УДК 340.12
DOI: 10.21564/2663-5704.49.229782

Трофименко Володимир Анатолійович, кандидат юридичних наук, доцент, доцент кафедри філософії, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
e-mail: v.a.trofymenko@nlu.edu.ua
ORCID ID: 0000-0003-2240-3727

Мішанчук Анастасія Володимирівна, студентка міжнародно-правового факультету, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
e-mail: mishanchuk.anastasija@gmail.com

КІБЕРТЕРОРИЗМ: СПРОБА ФІЛОСОФСЬКО-ПРАВОВОГО ОСМИСЛЕННЯ

Кібертероризм набуває все більшої небезпеки для суспільства в цілому і для окремих громадян зокрема. У статті розглянуто сучасні уявлення та погляди щодо розуміння сутності кібертероризму, його ключові елементи, джерела, особливості реалізації, специфіку та класифікації. Показано генезу поняття «кібертероризм» та його співвідношення з поняттям «тероризм».

Ключові слова: *безпека, кібербезпека, тероризм, кібертероризм, кіберпростір, кібернетика.*

Постановка проблеми. Українська держава продовжує інтеграційні процеси з міжнародною спільнотою, зокрема з Європейським Союзом і NATO. Але всебічна інтеграція призводить до того, що Україна «вимушено інтегрується» і в ті негативні процеси, від яких потерпає сучасний світ та з якими він намагається боротися. Зі швидким розвитком мережі Internet зростає його використання зі злочинними намірами. Новизна, рівень небезпеки, обсяги отриманих і майбутніх можливих збитків такого виду злочинності сприяли формуванню такого небезпечного явища, як кібертероризм. Відповідно, перед світовими науковцями постало нове завдання – найбільш точно і загально зрозуміти сутність поняття кібертероризму, дослідити його глибинні аспекти, розробити єдиний понятійний апарат і запропонувати систему превентивних заходів.

Аналіз останніх досліджень і публікацій. Тему інформаційного тероризму в межах українського кіберпростору, а також його нерозривної взаємодії

зі світовою мережею, теоретичні аспекти цього явища, розкриття понять, що стосуються кіберзлочинності, висвітлено у публікаціях таких вітчизняних дослідників, як С. Гнатюк, О. Геращенко, В. Остроухов, М. Присяжнюк, І. Діордіца, О. Трофименко, Ю. Прокоп, І. Арістова, В. Цимбалюк, О. Задерейко, О. Богданов, О. Дрожчан, М. Гуцалюк та ін. Опрацюванню явища тероризму в умовах глобалізації та бурхливого розвитку інформаційно-комунікаційних технологій присвятила свої роботи низка відомих іноземних вчених та філософів, зокрема Е. Тоффлер, Б. Хофман, А. Шмід, Д. Белл, Ж. Бодріяр, Е. Гіденс, Ф. Фукуяма та ін.

Формулювання цілей. Метою статті є аналіз сучасних уявлень про кібертероризм, його ключові елементи, джерела, особливості реалізації, специфіку та класифікації цього феномену.

Виклад основного матеріалу. Світова наукова спільнота переймається проблемою кібертероризму вже не перший рік. У період з 2012 по 2019 р. у Сполучених Штатах Америки різними науковими організаціями було проведено декілька опитувань стосовно визначеності та сталості поняття «кібертероризм» та рівню його загрози для суспільства. Підсумовуючи ці опитування, американські вчені С. Макдональд, Л. Джарвіс та С. Лавіс зробили наступні висновки. По-перше, відбувається постійне зближення та об'єднання постійних характеристик кібертероризму на фоні великої кількості теоретичних концепцій. По-друге, наукові розробки протидії кібертероризму продовжуються паралельно з наростаючою кіберзагрозою і скоєнням актів кібертероризму. І, по-третє, наукова спільнота не має єдиної думки стосовно того, якої сили заходи («драконівські», виключні тощо) необхідно застосовувати проти актів кібертероризму [1]. Як висновок, можна сказати, що науковці поки не винайшли єдиного механізму протидії кібертероризму. А чи можливо це зробити взагалі? Як сьогодні визначається кібертероризм?

