УДК343.92

КІБЕРТЕРОРИЗМ ЯК ФАКТОР ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ: ГЕНЕЗА ПОНЯТТЯ ТА ШЛЯХИ ПРОТИДІЇ

Геращенко О. С.

В даній науковій статті визначаються теоретичні засади кібертероризму (інформаційного тероризму) як загрози глобальній інформаційній безпеці України, а саме аналізуються погляди науковців щодо його тлумачення. Акцентується увага на законодавстві України щодо запобігання поширенню інформаційної зброї та кібертероризму в цілому.

Ключові слова: *тероризм, кібертероризм, терористична діяльність, протидія інформаційному тероризму, комп'ютерні технології, комп'ютерні мережі, інформаційна зброя, національна безпека України, інформаційний простір, комп'ютерні атаки*

В данной научной статье определяются теоретические основы кибертерроризма (информационного терроризма) как угрозы глобальной информационной безопасности Украины, а именно анализируются взгляды ученых о его толкования. Акцентируется внимание на законодательстве Украины относительно предотвращения распространения информационного оружия и кибертерроризма в целом.

Ключевые слова: *терроризм, кибертерроризм, террористическая деятельность, противодействие информационному терроризму, компьютерные технологии, компьютерные сети, информационное оружие, национальная безопасность Украины, информационное пространство, компьютерные атаки*

Rapid development of information and telecommunication technologies reaches every day everything new and new levels about what witnesses their active implementation to one and all spheres of activity of the person. Information networks, the Internet allow to communicate in only a few seconds. Therefore modern society doesn't imagine existence and normal functioning without information exchange in information and telecommunication systems any more. However, global distribution of information and communicative technologies in society led to emergence and development of essentially new type of terrorism - information terrorism or cyberterrorism.

Cyberterrorism is a new type of terrorism, at the same time already many works of domestic and foreign scientists are devoted to problems of its counteraction. But, unfortunately, in scientific community discussions concerning development of a general view on interpretation of the concept "cyberterrorism" are still conducted.

Cyberterrorism requires a detailed research also in the context of ways of its counteraction and prevention. Huge a gap on this matter is lack of fixing of basic provisions of cyberterrorism and methods of its counteraction at the legislative level. The most efficient direction in the solution of a complex problem of counteraction of cybercrime is international cooperation of law enforcement agencies in the sphere of information security on the basis of coordination of the national and international legal system presently.

In this scientific article theoretical bases of cyberterrorism (information terrorism) as threats of global information security of Ukraine are determined, namely views of scientists about its interpretation are analyzed. The attention is focused on the legislation of Ukraine concerning prevention of distribution of information weapon and cyberterrorism in general.

Keywords: *terrorism, cyberterrorism, terrorist activities, counteraction to information terrorism, computer technologies, computer networks, information weapon, homeland security of Ukraine, information space, computer attacks*

Постановка проблеми. Стрімкий розвиток інформаційних та телекомунікаційних технологій сягає з кожним днем все нових і нових рівнів, про що свідчить їх активне впровадження в усі без виключення сфери життєдіяльності людини. Інформаційні мережі, мережа Інтернет дозволяють обмінюватися інформацією за лічені секунди, крім цього впровадження комп'ютерних систем призвело до автоматизації різноманітних виробничих та управлінських процесів. Через це сучасне суспільство вже не уявляє собі існування та нормальне функціонування без інформаційного обміну в інформаційно-телекомунікаційних системах. Проте, глобальне поширення інформаційно-комунікативних технологій у суспільстві призвело до появи та розвитку принципово нового виду тероризму – інформаційного тероризму або кібертероризму. Вагомого значення у цьому контексті набуває науково-методичне забезпечення діяльності правоохоронних органів України щодо окреслення теоретичних, а також тактичних аспектів протидії інформаційному тероризму (кібертероризму).

Виходячи з цього, **метою даної наукової статті** є визначення теоретичних засад інформаційного тероризму (кібертероризму) як загрози глобальній інформаційній безпеці України, а також звернення уваги на законодавство україни щодо запобігання поширенню інформаційної зброї та кібертероризму в цілому.

