ТРИБУНА МОЛОДОГО ВЧЕНОГО

УДК 004.056: 341(045)
DOI https://doi.org/10.32837/yuv.v0i3.2202

І. Рульов,
аспірант кафедри міжнародного та європейського права
Національного університету «Одеська юридична академія»

СПІВВІДНОШЕННЯ КІБЕРТЕРОРИЗМУ ТА КІБЕРЗЛОЧИНУ

Постановка проблеми. Під час дослідження такого явища, як кібертероризм, дуже важливим стає питання розмежування такого явища із суміжними злочинами у сфері інформаційної безпеки. Уваги потребує чітке розмежування кібертероризму та кіберзлочину. Через невизначеність у законодавстві термінології ми можемо визначити необхідність детального дослідження цих явищ як небезпечних явищ та соціально небезпечних ризиків для держави. Це є важливим для побудови правильного категоріального апарату, з яким надалі зможуть працювати дослідники та законотворці. Також зазначимо, що оскільки кібертероризм – це наднаціональне явище, притаманне усім країнам світу, та яке виходить за межі юрисдикції однієї держави, вважаємо, що розглядати це явище має сенс через призму міжнародного права, а також діяльності міжнародних організацій у боротьбі з кіберзлочинністю.

Оцінка стану літератури. Питання поняття кіберзлочину і кібертероризму були освітлені у працях вітчизняних та іноземних вчених, таких як: Бутузов В., Веселова Л., Геращенко О., Гриник Р., Журавльов В., Романюк Б., Коваленко В., Васильковський І., Мокляк В., Сіренко О., Соколов А., Степанюк О., Collin B., Топчій В.

Метою статті є розмежування поняття кібертероризму із суміжним поняттям кіберзлочину, як явищ, які погрожують інформаційній безпеці. Відокремлення кіберзлочинів як окремої категорії злочинів. Досягнення відповідної мети можливо на основі вирішення таких **завдань**: 1) дослідження поняття кіберзлочину та кібертероризму; 2) проведення спільних ознак та відмінностей кіберзлочину та кібертероризму.

Виклад основного матеріалу. У XXI столітті важко уявити наше життя без кіберпростору, який все більш набуває місце в нашому житті. Навіть державний апарат та взаємодія громадян із державою здійснюються через комп'ютерні системи. Як зазначає професор М. Василенко, інформація потребує захисту від випливу навмисних дій зловмисників та природних чинників [3]. Саме тому велику небезпеку становлять злочини, пов'язані з інформаційним простором, вони можуть бути загрозою, як приватним особам, так і державі. Групу злочинів, здійснюваних із використанням комп'ютерних систем, згрупували в поняття кіберзлочинів. Як зазначає І. Васильковський, кіберзлочинність (або «злочин з використанням комп'ютерних технологій») – це економічний злочин, скоєний з використанням обчислювальної техніки та мережі Інтернет [9]. Ми

вважаємо, що кіберзлочини, значним чином, дійсно були здебільше економічними злочинами, але із впливом часу вони вийшли на новий рівень, а саме як соціально небезпечне явище, яке загрожує навіть інформаційній безпеці держави, тому ми вважаємо, що для більш повного дослідження питання кіберзлочину ми маємо звернутися до думки В. Бутузова. В. Бутузов вважає, що комп'ютерні злочини та кіберзлочини – різні види злочинів у сфері інформаційних технологій, класифікація яких відбувається за такими ознаками:

– ознакою віднесення певних злочинів у сфері високих інформаційних технологій до комп'ютерних є знаряддя вчинення злочину – комп'ютерна техніка. Причому об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації;

– ознакою віднесення злочинів у сфері високих інформаційних технологій до кіберзлочинів є специфічне середовище вчинення злочинів – кіберпростір (середовище комп'ютерних систем та мереж). Тому об'єктом злочинного посягання можуть бути відносини будь-якої галузі людської діяльності, що має свій прояв у кіберпросторі. З цього ми можемо дійти до висновку, що головною ознакою кіберзлочину є його скоєння за допомогою комп'ютерних систем та мереж. Тобто всі дії злочинного характеру, які здійснюються в мережі Інтернет, можуть підпадати під поняття кіберзлочину [1].

