УДК 340+35.078.3

БЕЙКУН Андрій Леонардович,
викладач кафедри забезпечення державної безпеки Київського інституту Національної гвардії України
кандидат юридичних наук, доцент,

ПРАВОВЕ ВИЗНАЧЕННЯ ТА ПОЗИЦІОНУВАННЯ РІЗНОВИДІВ «ІНФОРМАЦІЙНОЇ» ЗБРОЇ ТА ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Науковий інтерес до проблеми як тероризму взагалі, так і окремих його видів, об'єктивно посилився з початком повномасштабної збройної агресії російської федерації проти України. Це обумовлено тим, що тероризм як форма збройної, інформаційної чи інших видів боротьби, є найефективнішою формою не просто опору, а й будь-якої сучасної війни. Остання (форма) не має чіткої лінії фронту, будь-яких правил поведінки, відносин шляхетності, на неї не поширюються правила війни, норми міжнародного гуманітарного права.

На даний час, як на нормативно-правовому рівні, у програмних документах та теоретичних позиціях науковців не існує єдиного розуміння щодо понятійних категорій та змістового навантаження у сфері: інформаційної безпеки/небезпеки, інформаційних/кібернетичних загроз, інформаційної/ кібернетичної війни/агресії, інформаційного/кібернетичного тероризму, інформаційної/кібернетичної зброї.

Разом з тим, усіма розуміється як потенційна особлива небезпека використання сучасних технологій в якості інформаційної зброї для комп'ютерних систем органів державної влади, управління військами, баз обліку даних, фінансами і банками та економікою країни в цілому, дезорганізації населення, так і можливі алгоритми їх (технологій) використання.

За своєю результативністю інформаційна зброя може прирівнюватись до зброї масового ураження. З початком відкритої фази кібернетичної війни, в першу чергу, будуть зроблені кібернетичні атаки на комп'ютерні системи і сервери органів державного та військового управління, правоохоронних органів, банківських установ, атомних електростанцій тощо. Ці атаки можуть бути підкріплені активацією комп'ютерних вірусів, закладених ще в мирний час та використанням спеціальних пристроїв, які при вибуху створюють потужний електромагнітний імпульс, або біологічних засобів, здатних знищувати електронні схеми чи ізолюючі матеріали в комп'ютерах [1, с. 19].

Зрозуміло, що окреслення у правовому полі визначених вище категорій, надання їм правового змісту, можливе лише при наявності розуміння відповідних процесів як у національному, так і світовому інформаційному просторі.

Як зазначає О.Д. Довгань, процеси, що відбуваються в глобальному інформаційному просторі характеризуються такими основними тенденціями та особливостями:

– сучасна інформаційна ера, як свідчать уроки інформаційної агресії проти України, змінює традиційні уявлення про символи могутності й способи

досягнення світового панування; розвиток інформаційної сфери не визнає національно-державних меж і веде до утворення глобальних інформаційних мереж та інформаційних ресурсів, що нав'язують свої стандарти поведінки й мислення;

– змінюється роль і місце військово-політичних механізмів забезпечення безпеки й оборони; досягнення інформаційної переваги (домінування) забезпечує можливість випереджати суперника у прийнятті військово-політичних рішень і є основою успіху у воєнних діях;

– з'являється низка проблем, пов'язаних комунікативно-психологічними проблемами в сучасному українському інформаційному просторі, зумовлених поточним військово-політичним становищем України;

– з'являється необхідність врахування майбутніх викликів суб'єктам усіх рівнів за допомогою інформаційно-психологічної агресії, руйнування як системи цінностей, так і механізмів управління як основних технологій ведення гібридної війни [2, с. 7].

