УДК 323.28:004.92:321.011

КІБЕРТЕРОРИЗМ В УКРАЇНІ: ПОНЯТТЯ ТА ЗАПОБІГАННЯ КРИМІНАЛЬНО-ПРАВОВИМИ ТА КРИМІНОЛОГІЧНИМИ ЗАСОБАМИ

Топчій В.В., д. ю. н.,
завідувач кафедри кримінального права та кримінології
Навчально-науковий інститут права
Національного університету державної податкової служби України,
професор, заслужений юрист України

Автором досліджені прояви кібертероризму в Україні та проаналізовано нормативно-правову базу, яка передбачає кримінальну відповідальність за такі злочинні діяння; визначені перспективні напрями запобігання кібертероризму в Україні та чіткого нормативного врегулювання даного питання в Кримінальному Кодексі України.

Ключові слова: *тероризм, комп'ютерна злочинність, кіберзлочинність, кібертероризм.*

Автором исследованы проявления кибертерроризма в Украине и проанализирована нормативно-правовая база, которая предусматривает уголовную ответственность за такие преступные деяния; определены перспективные направления предотвращения кибертерроризма в Украине и четкого нормативного урегулирования данного вопроса в Уголовном Кодексе Украины.

Ключевые слова: *терроризм, компьютерная преступность, киберпреступность, кибертерроризм.*

Topchiy V.V. CRIMINAL LEGAL DESCRIPTION CYBER IN UKRAINE AND ITS ANTI WAYS

The article describes the current state of terrorism in Ukraine and ways of combating it, analyzes criminal legal characteristic of cyberterrorism and foreign experience. The author investigated cyberterrorism's manifestations in Ukraine and analyzed the regulatory framework which provides criminal penalties for such offenses; identified perspective directions of prevention of cyberterrorism in Ukraine and clear normative regulation of this issue in the Criminal Code of Ukraine.

Key words: *terrorism, computer crime, cybercrime, cyberterrorism.*

Розвиток інформаційних технологій та процес глобалізації зумовили появу нових загроз як міжнародній, так і національний безпеці, зокрема кібертероризму. Інформаційно-комунікативні технології настільки увійшли у наше життя, що ми вже не можемо уявити себе без комп'ютера. Але значення цих технологій для простого користувача не можна порівняти з їх важливістю для держави (банківський сектор, оборона, промисловість, сільське господарство, транспорт та будь-що інше). Так, з одного боку, розвиток комп'ютерних технологій полегшив життя, але з другого боку, це зумовило появу нових загроз як міжнародній, так і національній безпеці.

Актуальність дослідження даної проблеми полягає в першу чергу в тому, що тероризм як небезпечне явище у політичному, соціально-економічному житті, міжнаціональних відносинах світового співтовариства став об'єктом активної уваги політологів, юристів, істориків, психологів та інших науковців та характеризується необхідністю вивчення і узагальнення ряду важливих і складних подій міжнародного життя, що пов'язані з політикою та економікою, які є першочерговим об'єктом інтересу терористичних організацій сучасності. Але незважаючи на значний суспільний інтерес, чіткої теорії тероризму, яка б з точки зору кримінологічної науки викрила суттєві характеристики цієї небезпеки і тим самим вказала на шляхи його локалізації, створення можливостей для протидії, на сьогодні ще не розроблено.

Проблеми боротьби та розробки систем захисту інформаційних ресурсів, окремі питання здійснення протидії комп'ютерній злочинності та інших факторів, стримуючих створення інформаційного суспільства, розглядались в роботах таких фахівців, як В.О. Голубєв, О.В. Возженніков, О. Гончарєнко, Є. Лисіцин та інших.