Але важливо зазначити, що інструментом кіберзлочину можуть бути не тільки мережа Інтернет, як зазначає Л. Веселова. Кіберзлочинність не обмежується межами злочинів, вчинених у глобальній мережі Інтернет. Вона поширюється на всі види злочинів, вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть бути предметом (метою) злочинних посягань, середовищем, в якому скоюються правопорушення, і засобом чи знаряддям злочину. Такий підхід є більш вдалим та більш обґрунтованим щодо сутності кібернетичного простору, що формується за рахунок усіх можливих локальних та глобальних інформаційно-телекомунікаційних мереж, хоча мережа Інтернет серед них є переважаючою. З цього ми можемо дійти до висновку, що кіберзлочин може бути скоєний як за допомогою мережі Інтернет, так і обмежуючись закритими локальними мережами та носіями інформації. Це ще більш збільшує загрозу від кіберзлочинів, тому що навіть локальні мережі та системи, які взагалі не під'єднанні до мереж, а саме об'єкти інфраструктури можуть бути підтверджені злочинному втручанню у їх функціонування [4].

Ми вважаємо, що оскільки кіберзлочинність – це інтернаціональне явище, яке не обмежується кордонами держав, ми маємо звернутися до думки міжнародних організацій, компетентних у сфері протидії кіберзлочинам. Ще у 2000 році на форумі Конгресу ООН із попередження кіберзлочинності цей термін був розкрит у двох значеннях. По-перше, у вузькому розумінні, кіберзлочин – це будь-яке протиправне діяння, здійснюване за допомогою електронних операцій, метою якого є подолання захисту комп'ютерних систем і обчислюваних ними даних. У широкому розумінні кіберзлочин – це будь-яке протиправне діяння, вчинене у зв'язку з комп'ютерною системою чи мережею або за її допомогою, включаючи такі злочини, як незаконне зберігання, пропозиція або поширення інформації за допомогою комп'ютерної системи чи мережі. Як зазначає проф. О. Сіренко, кіберзлочин – це кримінальне правопорушення, що вчиняється за допомогою або через комп'ютерні системи, посягає на право захисту від несанкціонованого

поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію, і за яке передбачено кримінальну відповідальність [11]. Всі кібернетичні злочини є досить небезпечними, оскільки можуть зачепити будь якого громадянина але, на нашу думку, найбільш небезпечним кіберзлочином у наші часи є кібертероризм.

У інформаційну еру, поряд ыз класичними загрозами, з'явились загрози, пов'язані з розвитком високих інформаційних технологій. До таких загроз ми можемо віднести і кібертероризм. Термін «кібертероризм» був запропонований у 1980-х р. старшим науковим співробітником американського Інституту безпеки і розвідки (анг. – Institute for Security and Intelligence) Баррі Колліном, який використав його в контексті тенденції до переходу тероризму від фізичного до віртуального, погрожуючого перетин та злиття цих світів. Це показує, що поряд ыз технологічним розвитком суспільства все більш складними стають злочини. [15].

Поняття кібертероризму має в собі основну частину поняття тероризму через призму інформаційного поля, в якому живе людство в XXI сторіччі. Це збігається з думкою Соколова, який тлумачить кібертероризм як комплексну модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікт. Ми вважаємо, що Соколов дуже влучно розкрив поняття кібертероризму, однак питання стає щодо політичної мотивації кібертерориста, оскільки, окрім політичних цілей, на нашу думку, можуть бути як правовий нігілізм, так і бажання економічного збагачення [14].

Поняття «кібертероризму» дуже влучно розкрили в The National Conference of State Legislatures (USA), яку було створено для вироблення узгодженої політики з питань економіки і внутрішньої безпеки в США, яка визначає кібертероризм як використання інформаційних технологій терористичними групами і терористами-одинаками для досягнення своїх цілей, що може включати: використання інформаційних технологій для організації та виконання атак проти телекомунікаційних мереж, інформаційних систем і комунікаційної інфраструктури, або обмін інформацією, а також загрози з використанням засобів [5]. Як зазначає І.В. Діордіца, 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 [7]. Т.В. Смачило, А.Р. Кривцун визначає кібертероризм також як інформаційну атаку, додаючи, що «така інформаційна атака посягає на електронну інформацію, обчислювальні системи, банківські системи, технічні засоби передачі даних та інші системи інформаційної інфраструктури. Здійснюється окремими особами або терористичними угрупуваннями [13]. У дослідника з проблем тероризму В.П. Журавльова існує схожа точка зору щодо природи кібертероризму. Він вважає, що кібертероризм проявляється у двох формах: по-перше,

комп'ютерні економічні злочини, які вчиняються за допомогою спеціалістів хакерів, серед яких:

– махінації та маніпулювання системами обробки даних (несанкціонований переказ грошей та їх використання);

– шпигунство (проникнення до конфіденційних каналів зв'язку державних органів для отримання інформації, шпигунство з метою отримання інформації щодо закритих технологій);

– диверсія (завдання шкоди технічному та програмному забезпеченню вірусами, що порушують функціонування державних органів та інших установ);

– незаконне користування комп'ютерними послугами (програмами, покупки за рахунок інших тощо);

по-друге, розголошення таємниці – отримання комерційної та конфіденційної інформації (що нерозривно пов'язане з першим видом), серед чого:

– несанкціоноване отримання інформації для нецільового її використання особами, які не мають на це відповідного доступу;

– незаконний збір та перехоування інформації;

– порушення правил користування конфіденційною інформацією [8].