Термін «кібертероризм» з'являється задовго до того, як це явище набирає свого поширення. У середині 1980-х рр. його було впроваджено науковим співробітником одного з університетів США Беррі Колліном для позначення терористичних атак у віртуальному середовищі. До початку 1990-х рр.термін залишався непотрібним і використовувався лише для прогнозування майбутнього [2]. Слід зазначити, що він є синтезом понять «тероризм» і «кібернетичний простір». Під останнім розуміють середовище, яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем і забезпечення електронних комунікацій з використанням мережі інтернет та/або інших глобальних мереж передачі даних [3]. Згідно з українським тлумачним словником, слово «кібернетичний» має на увазі те, що діє на ґрунті кібернетики.

Кібернетика – це наука про загальні закони збереження, обробки та передачі інформації. З цього можна зробити висновок, що кібертероризм – це комплексна модель, що виражається у навмисній атаці на інформацію, яка зберігається та оброблюється комп'ютерами і комп'ютерними системами, що загрожує нормальному функціонуванню суспільства й породжує небезпеку для життя і здоров'я людей та призводить до інших тяжких наслідків [4].

Головне питання, яке виникає при теоретичному підході до кібертероризму, – це його співвідношення з тероризмом. Стосовно цього існує два підходи розуміння кібертероризму, як це слушно відмітив український науковець С. Гнатюк: «До сьогодні у наукових колах ведуться активні дискусії щодо того, чи є кібертероризм просто реалізацією актів тероризму у новому просторі (кіберпросторі) чи це принципово нове явище, яке має нові методи, засоби та інструментарій» [5, с. 120]. Автор наводить більше 20 визначень кібертероризму [5, с. 120–122], аналіз яких дозволяє зробити певний висновок: переважна частина українських науковців схильна до того, що кібертероризм – це один із сучасних проявів тероризму, тоді як іноземні науковці іноді намагаються розглядати його як самостійний злочин. При цьому деякі з іноземних дослідників наголошують на розпливчатості самого терміна «тероризм». Це відмічають і А. Розенцвейг, К. Коваленко та А. Губарева у своїй роботі «Основні підходи та визначення міжнародного кібертероризму» [6, p. 121]. Вони пишуть: «Ні для кого не є секретом, що не існує єдиного точного, фіксованого розуміння поняття тероризм, кожний автор тлумачить його на власний розсуд».

Науковці з обережністю підходять до розуміння сутності кібертероризму. Американські автори – дослідники С. Гордон і Р. Форд пишуть: «Термін "кібертероризм" стає все більш поширеним у популярній культурі, але чітке і повне визначення цього терміна, здається, важко знайти. Якщо цей термін складно визначити, то в розумінні того, що є кібертероризм, існує велика суб'єктивність. Після терактів 11 вересня це дещо збиває з пантелику. У спробі дати більш логічне визначення кибертероризму вивчаються визначення та атрибути тероризму і терористичних подій» [7, p. 636]. На подібні складнощі вказують також словенські вчені Б. Джерман-Блажич та Т. Клобучар, які наголошують на наступному: «На шляху розробки програми досліджень кіберзлочинності та кібертероризму є розуміння технічних проблем і відсутність рішень. Дослідження кіберзлочинності й кібертероризму зіштовхується з низкою проблем, таких як швидкість розвитку технологій, складність площини та міждисциплінарність» [8, p. 157]. На концептуальності дослідження кібертероризму наполягає й африканський учений Н. Веерасамі: «Кібертероризм оточений різноманітними теоріями. Однак існує потреба в більш структурованому підході до розуміння різних компонентів кібертероризму»

[9, p. 129]. Пізніше той же Н. Веєрасамі зі своїми колегами М. Гроблер і Б. Вон Солмс пропонують створити онтологію кібертероризму: «Використання онтології, спеціально розробленої для кібертероризму, створить загальну основу для обміну концептуальними моделями. Використовуючи технологію, внутрішній та зовнішній бік поля (у нашому випадку кібертероризм) можна уловити разом з відношеннями між сферами. Пропонується створити онтологію для визначення того, чи можна класифікувати кіберподію як кібертерористичну атаку або допоміжну діяльність. Роль онтологічної моделі кібертероризму постає у забезпеченні кращої структури та відображенні взаємозв'язків, взаємодій та впливаючих факторів за рахунок виявлення змісту та меж в області кібертероризму. Онтологія має розроблятись із використанням структури кібертероризму, яка охоплює фактори впливу, поряд зі скомпільованою онтологією класифікації мережевих атак… Онтологія дозволяє отримати загальний погляд на конкретну область, щоб згенерувати знання, яким можна ділитись та повторно використовувати. Онтологія може бути доповнена конкретними динамічними примірниками інформації і, відповідно, може використовуватись для генерації реальних сценаріїв» [10, p. 286].

