УДК 342.9

І. В. Діордіца
кандидат юридичних наук, доцент

ПОНЯТТЯ І ЗМІСТ КІБЕРТЕРОРИЗМУ

У сучасному суспільстві зросло значення інформації. Інформація набула цінність не тільки з погляду державної таємниці, а й у плані комерційної таємниці, конфіденційної інформації, персональних даних. Завдяки розвитку засобів цифрової цивілізації, значному розширенню обсягів застосування в буденному житті різноманітних засобів програмного забезпечення, відбулося широкомасштабне проникнення засобів автоматизації професійної діяльності, мережевих комунікацій, засобів візуалізації та оброблення даних у сферу економіки. Водночас інформація і знання розглядаються як інтелектуальний капітал, як товар, який має свою вартість. У міру формування інформаційного суспільства рівень економічної безпеки країни все більше буде визначатися здатністю впровадження інформаційно-комунікаційних технологій в економічні, соціальні, військові, технологічні та культурні сфери суспільства. Тому проблеми забезпечення взаємозв'язку економічної й інформаційної безпеки держави привертають сьогодні все більшу увагу фахівців, які працюють у сфері інформаційних технологій, економіки, політики, права та міжнародних відносин.

Як підкреслюється в Окінавській хартії глобального інформаційного суспільства, інформаційно-комунікаційні технології є одним із найбільш важливих факторів, що впливають на формування суспільства XXI століття. Їх революційний вплив стосується способу життя людей, їхньої освіти й роботи, а також взаємодії уряду та громадянського суспільства. Інформаційні технології швидко стають життєво важливим стимулом розвитку світової економіки [1].

Водночас бурхливо розвиваються в суспільстві процеси інформатизації, які разом з усіма своїми перевагами створили безліч нових проблем, викликів і загроз у сфері національної безпеки. Головним чином це стосується інформаційних загроз терористичного характеру. До 1990-х років про тероризм говорили лише як про локальне явище, але нині він став феноменом світового масштабу, причому роль інформаційних технологій передусім у реалізації демонстративності актів тероризму дедалі стає вагомішою. З-поміж іншого окремим видом тероризму стає кібертероризм, який фактично корелює з розвитком віртуального світу, симуляризацією інформаційних потоків. Нині можемо спостерігати значне збільшення уваги питанню протидії кібертероризму, разом із тим багато питань залишаються невивченими з позицій юридичних наук, що й обґрунтовує актуальність статті.

Основними завданнями, вирішенню яких присвячена стаття, є такі:

– охарактеризувати поняття й розуміння тероризму на сучасному етапі;

– проаналізувати наявні підходи до визначення кібертероризму;

– визначити рівень ефективності чинної нормативно-правової бази, яка передбачає кримінальну відповідальність за вчинення відповідних правопорушень;

– сформулювати перспективні напрями державної політики протидії кібертероризму в Україні.

Виходячи із цього, метою статті є дослідження поняття і змісту кібертероризму на сучасному етапі.

У роботі використано як наукові доробки зарубіжних дослідників, так і праці вітчизняних науковців, які займаються проблемою тероризму й кібертероризму. Окремо виділимо наукову школу В.А. Ліпкана [2–5], дослідники якої присвячували свої доробки питанням боротьби з тероризмом, національній безпеці України, правовим засадам розвитку інформаційного суспільства в Україні (оскільки кібертероризм має місце саме в інформаційному суспільстві) та інформаційній безпеці України.

Проблемам забезпечення інформаційної безпеки держави свої наукові праці присвятили і такі вчені, як О.В. Кубишкін [6], В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа [7] та ін. Також було використано роботи дослідників кіберзлочинності, кібербезпеки й кібертероризму: О.Г. Широкової-Мурараш, Ю.Р. Акчуріна [8], В.В. Топчія [9]. Окрему увагу було приділено працям Г.В. Форос, А.В. Форос [10], Є.А. Макаренко, М.М. Рижикова, М.А. Ожевана [11] і В.К. Грищука [12].

Розпочинаючи будь-які наукові дослідження, необхідно чітко визначитися з понятійно-категорійним апаратом. Акцентуємо увагу на тому, що серед науковців і практиків немає єдності в термінологічному позначенні кібернетичної терористичної діяльності – кібертероризму. Здійснений нами формальний, догматичний і герменевтичний аналізи уможливили виділити різні трактування кібертероризму: «інформа-

ційний тероризм», «комп'ютерний тероризм», «кібертероризм», «технологічний тероризм», «віртуальний тероризм» тощо. При цьому зміст зазначених понять також визначається по-різному. Складність у формулюванні цих понять існує, очевидно, як через неможливість виділення єдиного об'єкта протиправного посягання, так і через досить велику кількість предметів протиправних посягань із погляду їх правової охорони.

