Literature

1. Shane J N (2019) Diplomacy and drama: the making of the Chicago Convention. *Air and Space Lawyer,* 32 (4: Special Issue), (2019), 1-24.

2. International Civil Aviation Organization (ICAO), *Convention on Civil Aviation ('the Chicago Convention'),* 7 December 1944, (1994) 15 U.N.T.S. 295, available at: https://www.refworld.org/docid/3ddca0dd4.html

3. Abeyratne, Ruwantissa, Legal and regulatory issues in international aviation. UK: *Transnational Publisher*, 1996. 260 p.

4. Jorge E. Núñez. Territorial Disputes and State Sovereignty: International Law and Politics. The Netherlands: Routledge research in international law, Taylor & Francis Group, 2020. 220 p.

5. Moon Jr. Albert I. (1963) A Look at Airspace Sovereignty. *Journal of Air Law and Commerce,* Vol. 29, Issue 4, Art. 4, pp. 328-345.

6. Cooper J.C. The Chicago Convention - After Twenty Years, *Journal of Air Law and Commerce*, Vol. 19, Issue 3, Art. 1. 1965. p. 333-344.

УДК 340.113:004.056 (477) (043.2)

Гавва С.К., здобувачка вищої освіти
другого (магістерського) рівня,
Головко С.Г., к.і.н., доцент,
Національний авіаційний університет, м. Київ, Україна

СУЧАСНИЙ КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Модернізація суспільства та розвиток інформаційних технологій призвели до масового використання ресурсів Інтернету. З появою глобальної мережі виник один з найбільш небезпечних різновидів кіберзлочинності, а саме кібертероризму, який під час терористичних акцій вдається до новітніх досягнень науки і техніки.

Уперше термін «кібертероризм» був використаний 1980 року старшим науковим співробітником Каліфорнійського інституту безпеки і розвідки Баррі Колліном. У ті роки мережа ARPANET Управління перспективних розробок Міноборони США об'єднувала всього кілька десятків комп'ютерів. Дослідник був упевнений, що з часом можливості кібермереж будуть використані терористами, хоча і вважав, що станеться це приблизно у першому десятилітті XXI ст. [1].

На сучасному етапі терористи активно використовують можливості мережі Інтернет, а саме: легкий доступ до мережі, практично повна відсутність цензури, великий масштаб аудиторії, анонімність тощо. У наші дні вони розглядають глобальну мережу головним чином як засіб пропаганди та передачі інформації.

Директор Джорджтаунського інституту забезпечення безпеки інформації при Університеті Джорджтауна та експерт Центру досліджень тероризму США Дороті Деннінг вважає, що діяльність терористів в мережі Інтернет можна розділити на три групи: активність, хакерство та кібертероризм. Під активністю пропонується розуміти просте використання комп'ютерних технологій з метою пропаганди ідей, залучення коштів і нових послідовників.

Під хакерством розуміються протизаконні атаки на комп'ютерні мережі, секретні бази даних і сайти для отримання будь-якої інформації або розкрадання грошей. Кібертероризм, хоча і схожий за способами здійснення з хакерством, але все ж представляє собою, на думку Деннінг, зовсім інший вид комп'ютерних атак, який планується з іншими цілями, а саме: нанесення великої шкоди життєво важливим об'єктам інфраструктури за допомогою інформаційних технологій [2].

Кібертероризм, який стає все більш привабливою формою для терористичних організацій, має такі властивості: високий ступінь анонімності, відсутність необхідності розташування поряд з метою.

Кібертероризм несе значну загрозу як для національної, так і для загальної безпеки держави і суспільства, у зв'язку з тим, що кібератаки відбуваються на найбільш значущі для держави і світової спільноти об'єкти. Він може здійснюватися у вигляді протизаконного доступу до даних, впливу на системи даних шляхом їх блокування, пошкодження та знищення. Як один із видів тероризму, кібертероризм завжди переслідує цілі, пов'язані з чиненням тиску на органи влади, міжнародні організації, залякуванням населення, дестабілізацією інфраструктури, що є істотною відмінністю від інших злочинів у кіберпросторі. Акти комп'ютерного тероризму загрожують виникненням політичних та економічних криз світового масштабу. Тому є необхідність об'єднання сил держави та держав на світовій арені для боротьби з цим негативним явищем.

Наразі Україна переживає найбільшу кількість кібератак за всю свою історію. Через три дні після лютневого вторгнення росії кібератаки на державно-військовий сектор України зросли на 196% порівняно з довоєнним періодом [3]. Рекордом стали 275 DDoS-атак, тобто атаки на комп'ютерні системи органу, організації, установи з метою порушення доступності вебресурсів, що атакуються.

За даними Головного управління розвідки Міністерства оборони України ворог здійснює масовані кібератаки на об'єкти критичної інфраструктури українських підприємств та установ критичної інфраструктури союзників України. Ворожі кібервійська координують дії з наземними та ракетними атаками. Активність російських хакерів не зменшується, вони й далі намагаються атакувати українську інфраструктуру, не гребуючи цивільними цілями.

На сьогоднішній день нормативна правова база протидії кібертероризму як на національному, так і на міжнародному рівні знаходиться лише на стадії розробки. Від того, наскільки якісно і швидко будуть розроблені нові, сучасні нормативно-правові акти у цій сфері, безпосередньо залежить ефективність діяльності державних органів, включаючи питання міжнародної співпраці.

Отже, здійснення високотехнологічних терористичних актів у XXI ст. здатне викликати глобальну інформаційну кризу і поставити під загрозу існування окремих регіонів світу. Тому світ має об'єднати свої зусилля для подолання зазначеної проблеми.

Література

1. Krasavin S. Computer Crime Research Center (CCRC). URL: http://www.crime-research.org/library/Cyber-terrorism.htm.

2. Denning D.E. Is Cyber Terror next? *SSRC – Social Science Re-search Council*. URL: https://items.ssrc.org/after-september-11/is-cyber-terror-next/.

3. Курочко Н. Як росія та Україна воюють на кіберфронті. URL: https://www.epravda.com.ua/columns/2022/09/28/691925/.

УДК 343.95(043.2)

Грубінко А.В., д.і.н., професор,
Західноукраїнський національний університет, м. Тернопіль, Україна

ОКРЕМІ АСПЕКТИ ПСИХОЛОГІЧНОЇ ПІДГОТОВКИ ПРАВНИКА

Використання науки психології може налаштувати правників на ідеї, які важко відкрити органічно, і допомогти юристам уникати помилкових висновків зі свого досвіду на практиці. Психологія робить великий внесок у вирішення широкого спектру завдань правника. Для суспільної практики важливі правники, які знаються на когнітивній та соціальній психології, більш ефективні в таких завданнях, як опитування клієнтів і свідків, консультування клієнтів, ведення переговорів і посередництво, проведення розшуків і належної обачності, писати, етично поводитися, бути продуктивним і успішним, та зрештою бути щасливим.

Незважаючи на важливість міжособистісних аспектів адвокатської діяльності та корисність психології для оволодіння цим аспектом професії, навчальні програми закладів вищої освіти включають відносно мало знань психології. Тим не менш, навіть заклики додавати більше практичних навичок у фаховій юридичній підготовці особливо не акцентують увагу на тому, що юристам потрібні хороші міжособистісні навички комунікації і прийняття рішень [1].