Література:

1. Moore, J. A. and Pubantz, J. (2006)The New United Nations International Organization in the Twenty-First Century, New Jersey: Pearson Prentice Hall. – 167 P.

2. Решетов Ю. А. Борьба с международными преступлениями против мира и безопасности / Ю. А. Решетов. – М.: Междунар. отношения, 1983. – 224 с.

3. BrzoskaM. (2001)Design and Implementation of Arms Embargoes and Travel and Aviation Related Sanctions: Results of the «Bonn-Berlin-Process»,BICC. – 129 P.

4. Кононова К. О. Санкционные резолюции Совета Безопасности ООН и их имплементация в национальных правових системах государств-членов (на примере правовой системы Российской Федерации: дис. …к.ю.н.: 12.00.10 / Ксения Олеговна Кононова; [наук. керівник В. С. Иваненко]; СПбГУ. – Санкт-Петербург, 2009. – 206 С.

5. Gowlland-Debbas V. (2003) The Domestic Implementation of UN Sanctions, in Review of the Security Council by Member States/ Erika de Wet, André Nollkaemper (eds.), *Antwerpen/Oxford/New York:*Intersentia, pp.63–76.

М. В. Камчатний[1]

НОРМАТИВНО-ПРАВОВЕ ЗАКРІПЛЕННЯ ПИТАНЬ КІБЕРБЕЗПЕКИ У МІЖНАРОДНОМУ ПРАВІ

В сьогоднішньому глобальному світі інформаційні технології використовуються для забезпечення національної та військової безпеки, що стало поштовхом для виокремлення окремої середи – кіберпростору. Він не має загальноприйнятих кордонів чи меж, проте повністю може вважатися міжнародним простором. Серед відомих міжнародному праву земного, повітряного, морського, космічного просторів, кіберпростір ще не має єдиного чіткого визначення, так само як і міжнародні відносини у ньому.

Вже визнаним є той факт, що замість зброї в її загально-прийнятому розумінні, для регулювання використання якої існує значна кількість міжнародних угод, з'являється небезпека завдати шкоди іншими засобами, зокрема з використанням комп'ютерних технологій.

[1] Аспірант кафедри міжнародного права Національного юридичного університету імені Ярослава Мудрого

Передові держави світу останніми роками активно утворюють відповідні органи із захисту від кібератак та забезпечення кібербезпеки. Наприклад, у Європейському Союзі функціонує Агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), у Сполучених Штатах Америки кібербезпекою займається Агентство Національної Безпеки, у НАТО створений Комітет з кібернетичної оборони (The Cyber Defence Committee), а також Спільний центр з кібернетичної оборони (Cooperative Cyber Defence Centreof Excellence) та ін. Відповідно, ці органи готують нормативні акти, що регулюють певні аспекти у сфері кібербезпеки, забезпечують професійними кадрами, обмінюються досвідом, проводять навчання щодо відвернення кібератак (як це, наприклад, було у НАТО у 2008 в результаті кібератак на Естонію).

Окрему увагу питанням кібербезпеки приділяє і Організація Об'єднаних Націй (далі – ООН). 20 грудня 2002 року резолюцією 57/239 Генеральної Асамблеї були прийняті «Елементи для створення глобальної культури кібербезпеки». Як вказується у 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 році Всесвітньою асамблеєю зі стандартизації електрозв'язку Міжнародного союзу електрозв'язку було прийнято Резолюцію 50 «Кібербезпека», якою, серед іншого, було підкреслено, що всім зацікавленим сторонам необхідно разом працювати над розробкою стандартів та принципів в цілях захисту від кібератак та полегшення виявлення джерел атак. Крім того, варто сприяти глобальним узгодженим та сумісним процесам обміну інформацією, що стосується реагування на інциденти. Також в 2012 році ООН було підготовлено Доповідь групи урядових експертів з досягнень у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки. Група, серед іншого, погодилася, що заходи по зміцненню довіри, такі як 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 та усунення хибних уявлень. Важливим є те, що за результатами Доповіді було підтверджено, що на кіберпростір поширюється дія міжнародного права, зокрема, Статуту ООН.