Передусім зупинимося на дослідженні такої категорії, як *«тероризм»*. У найбільш загальному розумінні сутність тероризму полягає у використанні насильства з метою залякування. Суб'єкт терористичного насильства – окремі особи або неурядові організації. Об'єкт насильства – влада в особі окремих державних службовців або суспільство в особі окремих громадян (у тому числі іноземців або держслужбовців інших держав), а також приватне й державне майно, інфраструктури, системи життєзабезпечення. Мета насильства – домогтися бажаного для терористів розвитку подій – революції, дестабілізації суспільства, розв'язання війни з іноземною державою, здобуття незалежності, зміни правового режиму, зміни кордонів або порушення територіальної цілісності чи недоторканності державних кордонів, зменшення обсягу прав людини.

Визначення поняття *«тероризм»* є досить складним завданням. Форми й методи терористичної діяльності істотно змінювалися з часом. Це явище має стійку негативну оцінку, що породжує довільне тлумачення. З одного боку, існує тенденція розширеного трактування, коли деякі політичні сили без достатніх підстав називають терористами своїх супротивників. З іншого – звуження. Самі терористи схильні називати себе солдатами, партизанами, диверсантами в тилу противника й ін. Звідси труднощі як юридично-правових дефініцій, так і загальнотеоретичного осмислення тероризму. До сих пір законодавці різних країн не дійшли єдиного розуміння щодо визначення тероризму.

В історичному аспекті термін «тероризм» уперше з'явився в 1798 році, коли філософ Еммануїл Кант використовував його для опису песимістичного погляду на долю людства. У той же рік цей термін можна було знайти в додатку до великого словника Французької академії, це було викликано ексцесами революційного терору, і тому термін не мав такого значення, яке ми сьогодні в нього вкладаємо. Нині під цим терміном у більшості випадків розуміються дії різних рухів, які впливають на уряд держави з метою радикальної зміни його політичного та соціального управління, при цьому об'єктом впливу є не тільки держава, а й внутрішня соціальна система [6], а також інформаційна безпека загалом.

Використовуючи національну законодавчу базу, зауважимо, що під *тероризмом* розуміється суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади, або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей, або погрози вчинення злочинних дій з метою досягнення злочинних цілей [13].

Терористична діяльність – діяльність, яка охоплює планування, організацію, підготовку та реалізацію терористичних актів; підбурювання до вчинення терористичних актів, насильства над фізичними особами чи організаціями, знищення матеріальних об'єктів у терористичних цілях; організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само як і участь у таких актах; вербування, озброєння, підготовку та використання терористів; пропаганду й поширення ідеології тероризму; фінансування завідомо терористичних груп (організацій) або інше сприяння їм [13]. Щодо міжнародного трактування цієї категорії, то навіть у Міжнародній конвенції про боротьбу з фінансуванням тероризму та Міжнародній конвенції про боротьбу з актами ядерного тероризму не міститься уніфікованого визначення.

У Великому тлумачному словнику української мови «*тероризм*» визначено як здійснювання, застосування терору; діяльність і тактика терористів [14, с. 640]. Терор – найгостріша форма боротьби проти політичних і класових супротивників із застосуванням насильства аж до фізичного знищення [14, с. 640].

Як було зазначено вище, нині не існує уніфікованої дефініції «тероризм», по-перше, це є негативним для загального тлумачення та притягнення винних осіб до відповідальності, по-друге, посилює актуальність теми дослідження. Також зауважимо, що під *тероризмом* варто розуміти діяльність (включаючи підготовку, безпосереднє здійснення, підбурювання, фінансування й інші схожі дії), метою якої є залякування певного об'єкта, частіш за все йдеться про політичну арену.

Тероризм дуже часто розглядають як фонове явище для вчинення інших міжнародних злочинів. Проте тероризм як соціальне явище хоча і є злочином, але вимагає окремого розгляду, оскільки має значну специфіку порівняно з іншими злочинами насамперед через свою політичну спрямованість. Зазначена специфіка викликає й особливий режим боротьби з тероризмом. Що стосується інформаційного

або кібертероризму, то специфічність сфери здійснення дій – інформаційний простір – ще більш відмежовує інформаційний тероризм від комп'ютерної злочинності. Підтримуємо наукову позицію, згідно з якою інформаційний тероризм повинен розглядатися окремо від комп'ютерних злочинів [6].

