Муравська (Якубівська) Ю.Є.
к.е.н., доц., доц. кафедри економічної безпеки та фінансових розслідувань
Тернопільський національний економічний університет

ФОРМУВАННЯ ПОНЯТІЙНОГО АПАРАТУ У СФЕРІ КІБЕРБЕЗПЕКИ: ІНОЗЕМНИЙ ДОСВІД ТА НОРМАТИВНО-ПРАВОВА РЕГЛАМЕНТАЦІЯ

На сьогодні існує розгалужена система термінів, які окреслюють безпекове поле «ІТ-простору», однак гострою залишається питання їх нормативного формулювання, насамперед власне категорії «кіберпростір». Незважаючи на активне вживання термінів з приставкою «кібер», дотепер нормативно ненормованим є фундаментальне поняття кіберпростору як сфери реалізації потенційно загрозливих дій проти держави, суспільства чи людини. Неодноразово автори офіційних документів (в тому числі документів у сфері безпеки НАТО) використовують його, залишаючи оцінку на за читачем відповідно до ступеня його ерудиції. Порівняно усталеним є визначення кіберпростору як особливого, самостійного виду простору, який охоплює не тільки виключно інформаційну інфраструктуру, але й чітку частку власне інформаційного простору (інформації, яка в ньому циркулює).

В урядових матеріалах Європейського Союзу можна знайти наступне формулювання кіберпростору: «це віртуальний простір, в котрому циркулює електронна інформація світових ПК» [2].

В документі у сфері безпекознавства Англії під назвою «Стратегія безпеки кіберпростору для Об'єднаного Королівства» кіберпростір ідентифікується як «усі типи мережевої цифрової активності, який включає в себе дії та контент, які здійснюються через цифрові мережі»[1]. У той же час категорія «кіберпростір» так і не ідентифікована в єдиному на сьогоднішні міжнародному документі, що направлений на протидію злочинам у кіберсфері під назвою «Конвенція про кіберзлочинність».

В прийнятій у 2011 році в Німеччині «Стратегії кібербезпеки» кіберпростір визначається як «доступна через Інтернет інформаційна інфраструктура, яка перебуває поза територіальними межами» [2].

У «Національній стратегії кібербезпеки» Нідерландів [2] узагалі не згадується жодного разу категорія «кіберпростір».

В стратегічних документах Франції під назвою «Біла книга національної безпеки та оборони» [3] та «Оборона та безпека інформаційних систем. Стратегія для Франці» [2] формулювання поняття кіберпростору розпорошене по цілому документу.

«Національна військова стратегія США» визначає кіберпростір як «... поле, що визначає можливість вживання електромагнітних та електронних засобів для запам'ятовування, модифікації та обмінювання відомостями через мережеві системи та пов'язану з ними фізичну інфраструктуру». Дане формулювання було покладено в основу також і опрацьовування документа «Кіберкомандування повітряних сил» (2008 р.) та «Стратегії національної безпеки США» (2010 р.). У той же час комплексний документ з оцінювання стану кібербезпекового простору США та імовірних напрямів його поліпшення під назвою «Кібербезпековий огляд США» 2009 року визначає кібербезпеку у відповідності до формулювання, поданого у Президентській Директиві з національної безпеки, а також у Президентській Директиві з внутрішньої безпеки, які розкривають кіберпростір як «...комп'ютерні системи, взаємозалежні мережі, IT-інфраструктури, які включають телекомунікаційні мережі, Інтернет, комп'ютерні процесори, а також контролери у важливих сферах», користуючись поняттям, запозиченим з іншого документа Збройних сил США – «Словник воєнних та пов'язаних з даною сферою термінів». Головною відмінністю поміж наведеними дефініціями є наголос на гуманітарній або технологічній складовій. Якщо формулювання запропоноване в «Національній військовій стратегії для дій у кіберпросторі» робить основоположним елементом власне інформацію, яка формується або переходить за допомогою предметної інфраструктури, то дефініція з

«Кібербезпекового огляду» зосереджує увагу виключно на інфраструктурі, лишаючи поза увагою інформацію, яка в ній циркулює [4]. Зважаючи на той факт, що обидва формулювання були запропоновані Збройними Силами США, можемо дійти висновку, що стале поняття кіберпростору на сьогодні відсутнє, як і відсутня відповідна дефініція і в документах інших країн.

Зважаючи на вищевказане, можемо стверджувати, що незважаючи на широке вживання поняття «кіберпростір» як у офіційних документах, так і в науковій літературі, фігурують переконливі сумніви відносно перспективи його використання у суто прикладній сфері. Значною мірою власне через це переважна більшість країн світу продовжують протидію злочинницьким діянням в кіберпросторі, користуючись «традиційним» законодавством (зокрема, щодо питання порушення функції телекомунікаційних мереж, одержання несанкціонованого доступу до інформації).