Отже, розуміння поняття «безпека» як цінності, сьогодні вважається класичним у наукових школах США та провідних країн Європи. Безпека розуміється як засіб збереження та підтримання таких цінностей, як добробут, сталий розвиток тощо. Вважається, що система цінностей є фундаментальним фактором, що визначає сутнісне наповнення змісту поняття «безпека» та, відповідно, - цілі, засоби, способи і методи держави у намаганні її забезпечити. Оптимальність тут досягається не відсутністю будь-яких негативних факторів та процесів, що впливають на систему, а їх мінімізацією. Безпека будь-якої соціальної системи – це стан її оптимального функціонування і розвитку. Саме такий стан гарантує достатню захищеність системи та її відносну непорушність. Тому доцільно погодитися з думкою окремих дослідників, що зміст поняття «безпека» ширший, ніж «стан захищеності» соціальної системи від внутрішніх і зовнішніх загроз, а тим більше – «стан її непорушності» [3, с. 219-220].

Зрозуміло, що понятійним категоріям «безпека» чи «стан захищеності» об'єктивно кореспондує поняття «тероризм». Проблема тероризму взагалі ніколи не втрачає своєї актуальності як для правової теорії, так і для практичної діяльності правоохоронних та інших державних органів. Проте, мега-масштабів вона набула лише у теперішній час, коли з'явилися і в подальшому були ідентифіковані та класифіковані нові види тероризму, зокрема, - інформаційний/кібернетичний тероризм.

Безперечно, що сучасний інформаційний/кібернетичний тероризм потребує розроблення нових концептуальних підходів, тому, виходячи з наведеного, виникла необхідність проведення аналізу дефініцій терміна «кібернетична безпека», які наведені у ряді загальнодержавних програмних документах як національних, так і провідних країн світу.

Так, у Стратегії забезпечення національної безпеки Франції, присвяченій і питанням кібербезпеки, існує таке визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними. Зазначений програмний документ

робить акцент на технічні засоби захисту інформації, боротьбу з кіберзлочинністю і встановлення кіберзахисту. Відповідно до цього визначення кібербезпека розуміється як деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об'єктів, на які можуть діяти які небудь загрози з кіберпростору, послуг інформаційних систем, - це визначення терміна дозволяє мати на увазі наявність якихось загроз функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Це положення має важливий методологічний зміст у розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки [2, с. 11; 4, с. 314].

У німецькій аналогічній стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків. В ній стверджується, що кібербезпека повинна базуватися на комплексному підході. Це досить прагматична точка зору, яка дозволяє розробляти практичні кроки щодо забезпечення кібербезпеки, проте вона не надає достатніх методологічних підстав для проектування та оцінки систем, що забезпечують цю безпеку. Про зазначене побічно свідчить зміст десяти стратегічних напрямів у Стратегії забезпечення кібербезпеки, оголошених федеральним урядом Німеччини. Стратегія Німеччини закладає основу для безпеки критично важливих інформаційних систем та зосереджена на запобіганні і кримінальному переслідуванні кібератак, а також на запобігання виходу з ладу IT-обладнання, викликаного випадковими чинниками. Особливо останнє стосується критично важливих інформаційних систем. У стратегії аналізується, чи потрібно проводити додаткові дії (і якщо так, то де саме) щодо захисту IT-систем шляхом надання основних функцій безпеки, сертифікованих державою, а також підтримкою малого і середнього бізнесу за допомогою створення нової робочої групи [2, с. 12-13].