Над даною проблематикою також працювали такі вітчизняні та зарубіжні науковці різних соціальних сфер, як С. Хантінгтон, С. Хоффман, М. Делягін, В. Кутирьов, Г. Мірською, І. Міхеєв, В. Хорос, В. Антипенко, В. Крутов, В. Ліпкан, С. Телешун та інші. Проте питань, які залишилися невирішеними та потребують наукового обґрунтування, залишилося ще багато, адже реалією теперішнього часу є той факт, що тероризм все більше загрожує безпеці більшості країн, тягне за собою величезні політичні, економічні, соціальні та моральні втрати. У сучасних умовах спостерігається поширення терористичної діяльності негативно налаштованих осіб, груп і організацій, ускладнюється її характер, зростає тяжкість вчинених терористичних актів. Тема набуває ще більшої загостреності та актуальності, зважаючи на той факт, що вона направлена на розкриття проблеми кваліфікації кібертерористичних проявів, які дедалі частіше виникають в практичній діяльності.

Основними завданнями, розв'язанню яких присвячена дана стаття, є наступні: охарактеризувати сучасний стан тероризму в Україні та окреслити шляхи його протидії; дослідити прояви кібертероризму в Україні та проаналізувати нормативно-правову базу, яка передбачає кримінальну відповідальність за такі злочинні діяння; визначити перспективні напрями запобігання кібертероризму в Україні та чіткого нормативного врегулюван-

ня даного питання в Кримінальному Кодексі України.

Слово тероризм походить від латинського «terror», яке в перекладі на українську мову означає «страх» чи «жах» [5]. Терористичні організації все частіше використовують нові інформаційні технології та мережу Інтернет із злочинними намірами поповнення коштів, здійснення пропаганди або передачі секретної інформації [3].

Відомий український політолог С. Телешун розрізняє три основні види терору, в основу класифікації яких покладено громадянство терористів і потерпілих від них, а також місце здійснення теракту: внутрішній – відповідні дії громадян однієї держави проти співвітчизників на власній території; транснаціональний – відповідні дії громадян однієї держави проти співвітчизників на території інших держав; міжнародний – відповідні дії груп громадян, однорідних або змішаних за національним складом, проти будь-яких осіб на території третіх країн [9, с. 163]. На думку І. Мехеєва, тероризм можна класифікувати на такі самостійні види: за територіальною ознакою: міжнародний; внутрідержавний; за злочинною мотивацією: політичний; релігійний; націоналістичний; економічний; за формою прояву: використання з терористичною метою вибухових пристроїв; захоплення повітряного судна та інше злочинне втручання в діяльність цивільної авіації; захоплення морського судна та інше злочинне втручання в діяльність міжнародного судноплавства; захоплення заручників; інші форми тероризму [6].

Можна також назвати інші форми тероризму: «хімічний», «біологічний», «психологічний». Останнім часом занепокоєння правоохоронних органів і вчених, що досліджують проблеми тероризму, викликає така нова форма тероризму, як високотехнологічний тероризм, складовими якого є кібертероризм (електронний, комп'ютерний) і космічний тероризм [2, с. 34–35].

На думку С.Хоффмана, міжнародний тероризм виявився можливим завдяки широкому набору засобів комунікації. Базою для ісламського тероризму, наприклад, слугує не тільки рух на підтримку палестинської боротьби і проти силової американської присутності. Його підживлює також опір «несправедливій економічній глобалізації» і західній культурі, в якій вбачається загроза для місцевих релігій і культур [10].

Важливим аспектом досліджень сучасного міжнародного тероризму є необхідність врахування безлічі чинників політичного, економічного і соціального порядку, що впливають на його розвиток і розповсюдження. У цьому плані вивчення тероризму безпосередньо пов'язано з дослідженнями глобалізації.

Антипенко В., досліджуючи причини і джерела тероризму, розглядає їх крізь призму наукових поглядів теоретика війни К. Клаузевіца і оцінює сучасний тероризм як світову загрозу, чия невпинна ескалація дає підстави стверджувати про доленосність цілей, заради яких ця терористична боротьба точиться. Розвиваючи свою думку, В. Антипенко аналізує статтю А. Арсеєнка «Глобалізація чи поляризація: що чекає світ», в якій констатується загострення соціальних проблем і одна із головних причин цього – те, що за останні 15 років дохід на душу населення знизився більш ніж у 100 країнах і що «сьогодні навіть західні дослідники змушені визнати, що глобалізація веде до «суспільства 20:80», яке характеризується вилученням 80% населення світу із соціального життя. Це стало «пасткою для ліберальної демократії», оскільки в XXI ст. боротьба за перерозподіл ресурсів може вилитися у «війну всіх проти всіх» [1, с. 276].