Уперше занепокоєність можливими наслідками використання всесвітньої інформаційної мережі була висловлена в 1993 році Елвіном Тоффлером, коли широка публіка ще мало що знала про Інтернет. Е. Тоффлер уже тоді передбачав, що терористи будуть намагатися завдати удар по інформаційній і телекомунікаційній інфраструктурах Сполучених Штатів Америки. Із тих пір було здійснено значну кількість досліджень, і думки експертів щодо поняття «кібертероризм» полярно поділилися [8, с. 5].

Визначення інформаційного або кібертероризму можна знайти як у міжнародно-правових документах і проектах конвенцій, так і в дослідженнях фахівців із цієї проблеми. Однією з характерних рис визначень інформаційного тероризму є те, що в більшості з них згадується тільки один аспект інформаційної безпеки, а саме той, який пов'язаний із засобами обробления інформації, що звужує поняття інформаційного тероризму, тим самим обмежуючи сферу правового регулювання, що не сприяє ефективній співпраці держав у справі боротьби з інформаційним тероризмом [6].

Однак наголосимо на тому, що загальноприйнятого визначення наразі не існує. Але в теоретичному аспекті йдеться про інтеграцію таких понять, як «тероризм» і «комп'ютерний злочин» [15].

Зупинимося більш детально на наявних доктринальних дефініціях.

Науково-технічний прогрес, створивши нові інформаційні технології, в короткі терміни революційно трансформував процеси створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Сьогодні його результати нерідко використовують і злочинці. Проникнення в інформаційну сферу та її використання кримінальними, в тому числі й терористичними, елементами породило явища, які називаються кіберзлочинністю й кібертероризмом. *Кібертероризм* – проведення «атак» на комп'ютерні системи. Засоби та методи кібератак уже давно освоєні як міжнародними екстремістськими організаціями, так і національними сепаратистськими рухами. Перші приклади «комп'ютерного тероризму» з'явилися наприкінці 1990-х рр., що пов'язано як із розвитком комп'ютерних мереж, так роллю комп'ютерів, що зростає, у всіх сферах життя. Як наслідок до них збільшилася увага різних «кіберхуліганів» і «кібертерористів», які здійснюють напади за допомогою несанкціонованого доступу, щоб заважати нормальній роботі відповідних установ [12, с. 100].

Під *кібертероризмом* розуміють навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту [9].

Щодо міжнародного закріплення цього терміна, то в Конвенції Ради Європи про кіберзлочинність не міститься окремого визначення кібертероризму.

Положення Конвенції Ради Європи «Про кіберзлочинність» відображено в Законі України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23.12.2004 року, відповідно до якого в розділі 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» викладено в новій редакції статті 361, 362, 363 Кримінального кодексу та передбачено кримінальну відповідальність за статтями 361-1, 361-2 і 363-1 [11, с. 256].

Відповідно до проекту конвенції про посилення захисту від кіберзлочинів і кібертероризму, *інформаційний або кібертероризм* являє собою навмисне застосування незаконно встановленого повноваження, насильства, руйнування або проникнення в кіберсистеми, якщо подібні дії можуть спричинити смерть чи заподіяти шкоду особі або особам, істотну шкоду майну, значну економічну шкоду або зумовити цивільний безлад [6].

У середині 1980-х років Беррі Коллін, співробітник американського Інституту безпеки та розвідки, запровадив термін *«кібертероризм»* для визначення терористичних дій у віртуальному просторі [9].

Центр стратегічних і міжнародних досліджень визначає *кібертероризм* як використання комп'ютерних мережевих інструментів для припинення функціонування критичних об'єктів національної інфраструктури (зокрема енергетичних, транспортних, урядових) або для примусу чи залякування уряду або цивільного населення [16].

Також *кібертероризм* визначають як залякування суспільства шляхом використання високих технологій для досягнення політичних, релігійних або ідеологічних цілей, а також дії, що призводять до відключення чи видалення критичних для інфраструктурних об'єктів даних або інформації [17].

