УДК 343.3/.7
DOI:10.24144/2078-1431.2021.1(26).70-81

Сергій Кучерина,
кандидат військових наук, доцент,
провідний науковий співробітник науково-дослідної лабораторії військового права, права національної та міжнародної безпеки НДІІП НАПрН України
Денис Олейніков,
кандидат юридичних наук,
начальник відділу наукової
та науково-дослідної роботи ІПЮК
для СБУ НЮУ ім. Ярослава Мудрого

ПРОБЛЕМНІ АСПЕКТИ ВПРОВАДЖЕННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРТЕРОРИЗМ

У роботі досліджено зміст кібертероризму, соціальні передумови до його криміналізації як суспільно небезпечного діяння. В загальному вигляді окреслено основні парадигми сучасного розуміння кібертероризму, визначено деякі категорії, які є його невід'ємними складовими. Отримані результати дозволили визначити низку проблемних аспектів впровадження кримінальної відповідальності за кібертероризм. Додатково надано окремі рекомендації щодо обов'язкових складових елементів складу злочину «кібертероризм» та посилення кримінально-правового захисту об'єктів критичної інформаційної інфраструктури.

Ключові слова: *кібертероризм, терористична діяльність, кримінальна відповідальність.*

The paper investigates the content of cyberterrorism, the social prerequisites for its criminalization as a socially dangerous act. As a result of the analysis of normative legal acts, individual legislative initiatives and existing scientific views, the main paradigms of the modern understanding of cyberterrorism are outlined in general form, and individual categories are identified that are its integral components. The results obtained made it possible to identify a number of problematic aspects of the introduction of criminal responsibility for cyberterrorism, to which the author attributed: lack of a clear understanding of the content, signs and components of this type of socially dangerous activity; the need for a conceptual study of the content of information terrorism, a component of which is cyberterrorism; lack of effective criminal law protection of critical information infrastructure facilities; the need for legislative improvement of the institution of crimes of a terrorist nature due to the consolidation of cyber terrorism as one of such crimes. Additionally, separate recommendations are given on the mandatory components of the elements of the crime of «cyberterrorism» and the strengthening of the criminal law protection of critical information infrastructure facilities.

Key words: *cyberterrorism, terrorist activity, criminal responsibility.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій та процес глобалізації зумовили появу нових видів суспільно небезпечних дій у кіберпросторі. До найбільш небезпечних з них належить кібертероризм, який, паралельно з розвитком цифрових можливостей, нарощує потенційну небезпеку. З іншого боку, динамічність законодавчого процесу, яка б відповідала потребам правозастосовних органів, задіяних до боротьби з кібертероризмом, поки що є значно повільнішою. Цей дисонанс породжує незахищеність найважливіших благ і цінностей, які є об'єктами кримінально- правової охорони, та обумовлює необхідність активізувати розроблення дієвого механізму протидій терористичній діяльності в кіберпросторі.

Результати аналізу наукових публікацій. Ті або інші аспекти кібертероризму в своїх працях досліджували такі вітчизняні науковці: В. Л. Бурячок, С. О. Гнатюк, Д. Б. Дубов, С.О. Ігнатов, С. В. Казмірчук, О. Г. Корченко, Р. М. Кравченко, С. В. Мельник, Є. В. Паціра, Г.А. Піскорська, В. П. Харченко.

Незважаючи на істотний вклад названих вище фахівців у розвиток вчення про кібертероризм, питання про кримінальну відповідальність за цей вид терористичної діяльності до сих пір не вирішене. Наразі в науці відсутні роботи, які б висвітлювали аспект проблемних питань впровадження кримінальної відповідальності за кібертероризм.

Метою статті є теоретична оцінка можливості й доцільності виділення кібертероризму як самостійної форми злочинної діяльності та аналіз проблемних аспектів, з якими в перспективі може стикнутись законодавець на шляху до криміналізації кібертероризму.

Виклад основного матеріалу. Обираючи об'єкти кримінально-правової охорони і встановлюючи кримінально-правові заборони, законодавець повинен враховувати, перш за все, соціальну обумовленість правового припису, цінність окремих суспільних відносин, їх роль та значення для всієї системи зазначених відносин [1, с. 171]. Ефективність норми кримінального права визначається, з одного боку, її соціальною обумовленістю, з іншого ж боку, необхідно враховувати правильність конструювання складу злочину, яка є важливою умовою практичної реалізації принципів кримінального права, зокрема принципу законності. На певне поєднання цих аспектів вказував А.Е. Жалінський, підкреслюючи, що «раціональність» кримінальної правотворчості «являє собою оптимальний соціальний вибір засобів вирішення існуючих або тих, що назрівають, соціальних конфліктів, коли використання кримінального права… найбільшою мірою відповідає реальним запитам суспільства і тягне найменші соціальні витрати при забезпеченні оптимального набору позитивних результатів», вимагаючи дотримання таких умов: «аналіз попиту на кримінальне право, вибір найбільш ефективного варіанта регулювання, виявлення і мінімізації можливих наслідків, побудова оптимальної моделі» [2, с. 264].