Для України раніше ця проблема не поставала так гостро, але з приєднанням до глобального інформаційного простору потенційна загроза існує. І поки кібертероризм з розряду «потенційної» загрози не перейшов до розряду «реальної» загрози, слід застосовувати превентивні заходи для недопущення його становлення. Основою забезпечення боротьби з кібертероризмом є створення ефективної системи заходів із запобігання, виявлення та припинення такого виду злочинності.

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. Сучасний рівень науково-технічного прогресу дає підстави виокремити такі форми прояву космічного тероризму: знищення космічних об'єктів, елементів наземних комплексів управління та інших структур космічних агентств; залякування окремих великих організацій, регіонів, країн вибором місць падіння захоплених космічних апаратів; залякування діями з космосу щодо морських, наземних і повітряних об'єктів.

З урахуванням переліченого вище, на нашу думку, під тероризмом слід розуміти протиправну діяльність, що полягає у вчиненні злочинних протиправних дій або в загрозі їх вчинення по відношенню до окремих осіб, груп чи групи осіб, матеріальних або нематеріальних об'єктів (цінностей), що супроводжуються залякуванням населення і навмисним створенням обстановки страху, пригніченості, напруженості з метою ухвалення рішень, вигідних для терористів, що характеризуються підвищеною суспільною небезпекою і публічним характером здійснення, тобто поняття «кіберзлочинність» об'єднує будь-який злочин, який можна здійснити за допомогою комп'ютерної системи або мережі та також проти комп'ютерної системи або мережі. Власне природа кіберзлочинів робить проблему всесвітньою, оскільки почасти не має значення, де саме вчинено подібний злочин.

Поняття тероризму має на увазі діяльність групи людей, а якщо ми говоримо про кібертероризм, то учасники цієї групи не просто знаходяться у різних країнах. І це не рядові спеціалісти-програмісти, а високоякісні професіонали, які володіють не тільки знаннями, але й останніми технологіями та розробками. Також становище ускладнює поширен-

ня мережі Інтернет, головна проблема якого міститься у складності контролю і зростанні чисельності користувачів. На сьогодні, за деякими даними, на планеті 1,7 млрд. користувачів Інтернет; для порівняння в 2000 році ця кількість становила лише 361 млн. користувачів [4]. Інтернет – головна зброя терористичних груп, яку вони використовують для зв'язку, проведення пропаганди, поширення інформацій, вірусів та інше.

В Україні на даний момент не розроблені нормативно-правові акти, що регулюють такий вид злочинності. Але головною зброєю у боротьбі з цією загрозою залишається законодавство, яке потребує подальшого вдосконалення. Якщо говорити про міжнародні правові акти в цій сфері, то першим і головним документом, в якому йде 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 нема такого виду злочину, як кібертероризм. Тому 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.

Саме тому, враховуючи останні зміни в суспільних відносинах, інформатизації та комп'ютеризації майже усіх ланок суспільної системи, український законодавець не стоїть осторонь цих змін. До Верховної Ради України був внесений на розгляд Проект Закону України «Про внесення змін до Кримінального Кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини)» (від 10 липня 2015 року реєстр. № 2328а).

В обґрунтування даного законопроекту наведено, що сучасний етап розвитку цивілізації характеризується сталою тенденцією до стрімкого збільшення ролі та значення електронного середовища інформаційно-телекомунікаційних систем (кіберпростору) для функціонування й розвитку державних і суспільних інститутів. За таких умов питання захисту життєво важливих інтересів людини, суспільства та держави в цьому середовищі набуває стратегічного значення. Крім того, Україна зазнає комплексного тиску з боку Російської Федерації, який включає скоординовані політичні, економічні, енергетичні, інформаційні, військові й розвідувально-підривні заходи. Збільшення масштабів соціальної небезпеки протиправних діянь в інформаційній сфері зумовлює необхідність посилення протидії загрозі поширення комп'ютерної злочинності та її крайньої форми – кібертероризму. Інформаційно-телекомунікаційні технології можуть бути використані як засіб зброї, які створюються з метою виведення з ладу критично важливих систем та об'єктів життєзабезпечення. Руйнування інформаційної інфраструктури критично важливих об'єктів України шляхом несанкціонованого доступу до інформації або впровадження в них шкідливих програм може завдати значної шкоди національній безпеці України, а також призвести до катастроф, людських жертв та інших тяжких і особливо тяжких наслідків. Заходами кримінально-правової протидії кібертероризму можна домогтися істотного поліпшення стану захищеності критично важливих об'єктів інформаційної інфраструктури України, що в даний час залишає бажати кращого. Проект Закону підготовлено з метою посилення кримінальної відповідальності за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