Сьогодні кількість кібератак і прикладів кібертероризму дедалі зростає, а рівень шкоди суттєво збільшується. Найбільшу проблему становить відсутність чіткого законодавства, в якому було б чітко визначено це поняття, передбачено відповідальність за протиправні діяння, що свідчить про недостатнє осмислення цього явища. Труднощі у визначенні поняття «кібертероризм» пов'язані переважно з тим, що складно відокремити сам кібертероризм від акцій інформаційної війни й застосування інформаційної зброї, від злочинів у сфері комп'ютерної інформації або патріотичних поривів населення країн і регіонів. Додаткові труднощі виникають у разі спроби виявити специфіку цієї форми тероризму. Так, наприклад, психологічний та економічний аспекти кібертероризму тісно переплетені, і неможливо однозначно визначити, який із них має більше значення.

Кібертероризм є однією з форм маніпулятивного впливу на суспільну свідомість, коли для досягнення своїх політико-ідеологічних цілей і установок терористи використовують комп'ютери, спеціальне програмне забезпечення, телекомунікаційні мережі, а також сучасні інформаційні технології, забезпечуючи тим самим несанкціонований доступ до тих чи інших ресурсів, інформаційних і програмних ресурсів, технологічних процесів. Демонстрація терористами можливості доступу до певних ресурсів, об'єктів і систем і загроза використання цієї можливості на шкоду суспільству впливає на психологічний стан і поведінку людей [18].

Для кібертероризму є характерним, по-перше, використання комп'ютера або іншого гаджета, що має доступ до мережі, як інструмента злочину; по-друге, існування Інтернету як міжнародного інформаційного простору, в якому перебуває об'єкт злочину; по-третє, зловмисна атака з боку кримінальних індивідів чи їх угруповань на такі специфічні об'єкти, як інформація, програми, комп'ютери, локальні та глобальні мережі [15].

Тероризм у сфері комп'ютерних технологій має такі ознаки: анонімність, віддаленість дійової особи, відносна дешевизна, відсутність необхідності використання вибухівки й самогубних акцій, великий розголос у ЗМІ. Але в нього є й недоліки: через складність систем важко контролювати атаку та досягти бажаної шкоди безпосередньо людям, акція не набуває такого драматичного й емоційного характеру, як це буває при застосуванні інших засобів. Також кібертероризму властива така особливість: нові інформаційні технології є нерідко знаряддям ширшої терористичної операції [12, с. 102].

На думку вчених, найбільшу небезпеку становить кібертероризм, зокрема тероризм спланований, учинений чи скоординований у кіберпросторі, тобто в терористичних акціях використовуються новітні досягнення науки й техніки в галузі новітніх інформаційних технологій [19, с. 50].

Як складне соціально-політичне явище, що має різноманітні форми вияву, тероризм можна *класифікувати* за найістотнішими ознаками, тобто провести його класифікацію, виділивши й охарактеризувавши основні його види, що дає змогу розуміти сутність цього явища та визначимо, до якого з видів можна зарахувати кібертероризм як видове явище. Так, В.А. Ліпкан пропонує такі підстави класифікації тероризму: за територією вчинення; за елементами виявів (за суб'єктами, мотивами, цілями, засобами, методами, об'єктами, змістом діяльності, характером наслідків); за рівнем організації; за видами терористських груп (організацій). За територією вчинення тероризму виділяють такі види: 1) транснаціональний; 2) тотальний (внутрішній); 3) селективний; 4) локальний.

За суб'єктами розрізняють: а) акти тероризму, що вчиняються особами, які перебувають на державній службі та спеціально підготовлені для цієї мети; б) акти тероризму, що вчиняються пригнобленими етнічними меншинами, які прагнуть до культурної й політичної автономії, так званий «іредентизм»; в) акти тероризму, що вчиняються релігійними фанатиками; г) акти тероризму визвольних рухів у державах «третього світу», ґ) акти тероризму, що вчиняються окремими індивідами чи організаціями осіб. Базуючись на висновках В. А. Ліпкана, можемо виділити такі мотиви вчинення терористичних актів: 1) політичні; 2) релігійні; 3) націоналістичні; 4) помсти; 5) прагнення до самоствердження.

За видами цілей: а) підрив – придушення або знесилення супротивника з метою отримання поступок; б) провокування до дій чи бездіяльності тих чи інших сил з метою зміни політики, яка проводиться в державі, здійснення вигідних терористам тих чи інших дій (утримання від таких); в) демонстративність – збудження та притягнення уваги громадськості до тієї справи, за яку ведуть боротьбу терористи.