При цьому необхідно враховувати, що заборона має бути адекватною в частині підтвердження здатності кримінального права і системи кримінальної юстиції протидіяти певному типу суспільно небезпечної поведінки, а інструментальна здатність альтернативних засобів протидіяти такій поведінці є або більш витратною, або взагалі недієвою.

О.Д. Нечаєв виділяє такі стадії процесу адекватизації: 1) визначення інструментальної здатності кримінального права і системи кримінальної юстиції протидіяти спричиненню шкоди забороною визначеного типу поведінки; 2) перевірка інструментальної здатності альтернативних засобів попереджувати шкоду; 3) оцінка соціальної витратності кримінально-правових і альтернативних засобів [3, с. 169]. Не вдаючись до докладного аналізу наведеної вище позиції, все ж зауважимо, що зазначеним науковцем враховано статичну й ідеальну модель процесу адекватизації кримінально-правової заборони, оскільки, як свідчить досвід, законодавець вдається до оцінки необхідності кримінально-правової заборони того або іншого типу поведінки лише в тому разі, коли вона вже продемонструвала свою суспільну небезпечність в умовах неефективності існуючих засобів протидіяти їй.

Вказане досить точно характеризує певні законодавчі та наукові зусилля в сфері протидії такому негативному явищу, як кібертероризм, що останнім часом набуває стрімкого поширення. В Рішенні Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», введеному в дію Указом Президента України від 15 березня 2016 року № 96/2016, наголошено на наступних кроках, необхідних для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави:

– створення національної системи кібербезпеки;
– посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;
– забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура) [4].

Відповідно станом на 2016 рік непрямо було зроблено висновки про те, що спроможності сектору безпеки і оборони для забезпечення ефективної боротьби, зокрема із кібершпигунством, повинні бути посилені, що свідчить про недостатність на той час засобів протидії цьому негативному явищу. Підтвердженням цього є окремі законодавчі ініціативи, які передували прийняттю Стратегії кібербезпеки України. Так, у пояснювальній записці до проєкту Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» від 24 липня 2015 року в обґрунтування необхідності прийняття вказаного Закону автори вказали таке: «Розвиток інформаційних технологій, які заполонили майже всі сфери життєдіяльності, несе з собою не тільки позитивні, а й негативні тенденції та явища. Використання інформаційних технологій викликало новий вид злочинів, які загально можна окреслити як кіберзлочини. Серед них окремо можна виділити такий вид злочи-

нів, як кібертероризм - умисна атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків» [5].

Сьюзан В. Бренер виділяє такі ознаки кіберзлочинів, що відрізняють їх від звичайних злочинних посягань та значно підвищують їх суспільну небезпечність. По-перше, кіберзлочини не вимагають фізичного зближення між жертвою та суб'єктом злочину в момент вчинення останнього. По-друге, кіберзлочин часто є «автоматизованим злочином». Це означає, що суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість кіберзлочинів, що вчиняються, до кількох тисяч. По-третє, на суб'єкта кіберзлочину не впливають окремі обмеження, які існують у реальному, фізичному світі. Так, кіберзлочини можуть бути вчинені моментально, і тому потребують швидкої реакції у відповідь. І, по-четверте, кіберзлочинність й досі залишається новим феноменом, і наука ще не здатна встановлювати моделі поширення різних видів кіберзлочинів географічно та демографічно, як це робиться для злочинів, що вчиняються у реальному, фізичному світі [6, с. 33]. Як вказує Аллан Р. Стейн, найбільш проблемною характеристикою Інтернету з точки зору юрисдикційної політики є те, що він стирає межу між внутрішньодержавною і міжнародною передачею інформації [7, с. 434]. Проте ця «характеристика» є проблемною не тільки в контексті юрисдикційних питань, але і в контексті реально існуючої можливості суб'єкта завдати шкоди в режимі реального часу об'єктам, що знаходяться в інших містах, державах і навіть на інших континентах.