Аналіз останніх досліджень і публікацій. Окремі теоретичні аспекти інформаційного тероризму (кібертероризму) як фактора загрози національній безпеці України, а також з'ясування українського законодавства у напрямі запобігання поширенню інформаційної зброї та кібертероризму в цілому, досліджувалися у працях Арешонкова В.В., Баєва О.О., Батуріна Ю.М., Березовської І.Р., Біленчука П.Д., Бутузова В.М., Гавловського В.Д., Горової С.В., Гуцалюк М.В., Хахановського В.Г., Шульги О.О., Зимовця В.В., Корченка О.Г., Кудінова В.А., Пилипчука В.Г., Дворникова В.С., Козонова Погорецького М.А., Шеломенцева В.П., Мельника С.В., Тихомирова О.О., Дубова Д.В., Ожевана М.А., . Шеломенцева В.П., Голубєвої В.О., Рижкової Е.В., Гавриша С.Б., Довгань О.Д., Хлань В.Г., Малышенка Д.Г. та інших вчених.

Виклад основного матеріалу дослідження. Кібертероризм є новим видом тероризму, водночас проблемам його протидії присвячено вже чимало праць вітчизняних та іноземних вчених. Але, на жаль, у наукових колах і досі ведуться активні дискусії з приводу вироблення спільного погляду на тлумачення поняття "кібертероризм". З метою якісного проведення наукового дослідження, а також досягнення поставленої мети

дослідження, пропонуємо, в першу чергу, визначитись із тлумаченням поняття "кібертероризм".

В українській і зарубіжній науковій літературі, пов'язаній з дослідженням кіберзлочинності, наявні різні підходи до визначення кібертероризму. Наведемо лише деякі з них. Так, на думку В.П. Харченка під кібертероризмом варто розуміти застосування методів тероризму (створення в соціальній сфері обстановки страху, неспокою, пригніченості з метою прямого або непрямого впливу на прийняття будь-яких рішень) у кіберпросторі [1, с. 132]. У своєму дослідженні на тему "Ознаковий принцип формування класифікацій кібератак" Корченко О.Г. розуміє кібертероризм як "принципово новий вид тероризму, який передбачає використання ресурсів інформаційних систем не лише як предмет злочинних посягань, а й середовище чи засіб скоєння злочину" [2, с. 35]. В обґрунтованому підході Старостіної Є.Т. до вироблення єдиного поняття "кібертероризм" доводиться позиція щодо доцільності тлумачити кібертероризм як різновид тероризму, в основу якого покладено спосіб здійснення терористичних дій, що виник у процесі розвитку інформаційно-телекомунікаційних технологій та впровадження їх у всі сфери сучасного суспільства [3].

На думку Малишенко Д.Г. кібертероризм – це різновид тероризму (поряд з ядерним, хімічним, космічним, сейсмічним, бактеріологічним, технологічним та ін.), який виник у процесі інформатизації суспільства і полягає у нанесенні збитків інформаційним системам за допомогою комп'ютерних атак [4]. Не можна оминути позицію Бутузова В.М., який під час монографічного дослідження на тему "Протидія комп'ютерній злочинності в Україні (системно структурний аналіз)" запропонував визначити кібертероризм саме як "вчинення терористичними угрупованнями або окремими особами комп'ютерних атак на певні елементи інформаційної інфраструктури, спрямовані на проникнення у комп'ютерні системи, перехоплення управління комп'ютерною системою, порушення функціонування засобів комп'ютерного обміну в мережі, справляти інший деструктивний вплив, що може привести до тяжких наслідків і здійснення впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади шляхом залякування населення та органів державної влади погрозами вчинення вищезазначених протиправних дій [5, с. 68].

Водночас, деякі вчені пропонують розуміти під терміном "кібертероризм" дії з дезорганізації інформаційних систем, що створюють небезпеку загибелі людей, заподіяння значної майнової шкоди або настання інших суспільно небезпечних наслідків, якщо такі дії вчинені з метою порушення суспільної безпеки, залякування населення або впливу на ухвалення певних рішень органами влади, а також якщо виникає загроза здійснення вказаних дій з тією самою метою [6, с. 80].

