4. Стивен Ливингстон. Международное право в области прав человека и содержание под стражей // Интерайтс Бюллетень. – 2002. − № 6. [Електронний ресурс]. – Режим доступу: http://www.hrights.ru/text/inter/b6/Chapter81. htm

5. Толстенко Ю. О. Діяльність міжнародних неурядових організацій в пенітенціарній сфері / Ю. О. Толстенко // Юридична осінь 2013 року: матер. наук.-пр. конф. мол. учених та здобувачів (м. Харків, 14 листопада). – Харків: НУ «ЮАУ ім. Я. Мудрого»: Право, 2013.

6. Толстенко Ю. О. Практика Європейського суду з прав людини у сфері захисту прав та свобод засуджених до кримінальних покарань / Ю. О. Толстенко // Особистість. Право. Суспільство.: матеріали міжн. наук.-пр. конф., присв. 10-ти 21 річчю Полт. юр. інституту (м. Харків, 15 березня 2012 р.). – Харків.: «Точка», 2012.

Діхтярь А.В.
студентка,
Науковий керівник: **Бруслик О.Ю.**
кандидат юридичних наук, асистент,
Полтавський юридичний інститут
Національного юридичного університету
імені Ярослава Мудрого

КІБЕРНЕТИЧНИЙ ТЕРОРИЗМ ЯК ФОРМА ТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ: МІЖНАРОДНИЙ АСПЕКТ

На сьогодні, враховуючи сучасні тенденції розвитку інформаційного суспільства, виникає проблема, обумовлена появою нових загроз соціальній інженерії, зокрема, кібертероризм як засіб здійснення маніпулятивного впливу на населення відповідної держави.

Слід зазначити, що на доцільності розгляду питання стосовно запобігання інформаційному терору, у тому числі кібернетичному тероризму, в аспекті міжнародної безпеки, вперше було наголошено у Резолюції No 60/45 «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки», яка була прийнята на сесії Генеральної Асамблеї ООН. Так, було зазначено, що поширення та використання інформаційних технологій і засобів зачіпають інтереси всієї міжнародної спільноти; ці технології та засоби потенційно можуть бути використані з метою дестабілізації міжнародної безпеки як у воєнній, так і в цивільній сферах [1].

Саме поняття кібертероризму як на рівні національного, так і міжнародно-правового регулювання залишається невизначеним, оскільки зумовлюється суперечливою правовою природою такої форми терористичної діяльності. Одна частина науковців надає даній дефініції досить широкого значення, включаючи до неї кіберзлочинність, коли в дійсності обидва поняття не є синонімами і мають бути відокремлені один від одного; інша – ототожнює інформаційний терор з кібернетичним, що також є невірним, адже такі явища співвідносяться між собою як ціле та частина. Утім, переважна більшість науковців схиляються до позиції, що кібертероризм являє собою тероризм, що спланований, вчинений чи скоординований у кіберпросторі,

тобто в терористичних акціях використовуються досягнення науки і техніки в галузі новітніх інформаційних технологій [2, с. 13].

Отже, фактично для кваліфікації кібернетичного тероризму необхідною є наявність, передусім, мети терористичної діяльності, яка має бути реалізована шляхом вчинення відповідних дій у кіберпросторі. Враховуючи пріоритет міжнародно-правових норм, для визначення мети тероризму і, як наслідок, його вищезазначеної форми, варто керуватися положеннями Шанхайської конвенції про боротьбу з тероризмом, сепаратизом та екстремізмом, в якій передбачено, що спрямованість на те, щоб викликати смерть фізичної особи або заподіяти їй тяжке тілесне ушкодження, завдати шкоди будь-якому матеріальному об'єкту, а також залякати населення, порушити громадську безпеку або змусити органи влади або міжнародну організацію вчинити будь-яку дію чи утриматися від її здійснення становлять мету тероризму [3]. Поняття «кіберпростір» як обов'язковий елемент об'єктивної сторони даного складу злочину передбачений у Рекомендації ЮНЕСКО «Про розвиток та використання багатомовності та загальному доступі до кіберпростору» від 2003 р., яка являє собою чи не єдиний міжнародний документ, де зазначено сутність даної дефініції. Так, кіберпростором є віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою [4].