З цією метою проектом Закону пропонується доповнити статті 258 і 361 Кримінального кодексу України положеннями, що передбачають посилення відповідальності за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку об'єктів підвищеної небезпеки (об'єктів критичної інформаційної інфраструктури), встановивши більш сувору відповідальність за злочини, передбачені вказаними статтями КК України [8].

Проаналізувавши даний законопроект, можна дійти висновку, що положення, які він містить є дійсно важливими та, в першу чергу, нагальними для нашого суспільства. Підтримую думку, що ухвалення зазначеного законопроекту є надзвичайно актуальним, оскільки він дозволить забезпечити на законодавчому рівні захист інформаційних (автоматизованих), інформаційно-телекомунікаційних систем, електронних реєстрів та баз даних державної форми власності, об'єктів критичної національної інформаційної інфраструктури.

Висновки та перспективи подальших розвідок.

Ефективна боротьба з тероризмом можлива тільки на основі превентивних методів. Запобігання йому має полягати у виявленні, усуненні, нейтралізації, локалізації і мінімізації дії тих чинників і причин, які або породжують тероризм, або йому сприяють. Необхідно поглибити наукові дослідження з проблеми тероризму з урахуванням сучасних тенденцій розвитку світової спільноти, залучаючи до цього фахівців різних галузей знань: юристів, економістів, політологів, психологів, філософів, медиків та ін. Існує необхідність вироблення ретельно регламентованого порядку висвітлення в ЗМІ ситуацій, пов'язаних з актами тероризму. З метою підвищення ефективності контртерористичних і антитерористичних операцій слід поліпшити співпрацю силових відомств, які займаються боротьбою з тероризмом. Перспективними є подальші наукові дослідження щодо розробки нових методів і механізмів боротьби з тероризмом, а також поглиблене з'ясування й усунення причин цього небезпечного явища.

15 жовтня 2015 року відбулася презентація новоствореного департаменту кіберполіції в Міністерстві внутрішніх справ. За словами глави Уряду, проблема кіберзлочинності тур-

бує не тільки Україну, але й увесь світ. Одним з аспектів тероризму є крадіжка і злом баз даних як зарубіжних, так і вітчизняних державних органів влади. Під загрозою злому можуть перебувати державні реєстри з персональними даними громадян. Захистити ці онлайн-сервіси від кіберзлочинців повинні працівники новоствореного департаменту. Глава уряду підтримав рішення міністра внутрішніх справ України щодо створення нового підрозділу. У кіберполіцію, яка стала міжрегіональним територіальним підрозділом Національної поліції, планують набрати близько 400 працівників, серед яких 187 інспекторів та 39 спеціальних агентів інформаційних технологій [11].

Проте незрозумілою є позиція щодо недоцільності прийняття законопроекту про посилення відповідальності за кіберзлочинність та кібертероризм, але прийняття нової кіберполіції. Дії є непослідовними з точки зору протидії тероризму загалом та кібертероризму зокрема. На мою думку, заходи запобігання кібертероризму повинні бути комплексними і включати як реформування чинної структури правоохоронних органів, так і нормативне врегулювання даного питання.

Отже, зробивши аналіз та дослідження щодо кібертероризму, його проявів та шляхів запобігання, слід наголосити в першу чергу на важливості його виокремлення в Кримінальному кодексі України та посиленні відповідальності, на що й спрямований вказаний запропонований законопроект. Окрім цього, хочу зауважити, що в діючому кримінальному законодавстві відсутній термін «тяжка шкода здоров'ю», саме тому пропонуємо його замінити на визначення «тяжкі наслідки», який може включати і заподіяння тілесних ушкоджень, і смерть особи.