На думку прихильників іншого підходу комп'ютерний тероризм (кібертероризм) слід розглядати як один із різновидів неправомірного доступу до комп'ютерної інформації, розміщеної в окремій обчислювальній машині чи в мережі ЕОМ [7, с. 318]. Зазначимо, що такий доступ здійснюється з метою модифікації, знищення зазначеної інформації чи ознайомлення з нею, що забезпечує формування обстановки, за якої функціонування даної ЕОМ чи мережі виходить за межі, передбачені штатними умовами експлуатації, й виникає небезпека загибелі людей, заподіяння майнового збитку або настання будь-яких інших суспільно небезпечних наслідків.

Заслуговує на увагу позиція Дороті Денінга, експерта американського Центру досліджень тероризму, який визначив кібертероризм як елемент класифікації терористичної діяльності в Інтернеті та представив його як комп'ютерні атаки, спланованої з метою нанесення максимального збитку життєво важливим об'єктам інформаційної інфраструктури.

Враховуючи те, що в українському законодавстві відсутнє поняття "кібертероризм" та його визначення, пропонуємо погодитися із визначенням, наданим Пилипчуком В.Г. та Дзьобань О.П., а саме кібертероризм – це навмисна, політично вмотивована атака на об'єкти інформаційного простору (інформацію, що обробляється, комп'ютерну систему, мережу, а також на людину), що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної або суспільної безпеки, залякування населення, провокації військового конфлікту, чи загрозу вчинення таких дій [8].

Прикладами даного виду тероризму можна навести наступні події. Так, по-перше, напередодні здійснення газової атаки в токійському метро в 1995 році Японське терористичне угруповання "Аум Сінрікьо" створило комп'ютерну систему, що була здатна перехоплювати повідомлення поліцейських радіостанцій і відслідковувати маршрути руху поліцейських автомобілів. По-друге, у 2000 р. із пригороду Маніли в Інтернет запущено вірус "I love you" (інша назва "Love Bug"), що дуже швидко поширився по усьому світу і заразив більше 45 млн. комп'ютерних мереж (у т.ч. мережі Білого дому, ЦРУ, Міністерства оборони і Конгресу США, Британського Парламенту тощо); масштабна DoS-атака, що зробила недоступними протягом 2-3 годин сервери великих компаній Yahoo, eBay, CNN та ZDNet [9, с. 123]. По-третє, резонансне зараження 16 листопада 2001 року комп'ютерної мережі Укртелеком вірусом "Nimda", який серйозним чином вплинув на працездатність обчислювальної мережі Генеральної дирекції ВАТ "Укртелеком", яка налічує більше 700 комп'ютерів та десятки серверів. Як наслідок, це спричинило тимчасове відключення комп'ютерів від Інтернету, а також вивело з ладу систему корпоративної електронної пошти. За попередніми підрахунками, збитки від атаки складають більше 1 млн. грн. [10, с. 73]. По-четверте, у 2013 р. невідомі хакери отримали доступ і опублікували персональні дані 40 тис. солдатів армії США та більше 2 млн. партійних функціонерів керуючої партії Республіки Корея; активісти хакерського угруповання WikiCrew за допомогою DDoS-атаки вивели з ладу офіційний сайт Агентства національної безпеки США; хакерська група Syrian Electronic Army провела кібератаку на інформаційну інфраструктуру системи водопостачання ізраїльського м. Хайфа [9, с. 123]. Та наостанок, поштовий комп'ютерний вірус SirCam "викрадав" документи з органів державної влади, в тому числі адміністрації Президента України. Згадані приклади є свідченням актуальності досліджуваної теми, а також необхідності у розробленні тактичних прийомів протидії інформаційному тероризму.

Безперечно, головною зброєю у боротьбі з кібертероризмом залишається законодавство. Протидія інформаційному тероризму як складовій терористичної діяльності ґрунтується на засадах, визначених Законом України "Про боротьбу з тероризмом" [11, ст. 3]: 1) законності та неухильного додержання прав і свобод людини і громадянина; 2) комплексного використання з

цією метою правових, політичних, соціально-економічних, інформаційно-пропагандистських та інших можливостей; 3) пріоритетності попереджувальних заходів; 4) невідворотності покарання за участь у терористичній діяльності; 5) пріоритетності захисту життя і прав осіб, які наражаються на небезпеку внаслідок терористичної діяльності; 6) поєднання гласних і негласних методів боротьби з тероризмом; 7) нерозголошення відомостей про технічні прийоми і тактику проведення антитерористичних операцій, а також про склад їх учасників; 8) єдиноначальності в керівництві силами і засобами, що залучаються для проведення антитерористичних операцій; 9) співробітництва у сфері боротьби з тероризмом з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з тероризмом.