Ми можемо побачити, що кібертероризм відрізняється від звичайного тероризму окремим засобом вчинення, а саме за допомогою інформаційних технологій, саме тому ми можемо відзначити велику загрозу кібертероризму. У той час як технології все більш проникають в наше життя, все більш небезпечними стають кіберзлочини, тому так важливо сформувати належний понятійний апарат для законодавчого закріплення протидії кіберзлочинам та кібертероризму. Як зазначає В.В. Топчій, 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 [16]. Кібертероризм вчиняється з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту, і зараз, коли інформаційні технології та мережа Інтернет використовується майже усіма, стало дуже просто навести панічний настрій у громадян, наприклад на головному сайті міської ради викласти інформацію, яка не відповідає дійсності та лякає населення. Тим більш ми маємо дослідити кібертероризм як злочин, який здійснюється за допомогою інформаційних технологій, а саме як вид кіберзлочину.

Ми вважаємо, що кібертероризм є одним із найнебезпечніших видів кіберзлочину через його дуже небезпечні наслідки, а саме: велике коло потерпілих, великий суспільний резонанс, що створює панічний настрій у населення. Як зазначає Р.О. Гриник, керівники ряду радикальних мусульманських організацій Близького Сходу надають дедалі більшого значення використанню у своїй діяльності саме сучасних інформаційних технологій, розглядаючи їх як ефективний різновид зброї в боротьбі з режимами Ізраїлю, Саудівської Аравії і підтримуючих їх західними країнами. Це, по-перше, досить недорогий засіб здійснення терористичного акту (тому до кібертероризму вдаються в основному країни з нерозвиненою економікою країни), а по-друге, складнощі з виявленням кіберзлочинця [7]. Знаковим для ефективного виявлення кибергроз може стати створення центру забезпечення інформаційної безпеки (SOC), який повинен відігравати роль центрального штабу, що координує всю роботу в цьому напрямі. Сьогодні все частіше можна спостерігати трансформацію функцій SOC від пасивного захисту до активної оборони, ретельно спла-

нованої, безперервної, націленої на виявлення і нейтралізацію прихованих зловмисників [2]. Зазначимо, що в Ізраілі понад 20 років існує Національне кібербюро Ізраілю (INBC), яке протидіє кіберзагрозам із боку терористичних організацій. Як зазначає С.В. Мельник, 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 [11].

Поняття тероризму включає в себе не тільки терористичні злочини, а й інші діяння, що сприяють їм, та фактично відповідає категорії «терористична діяльність», яка використовується в Законі України «Про боротьбу з тероризмом» № 638-IV від 20 березня 2003 р. Відповідно до ст. 1 зазначеного Закону терористична діяльність – це діяльність, яка охоплює:

1) планування, організацію, підготовку та реалізацію терористичних актів;

2) підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів у терористичних цілях;

3) організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само, як і участь у таких актах;

4) вербування, озброєння, підготовку та використання терористів;

5) пропаганду й поширення ідеології тероризму;

6) проходження навчання тероризму;

7) виїзд з України та в'їзд в Україну з терористичною метою, фінансування тероризму;

8) інше сприяння тероризму.

Через це ми можемо дійти висновку, що якщо перелічені дії будуть зроблені за допомогою технічних засобів, вони, як зазначив Баррі Коллін, переходять фізичного тероризму до віртуального. Як зазначає В. Мокляк, під терористичною діяльністю розуміється сукупність дій з організації, керівництва, ресурсного забезпечення та сприяння функціонуванню злочинних об'єднань терористичного спрямування, а також підготовка й учинення терористичних актів та інших злочинів у терористичних цілях, а значить, всі ці дії, вчинені з метою проведення терористичного акту через інформаційні системи, можна розцінювати як кібертероризм. Із цього ми можемо зробити висновок, що діяльність терористичних груп у мережі Інтернет, які здійснюють перелічені в Законі України «Про боротьбу з тероризмом», може бути кваліфікована в майбутньому як кібертероризм, особливо це стосується протизаконних закликів до тероризму в мережі Інтернет [10].