Зважаючи на вищезазначену термінологічну невпорядкованість у відношенні до фундаментального поняття, складнішим постає питання дефініції похідних від нього категорій, які активно вживаються в офіційних документах більшості країн світу та організацій у сфері безпекознавства, а саме: «кібертероризм», «кібербезпека», «кібератака», «кібервійна», «кіберзахист», «кіберзброя» тощо. Станом на сьогодні переважна більшість цих понять є сильно узагальненими, а у їх визначенні щораз частіше проявляється політична складова. Найбільш яскраво це виражається у вживанні понять «кібервійна» та «кібертероризм».

В дійсності ж, до сьогодні переважна більшість небезпек критично важливій інфраструктурі інформаційно розвинених держав (як наприклад, Бельгія, Великобританія, США, Німеччина, Японія) доходили не від окремих терористичних груп, які лише переробили тактику здійснення власної інформаційної війни, а від свідомо підготовлених, матеріально та інформаційно забезпечених спеціалізованих груп, які діють в інтересах певних країн і є реально продовженням дії їх так званої «воєнної машини».

Практичне формулювання «кібертероризму», запропоноване співробітником ФБР США Полліттом М., звучить наступним чином: «Кібертероризм - це планова, політично умотивована атака проти комп'ютерних систем, інформації, комп'ютерних програм, внаслідок якої відбуваються злочинні дії з боку спеціалізованих груп чи таємних агентів» [4].

Варто зауважити, що в контексті чинного на сьогодні вітчизняного нормативно-правового поля зазначена проблема приймає інший кшталт, адже в Законі України «Про боротьбу з тероризмом» у формулюванні поняття «тероризм» відсутнє положення про політичну мотивацію терористичної дії, а у визначенні поняття «технологічний тероризм» однією з умов зауважено власне вчинення «з терористичною метою із використанням… комп'ютерних систем та комунікаційних мереж» [5].

Саме тому, «технологічним тероризмом» потенційно може бути названо і замах або простий «злам» сайту фізичної особи, приватної компанії чи навіть державного органу.

Отож, питання формулювання еквіваленту категорії «кібертероризм» у вітчизняному законодавстві є елементом більш широкого питання щодо потреби в перегляді поняття «тероризм».

Значно вищого ступеня політизації набуває вживання категорії «кібервійна», яка останнім часом щораз частіше застосовується високопосадовцями європейських країн, в тому числі в офіційних документах і виступах. У переважній більшості випадків під вказаним терміном розуміються небезпеки для інформаційної інфраструктури, або система кібератак на інформаційні мережі та об'єкти критичної інфраструктури власне країни. На даному фоні актуалізуються намагання схарактеризувати кібервійну як конфігурацію класичної війни з придатними наслідками та перспективами для військових організацій (включно з ймовірністю відповіді на кібернапад кінетичною зброєю).

Світове співтовариство й до сьогодні не напрацювало відповідного набору правил, принципів, норм, які б регулювали інформаційну безпеку на

інтернаціональному рівні і надавали адекватно допустимий порядок реалізації у кіберпросторі власне воєнних операцій, а також формували перспективу зберігання нейтралітету, так само, як це прийнято в класичних війнах. Це, наприклад, актуально для України, котра офіційно оповістила про прагнення отримати позаблоковий статус, однак, потенційно може стати жертвою кібернападів у випадку гострої сутички протиборчих військових блоків або сил.

Закономірність вживання поняття «кіберпростору», а також похідних від нього, є об'єктивною необхідністю у сфері безпекознавства в контексті протидії теперішнім загрозам національній безпеці від протиправного застосування новітніх інформаційних технологій. Така потреба обумовлена насамперед ширшим, ніж вживання категорій «злочини, які здійснюються за допомогою інформаційних технологій» або «комп'ютерні злочини», охопленням потенційних проблемних питань у сфері безпекознавства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space [electronic resource]. - Access: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

2. Cyber Security Strategy / European Union Agency for network and information security [electronic resource]. - Access: http://www.enisa.europa.eu/media/news-items

3. The French White Paper on defence and national security [electronic resource]. - Access:
http://www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/white_paper_press_kit.pdf

4. What is Cyber-terrorism? [[electronic resource]. - Access: http://www.crime-research.org/library/Cyberterrorism.htm

5. Про боротьбу з тероризмом : закон України [Електронний ресурс]. – Режим доступу:http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=638-15