Протидія інформаційному тероризму правоохоронними органами України здійснюється шляхом оперативно-розшукової діяльності щодо виявлення, розкриття, профілактики окремих видів кіберзлочинів; інформаційно-аналітичної розвідки в комп'ютерній мережі, електронної телекомунікації; кримінально-процесуальної і криміналістичної діяльності щодо розкриття, розслідування злочинів і притягнення винних до відповідальності; спеціально кримінологічних заходів [12, с. 44].

На жаль, в правовому полі Україні не існує конкретного нормативно-правового акту, який закріплював б основні засади щодо кібертероризму та його протидії. Проте, з 2011 року робилося чимало спроб вирішити це питання на законодавчому рівні, в тому числі – у межах профільного закону України [13]. На сьогодні, на розгляд Верховній Раді України внесено проект Закону України № 2126а від 19.06.2015 "Про основні засади забезпечення кібербезпеки України", яким пропонується закріпити правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України [14]. Водночас, відповідно до зазначеного законопроекту кібертероризм визначається як терористична діяльність, що провадиться у кіберпросторі або з його використанням [14, ст. 1]. Стосовно суб'єктів забезпечення кібербезпеки постійної готовності, то на Службу безпеки України пропонуться покласти створення у межах затвердженої чисельності та забезпечення функціонування підрозділу з протидії кібертероризму та кіберзагрозам у сфері державної безпеки; а також вживання заходів з протидії кіберзагрозам державній безпеці або іншим життєво важливим інтересам держави [14, ст. 8]. Даним законопроектом не визначено перелік шляхів (способів) протидії кібертероризму, проте міститься норма статті банкетного характеру, відповідно до якої порядок запобігання, виявлення та усунення наслідків кібератак та кібертероризму, регламентується спільними нормативно-правовими актами суб'єктів забезпечення кібербезпеки.

Зазначимо, що тактика боротьби та протидії комп'ютерному тероризму визначається відповідно до розвитку науково-технічного прогресу, наукових досягнень у різних галузях науки, економічних, політичних умов і можливостей органів державної влади, а також правових засад [15, с. 51]. З огляду на це, а також на вище зазначений законопроект, пропонуємо впровадити у законопроект наступні тактичні прийоми запобігання поширенню інформаційної зброї та кібертероризму. По-перше, необхідно відпрацювати методики аналізу комп'ютерної злочинності, як особливий вид злочинності, та специфічні соціальні відносини у цій сфері. По-друге, здійснити розробку методів стеження за оперативним станом і викриття фактів наявності латентної злочинності в цій сфері. По-третє, розробити систему обліку жертв (потерпілих) від даних злочинів(як фізичних так і юридичних осіб) та визначити віктимогенний і криміногенний потенціал. По-четверте, розробити методику прогнозування ймовірної індивідуальної злочинної поведінки з боку виявлених осіб; розробити методичні засади планування у сфері боротьби з окремими видами комп'ютерних злочинів. По-п'яте, розробити критерії оцінки та підсумкові матеріали щодо стану і рівня ефективності здійснення тактичних превентивних заходів та стану змін в оперативній обстановці і поведінці осіб, з боку яких існує ймовірність вчинення даних злочинів. По-шосте, створити спеціалізовані підрозділи у сфері боротьби з комп'ютерними злочинами та інформаційним тероризмом. А також проводити наукові розробки щодо створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси.

Підводячи підсумок вище викладеному, необхідним є зазначити, що однією з причин виникнення тероризму є його соціальний характер, який виражається в існуванні відмінностей між рівнем життя людей, що є край актуальним питанням на сьогодні. Сучасне інформаційне суспільство створює принципово нові складнощі для системи національної безпеки. Через це Україна потребує пошуку нових можливостей гарантування її безпеки.

