikk, Eneken, Kaska, Kadri & Vihul, Liis. (2010). International Cyber Incidents: Legal Considerations, Tallinn, Cooperative Cyber Defense Centre of Excellence (CCD COE), 15–34. ccdcoe.org. Retrieved from https://ccdcoe.org/publications/books/legalconsiderations.pdf.

7. Melikishvili, Alexander. (2009). Recent Events Suggest Cyber Warfare Can Become New Threat (WMD Insights, December 2008/January 2009 Issue). www.wmdinsights.com. Retrieved from http://www.wmdinsights.com/I29/I29_G3_RecentEvents.htm.

8. Andryeyeva, O.M., Musiyenko, K. (2011). Kiberzbroya ta analiz yiyi destruktyvnoyi diyal'nosti na prykladi vplyvu virusu novoho pokolinnya STUXNET na irans'ku yadernu prohramu. Perspektyvy vidnosyn Ukrayiny zi USA, RF, EU & NATO v postkryzovomu sviti, 29–34 [in Ukrainian].

9. Resolution Adopted by the General Assembly 53/70. (1999). Developments in the Field of Information and Telecommunications in the Context of International Security. ccdcoe.org. Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-981204-ITIS.pdf

10. Resolution adopted by the General Assembly 55/63. (2001). Combating the criminal misuse of information technologies. ccdcoe.org. Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-001204-CriminalMisuseIT.pdf.

11. Resolution Adopted by the General Assembly 57/239. (2003). Creation of a global culture of cybersecurity. ccdcoe.org. Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-021220-CultureOfCS.pdf

12. Konventsiya pro kiberzlochynnist'. (2007). Ofitsiynyy visnyk Ukrayiny vid 10.09.2007, No. 65, 107.

13. Convention on Cybercrime. (2016). Chart of signatures and ratifications of Treaty 185. Status as of 28.09.2016. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=yvTbDHWU.

14. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CETS No. 189. (2006). The Council of Europe. conventions.coe.int. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

15. Rehlament Mizhnarodnoho soyuzu elektrozvyazku. (2012). Materialy Vsesvitnya konferentsiya elektrozvyazku MSE, Zheneva [in Ukrainian].

16. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. (1995). Official Journal of the European Communities, No. L 281/31, 24 October.

17. Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. (2004). Official Journal L 077, 13/03/2004, 0001–0011.

18. European Commission. Network and Information Security (NIS) Directive. (2016). Digital Single Market, Digital Economy & Society, Directive (EU) 2016/1148. Retrieved from https://ec.europa.eu/digital-single-market/news/network-and-information-security-nis-directive.

19. Centre is the first International Military Organization hosted by Estonia. (2008). NATO Cooperative Cyber Defence Centre of Excellence, 28 October 2008. ccdcoe.org. Retrieved from https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html.

20. Michael, N. (2013). Schmitt, the «International Group of Experts». Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. issuu.com/nato_ccd. Retrieved from https://issuu.com/nato_ccd_coe/docs/tallinnmanual.

21. Cyber security strategy documents. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia. ccdcoe.orgю Retrieved from https://ccdcoe.org/cyber-security-strategy-documents.html.

22. Stratehiya natsional'noyi bezpeky Ukrayiny. (2015). Zatverdzhena Ukazom Prezydenta Ukrayiny vid 26.05.2015 № 287/2015. Ofitsiynyy visnyk Ukrayiny, 43 [in Ukrainian].

23. Framework for Cooperation on Cyber Defence Between NATO and Partner Nations. (2009). NATO/EAPC Unclassified, Document EAPC(C)D(2009)0010. uan.ua. Retrieved from http://uan.ua/sites/default/files/41210385dod2.pdf.

24. Michael, N. Schmitt. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. Harvard Internatinal Law Journal, Vol. 54, December.

25. Dubov, D.V. (2016). Heopolitychne supernytstvo u kiberprostori yak chynnyk vplyvu na natsionalnu bezpeku Ukrayiny. Doctor's thesis. Kyiv [in Ukrainian].

26. Pazyuk, A.V. (2015). Mizhnarodno-pravove rehulyuvannya informatsiynoyi sfery (teoretychni i praktychni aspekty). Doctor's thesis. Kyiv [in Ukrainian].

Kamchatniy M. V., Postgraduate Student of the Department of International Law, Yaroslav Mudryi National Law University, Ukraine, Kharkiv.

e-mail: n.kamchatniy@gmail.com ; ORCID 0000-0002-0986-3211

History of international legal regulation of the issues related to the use of computer technologies

The article studies the genesis of legal regulation of cybersecurity in international law, the definition of the place of the problem in relations between subjects of international law. Examples of high-profile cyberattacks that took place internationally are shown.

In recent years, human dependence on new technologies has grown rapidly. However, the use of such technologies also opens new ways to abuse via the Internet. With the development of new technologies cyberspace becomes as important space as land, air, water or space in which states compete for ensuring their national interests. Such space also attracts the attention of international terrorist groups, transnational organized crime etc.

A number of scientists devoted their papers to the subject of cybersecurity, among them A. Pazyuk, D. Dubov, A. Merezhko. Much more attention on the issue of cybersecurity research in international law was paid by foreign experts, including M. N. Schmitt, W. Heintschel von Heinegg, V. Boothby.

The article shows examples of international norms in cyberspace. Accordingly the foundations for further cooperation among the States were laid by the number of Resolutions of the General Assembly of the United Nations. One of the main documents in this field within the Council of Europe is ratified by 49 states Convention on Cybercrime in 2001 and Optional Protocol to the Convention of 2003. Within the EU the first document regulating cyberspace is Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In 2016 EU has adopted the EU Network and Information Security (NIS) Directive. As an example of doctrinal codification the Tallinn Manual on the International Law Applicable to Cyber Warfare was issued in 2013.

It is also mentioned in the article that states are actively working on preparing national legislation and adopting strategies for cybersecurity

It is noted that the issue of cybersecurity is becoming more acute problem not only at the national level and therefore requires expansion of international legal cooperation between subjects of international law to maintain peace and prevent solving cyber warfare, which may be accompanied by kinetic.

Keywords: cybersecurity; cyberspace; cyberattack; cybercrime; international information security.

Надійшла до редколегії 01.09.2016 р.