Варто зауважити, що на практиці кібертероризм найчастіше спрямовується задля здійснення пропагандистського впливу на громадську думку та виведення з ладу віртуальної інфрастуктури. Стосовно першого виду кібернетичного тероризму, то на сьогодні основну його ціль складає досягнення того факту, щоб терористичний акт отримав суспільний резонанс, наприклад, за допомогою інтернету або ЗМІ як основних інструментів інформаційного впливу на соціум. Нині, в умовах проведення інформаційної війни, терористичним організаціям створено умови для використання кіберпростору для здійснення розповсюдження пропаганди серед населення, наприклад, у зв'язку з функціонування відповідних веб-сайтів терористичних угрупувань.

Другий вид кітертероризму безпосередньо має на меті проведення так званих «підривних атак», до яких належить порушення нормальної роботи комп'ютерних систем такими засобами, як «електронні бомби», надсилання «інформаційного сміття» та хакерські методи псування змісту веб-сайтів, які, як правило, не призводять до незворотних наслідків, однак можуть викликати безлад та тягти за собою значні економічні збитки [5, с. 52]. Так, прикладом безпосередньої реалізації даного виду кібернетичного тероризму на практиці стало запровадження у червні 2017 року так званого вірусу Petya, від поширення якого низка комерційних та державних структур зазнала відповідних економічних втрат у більш ніж 60 країнах світу. За офіційними даними розмір матеріальних збитків від проведеної кібератаки становить близько 8 млрд доларів, що були отримані внаслідок легального оновлення M.E. Doc. У зв'язку з цим можна стверджувати, що такий акт кібертероризму завдав значної шкоди матеріальним об'єктам не лише на локальному та державному, а й навіть на міжнародному рівнях, з огляду на що актуалізується

питання стосовно збільшення фінансування захисту кіберпростору в окремих країнах та здійснення інших превентивних заходів проти подальшого становлення та функціонування кібернетичного тероризму.

Таким чином, кібертероризм на сучасному етапі являє собою загрозу як національній, так і міжнародній безпеці, адже становить необхідну приналежність до самої терористичної діяльності в умовах глобалізації. Для протидії та запобіганню проявам кібернетичного тероризму, варто криміналізувати таке діяння у національному законодавстві держав, де його не передбачено як кримінально каране, а також створити міжнародні механізми превенції та мінімізації даного виду правопорушення у міжнародному інформаційному просторі.

Список використаних джерел:

1. Резолюція «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» : ООН; Резолюція, Міжнародний документ від 08.12.2005 № 60/45 [Електронний ресурс]. – http://zakon2. rada.gov.ua/laws/show/995_e45

2. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / Б.М. Романюк, В.Д. Гавловський, М.В. Гуцалюк та ін. ; за заг. ред. проф. Я.Ю. Кондратьєва. – К.: Паливода А.В., 2004. – 144 с.

3. Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом : от 15 июня 2001 г. [Электронный ресурс]. – Режим доступа: http://www.conventions.ru/ view_base.php? id=1070.

4. Рекомендация о развитии и использования многоязычия и всеобщем доступе к киберпространству [Электронный ресурс]. – Париж, ЮНЕСКО, 2003. – Режим доступа: http://www.unesco.org

5. Мережі і мережеві війни. Майбутнє терору, злочинності та бойових дій / за ред. Дж. Арвкілла, Д. Ронфельдт. – К.: Києво-Могилянська академія, 2005. – 350 с.

Коляда І.С.
студентка,
Національний юридичний університет
імені Ярослава Мудрого

М'ЯКЕ ПРАВО ЯК СПОСІБ РЕГУЛЮВАННЯ МІЖНАРОДНИХ ВІДНОСИН

Загальновизнаним є твердження, що виникнення поняття «м'якого права» обумовлено стрімким розвитком міжнародних відносин, їх урізноманітненням і ускладненням їхнього змісту. Питання природи, структури та взагалі явища «м'якого права» навіть сьогодні породжує численні дискусії та відзначається значною неоднорідністю поглядів на них, що свідчить про актуальність цієї проблеми.

У теорії сучасного міжнародного права до сьогодні не існує єдності у поглядах щодо того, чим є «м'яке право» і які саме норми охоплюються цим поняттям.