За засобами діяльності ділять на матеріальні (інформаційна; економічна; геноцидна; фізична; технологічна) і нематеріальні (не зафіксовані на матеріальних носіях погрози; хибні повідомлення про вибухи, які готуються, вбивства, отруєння тощо) [12, с. 132].

На нашу думку, кібертероризм є транснаціональним діянням, яке вчиняється окремими індивідами чи організаціями осіб. Мотивами вчинення можуть бути як політичні, так і помсти або прагнення до самоствердження. Цілі

можуть переслідуватися найрізноманітніші, як підрив, так і демонстративність. Кібертерористи можуть використовувати як матеріальні, зокрема інформаційні – демагогію, пропаганду помилкових ідей, залякування за допомогою ЗМІ, так і нематеріальні, наприклад, хибні повідомлення про вибухи тощо.

За способами вчинення: а) провокування збройного заколоту, повстання чи військового перевороту для захоплення або зміни влади; б) порушення системи державного управління за допомогою вбивств політичних лідерів, шантажу, навіювання жаху, відчаю, психологічної пригніченості; в) руйнування основ конституційного ладу, цивілізованого життя і створення хаосу у функціонуванні систем зв'язку й життєзабезпечення, транспортних засобів, роботі організацій та установ сучасного суспільства. Кібертероризм може бути зараховано до кожного із цих видів.

За об'єктом спрямованості: а) акти тероризму, що вчиняються проти безпеки держави; б) акти тероризму, що вчиняються проти безпеки осіб; в) акти тероризму, що вчиняються щодо майна або окремих фізичних чи юридичних осіб. На нашу думку, за цим критерієм кібертероризм однозначно може бути зарахований до першого виду.

За змістом діяльності: діяльність терористичної групи (особи, організації), спрямована на зміни в зовнішньому (навколишньому) світі, і внутрішня діяльність терористських груп, спрямована на забезпечення власного існування. Щодо кібертероризму, то його змістом є діяльність, спрямована на певні зміни.

За характером наслідків діляться на такі, що спричиняють: а) шкоду здоров'ю; б) створення загрози чи заподіяння шкоди життю людей або їхньому здоров'ю, матеріальної, моральної чи всіх видів у сукупності; в) людські жертви, які можуть бути груповими, а також одиничними; г) матеріальну шкоду [12, с. 132]. У випадку кібертероризму йдеться передусім про матеріальну шкоду.

Кібертероризм може розглядатися нами як загроза кібернетичній безпеці. Спеціальними суб'єктами забезпечення кібернетичної безпеки є державні органи, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю й кібертероризмом, а також на забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури. До таких суб'єктів належать Міністерство внутрішніх справ України; Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; Міністерство юстиції України; Генеральна прокуратура України [20].

Зважаючи на викладене, вважаємо, що термін «*кібертероризм*» є синтезом понять «*кібербезпековий простір*» і «*тероризм*», і до сьогодні в наукових колах ведуться активні дискусії щодо того, чи є перший просто реалізацією актів тероризму в новому просторі, чи це принципово нове явище, яке має нові методи, засоби та інструментарій.

Поки кібертероризм із розряду «потенційної» загрози не перейшов до розряду «реальної» загрози, варто застосовувати превентивні заходи для недопущення його становлення. Основою забезпечення боротьби з кібертероризмом є створення ефективної системи заходів із запобігання такому виду злочинності, виявлення та припинення його [9].

В Україні сьогодні не розроблені нормативно-правові акти, що регулюють такий вид злочинності. Але головною зброєю в боротьбі із цією загрозою залишається законодавство, яке потребує подальшого вдосконалення. Якщо зазначати міжнародні правові акти в цій сфері, то першим і головним документом, у якому йдеться про боротьбу з кіберзлочинністю, є Європейська конвенція 2001 року. Цей документ націлено на здійснення загальної політики з питань кримінального права, метою якої є захист суспільства від кібертероризму шляхом прийняття потрібних законодавчих актів, а також за допомогою розширення міжнародного співробітництва. В українському законодавстві навіть немає такого виду злочину, як кібертероризм. Тому найбільш дієвим напрямом у вирішенні комплексної проблеми протидії кіберзлочинності в наш час є міжнародне співробітництво правоохоронних органів у сфері інформаційної безпеки на основі узгодження національного та міжнародного законодавства [9].