Поділяючи точку зору вказаних вище авторів, погоджуємось з авторами проєкту Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» у тому, що «в сьогоднішньому стані підвищеної зовнішньої небезпеки дуже важливо законодавчо визначити поняття кібертероризму і встановити суворо кримінальну відповідальність за вчинення актів кібертероризму, які можуть бути скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокацій військового конфлікту та спрямовані на підрив національних інтересів і національної безпеки» [5].

Автори законопроєкту, знаходячись у відповідній парадигмі розуміння кібертероризму, визначили його як умисну атаку на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків, якщо такі дії були скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту.

Визначення інформаційного або кібертероризму, як зауважує О.В. Кубишкін, можна знайти як у міжнародно-правових документах і проєктах конвенцій, так і в дослідженнях фахівців із цієї проблеми. Однією з характерних рис визначень інформаційного тероризму є те, що в більшості з них згадується тільки один аспект інформаційної безпеки, а саме той,

який пов'язаний із засобами оброблення інформації, що звужує поняття інформаційного тероризму, тим самим обмежуючи сферу правового регулювання, що не сприяє ефективній співпраці держав у справі боротьби з інформаційним тероризмом [8]. Наведена думка відкриває одну із існуючих проблем сучасної науки – ототожнення кібертероризму та інформаційного тероризму як синонимів. Авторська позиція буде наведена далі.

Наразі ж поняття кібертероризму закріплено в п. 13 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», де він визначається як терористична діяльність, що здійснюється у кіберпросторі або з його використанням. Отже, в контексті дослідження змісту кібертероризму як суспільно небезпечного явища в розумінні законодавця, підкреслимо, що його утворюють 2 основні складові, які, на перший погляд, належать до об'єктивної сторони складу злочину:

а) терористична діяльність - діяльність, яка охоплює:
- планування, організацію, підготовку та реалізацію терористичних актів;
- підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів у терористичних цілях;
- організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само як і участь у таких актах;
- вербування, озброєння, підготовку та використання терористів;
- пропаганду і поширення ідеології тероризму;
- проходження навчання тероризму;

б) кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Яким чином співвідносяться названі складові кібертероризму? Дещо випереджаючи відповідь на це питання, зазначимо, що кіберпростір як такий, на нашу думку, не можна вважати місцем вчинення злочину. Погодимось у цьому контексті із Т.В. Родіоновою, яка зазначає, що «для кримінально- правової кваліфікації можуть мати значення лише ті ознаки місця, що мають передбачені кримінально-правовою нормою характеристики або випливають зі змісту кримінального закону на підставі застосування прийомів тлумачення. Якщо не брати це до уваги, то у тлумаченні кримінального закону виникатиме плутанина, причиною якої стане змішування кримінально-процесуального та кримінально-правового аспектів розуміння ознаки місця вчинення злочину» [9, с. 43]. Аналізуючи поняття «місце вчинення злочину», В.Г. Мороз визначає його як «територію, інше місце, яке характеризується фізичними, соціальними і правовими критеріями, де було розпочато, продовжено чи припинено злочинне діяння» [10, с. 133]. Означене визначення зроблене на підставі

докладного аналізу наукових позицій і думок вітчизняних та іноземних фахівців, з огляду на що необхідності робити додатковий аналіз у контексті досліджуваної теми немає.

Отже, визначати кіберпростір місцем вчинення злочину нелогічно, оскільки напряму використати його без застосування комп'ютерної техніки, гаджетів, відповідного програмного забезпечення та можливості отримання доступу, наприклад, до мережі Інтернет, неможливо. Таким чином, реалізація злочинного умислу при вчиненні кібертероризму, як і будь-якого із кіберзлочинів, здійснюється за допомогою відповідних засобів та знарядь, до яких, власне, і належить кіберпростір. Так само, наприклад, категорія насильницьких злочинів отримала свою назву не за місцем свого вчинення, а за іншими ознаками.