В Україні питанням забезпечення кібербезпеки не приділяється належної уваги, особливо в сучасних умовах збройного протистояння на сході країни. Фактично в Україні досі відсутні нормативні акти, які описували б загрози Україні безпосередньо в кіберпросторі, а відтак, визнали б їх. Відповідно до цього, попре спроби та деякі запропоновані проекти (наприклад, Проект Закону про кібернетичну безпеку 2207а від 22.06.2013, Проект Концепції інформаційної безпеки України), в Україні досі нема цілісної державної політики та програми з кібербезпеки. Чи не єдиним документом на сьогодні є Конвенція про кіберзлочинність, ратифікована Верховною Радою України 07.09.2005, проте і вона не достатньо відповідає сучасним реаліям загроз у кіберпросторі, а тому з цього питання залишається багато прогалин. Ці фактори роблять Україну вразливою перед загрозами у кіберпросторі, підкреслюють необхідність створення профільних державних органів, навчання спеціалістів, а найголовніше –підготовку нормативно-правової бази, що регулювала б ці питання. Підтвердженням вразливості є той факт, що кіберзлочинами в українському законодавстві є передбачені кримінальним законом суспільно небезпечні діяння, закріпленні в Розділі XVI Кримінального кодексу України «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Тому, з точки зору кримінального права, до кіберзлочинів відносяться тільки злочини, передбачені розділом XVI КК України, поняття яких є значно вужчим, ніж ті загрози, що існують на сьогоднішній день.

Як висновок, варто навести пункт D доповіді Генерального секретаря ООН, зробленої у 2012 році, де вказується, що одне з найсерйозніших завдань –необхідність знайти способи вирішення проблеми кібербезпеки, не підриваючи при цьому можливостей Інтернету по сприянню інноваціям і наданню більш цінної інформації і перспективних послуг, потрібних користувачам. Тож, міжнародне співтовариство також підкреслює необхідність вирішення цих проблем в рамках угод про права людини.

Література:

1. Конвенція про кіберзлочинність (набула чинність 01.07.2006) // Верховна Рада України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575

2. 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 (Text with EEA relevance) //Official Journal L 077 , 13/03/2004 P. 0001–0011[Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX: 32004R0460:EN:HTML

3. Бородакий Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Бородакий Ю. В., Добродеев А. Ю. // [Електронний ресурс]. – Режим доступу:http://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1

4. Дубов Д. В. Стратегічні аспекти кібербезпеки України. / Національна безпека та її складники [Електронний ресурс]. – Режим доступу:http://sp.niss.gov.ua/content/articles/files/16–1446038514.pdf

5. A/67/66−E/2012/49, Генеральная Ассамблея Экономический и Социальный Совет. / Организация Объединенных Наций. [Електронний ресурс]. – Режим доступу:
http://unctad.org/meetings/en/SessionalDocuments/a67d66_ru.pdf

6. Проект Закону про кібернетичну безпеку України// Верховна Рада України[Електронний ресурс]. – Режим доступу:
http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47240

7. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Електронний ресурс]. – Режим доступу: http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33_Russian.pdf

8. Проект. Концепція інформаційної безпеки України. [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf

М. М. Камышанский[1]

АКТЫ МЕЖДУНАРОДНЫХ МЕЖПРАВИТЕЛЬСТВЕННЫХ ОРГАНИЗАЦИЙ КАК ИСТОЧНИКИ ЮРИДИЧЕСКИХ ОСНОВАНИЙ МЕЖДУНАРОДНО-ПРАВОВОЙ ОТВЕТСТВЕННОСТИ ГОСУДАРСТВ

Для теории и практики международного публичного права вопросы о юридических основаниях международно-правовой ответственности

[1] Аспирант кафедры международного права Национального юридического университета имени Ярослава Мудрого