Кібертероризм спрямований на проникнення в інформаційно-телекомунікаційну систему, перехоплення управління, пригнічення засобів мережевого інформаційного обміну і здійснення інших деструктивних дій. Небезпека такого виду інформаційного тероризму полягає в тому, що він не має національних меж, і в проблематичності виявлення терориста в інформаційному просторі, адже хакери здійснюють терористичну діяльність через підставні комп'ютери, що ускладнює його ідентифікацію та визначення місцезнаходження.

Сьогодні кібертероризм є одним із найнебезпечніших видів злочинності. Кібератаки можуть завдати значної шкоди на локальному, державному й навіть міжнародному рівнях. Адже зовнішні кібератаки можуть переслідувати й більш серйозні цілі, ніж пасивний збір даних, а об'єктами кібертероризму можуть бути грошова та секретна інформація, апаратура

контролю над космічними приладами, ядерними електростанціями, воєнними комплексами, головні комп'ютерні вузли тощо [21, с. 55].

Нині існують дві великі організації, готові взяти на себе провідну роль у боротьбі з кіберзлочинністю на міжнародному рівні. Це Підрозділ із боротьби з тероризмом ОБСЄ – організація, що діє під егідою ООН, а також Інтерпол. Крім того, у Європейському Союзі розпочав роботу Центр із боротьби з кіберзлочинністю (European Cyber Crime Centre). Країни-члени Європейського Союзу та європейські інституції мають намір підтримувати Центр із боротьби з кіберзлочинністю для створення оперативних і аналітичних можливостей її розслідування та для співпраці з міжнародними партнерами.

Аналізуючи й досліджуючи розвиток кіберзлочинності на території України, не можна впевнено сказати, що концепція держави спрямована на об'єднання зусиль щодо протидії цьому феномену. Правовим документом, який регулює цю сферу в Україні, є Доктрина інформаційної безпеки України, де одним із ключових проблемних питань є забезпечення техногенної безпеки, в тому числі у сфері її інформаційних аспектів і боротьби з технологічним.

Проте вона не є дієвим регулятором у своїй сфері. Крім того, так і не ухвалено закон про засади державної інформаційної політики. Так само в Україні не створено кіберкомандування, що могло б швидко реагувати на виклики в інформаційній сфері безпеки держави. Підсумовуючи, потрібно зазначити, що проблема протидії актам інформаційного тероризму – це комплексна проблема. Сьогоднішні закони повинні відповідати вимогам сучасного розвитку. Із цією метою урядові нашої держави необхідно проводити цілеспрямовану роботу з гармонізації та вдосконалення законодавства у сфері інформаційної безпеки держави. Україні насамперед потрібно розробити ефективну інформаційну політику, спрямовану на інформування громадян і забезпечення розуміння ними того, в чому полягають причини тероризму, – підвищення медіаграмотності (вміння протистояти спробам маніпулювання собою за допомогою інформаційних потоків) і довіри до держави та інші складові, які допоможуть вибудувати систему захисту кожної людини від негативного впливу інформаційного тероризму [21, с. 56].

Окремо звернемо увагу на *кіберполіцію* як структурний підрозділ Національної поліції України, що спеціалізується на запобіганні кримінальним правопорушенням, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних і комп'ютерних інтернет-мереж і систем [22], а також окремим завданням варто виділити боротьбу з кібертероризмом.

Зауважимо, що загальної кількісної оцінки стосовно видів кібератак і методів їх застосування досі немає. Комплексних статистичних досліджень у цьому плані не було. Але ще в далекому 1984 році Фред Коен (F. Cohen) у праці "Computer Viruses: theory and experiments", присвяченій математичним основам вірусної технології, довів: із того, що множина всіх можливих злоякісних кодів нескінченна, випливає нескінченність множини самих атак [7, с. 43].

Акцентуємо увагу на тому, що, на нашу думку, кібертероризм є видовим, а інформаційний тероризм – родовим поняттям одного негативного явища. Боротьба з ними повинна проводитися шляхом застосування узгоджених заходів, а не окремо. Кібертероризм може завдавати школи не лише інформації, а й безпеці держави загалом.

Аргументом на користь того, що інформаційний і кібертероризм – це не одне й те саме, слугує їх етимологічне тлумачення. Інформаційний – стосується інформації, який містить інформацію [14, с. 282].

Кібернетичний – який створено, працює на основі принципів, методів кібернетики. Кібернетика – наука про загальні закони одержання, зберігання, передачі та обробки інформації [14, с. 298].