Хочу зауважити також на тому, що профілактична робота, яка спрямована на протидію кіберзлочинності загалом проводиться. Зокрема в Україні створено Центр з питань боротьби з комп'ютерними злочинами та розроблена Концепція стратегії реалізації державної політики з боротьби з кіберзлочинністю. Якщо прослідити виявлення злочинів у сфері високих інформаційних технологій, то, згідно зі статистикою МВС України, у 2005 році було виявлено 615 злочинів, у 2006 році – 583, у 2007 році – 656, а у 2008 році – 691, у 2009 році – 707. З наведених даних ми бачимо, що у 2006 році порівняно з 2005 роком спостерігається падіння виявлення, але вже у 2007 році показники перевищили данні 2005 та 2006 років, та продовжили ріст у 2008 і 2009 роках [7].

А от що стосується профілактики та протидії саме кібертероризму на нормативному рівні, це взагалі не врегульовано, що потребує детального вивчення та опрацювання. Головною прогалиною, яка є на даний час, цієї проблеми – це недосконаліть національного та міжнародного законодавства. Тому слід дійсно посилювати відповідальність за таку глобальну проблему, як кібертероризм, адже це – нова загроза інформаційного суверенітету держави, якій необхідно запобігати, допоки вона не укорінилася в державну та соціальну систему нашої країни.

ЛІТЕРАТУРА:

1. Антипенко В.Ф. Протидія сучасному тероризму з позицій оцінки його міжнародної сутності // Тероризм і боротьба з ним. Президенту України, ВРУ, Уряду України, органам центр. і місцев. виконав. влади. Аналіт. розробки, пропоз. наук. і практ. працівників: Міжвід. наук. зб. ; за заг. ред. А.І.Комарової, Ю.В.Землянського, В.О.Євдокимова та ін. – К. : НДІ «Проблем людини», 2000. – Т. 19(1). – 610 с.

2. Богданов О.І Високотехнологічний тероризм нової епохи / О.І. Богданов // Проблеми безпеки особистості, суспільства, держави. – 2005. – № 4. – С. 34–37.

3. Бойченко О.В. Кібертероризм у складі сучасних проблем національної безпеки / О.В. Бойченко, О.О. Ончурова // Форум права. – 2010. – № 2. – [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/j-pdf/FP_index.htm_2010_2_12.pdf.

4. Глебов А.Г. Статистика использования Интернет / А.Г. Глебов // [Електронний ресурс]. – Режим доступу : http://www.promovare-site.md/view_article.php?id=5.

5. Литвинов В.Д. Латинсько-український словник / В.Д. Литвинов. – К. : Укр. Пропілеї, 1998. – 644 с.

6. Михеев И.Р. Терроризм: понятие, ответственность, предупреждение / И.Р. Михеев // [Електронний ресурс]. – Режим доступу : http://crime.vl.ru.

7. Офіційна статистика Міністерства внутрішніх справ України [Електронний ресурс]. – Режим доступу : http://mvs.gov.ua.

8. Про внесення змін до Кримінального Кодексу України (щодо посилення відповідальності за кібертероризму та кіберзлочини)» (від 10 липня 2015 року реєстр.№ 2328а): Проект Закону України, внесений народним депутатом України Мирним І.М. // [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55972

9. Телешун С.Д. Сучасний тероризм: українські реалії / С.Д. Телешун // Політ. менеджмент. – 2005. – № 1 (10). – С. 163–169.

10. Хоффман С. Столкновение глобализаций: Как сделать мир более пригодным для жизни. Новая парадигма? / С. Хоффман // [Електронний ресурс]. – Режим доступу : http://www.imperativ.net/imp11/hoffman.html.

11. Цензор.НЕТ. Стартовал набор в новую украинскую киберполицию // [Електронний ресурс]. – Режим доступу : http://censor.net.ua/news/356402/startoval_nabor_v_novuyu_ukrainskuyu_kiberpolitsiyu.