В аналогічному програмному документі Канади стверджується, що з метою забезпечення найсучаснішого використання кіберпростору, який є стратегічним активом, необхідно передбачати і протистояти кіберзагрозам, що виникають. У канадській Стратегії кібербезпеки не міститься чіткого визначення того, що являє собою кібербезпека. Відповідно до цього документа, під кібербезпекою можна розуміти захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак. З іншого боку, надано досить докладне визначення кібератаки, а кібербезпека – це засіб захисту від цих загроз. Кібератаки включають ненавмисні або несанкціонований доступ, використання, маніпуляції, переривання або знищення (через електронні засоби) електронної інформації та/або електронної та фізичної інфраструктури, що використовується для обробки, зв'язку, та/або баз даних. При цьому рівень кібербезпеки визначається рівнем шкоди, що може бути завданий від кібератаки. У цілому, канадська Стратегія все ж таки розглядає основну шкоду від реалізації кіберзагроз як збиток, який можуть мати системи життєзабезпечення та підтримки діяльності всієї країни, бізнесу та окремого громадянина. Вона, в цілому, передбачає три напрями: захист урядових систем (встановлення чітких ролей і відповідальності, посилення безпеки кіберсистем федерального рівня і підвищення інформованості уряду в області кібербезпеки); співпраця з метою захисту ключових кіберсистем, що знаходяться за межами Федерального Уряду (ряд партнерських

проектів державного рівня із залученням приватного сектора і секторів критичних інфраструктур) та забезпечення безпеки канадських громадян в онлайн-середовищі [2, с. 14].

Одна із останніх, прийнятих за часом, національних Стратегій кібербезпеки (Турецька Республіка) містить наступне визначення: кібербезпека – захист інформаційних систем, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам. Водночас, під кіберпростором розуміється середовище, що складається з інформаційних систем, розподілених по всьому світу, в тому числі мереж, що з'єднують ці системи. Національний кіберпростір визначається як простір, який складається з інформаційних систем суб'єктів, що перебувають під юрисдикцією Турецької Республіки [2, с. 15].

У Нідерландах також приділяють велику увагу наявності загроз інформаційній інфраструктурі в умовах широкого застосування цифрових (комп'ютерних) технологій. Національним координатором з безпеки та боротьби з тероризмом в 2013 році була опублікована Національна стратегія кібербезпеки. На думку авторів Стратегії, кібербезпека – це сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі кіберсистем або неправильного їх використання, а також з їх відновлення після реалізації цих загроз. До збоїв Стратегія відносить зниження надійності кіберсистем, обмеження доступності та порушення конфіденційності та/або цілісності інформації, що зберігається в цих системах. Таке тлумачення робить дуже складним вирішення проблеми визначення критеріїв забезпечення кібербезпеки. Однак у Стратегії Нідерландів зроблено важливий в методологічному аспекті висновок – кібербезпека може бути досягнута тільки в системній кореляції з вирішенням проблем захисту та забезпечення основних прав, цінностей і соціально-економічних вигод членів соціуму [2, с. 16].

Політикою кібербезпеки австралійського уряду є підтримка безпечної, стійкої і надійної роботи електронного операційного середовища, яке підтримує національну безпеку Австралії та максимізує переваги цифрової економіки. В опублікованій у 2009 році Стратегії під кібербезпекою розуміється забезпечення доступності, цілісності та конфіденційності кіберсистем Австралії, а також захист фізичних осіб, особливо неповнолітніх, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання кіберпростору для цілей сексуальної експлуатації [2, с. 18].

В національному Законі «Про основні засади забезпечення кібербезпеки України» викладено таке визначення кібербезпеки: «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». При цьому в Законі кіберпростір позиціонується як: «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет

та/або інших глобальних мереж передачі даних». Останнє визначення має дуже низький методологічний потенціал і не дозволяє конкретизувати особливості кібербезпеки. Більше того, абсолютно необґрунтовано, як вбачається, до кібербезпеки віднесені проблеми «…захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору…» в загальному сенсі, внаслідок чого до проблематики кібербезпеки можуть бути віднесені форми суспільних відносин, абсолютно не притаманних заявленій проблематиці.