Одна частина дослідників схильна до визначення терористичних виявів, у яких комп'ютер є або об'єктом, або знаряддям посягань, як кібертероризм. Дослідники ж другої групи терористичні вияви з використанням новітніх досягнень науки й техніки в галузі інформаційних технологій зараховують до інформаційного тероризму [10, с. 256].

Злочинці можуть проникнути в особисті комп'ютери та комп'ютерні системи установ, підприємств, організацій, включаючи банки, секретні служби, дослідницькі установи, патентні агентства, штаби партій, у спільні комп'ютерні мережі. Крім того, інформаційна революція вплинула на військову справу. Вона дала можливість військову компанію провести у віртуальному варіанті. До того ж віртуальною може стати й сама війна, хоча результати її будуть цілком реальні. Інформаційна війна, наприклад.

Отже, резюмуємо, що поняття кібертероризму виникло на межі XX–XXI століть задовго до початку масового використання Інтернету. Термін «кібертероризм» є синтезом понять «кібербезпековий простір» і «тероризм». Під тероризмом варто розуміти діяльність, метою якої

є залякування певного об'єкта, частіш за все йдеться про політичну арену, а кібертероризм – протиправне діяння, яке вчиняється з метою досягнення негативних наслідків, наприклад, отримання матеріальних благ чи загроза інформаційній безпеці держави. Кібертероризм має місце в кібербезпековому просторі.

Для кібертероризму характерним є використання комп'ютера як інструмента злочину та існування Інтернету як міжнародного інформаційного простору, в якому перебуває об'єкт злочину. Зловмисна атака з боку кримінальних індивідів чи їхніх угруповань учиняється на такі специфічні об'єкти, як інформація, програми, комп'ютери, локальні та глобальні мережі.

Кібертероризм є видовим, а інформаційний тероризм – родовим поняттям одного негативного явища – тероризму.

Література

1. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/998_163.
2. Ліпкан В.А. Боротьба з тероризмом : [монографія] / В.А. Ліпкан, Д.Й. Никифорчук, М.М. Руденко. – К. : Знання, 2002. – 254 с.
3. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення : [монографія] / В.А. Ліпкан. – К. : Текст, 2003. – 180 с.
4. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян ; за заг. ред. В.А. Ліпкана. – К. : ФОП О.С. Ліпкан, 2015. – 664 с.
5. Ліпкан В.А. Інформаційна безпека України : [глосарій] / В.А. Ліпкан, Л.С. Харченко,О.В. Логінов. – К. : Текст, 2004. – 136 с.
6. Кубишкін О.В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави / О.В. Кубишкін [Електронний ресурс]. – Режим доступу : http://pravolib.pp.ua/informatsionnyiy-terrorizm-15103.html.
7. Інформаційна та кібербезпека: соціотехнічний аспект : [підручник] / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа] ; за заг. ред. В.Б. Толубка. – К. : ДУТ, 2015. – 288 с.
8. Широкова-Мурараш О.Г. Кіберзлочинність та кібертероризм як загроза міжнародній інформаційній безпеці: міжнародно-правовий аспект / О.Г. Широкова-Мурараш, Ю.Р. Акчурін // Правова інформатика : науковий фаховий журнал з питань правової інформатики, інформаційного права та інформаційної безпеки. – К. : Тов-во «ПанТот», 2011. – № 1. – 12 с.
9. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами / В.В. Топчій [Електронний ресурс]. – Режим доступу : http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf.
10. Форос Г.В. Інформаційний тероризм як загроза національній безпеці України / Г.В. Форос, А.В. Форос // Правова держава. – 2010. – № 12. – С. 256–261.
11. Макаренко Є.А. Міжнародна інформаційна безпека: сучасні виклики та загрози / Є.А. Макаренко, М.М. Рижиков, М.А. Ожеван. – К. : Центр вільної преси, 2006. – 916 с.
12. Тероризм: теоретико-прикладні аспекти : [навчальний посібник] / [кол. авторів] ; за заг. ред. проф. В.К. Грищука. – Львів : ЛьвДУВС, 2011. – 328 с.
13. Про боротьбу з тероризмом : Закон України від 20.03.2003 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/638-15.
14. Великий тлумачний словник сучасної української мови / укл. О. Єрошенко. – Донецьк : ТОВ «Глорія Трейд», 2012. – 864 с.
15. Формування спільної політики ЄС у галузі безпеки й оборони в контексті боротьби з сучасним кібертероризмом [Електронний ресурс]. – Режим доступу : http://www.viche.info/journal/2016/.
16. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: James A. Lewis [Електронний ресурс]. – Режим доступу : https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.
17. Tafoya W.L. Cyber Terror // FBI Law Enforcement Bulletin, 2011 [Електронний ресурс]. – Режим доступу : http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror.
18. Потеряхіна І.С. Роль кібертероризму в сучасних міжнародних відносинах / І.С. Потеряхіна [Електронний ресурс]. – Режим доступу : http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/183-protsesy-rehionalizatsii/368-rol-kiberteroryzmu-v-suchasnykh-mizhnarodnykh-vidnosynakh.
19. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій : [наук.-практ. посіб.] / [Б.М. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов] ; за заг. ред. проф. Я.Ю. Кондратьева. – К. : Вид. ПАЛИВОДА А.В., 2004. – 144 с.
20. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2. – С. 299–309.
21. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни / Т.П. Яцик // Науковий вісник Національного університету державної податкової служби України. Серія «Економіка, право». – 2014. – № 2. – С. 55–60.
22. Аваков А. До кіберполіції наберуть 400 співробітників [Електронний ресурс]. – Режим доступу : https://www.npu.gov.ua/uk/publish/article/1668681.