Складно погодитись також і з точкою зору О. Самойленко, яка називає кіберзлочини «злочинами, учиненими з використанням обстановки кіберпростору» [11, с. 130]. Так, наприклад, І.В. Діоріца вказує на те, що обстановка вчинення злочину передбачає сукупність умов об'єктивного характеру, в яких вчиняється суспільно небезпечне діяння та настають суспільно небезпечні наслідки (наприклад, ст. 116 КК передбачає відповідальність за умисне вбивство, що вчиняється в певній обстановці – внаслідок незаконних дій з боку потерпілого, і викликає у винної особи стан сильного душевного хвилювання) [12, с. 59]; М.Й. Коржанський під обстановкою вчинення злочину вважає «…сукупність тих обставин, умов, при наявності яких злочин був вчинений (кримінально-правове значення має лише обстановка, яка вказана в диспозиції кримінально-правової норми)» [13, с. 169]; О.О. Астахова під обстановкою вчинення злочину пропонує розуміти «сукупність об'єктивних умов (обставин), визначених у законі про кримінальну відповідальність або таких, що випливають з його змісту, в яких вчиняється злочин або є збігом подій та обставин, в яких протікає зовнішній акт злочинної поведінки, що створюють вплив на ступінь суспільної небезпеки вчиненого та які набувають у цьому зв'язку кримінально-правового значення» [14, с. 62].

На підставі наведеного вважаємо правильним визначити кіберпростір не як місце вчинення злочину, а як елемент обстановки вчинення злочину. Зазначене дозволить дещо змістити акцент із зовнішніх ознак на сутність самого злочину. Фактично кібертероризм відрізняється від звичайної терористичної діяльності виняткового елементом обстановки вчинення злочину. Отже, відповідаючи на питання щодо співвідношення терористичної діяльності та кіберпростору як складових кібертероризму, припустимо, що вони співвідносяться як діяння та елемент обстановки. І цей висновок дозволяє значно розширити існуючу парадигму розуміння кібертероризму до переліку всіх форм терористичної діяльності, передбачених Законом України «Про боротьбу з тероризмом», враховуючи і ті, за які не передбачено кримінальну відповідальність.

В існуючій редакції Кримінального кодексу України за окремі форми терористичної діяльності, яка вчиняється у кіберпросторі, вже передбачено кримінальну відповідальність. Мова йде, наприклад, про окремі види терористичної діяльності, які за способом вчинення можуть передбачати вико-

ристання мережі Інтернет: а) розповсюдження, виготовлення чи зберігання з метою розповсюдження матеріалів з закликами до вчинення терористичного акту, б) сприяння вчиненню терористичного акту; в) фінансування тероризму і т.і. Аналогічна ситуація має місце щодо окремих злочинів, які, хоча й не охоплюються змістом «терористична діяльність», проте традиційно в науці кримінального права вважаються злочинами терористичного спрямування, як, наприклад, завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності.

В контексті питання про форми терористичної діяльності, які можуть вчинятись у кіберпросторі, проте не носять технологічно руйнівного характеру, виникає потреба відмежувати такі дії від кібертероризму. Це дуже просто зробити, якщо розглядати кіберпростір як частину інформаційного простору.

Так, Д.О. Ковлагіна під інформаційним простором пропонує розуміти не обмежену кордонами сферу існування суспільних відносин, пов'язану з використанням інформації, інформаційних технологій і інформаційних ресурсів [15, с. 67]. Доступ до кіберпростору забезпечується винятково за допомогою технічних приладів, об'єднаних мережею Інтернет чи іншою глобальною мережею передачі даних. Доступ до інформаційної сфери забезпечується більш широким колом засобів, включаючи, наприклад, засоби масової інформації, телекомунікаційні мережі і т.і.

Враховуючи отриманий вище висновок як критерій розмежування та продовжуючи логіку розподілу, одразу визначимо кібертероризм як складову інформаційного тероризму, оскільки кіберпростір цілком очевидно є складовою інформаційного простору. А, отже, кібертероризму притаманний більш технологічний характер, пов'язаний із посяганням на об'єкти критичної інформаційної інфраструктури, хоча це не виключає вибір суб'єктом і інших об'єктів злочинного посягання.

Для прикладу, в КК РФ передбачена кримінальна відповідальність за неправомірний вплив на критичну інформаційну структуру РФ (ст. 274.1), до якої може бути притягнуто особу за:

- створення, розповсюдження і (чи) використання комп'ютерних програм чи іншої комп'ютерної інформації, завідомо призначених для неправомірного впливу на критичну інформаційну інфраструктуру РФ, у тому числі для знищення, блокування, модифікації, копіювання інформації, яка в ній міститься, чи нейтралізації засобів захисту вказаної інформації;
- неправомірний доступ до охоронюваної комп'ютерної інформації, яка міститься в критичній інформаційній інфраструктурі РФ, у тому числі з використанням комп'ютерних програм чи іншої комп'ютерної інформації, які завідомо призначені для неправомірного впливу на критичну інформаційну інфраструктуру РФ, чи інших шкідливих комп'ютерних програм, якщо він призвів до завдання шкоди критичній інформаційній інфраструктурі РФ;
- порушення правил експлуатації засобів зберігання, обробки чи передачі охоронюваної комп'ютерної інформації, що міститься в

критичній інформаційній інфраструктурі РФ, чи інформаційних систем, інформаційно- телекомунікаційних мереж, автоматизованих систем управління, мереж електрозв'язку, що належать до критичної інформаційної інфраструктури РФ, або правил доступу до вказаних інформації, інформаційних систем, інформаційно-телекомунікаційних мереж автоматизованих систем управління, мереж електрозв'язку, якщо це призвело до завдання шкоди критичній інформаційній інфраструктурі РФ [16].