Висновки

Таким чином, кіберзлочин є комплексним поняттям, яке включає в себе ознаки кіберзлочину як особливого соціально небезпечного явища, притаманного суспільству з високо розвиненими інформаційними технологіями. У свою чергу, кібертероризм є одним із найнебезпечніших видів кіберзлочини, оскільки спрямований на вкрай важливу складову частину суспільства і держави, а саме на національну та інформаційну безпеку.

Потрібно розуміти, що кібертероризм – це нове явище в суспільстві, і його не можна розглядати так само, як колишні види злочинів та терористичних атак.

Ми змогли розмежувати кібертероризм та кіберзлочин через доктринальні джерела, але ми можемо

визначити необхідність детального дослідження цих явищ.

Ми можемо охарактеризувати кібертероризм та кіберзлочиність як частину і ціле, тобто будь-який акт кібертероризму є кіберзлочином (за аналогією, будь який терористичний акт є злочином), але їх відрізняє спеціальні засоби здійснення злочину.

Кібертерористичний акт відрізняється метою від кіберзлочину, мається на увазі залякування і паніка для досягнення свої цілей. Розмежування цього є важливим для побудови правильного категоріального апарату, з яким надалі зможуть працювати дослідники та законотворці.

Також зазначимо, що оскільки кібертероризм – це інтернаціональне явище, воно може загрожувати будь якій державі, незважаючи на кордони. Це вказує, що поняття кібертероризму має розглядатися не тільки в контексті вітчизняного права, а й міжнародного, яке націлено на подолання проблем міжнародного характеру, саме яким і є кібертероризм.

Потрібно надалі досліджувати питання кібертероризму як перспективну та важливу для інформаційної безпеки сферу, а також законодавчо закріпити такі поняття, як кіберзлочинність та кібертероризм, у законодавстві, а також закріпити у Кримінальному кодексі України відповідальність саме за кіберзлочини та кібертерористичні акти, тому що рано чи пізно та або інша атака зловмисників завершиться успіхом, тож потрібно бути готовим до нових загроз. Це надасть змогу правильно кваліфікувати такі злочини, а також змогу підняти рівень Українського законодавства до міжнародних стандартів.

Стаття присвячена дослідженню таких понять, як кібертероризм та кіберзлочин, а також їх співвідношенню. Розкрито поняття кіберзлочину як окремої категорії злочинів, притаманних інформаційній ері людства, розглянуто його ціль, мета, засоби скоєння. Визначено історичний розвиток поняття кіберзлочину та його суспільну небезпечність із впливом часу. Досліджені наукові підходи доктринального характеру до поняття кіберзлочину. Проаналізовані погляди інших вчених щодо поняття кіберзлочину. Відокремлено кіберзлочин як окремий вид суспільно небезпечної діяльності. Досліджено, що кіберзлочин є комплексним поняттям, яке включає в себе ознаки кіберзлочину як особливого соціально небезпечного явища, притаманного суспільству з високо розвиненими інформаційними технологіями.

Визначено поняття кібертероризму. Розкрито підходи до поняття кібертероризму та виникнення поняття кібертероризму як соціально небезпечного діяння. Досліджено суспільну небезпечність кібертероризму та його відокремлення від звичайного тероризму.

Досліджено співвідношення понять кіберзлочину та кібертероризму. Визначено спільні риси в поняття кіберзлочину та кібертероризму. Розкрито поняття кібертероризму як складової частини поняття кіберзлочину. Визначено відмінність у соціальній небезпечності кібертероризму як більш небезпечного явища, ніж кіберзлочин. Проаналізовано законодавств України, як джерело поняття кібертероризму, та визначено недоліки у вітчизняному законодавстві щодо протидії кіберзлочинності та кібертероризму. Розкрито поняття кібертероризму як інтернаціонального явища та його небезпечність не тільки для приватних осіб, а й для національної безпеки держави.

Розроблено пропозиції стосовно вдосконалення законодавства

Україні в галузі інформаційної безпеки, що полягають у приведенні норм законодавства до Європейського законодавства в галузі протидії кіберзлочинності та кібертероризму.

Ключові слова: кібертероризм, кіберзлочин, інформаційна безпека, національна безпека, кібербезпека.

