3. ICAO Assembly Resolution A 35-14 Annex A: «Improvement of Safety Oversight» in ICAO Doc. 9848.
4. Paul S. Dempsey, The Role of the international Civil Aviation Organization on Deregulation, Discrimination, Dispute Resolution. 52 J.Air L.& Com. 529 (1987).
5. D. Freer. ICAO at 50 Years: Riding the Flywheel of Technology, 49 ICAO J (September 1994), 19, 28.
6. Бордунов В.Д. Правовой механизм деятельности международных авиационных организаций. – М.: Наука, 1989. – 168 с.
7. Huang Jiefang. Aviation Safety, ICAO and obligation Erga Omnes. Chinese Journal of International Law (2009), Vol.8, No.1, 63-79.
8. Конвенція про міжнародну цивільну авіацію 7 грудня 1944 р. – ООН, 2016. 34 с.
9. Michle Milde, The Chicago Convention – Are Major Amendments Necessary Or Desirably 50 years Later?, 19 Annals of Air & Space L. 401, 426 (1994).
10. ICAO Assembly Resolution A 29-13: "Improvement of Safety Oversight" in ICAO Doc. 9848.
11. DOT Order 93-10-26, DOT Order 85-7-45, Order 95-9-15.
12. Huang Jiefang. Aviation Safety, ICAO and obligation Erga Omnes. Chinese Journal of International Law (2009), Vol.8, No.1, 63-79.
13. M. Milde. Aviation Safety Oversight Audits and the Law, XXXVI Annals of Air and Space Law (2001).
14. B.G. Ramcharan, The Consept of Demmension of the Righ to Life, in International Law (Dorderecht: Martinus Nijhoff Publishers, 1985) 1, 2.
15. Barcelona Trection (Belgium v. Spain) (Second pfase) ICJ Reports 970, 32.

ВПЛИВ КІБЕРЗАГРОЗИ НА ОСВІТУ

Невара Л.М.
кандидат юридичних наук,
доцент кафедри міжнародного права
Національний авіаційний університет

На сьогоднішній день кіберзагрози становлять один із найбільш значних викликів глобальній і національній безпеці та потребують відповідальної поведінки держав у кіберпросторі шляхом застосування міжнародно-правових норм, здійснення практичних заходів щодо забезпечення кібербезпеки. Виникла гостра необхідність у розробці механізмів гарантування безпечного використання мережі Інтернет, створенні мережевих інфраструктур, науковій роботі та розробок, проведенні відповідних заходів, як освітнього, так і практичного характеру.

Як зазначає Пазюк А.В.: «Розвиток інформаційно-комунікаційних технологій та їхній глобальний транскордонний вплив на суспільне життя усього людства спричинив появу новітньої планетарної соціальної

інфокомунікаційної сфери – кіберпростору, що є свідченням переходу людства у своєму розвиткові до фази так званого «інфокомунікаційного суспільства». А міжнародне право відіграє ключову роль у забезпеченні соціального прогресу шляхом вироблення загальнолюдських правових норм для усіх суб'єктів правових відносин у кіберпросторі [1, с. 5].

Їх визнання призвело до закріплення свобод і рамок контролю потоків інформаційної комунікації в Інтернеті у міжнародному праві і стало пріоритетним завданням міжнародної спільноти, міжурядових організацій як на універсальному, так і регіональному рівнях.

Інформаційні та комунікаційні технології (ІКТ) повинні бути використані для зміцнення системи освіти, поширення знань, доступу до інформації, якості та ефективності навчання, і більш ефективного надання послуг.

Взаємодію понять «освіта» та «інформаційна безпека» можна розглядати з двох боків. По-перше, інформаційна безпека стає дедалі більш актуальною у процесі навчання та викладання. На кожній стадії освітнього процесу як здобувачі освіти так і викладачі стикаються з певними ризиками та небезпеками, які виникають у процесі їхньої взаємодії з інформаційним середовищем. Наприклад, для початкової та середньої освіти актуальною є поширення в мережі Інтернет контенту, який може спонукати до жорстокості, має деструктивне ідеологічне забарвлення. Нещодавно постала також проблема кібертерору (кібербулінгу), тобто психологічного насильства через Інтернет, яка часто дає поштовх у доведенні до самогубства. Для університетів, які займаються науковими розробками, актуальності набуває безпека даних.