Іншою складовою інформаційної/кібернетичної безпеки є відповідний стан захищеності певних інформаційних масивів та захищеність від руйнівних інформаційно-психологічних впливів. Власне інформаційну безпеку (в розумінні, в першу чергу, як медіа-безпеку) регулює певна сукупність нормативно-правових актів і програмних документів, базовим з яких (за відсутності основного акту законодавства про інформаційну безпеку) слід позиціонувати Указ Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

Зрозуміло, що усталеним позиціям актів законодавства по регулюванню відповідного кола суспільних відносин, передують певні наукові понятійні конструкції та їх обгрунтування. Разом з тим, враховуючі проблемні аспекти та невизначеності, що залишились, доцільно розглянути позиції вітчизняних науковців з цього питання.

При розгляді загальної спрямованості та характерних ознак сучасного інформаційного тероризму, науковці, зокрема, Єрохіна Т.В., Леонов Б.Д., Сороківська О.А. виділяють таку універсальну ознаку, як психологічний вплив на осіб, що не є безпосередніми жертвами насильства, тобто створення загальної атмосфери страху, паніки серед значної кількості осіб, для чого терористи активно використовують засоби масової інформації, зокрема інтернет-мережі [5, с. 32-35; 6, с. 77-78].

У зв’язку з означеною більш-менш загальною позицією, у наукових колах розвивається концепція про інформаційний (чи медіа-) тероризм: і як самостійне деструктивне явище, і як алгоритм дій. При цьому інформаційний тероризм, як правило, намагаються розглядати як: а) злочин з самостійним складом («залякування, створення атмосфери страху за допомогою ЗМІ»); б) використання медіа-засобів у зв’язку з терористичними актами для досягнення терористами інших цілей [7, с. 33-34, 67].

Інші науковці, зокрема Васенин В.А., Попов Г.В. та Грицун О.О., досліджуючи питання інформаційного тероризму, оперують такими понятійними категоріями як «інформаційний тероризм» та «медіа-тероризм», акцентуючи при цьому увагу на подвійній ролі інформаційно-комунікаційних технологій у здійсненні актів інформаційного тероризму [8, с. 59-60, 113-115, 312]. Означені науковці більш змістовно розкривають об’єктний склад інформаційного тероризму (як злочину з самостійним суб’єктно-об’єктним складом), позиціонуючи інформаційно-комунікаційні системи та технології і як об’єкт злочину, і як засіб чи знаряддя (зброю) в руках терористів. При цьому підкреслюється, що достатньо важко провести чітку межу між інформаційним тероризмом та використанням інформаційних технологій у воєнних чи кримінальних цілях. Вказані дослідники, крім того, виокремлюють інформаційний тероризм від інших протиправних діянь в інформаційній сфері за

ціллю (цілеспрямованістю), що притаманні і терористичним актам в загальному їх розумінні. До цих цілей вони відносять: «залякування населення, створення атмосфери страху та паніки, створення атмосфери загрози повторення теракту, виклик великого суспільного резонансу, наслідки, небезпечні для життя та здоров'я людей, поширення інформації про теракт для широкої аудиторії».

Ряд авторів (Шпак Ю.О., Ребріна Л.П., Цибульська Л.О.) намагаються взагалі відійти від визначення та самостійного позиціонування інформаційного тероризму як самостійного складу діяння (злочину) та оперують поняттям «інформаційна війна» як більш узагальненим і таким, що включає в себе також і інформаційний тероризм, при цьому не надаючи право останньому на «самостійність». Узагальнена позиція цих дослідників полягає у тому, що інформаційний тероризм позиціонується виключно і тільки як складовий елемент інформаційної війни, а не підміняє її в цілому [9, с. 136-139; 10, с. 262-264].

Отже, інформаційний/кібернетичний тероризм в усіх його проявах і класифікованих різновидах характеризується формуванням таких негативних явищ, як багатоплановість руйнівного впливу на різні сфери суспільного життя – політичну, економічну, соціальну, духовну, а також на національну безпеку: суспільну, державну, воєнну, інформаційну тощо. Беззаперечно, що інформаційний/кібернетичний тероризм із його політично вмотивованою насильницькою ідеологією становить серйозну небезпеку для світової спільноти та окремих держав, зокрема й для України.