Анотація

Діордіца І. В. **Поняття і зміст кібертероризму.** – Стаття.

У статті досліджено поняття «тероризм» і запропоновано його узагальнене розуміння як діяльності, метою якої є залякування певного об'єкта, частіш за все йдеться про політичну арену, а кібертероризм – протиправне діяння, яке вчиняється з метою досягнення негативних наслідків, наприклад, отримання матеріальних благ чи загроза інформаційній безпеці держави. Акцентовано увагу на тому, що термін «кібертероризм» є синтезом понять «кібербезпековий простір» і «тероризм». Визначено основні особливості й характеристику кібертероризму. Аргументовано, що кібертероризм є видовим, а інформаційний тероризм – родовим поняттям одного негативного явища – тероризму. Також було наголошено на відсутності уніфікованого визначення терміна «кібертероризм».

Ключові слова: тероризм, кібертероризм, кіберпростір, інформаційний тероризм, кібервійна, інформаційна війна, інформаційне суспільство.

Аннотация

Диордица И. В. **Понятие и содержание кибертерроризма.** – Статья.

В статье исследовано понятие «терроризм» и предложено обобщенное его понимание как деятельности, целью которой является запугивание определенного объекта, чаще всего речь идет о политической арене, а кибертерроризм – противоправное деяние, которое совершается с целью достижения негативных последствий, например, получение материальных благ или угроза информационной безопасности государства. Акцентировано внимание на том, что термин «кибертерроризм» является синтезом понятий «пространство кибербезопасности» и «терроризм». Определены основные особенности и характеристика кибертерроризма. Аргументировано положение о том, что кибертерроризм является видовым, а информационный терроризм – родовым понятием одного негативного явления – терроризма. Также было отмечено отсутствие унифицированного определения термина «кибертерроризм».

Ключевые слова: терроризм, кибертерроризм, киберпространство, информационный терроризм, кибервойна, информационная война, информационное общество.

Summary

Diorditsa I. V. **The concept and content of cyber terrorism.** – Article.

It was concluded that the notion of cyber terrorism has emerged at the beginning of XXI centuries, before the mass use of the Internet. It was marked that the term “cyberterrorism” is a synthesis of the concepts of “cyber safe space” and “terrorism”. It was offered to understand terrorism as the activities which purpose is to intimidate a certain object, mostly often refers to the political arena, and cyberterrorism – lawful act that is committed with the aim of achieving of the negative consequences, such as obtaining of any material goods or threats to information security. Cyberterrorism takes place in the cyber safe space. It was marked that cyber terrorism is characterized by the use of the computer as a tool of the crime and the existence of the Internet as an international information space, in which is the object of the crime. Malicious attacks by criminal individuals or groups are committed at the following specific items, such as information, programmes, computers, local and global networks. It was argument that the cyberterrorism is a species, and information terrorism – a generic term of the negative phenomenon – terrorism. It was also stressed on the lack of a uniform definition of “cyberterrorism” both in doctrine and the legislation.

Key words: terrorism, cyber, cyberspace, information terrorism, cyberwarfare, information warfare, information society.