Кібертероризм є видовим поняттям значно ґрунтовнішого явища – тероризму. Вони можуть існувати окремо один від одного або ж перебувати у безпосередній єдності, тобто інформаційні технології нерідко можуть бути знаряддям великої терористичної операції, стаючи інструментом здійснення терактів. Природа кібертероризму якісно відрізняється від сутності тероризму, хоча вона увібрала в себе деякі притаманні йому ознаки.

Серед подібності слід виділити масовий характер дій. Це вказує на необмежене коло осіб, які підпадають під це насильство, і передбачає потенційну можливість його поширення на ще більшу кількість людей, у випадку кібертероризму – електронно-обчислювальних машин. Після запуску механізму, поширення небезпечного програмного забезпечення відбувається автоматично, без утручання виконавця. З одного боку, терористи можуть мати на меті заволодіння якомога більшою кількістю персональних даних з наміром подальшої їхньої реалізації, що є загальносуспільною загрозою. З іншого боку, вони можуть перейти від недиференційованого об'єкта до конкретної фізичної або юридичної особи. Відтак злочин матиме індивідуальний характер і буде небезпечним лише для людини, щодо життя, здоров'я, психологічного стану, власності, ділової репутації якої здійснено посягання. Проте це не знижує рівень небезпеки цього явища. Отримавши доступ до бази даних політиків, державних службовців, бізнесменів або інших публічних осіб, які користуються авторитетом серед населення, терористи зосереджують у своїх руках потужну модельно-організаційну зброю, за допомогою якої вони можуть

здійснювати маніпулювання, залякування, формування кола підтримки або стримування супротиву.

Переважна більшість визначень кібертероризму говорить про політичну вмотивованість як про обов'язкову складову, що підкреслює специфіку цієї діяльності. Однак, ураховуючи кібератаки, які були здійснені не задля дестабілізації політичного життя, а з метою наживи, можна зробити висновок, що сприйнятливішою є модель, у який політична вмотивованість є варіативною частиною поняття кібертероризму. Поряд з нею також мають місце економічні, національні, етнічні, ідеологічні, релігійні цілі.

На відміну від традиційного тероризму, в якому виконавець у результаті вербування або вживання наркотичних препаратів може не усвідомлювати протиправність своїх дій і всю повноту наслідків, інформаційна атака завжди є усвідомленою, оскільки її реалізація вимагає від суб'єкта тривалої, клопіткої, зосередженої мозкової роботи. Отже, кіберзлочинець має бути психічно здоровим.

Суб'єкт бажає настання певних негативних наслідків. Однак, через складність інформаційно-комунікаційних мереж незалежно від його волі можуть виникнути труднощі, які потягнуть за собою більшу шкоду, ніж було заплановано. У такому випадку його вину слід пояснити як умисел щодо дій і необережність щодо наслідків у формі злочинної недбалості. Злочинець не передбачав настання вищого ступеня суспільної шкоди, однак повинен був і міг їх спрогнозувати.

Кібертероризм розглядають як незаконну атаку або загрозу вчинення такої атаки, тобто він визнається злочином як на стадіях підготовки й замаху, так і на завершальній стадії. Крім того, фінансування, посередництво, підбурювання тощо також будуть підпадати під склад злочину тероризму. Однак юридична відповідальність може не настати, якщо особа або група осіб, які брали участь у підготовці акту кібертероризму, добровільно повідомили правоохоронний орган про підготовку такого акту до його здійснення і якщо ці дії призвели до його відвернення [11].

Суб'єктом тероризму є фізичні осудні особи, які досягли віку кримінальної відповідальності. При здійсненні хакерської атаки на інформацію вік виконавця не є суттєвим і визначальним, наприклад, у 1998 р. 12-річний хакер узяв під контроль паводкові шлюзи греблі Т. Рузвельта в Арізоні, внаслідок чого загроза затоплення нависла над двома містами з населенням понад 1 мільйон людей [5]. Зважаючи на те, що в деяких випадках кібертеростичні акти можуть виявитися ефективнішими і призвести до тяжчих наслідків, ніж акти традиційного тероризму, законодавець повинен додати кібертероризм до переліку злочинів, зазначених у ст. 22 КК України, за вчинення яких кримінальна від-

повідальність наступає з 14 років. Специфічною ознакою суб'єктів кіберзлочинності є високий рівень їх кваліфікації. Характерним також є і те, що всі відомі сьогодні хакерські групи й окремі особи прагнуть не афішувати свої дані та працюють виключно під псевдонімами й через підставні комп'ютери, що ускладнює процес їх ідентифікації та визначення місцезнаходження. При цьому слід відрізняти хакера-терориста від простого хакера, комп'ютерного злодія або хулігана, який діє з метою наживи або в хуліганських цілях [12]. Практика інформаційного тероризму широко застосовується у діяльності сепаратистських, екстремістських та інших транснаціональних рухів.

