***Задорожна А.Ю.***
*Херсонський національний технічний університет, студентка*
***Бараненко Р.В.***
*Херсонський факультет Одеського державного університету внутрішніх справ, професор кафедри професійних та спеціальних дисциплін, кандидат технічних наук, доцент*

# ДО ПИТАННЯ ВИЗНАЧЕННЯ ТЕРМІНУ «КІБЕРТЕРОРИЗМ»

На сьогоднішній день немає досить чіткого визначення поняття «кібертероризм». Термін доволі спірний, тому деякі автори обирають дуже вузьке визначення. Різні правові системи й урядові установи використовують різні визначення. Більш того, уряди різних країн неохоче узгоджують юридично зобов'язуюче визначення. Ці труднощі виникають через те, що цей термін є політично й емоційно зарядженим [Hoffman (1998), p. 23, See review in The New York Times Inside Terrorism]. Для того, щоб уникнути такого роду плутанини, пропонується використовувати найбільш загальне визначення кібертероризму, що включає до себе наступне [http://www.sagepub.com/sites/default/files/upm-binaries/5n72_ch_1 .pdf]:

Кібертероризм - це застосування насильства або загрози насильства з використанням засобів комп’ютерної техніки й телекомунікаційних мереж, з метою створення політичних, релігійних чи ідеологічних змін. Він може бути здійсненим тільки недержавними суб'єктами чи агентами, які працюють від імені своїх урядів.

Також кібертероризм можна визначити, як умисне використання комп'ютера, мереж та інтернет-простору з метою викликати руйнування й завдати шкоду для особистих цілей [Matusitz, Jonathan (April 2005). "Cyberterrorism:". American Foreign Policy Interests. 2: 137-147]. Цілі можуть бути політичними або ідеологічними, оскільки це може розглядатися як форма тероризму ["India Quarterly : a Journal of International Affairs". 42-43. Indian Council of World Affairs. 1986: 122. The difficulty of defining terrorism has led to the cliche that one man's terrorist is another man's freedom fighter].

Існує дискусія з приводу основного визначення обсягу кібертероризму. Існує розподіл на категорії за мотивацією, цілями, методами й центральним місцем використання комп'ютера в акті. Залежно від контексту, кібертероризм може значно перекриватися з кіберзлочинністю, кібервійною або звичайним тероризмом [What is cyberterrorism? Even experts can't agree at the Wayback Machine (archived November 12, 2009). Harvard Law Record. Victoria Baranetsky. November 5, 2009].

Якщо кібертероризм розглядати аналогічно традиційному тероризму, то він включає до себе тільки атаки, які ставлять під загрозу майно або життя, його може бути визначено як більш ефективне використання обчислювальної техніки та інформації на виконання завдань, зокрема, через Інтернет, викликаючи фізичну, реальну шкоду чи серйозні порушення об’єктів критичної інфраструктури.

Деякі дослідники заявляють, що кібертероризму не існує, й це дійсно питання злому або інформаційної війни [Harper, Jim. "There's no such thing as cyber terrorism". RT. Retrieved 5 November 2012]. Вони не згодні із загальноприйнятим визначенням, обґрунтовуючи це через неправдоподібність створення страху, значної фізичної шкоди або смерті в популяції з використанням електронних засобів, з урахуванням поточної атаки й захисних технологій.

Вікіпедія описує кібертероризм досить просто, як «акт інтернет - тероризму в терористичній діяльності, в тому числі акти навмисного, великомасштабного руйнування комп'ютерних мереж, особливо персональних комп'ютерів, підключених до інтернету, з використанням допоміжних засобів таких, як комп'ютерні віруси» [https://en.wikipedia.org/wiki/Cyberterrorism].

Марк Політ, спеціальний агент ФБР, запропонував робоче визначення кібертероризму, як «навмисний, політично мотивований напад на інформацію, комп'ютерні системи, комп'ютерні програми й дані, що призводить до насильства проти небойових цілей і проведений субнаціональними групами або таємними агентами»

[http://searchsecurity.techtarget.com/definition/cyberterrorism].

Крім того, щоб кваліфікувати напад як кібертероризм, він має привести до насильства проти осіб або майна, або принаймні, причинити досить шкоди, щоб генерувати страх. Атаки, які призводять до смерті або тілесних ушкоджень, вибухів або серйозних економічних втрат, є тому прикладами. Серйозні напади на об’єкти критичної інфраструктури можуть бути актами кібертероризму, в залежності від їх впливу.

Важливо розрізняти кібертероризм і «хактивізм», термін, введений ученими, щоб описати суміш злому з політичною активністю. (Під «зломом» тут розуміється прихована діяльність, здійснювана в Інтернеті, яка прагне виявити, маніпулювати або іншим чином використовувати вразливості в комп'ютерних операційних системах та іншому програмному забезпеченні. На відміну від хактивістів, хакери, як правило, не мають політичних цілей). Хактивісти мають чотири основні види зброї в їх розпорядженні: віртуальні блокади; атаки електронної пошти; злом і проникнення до комп'ютерів; комп'ютерні віруси й черв'яки [https://www.usip. org/sites/default/files/sr119.pdf].

Існує три рівня кібертерору за можливостями, визначених групою Monterey [Dorothy E. Denning (May 23, 2000). "Cyberterrorism". cs.georgetown.edu. Archived from the original on March 10, 2014. Retrieved June 19, 2016]:

- *Простий неструктурований:* можливість проводити основні атаки проти окремих систем, що використовують інструменти, створені кимось іншим. Організація має невеликий цільовий аналіз, управління й контроль або здатність до вивчення.

- *Просунуто-структурована:* можливість проводити більш складні атаки проти декількох систем або мереж і, можливо, модифікувати або створювати базові інструменти злому. Організація має елементарний об'єкт аналізу, управління й контролю, а також здатність до вивчення.

- *Комплексно-координоване*: можливість до скоординованих атак, здатних

викликати масове руйнування проти інтегрованих гетерогенних систем захисту (в тому числі криптографічних). Можливість створювати складні інструменти злому. Організація має дуже ефективний цільовий аналіз, управління й контроль, а також здатність до вивчення.

Тому сьогодні Україні доречно вживати активних кроків на шляху розбудови власної системи кібербезпеки. Постійні кібератаки проти США та ЄС з боку хакерів з Російської Федерації та КНР, а також проти Естонії (2007), Грузії (2008), Канади (2011) підтверджують актуальність досліджень в цьому напрямку.