З іншого боку, інформаційна безпека є складовою поняття «національна безпека», тому для будь-якої держави вона має пріоритетний характер. Таким чином, держави постають перед гострою потребою у професійних кадрах, забезпеченням якими займається освітній сектор [2]. Також важливе значення має визнання, сертифікація та акредитації знань, навичок і компетенцій, отриманих через формальну і неформальну освіту.

На сьогоднішній день у розвинених країнах спеціальність «інформаційна безпека» користується великим попитом. Цікавим є досвід США з реалізації освітніх проектів у рамках Національної ініціативи з кіберосвіти (NICE). Популярними є напрямки «інформаційна безпека», яка включає такі програми як «біометрика та інформаційна безпека», «інформаційна безпека та управління ризиками»; «комп'ютерна безпека», куди входять програми «комп'ютерна і мережева безпека», «комп'ютерні системи безпеки»; «розслідування комп'ютерних інцидентів», що охоплює програми «розслідування кіберзлочинів»; та «безпека комп'ютерних мереж», куди також входить програма «безпека безпровідних мереж» [3]. Загалом, за спеціальністю «кібербезпека» у США нараховується близько 50 програм. На тлі тотальної інформатизації суспільство все більше потребує спеціалістів зі знанням інформаційних технологій. Таку тенденцію неважко прослідкувати, адже, на багатьох спеціальностях, які не пов'язані з комп'ютерними технологіями взагалі, студенти можуть вивчати ІТ в якості курсу на вибір, як мінімум. Яскравим прикладом є С'юзан Войчицьки, генеральний директор YouTube, яка закінчила курси з вивчення комп'ютерів CS50 навчаючись на

історичному факультеті, і стала однією із самих впливових жінок у світі технологій. З іншого боку, спеціальності технічного напрямку готують спеціалістів з розвинутими управлінськими здібностями та здатністю вирішувати задачі й приймати рішення. Так, наприклад спеціальність «розслідування комп'ютерних інцидентів», яка поєднує галузь інформаційної безпеки з комп'ютерною криміналістикою та кримінальними правом. Студенти вчаться не лише аналізувати дані та шукати докази, але й проходять такі курси як «публічні виступи», «судові процеси».

В умовах сьогодення по всьому світу наразі відчувається все більша нестача кваліфікованих фахівців і практиків в галузі кібербезпеки. І державні, і недержавні центри досліджень припускають, що до 2022 року налічуватиметься близько 1,8 млн. вакантних робочих місць в галузі кібербезпеки [4]. З метою підготовки необхідних фахівців, кафедри та факультети всіх комп'ютерних наук запускають ініціативи зі створення нових програм з кібербезпеки або введення спеціальних дисциплін у межах існуючих програм.

В даному випадку слід особливо виділити фундаментальні дослідження та вищу освіту, оскільки вони дозволяють готувати викладачів, які, у свою чергу, зможуть готувати системних як адміністраторів так і спеціалістів з кібербезпеки у різних галузях [5]. Крім того, акцент на фундаментальних дослідженнях призведе до зростання кількості дослідницьких факультетів і, таким чином, кількість людей, освічених в цій галузі зростатиме.

Література:

1. Пазюк А.В. Міжнародне інформаційне право: теорія і практика: монографія. Київ, 2015. 447 с.

2. Towards Changes in Information Security Education. *Journal of Information Technology Education.* 2006. URL: http://jite.org/documents/Vol5/v5p221-233Hentea148.pdf (дата звернення: 11.10.2018).

3. Підготовка кадрів інформаціонної безпеки в США. URL: https://cyberleninka.ru/article/v/podgotovka-kadrov-v-oblasti-informatsionnoy-bezopasnosti-v-ssha (дата звернення: 12.12.2018).

4. Steve Morgan. Cybersecurity job market to suffer severe workforce shortage. URL: https://www.csoonline.com/article/3201974/it-careers/cybersecurity-job-market-statistics.html.

5. Mariana Hentea. A Perspective on Achieving Information Security Awareness. *Issues in Informing Science and Information Technology.* Southwestern Oklahoma State University, Weatherford, USA. 2015. P. 169-178. URL: http://proceedings.informingscience.org/InSITE2015/I14f89Hent.pdf (дата звернення: 12.12.2018).