Кібертерористу притаманне почуття безкарності. У зв'язку з недостатнім рівнем теоретичних розробок у галузі кібербезпеки, неефективністю превентивного законодавства, відсутністю єдиної процедури виявлення злочинця і притягнення його до юридичної відповідальності, низькою частотою розкриття кіберзлочинів у правопорушників виникає безсумнівне переконання в тому, що вони зможуть уникнути кримінального покарання. Анонімність у віртуальному просторі й віддаленість дійової особи розв'язує терористові руки, завдяки цьому він почувається більш захищено і тому може дозволити собі те, чого б не міг допустити в реальному житті, що розширює спектр несанкціонованих дій. Зростання технологій дає йому можливість отримання прибутку або досягнення інших цілей за відносно невеликих ризиків. ЗМІ, самі того не підозрюючи, активно сприяють поширенню кібертероризму, адже однією з причин здійснення посягання може бути бажання хакера до самоствердження і самоідентифікації. Бурхливий розголос у ЗМІ тільки спонукає до продовження чи навіть розширення такої діяльності. Однак акція не набуває такого драматичного й емоційного характеру, як це буває при застосуванні інших засобів. Із психологічної точки зору терористична діяльність є «обхідним» шляхом, тобто дає можливість без зміни соціального статусу, місця роботи, рівня освіченості отримати владу над багатшими, успішнішими й розумнішими людьми. Нерідко мотивом терориста може стати надання своїм ідеям особливої значущості, вони прагнуть переконати суспільство в правильності своїх думок, надати їм легітимності, сприймають свою істину як єдину, остаточну, вищу [13].

Основою кібертероризму є особливе місце, в якому він поширюється, а саме кіберпростір, який одночасно є середовищем, засобом і метою злочинного посягання. Електронно-обчислювальні машини, глобальні мережі передачі даних, несанкціоноване програмне забезпечення є знаряддям кібертерористів. Відтак, за даними «Лабораторії Касперського», найнебезпечнішими кіберзагрозами у світі є спеціально створена кіберзброя (апаратне і програмне забезпечення), маніпуляції в соціальних мережах, онлайн-покоління,

яке фактично живе у кіберпросторі, відповідно є дуже вразливим до кіберзагроз, втрати приватності і зламування мобільних пристроїв [14]. Першочерговим у тактиці кібертероризму є значні наслідки кібератаки, набуття широкого розголосу, отримання великого суспільного резонансу і навіювання атмосфери загрози через перспективу повторення акту без визначення об'єкта. Кібертероризм є відносно недорогим методом боротьби, тому його активно використовують радикальні мусульманські організації Близького Сходу й інші держави з недорозвиненою економікою. Він є транснаціональним явищем, саме тому важливим є об'єднання світу задля перемоги над спільним ворогом.

Звертаючись до законодавчого закріплення кібертероризму, варто наголосити, що сьогодні Україна має доволі-таки солідну й сучасну нормативно-правову базу, яка регламентує сферу кібернетичної безпеки [15, с. 152]. Центральне місце в системі законодавства про кібербезпеку посідає Закон України «Про основні засади забезпечення кібербезпеки України» [3]. Як зазначено у преамбулі цього нормативного акта, «Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки». Серед упроваджених законом понять має місце і «кібертероризм» – це «терористична діяльність, що здійснюється у кіберпросторі або з його використанням». Згідно із Законом, терористична діяльність зазвичай здійснюється щодо об'єктів критичної інфраструктури, які проводять діяльність і надають послуги в галузі енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій у банківських та приватних секторах, надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії та газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я, щодо комунальних, аварійних, рятувальних служб і інших підприємств, які мають стратегічне значення для економіки й безпеки держави або які є потенційно небезпечними. У цілому Закон дозволяє успішно реагувати на кібертероризм на сучасному етапі.