Rulov I. THE RATIO OF CYBERTERRORISM AND CYBERCRIME

The article is assigned to understanding of the concept, such as cyberterrorism and cybercrime, as well as their co-relation. To understand cybersecurity as a category of mischief in the information sphere inherent to people, in its purpose, and apparent in situation and tools being used to be committed. The historical development of understanding of cybercrime indicated the danger for national security in a present hour. Doctrinal scientific approach has been examined and exercised to understand cybercrime. The views of other scientists have been analyzed to commit to the understanding of cybercrime. Distinctly cybercrime is researched as a special case of a socially dangerous activity. It is researched that cybercrime is complex in its definition, which includes the signs of a cybercrime, as a special socially damaging phenomenon, being inherent to societies with highly developed information systems.

Cyberterrorism's definition has been finalized. The scientific approach to understanding of cyberterrorism has been found, through which the corpus delicti was defined as an act that threatens the national informational security. The borders that distinguish common terrorism from cyberterrorism have been defined.

The co-relation of cyberterrorism and cybercrime have been established. The features in common of both cybercrime and cyberterrorism have been found. The definition of cybercrime includes in itself cyberterrorism and is a part of cybercrime case. Cyberterrorism is a highly severe case of cybercrime that threatens national security. Ukrainian legislation has been analyzed, as source, to understand cyberterrorism and shortcomings of current legislation regarding cybersecurity and prevention of cyberterrorism have been found. The definition of cyberterrorism has been expanded, and recognized as an international phenomenon, bringing damage not only to the personal interests of citizen but also to the nation's security.

Proposals have been created to the full fill the gaps in Ukrainian legislation concerning information security that will bring us closer to European legislation norm regarding perversion and obstruction of cybercrime.

Key words: cyberterrorism, cybercrime, information security, national security, cyber security.

Література

1. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КІТ, 2010. 408 с.

2. Василенко М.Д. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення. Юридичний вісник. Одеса : ВД «Гельветика», 2018. № 4. С. 35–41.

3. Василенко М.Д. Безпека комп'ютерних систем в контексті законодавства та запобігання кіберзагроз. Юридичний вісник. Одеса : ВД «Гельветика». 2019. № 2. С. 70–76 (в співавторстві з Бойком В.Д.).

4. Веселова Л.Ю. Кібернетичні загрози у контексті сучасного сприйняття їх в Україні. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «ПРАВО». Випуск 29, 2020. DOI: https://doi.org/10.26565/2075-1834-2020-29-22. URL : https://periodicals.karazin.ua/law/article/view/15443.

5. Геращенко О.С. Кібертероризм як фактор загрози національній безпеці України: генеза поняття та шляхи протидії. Південноукраїнський правничий часопис. 2016. № 3-4. С. 39–42.

6. Гриник Р.О. Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. / Кіровоград. нац. техн. ун-т, Черкас. держ. технолог. ун-т та ін. ; [відп. за вип. : О.П. Доренський]. Кропивницький : КНТУ, 2016. 209 с.

7. Діордіца І.В. Поняття та зміст кібертероризму. URL : http://goal-int.org/ ponyattya-ta-zmist-kiberterorizmu/.

8. Журавльов В.П., Романюк Б.В., Коваленко В.В. Тероризм: сучасний стан та міжнародний досвід боротьби / Національна академія внутрішніх справ України, 2003. 403 с.

9. Васильковський І.І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2018. Вип. 1-2(10-11). С. 276–282. URL : http://nbuv.gov.ua/jpdf/ muvnudp_2018_1-2_46.pdf (дата звернення: 15.08.2020).

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

11. Мокляк В.В. Сучасна кримінологія: досягнення, проблеми, перспективи : матеріали міжнар. наук. конф., присвяч. 50-річчю каф. кримінології та кримін.-викон. права (Харків, 9 груд. 2016 р.) / М-во освіти і науки України, Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. кримінології та кримінал.-виконав. права. Харків : Право, 2016. С. 226–228.

12. Сіренко О.В. Поняття кіберзлочинів та особливості методики їх розслідування Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ.конф., м. Одеса : ОДУВС, 2017. С. 48–49.

13. Смачило Т.В., Кривцун А.Р. Феномен інформаційного тероризму як загрози міжнародній безпеці. URL : http://molodyvcheny.in.ua/files/ journal/2017/11/30.pdf.

14. Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. Санкт-Петербург : БХВ – Петербург; Арліт 2002. 496 с.

15. Collin B. The Future of Cyberterrorism. Crime & Justice International Journal. 1997. Vol. 13. Вип. 2.

16. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. Науковий вісник Херсонського державного університету. Серія : Юридичні науки. 2015. Вип. 6(3). С. 65–68. URL : http://nbuv.gov.ua/UJRN/ Nvkhdu_jur_2015_6(3)__16.