При підготовці та аналізі матеріалів з питань інформаційного/кібернетичного тероризму та інформаційної безпеки додатково, окрім текстуально зазначених вище, використовувались джерела, що знаходяться у переліку використаної літератури за нумерацією 11-17 [11-17].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Григор'єв В.І. Технології інформаційної війни / Історичні, теоретичні та методологічні аспекти національної безпеки / Реформування національної безпеки: історія, сучасність, перспективи: матеріали підсумкової науково-практичної конференції (19 травня 2016 року). К.: Інститут УДО КНУ імені Тараса Шевченка, 2017. С. 17-19.

2. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. К.: Вид-во НДІІП НАПрН. 2017. 107с. [Електронний ресурс]. Режим доступу: http://ippi.org.ua/sites/default/files/eskalaciya_kiberzagroz.pdf

3. Тоффлер Э. Третья волна: пер. с англ. М.: ООО "Издательство АСТ", 2002. 776 с.

4. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 1. С. 312-320.

5. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи. *Економічні науки: Вісник Хмельницького національного університету.* 2010. № 2. Т. 2. С. 32–35.

6. Реформування національної безпеки: історія, сучасність, перспективи: матеріали підсумкової науково-практичної конференції (19 травня 2016 року). К.: Інститут УДО КНУ імені Тараса Шевченка, 2017. 116 с.

7. Державна політика протидії тероризму: пріоритети та шляхи реалізації : збірник матеріалів «круглого столу» / за ред. М. Г. Гуцало. К. : НІСД, 2011. 120 с.

8. Протидія терористичній діяльності: міжнародний досвід і його актуальність для України: матеріали ІІ Міжнародної науково-практичної конференції (15 грудня 2017 року). / уклад.: Севрук Ю.Г., Попов Г.В., Лісова Н.В. – Київ: Національна академія прокуратури України, 2018. 430 с.

9. Цибульська Л.О. Роль інформаційних технологій у національному та світовому розвитку / Наук. пр. Чорноморського держ. ун-ту ім. Петра Могили. Сер.: Комп'ютерні технології. 2012. Т. 191, Вип. 179. С. 136–139. [Електронний ресурс]. Режим доступу: http://lib.chdu.edu.ua/pdf/naukpraci/ computer/2012/191-179-24.pdf.

10. Богуш В. Інформаційна безпека держави / голов. ред. Ю. О. Шпак. – Київ: МК-Прес, 2005. 432 с.

11. Протидія проявам тероризму, сепаратизму, екстремізму та нелегальній міграції в сучасних умовах: стан, проблеми та перспективи: матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 28 жовт. 2016 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2016. 356 с.

12. Федоренко О. Науково-інтелектуальні аспекти інформаційної безпеки України в умовах інформаційної війни / Наук. пр. Нац. б-ки України ім. В.І. Вернадського: зб. наук. пр. / НАН України, Нац. б-ка України ім. В.І. Вернадського, Асоц. б-к України. Київ, 2017. Вип. 46. С. 155–162.

13. Реформування національної безпеки: історія, сучасність, перспективи: матеріали ІІІ підсумкової науково-практичної конференції (16 травня 2019 року). К.: Інститут УДО КНУ імені Тараса Шевченка, 2019. 209 с. [Електронний ресурс]. Режим доступу: http://indo.univ.kiev.ua/images/ Digest _16.05.19.pdf

14. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. Женева: МСЭ, 2009. С. 55. [Електронний ресурс]. Режим доступу: //www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru

15. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков //: зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 22 березня 2011 р.). К. : Вид-во НА СБ України, 2011. Ч. 2. С. 43-48.

16. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2(42). 2014. [Електронний ресурс]. Режим доступу: http://ippi.org.ua/ sites/default/files/14boavpk.pdf

17. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. К. : Видавничий дім "СофтПрес", 2005. 316 с.