Висновки. За статистичними показниками, 40% респондентів в Україні вважають, що кібертероризм – це зовнішня загроза, 24% – внутрішня загроза, 36% упевнені, що загроза може виходити як ззовні, так і зсередини [16]. 60,9% українців почувають себе незахищеними в онлайн-середовищі. З цієї точки зору глобальну мережу можна розглядати як додатковий чинник підви-

щення загального неспокою. Задля встановлення стабільності та попередження злочинності в інтернеті функціонує підрозділ кіберполіції, однак 54,3% респондентів не вірять у те, що вона є ефективною і здатною забезпечити розкриття кіберзлочинів. Така зневіра унеможливлює успішність державно-публічної взаємодії, широкої співпраці з громадянським суспільством, яке у 39% випадків не ставить правоохоронців до відома про посягання на їхні права та свободи і покладається лише на власні сили. 69,9% опитаних упевнені, що держава не може забезпечити безпеку кожного окремого громадянина в інформаційному просторі. Критично важливі інфраструктурні компанії мають дотримуватися принципу «безпека понад усе» (security-first thinking). Оскільки понад 90% усіх несанкціонованих доступів, уражень і атак відбувається через людський фактор, то на підприємствах потрібно ввести прості регламентні норми, щоб максимально мінімізувати можливі витоки загроз і уражень [15].

Зважаючи на викладене, держава має запровадити відповідні технології навчання комплексних навичок і вмінь, які необхідні для реалізації цілей кібербезпеки у середній та вищій школах, проводити кібербезпекові інструктажі, підвищувати цифрову грамотність населення та культуру безпекового поводження в кіберпросторі, а також своєчасно повідомляти про виникнення нових загроз і шляхи їх уникнення.

ЛІТЕРАТУРА

1. Macdonald S., Jarvis L., Simon L. Cyberterrorism Today? Finding From a Follow-on Survey of Researchers. *Studies in Conflict & Terorism.* 2019. DOI: https://doi.org/10.1080/1057610X.2019.1696444.
2. Старостіна Є. Кібертероризм – підхід до проблем. *Центр дослідження комп'ютерної злочинності.* 2004. URL: http://www.crime-research.ru/articles/Starostina1/ (дата звернення: 14.03.2021).
3. Про основи засади кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163.19 (дата звернення: 14.03.2021).
4. Пояснювальна записка до Проекту Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» від 22.07.2015 № 2439a. URL: https://ips.ligazakon.net/document/GH1VR68A (дата звернення: 14.03.2021).
5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security.* 2013. № 2 (19). С. 118–129.
6. Rozentsvaig A. I., Kovalenko K. E., Gubareva A. V. Basic approaches and definitions of international cyberterrorism. *QUID – INVESTIGACION CIENCIA Y TECNOLOGIA*. 2018. № 2 SI. P. 120–124.

7. Gordon S., Ford R. Cyberterrorism? *COMPUTERS & SECURITY*. 2002. No. 7 (21). P. 636–647.
8. Jerman-Blazic B., Klobucar T. Towards the Development of a Research Agenda for Cybercrime and Cyberterrorism – Identifying the Technical Challenges and Missing Solutions. *COMBATTING CYBERCRIME AND CYBERTERRORISM: CHALLENGES, TRENDS AND PRIORITIES*. 2016. P. 157–174.
9. Veerasamy N. Towards a Conceptual Framework for Cyberterrorism. *Information Warfare and Security*: 4th International Conference (SO African Council Sci & Ind Res, Cape Town, South Africa, march 26–27, 2009). 2009. P. 129–137.
10. Veerasamy N., Grobler M., Von Solms B. Building an Ontology for Cyberterrorism. *Information Warfare and Security*: 11th European Conference (Inst Ecole Superieure Informatique, Elect & Automatique, Laval, France, jul 05–06, 2012). 2021. P. 286–295.
11. Коментар до Проекту Закону України «Про внесення змін Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» від 22.07.2015 № 2439а / Інститут проблем законодавства ім. Ярослава Мудрого. URL: https://ips.ligazakon.net/document/view/lh1vr68a?an=2&ed=2015_07_24 (дата звернення: 15.03.2021).
12. Гринюк Р. О., Пилипенко В. М. Кібертероризм як нова форма міжнародного тероризму. *Актуальні проблеми та досягнення в галузі кібербезпеки*: матеріали Всеукраїнської науково-практичної конференції (м. Кропивницький, 23–25.11.2016). Кропивницький, 2016. С. 61–62.
13. Остроухов В. В., Присяжнюк М. М. Інформаційно-психологічні аспекти тероризму в контексті філософії безпеки. URL: http://academy.ssu.gov.ua/ua/page/page_1581342902.htm (дата звернення: 10.03.2021).
14. Лабораторія Касперського. URL: https://www.securitylab.ru/ (дата звернення: 10.03.2021).
15. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. №3 (21). С. 150–157.
16. Родик Р. В., Дрожчана О. У. Кібертероризм як нова форма тероризму. URL: http://dspace.pdaa.edu.ua:8080/handle/123456789/5991 (дата звернення: 10.03.2021).