Кібертероризм як новий вид тероризму потребує детального та поглибленого дослідження. Аналіз триваючих дискусій в наукових колах з приводу тлумачення поняття кібертероризм надав можливість розглянути кібертероризм як спосіб здійснення терористичних дій, як різновид тероризму, як дії з дезорганізації інформаційних систем, як вчинення комп'ютерних атак, як різновид неправомірного доступу до комп'ютерної інформації тощо. Враховуючи те, що в українському законодавстві відсутнє визначення поняття "кібертероризм" нами було запропоновано погодитися із наступним визначенням "кібертероризм – це навмисна, політично вмотивована атака на об'єкти інформаційного простору (інформацію, що обробляється, комп'ютерну систему, мережу, а також на людину), що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної або суспільної безпеки, залякування населення, провокації військового конфлікту, чи загрозу вчинення таких дій".

Водночас, кібертероризм потребує детального дослідження також в контексті шляхів його протидії та запобігання. Величезною прогалиною з цього питання є відсутність закріплення основних положень кібертероризму та способів його протидії на законодавчому рівні. Найбільш дієвим напрямом у вирішенні комплексної проблеми протидії кіберзлочинності у наш час є міжнародне співробітництво правоохоронних органів у сфері інформаційної безпеки на основі узгодження національного та міжнародного законодавства. З огляду на це планується у наступній науковій публікації дослідити досвід зарубіжних країн щодо запобігання поширенню інформаційної зброї та кібертероризму з метою запозичення позитивного досвіду для України.

Література

1. Харченко В.П. Кибертерроризм на авиационном

транспорте / В.П. Харченко, Ю.Б. Чеботаренко, О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр. : Вип. 4 (28). — К. : НАУ, 2009. — С. 131-140.

2. Корченко О.Г. Ознаковий принцип формування класифікацій кібератак / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк, В.М. Кінзерявий, С.В. Казмірчук // Вісник Східноукраїнського національного університету імені Володимира Даля — №1, 2010. — С. 32-38.

3. Старостина Е. Подход к выработке единого понятия "кибертерроризм" [Электронный ресурс]. — Режим доступа: http://rudocs. exdat.com/ docs/index-198810. html – Назва з екрану.

4. Малышенко Д.Г. Противодействие компьютерному терроризму — важнейшая задача современного общества и государства / Д.Г. Малышенко // ВНИИ МВД России, "Вестник РАЕН". — № 4 — Т. 3. — 2004.

5. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно структурний аналіз): Монографія / В.М. Бутузов. — К. : КИТ, 2010. — 145 с.

6. Погорецький М.А. Поняття кіберпростору як середовища вчинення злочину / М.А. Погорецький, В.П. Шеломенцев // Інформаційна безпека людини, суспільства, держави — №2 (2), 2009. — С. 80.

7. Бутузов В.М. Сучасні загрози: комп'ютерний тероризм / Бутузов В.М. К.В. Тітуніна // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2007. – Вип. 17. – С. 316-324.

8. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації // Стратегічні пріоритети, № 4. – 2011. - Електрон. дан. (1 файл). – Режим доступу: http://www.nbuv.gov.ua/old_jrn/soc_gum/sp/2011_4/012-017.pdf - Назва з екрану.

9. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 2. – С. 118-129.

10. Дворников В.С., Козонова И.В., Бацазова А.З., Толасова З.М. Терроризм и биотерроризм. тактика и стратегия // Современные наукоемкие технологии. – 2005. – № 4 – С. 72-74.

11. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV. - [Електронний ресурс]. — Режим доступу: http://zakon0.rada.gov.ua/laws/ show/638-15 - Назва з екрану.

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

13. І. Костюк Україна в полі кібертероризму: загрози, реальність, протидія - [Електронний ресурс]. — Режим доступу: https://www.science-community.org/ru/node/155962 - Назва з екрану.

14. Про основні засади забезпечення кібербезпеки України: проект Закону України від 19.06.2015 р. № 2126а – [Електронний ресурс]. — Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657 - Назва з екрану.

15. Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // Інформаційна безпека людини, суспільства, держави — №3 (7), 2011. — С. 49-53.

Геращенко О.С.,
кандидат юридичних наук
Доцент кафедри тактико-спеціальної
та вогневої підготовки ОДУВС
Надійшла до редакції: 13.11.2016