REFERENCES

1. Macdonald, S., Jarvis, L., Simon, L. (2019). Cyberterrorism Today? Finding From a Follow-on Survey of Researchers. *Studies in Conflict & Terorism*. DOI: https://doi.org/10.1080/1057610X.2019.1696444.
2. Starostina, Ye. (2004). Kiberteroryzm – pidkhid do problem. *Tsenter doslidzhennia kompyuternoi zlochynosti*. URL: http://www.crime-research.ru/articles/Starostina1/ [in Russian].
3. Pro osnovni zasady kiberbrzpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 №2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

4. Poiasnyuvalna zapuska do Proektu Zakonu Ukrainy «Pro vnesennia zmin do Kryminalnoho kodeksy Ukrainy shchodo vstanovlennia vidpovidalnosti za kiberteroryzm» vid 22.07.2015 № 2439a. URL: https://ips.ligazakon.net/document/GH1VR68A [in Ukrainian].
5. Hnatyuk, S. (2013). Kibertorooryzm: istoriia rozvytku, suchasni tendentsii ta kontrzakhody. *Bezpeka informatsiyi – Ukrainian Scientific Journal of Information Security, 2, 118–129* [in Ukrainian].
6. Rozentsvaig, A. I., Kovalenko, K. E., Gubareva, A. V. (2018). Basic approaches and definitions of international cyberterrorism. *QUID – INVESTIGACION CIENCIA Y TECNOLOGIA, 2, 120–124.*
7. Gordon, S., Ford, R. (2002). Cyberterrorism? *COMPUTERS & SECURITY*, *7 (21), 636–647.*
8. Jerman-Blazic, B., Klobucar, T. (2016). Towards the Development of a Research Agenda for Cybercrime and Cyberterrorism – Identifying the Technical Challenges and Missing Solutions. *COMBATTING CYBERCRIME AND CYBERTERRORISM: CHALLENGES, TRENDS AND PRIORITIES, 157–174.*
9. Veerasamy, N. (2009). Towards a Conceptual Framework for Cyberterrorism. *Information Warfare and Security*: 4th International Conference (SO African Council Sci & Ind Res, Cape Town, South Africa, march 26–27, 2009). P. 129–137.
10. Veerasamy, N., Grobler, M., Von Solms, B. (2012). Building an Ontology for Cyberterrorism. *Information Warfare and Security*: 11th European Conference (Inst Ecole Superieure Informatique, Elect & Automatique, Laval, France, jul 05–06, 2012). P. 286–295.
11. Komentar do Proektu Zakonu Ukrainy «Pro vnesennia zmin do Kryminalnoho kodeksy Ukrainy shchodo vstanovlennia vidpovidalnosti za kiberteroryzm» vid 22.07.2015 №2439a. URL: https://ips.ligazakon.net/document/view/lh1vr68a?an=2&ed=2015_07_24 [in Ukrainian].
12. Hrynyuk, R. O., Pylypenko, V. M. (2016). Kiberteroryzm yak nova forma mizhnarodnoho teroryzmu. *Aktual'ni problemy ta dosyahnennya u haluzi kiberbezpeky*: materialy Vseukrayins′koyi naukovo-praktychnoyi konferentsiyi (m. Kropyvnyts′kyy, 23–25.11.2016). Kropyvnyts′kyy. P. 61–62 [in Ukrainian].
13. Ostroukhov, V. V., Prysyazhnyuk, M. M. (2017). Informatsiyno-psykholohichni aspekty teroryzmu v konteksti filosofiyi bezpeky. URL: http://academy.ssu.gov.ua/ua/page/page_1581342902.htm [in Ukrainian].
14. Laboratoriya Kaspers′koho. URL: https://www.securitylab.ru/ [in Russian].
15. Trofymenko, O., Prokop, Yu., Lohinova, N., Zadereyko, O. (2019). Kiberbezpeka Ukrayiny: analiz suchasnoho stanu. *Zakhyst informatsiyi – Protection of information*, *3 (21), 150–157* [in Ukrainian].
16. Rodyk, R. V., Drozhchana, O. U. (2018). Kiberteroryzm yak nova forma teroryzmu. URL: http://dspace.pdaa.edu.ua:8080/handle/123456789/5991 [in Ukrainian].

Трофименко Владимир Анатольевич, кандидат юридических наук, доцент, доцент кафедры философии, Национальный юридический университет имени Ярослава Мудрого, г. Харьков, Украина

Мишанчук Анастасия Владимировна, студентка международно-правового факультета, Национальный юридический университет имени Ярослава Мудрого, г. Харьков, Украина

КИБЕРТЕРРОРИЗМ: ПОПЫТКА ФИЛОСОФСКО-ПРАВОВОГО ОСМЫСЛЕНИЯ

Кибертерроризм приобретает все большую опасность для общества в целом и для отдельных граждан в частности. В статье рассмотрены современные представления и взгляды относительно понимания сущности кибертерроризма, его ключевые элементы, источники, особенности реализации, специфика и классификации. Показан генезис понятия «кибертерроризм» и его соотношение с понятием «терроризм».

Ключевые слова: *безопасность, кибербезопасость, терроризм, кибертерроризм, киберпространсво, кибернетика.*

Trofymenko Volodymyr Anatoliyovych, candidate of Legal Sciences, assistant professor, Department of Philosophy, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

Mishanchuk Anastasiia Volodymyrivna, a student, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

CYBERTERRORISM: AN ATTEMPT OF PHILOSOPHICAL AND LEGAL UNDERSTANDING

Problem setting. *Ukraine continues its integration processes with the international community, in particular, with the European Union and NATO. But comprehensive integration leads to the fact that Ukraine is forced to integrate into the negative processes from which the modern world suffers and with which it tries to fight. With the rapid development of the Internet, its use with criminal intent is probably developing at the same rate. Novelty, level of danger, volumes of received and future possible losses of this type of crime contributed to the formation of such a dangerous phenomenon as cyberterrorism. Accordingly, there is a new task for world scientists – to understand the essence of the concept of cyberterrorism most accurately and generally, to explore its deep aspects, to develop a single conceptual apparatus and to propose a system of preventive measures.*

Recent research and publications analysis. *The topic of information terrorism within the Ukrainian cyberspace, as well as its inseparable interaction with the world wide web, theoretical aspects of this phenomenon, disclosure of concepts related to cybercrime are covered in the publications of such domestic researchers as S. Hnatyuk, O. Gerashchenko, V. Ostroukhov, M. Prysyazhnyuk, I. Diorditsa, O. Trofimenko, Yu. Prokop, I. Aristova, V. Tsymbalyuka, O. Zadereiko, O. Bogdanov, O. Drozhchan, M. Gutsalyuk and others. A number of well-known foreign scientists and philosophers have devoted their works to the study of the phenomenon of terrorism in the context of globalization and the rapid development of information and communication technologies, in particular E. Toffler, B. Hoffman, A. Schmid, D. Bell, J. Baudrillard, E. Giddens, F. Fukuyama and others.*

Paper objective. *This article aims to formulate a generalized definition of «cyberterrorism», its key elements, sources, features of implementation, specificity and classification through the method of deduction (derivation of true knowledge from the general term «terrorism» to specific – «cyberterrorism»).*

Paper main body. *The opinion of domestic and foreign scientists on the concept of cyberterrorism is analyzed. Based on the considered opinions, the authors try to show the peculiarities of cyberterrorism and reveal its danger to society as a whole and individuals. Finally, the authors turn to the analysis of Ukrainian legislation on cyberterrorism.*

Conclusions of the research. *Taking into account all the mentioned above, the state should introduce appropriate training systems for integrated skills and abilities that are necessary to support the goals of cybersecurity in secondary and higher schools, conduct cybersecurity briefings, increase digital literacy and the culture of safe behavior in cyberspace, as well as timely report about new threats and ways to avoid them.*

Keywords: *security, cyber security, terrorism, cyber terrorism, cyberspace, cybernetics.*