Як бачимо, зазначена норма змішує умисне завдання шкоди, яке може бути вчинено із мотивами, притаманними терористичній діяльності, з діями, вчиненими з необережності, оскільки акцент російського законодавця зосереджено на недопущенні неправомірного впливу на критичну інфраструктуру, а не на захисті громадської безпеки як об'єкта кримінально- правової охорони. Відповідно і Глава КК РФ, в яку поміщено склад злочину, передбачений ст. 274.1, має назву «Злочини у сфері комп'ютерної інформації». Що ж стосується кібертероризму, то одразу зауважимо, що сама його сутність повинна мати суб'єктивне наповнення, пов'язане із відповідними цілями, притаманними терористичній діяльності. До них, відповідно до положень ст. 258 КК України, відносяться: а) порушення громадської безпеки; б) залякування населення; в) провокація воєнного конфлікту, міжнародного ускладнення; г) вплив на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями; д) привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста).

Натомість у диспозиції статті 258-6 КК України проєкту Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» від 24 липня 2015 року суб'єктивна сторона складу злочину «кібертероризм» містить обов'язкові цілі та «політичні мотиви», зміст яких відомий науці кримінального права, проте не розкривається у відповідних статтях, що обтяжує цей термін зайвим ступенем оціночності.

Підбиваючи підсумок проблемних аспектів кримінальної відповідальності за кібертероризм, виділимо такі висновки:

1. У сучасних умовах впровадження кримінальної відповідальності за кібертероризм ускладнено, перш за все, відсутністю чіткого розуміння змісту, ознак та складових цього виду суспільно небезпечної діяльності. І, як вбачається, намагання розкрити та визначити кібертероризм у відповідній статті КК України, на кшталт проєкту ст. 258-6, не вирішить цієї проблеми, а лише поставить низку нових теоретичних і практичних питань. Це пояснюється тим, що фактично за загальним розумінням законодавця та з огляду на позиції науковців і практиків, кібертероризм являє собою суспільно небезпечну діяльність, яка поєднує ознаки кримінальних правопорушень проти громадської безпеки та кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та

комп'ютерних мереж і мереж електрозв'язку (хоча в законодавстві окремих європейських країн так звані «комп'ютерні злочини» належать якраз до категорії злочинів проти громадської безпеки і громадського порядку [17]).

2. Поза увагою дослідників іноді залишається категорія об'єктів, на які здійснюється посягання суб'єкта, що переслідує цілі терористичного характеру. До цих об'єктів, як правило, належать критично важливі об'єкти інфраструктури, через кібератаку на інформаційну інфраструктуру яких і можливо досягти бажаного злочинного результату. Можна погодитись з Є.А. Капітоновою, що при кваліфікації кібертероризму необхідно пам'ятати про його ознаку – створення реальної небезпеки спричинення смерті осіб, значної майнової шкоди чи настання інших тяжких наслідків [18, с. 34], що додатково ускладнює і без того непросте завдання законодавчого конструювання складу вказаного злочину. Підкреслюємо, що відсутність дієвого кримінально-правового захисту об'єктів критичної інформаційної інфраструктури в якомусь сенсі є перешкодою щодо криміналізації кібертероризму.

3. Для розроблення концепції такого негативного явища, як кібертероризм, необхідно дослідити явище, частиною якого він є, - інформаційний тероризм. Без дослідження його змісту і форм, а також місця в загальній структурі терористичної діяльності будь-які законодавчі ініціативи, на жаль, не матимуть комплексного характеру і призведуть до змішування окремих понять і категорій. Чітке виділення кібертероризму як технологічної складової інформаційного тероризму, обмеження переліку об'єктів руйнівного впливу та характеру суспільно небезпечних наслідків є бажаними кроками в контексті розроблення норми (або норм), що передбачає кримінальну відповідальність за його вчинення.

4. Окремої уваги заслуговує питання конструювання суб'єктивної сторони складу злочину «кібертероризм», оскільки, як і будь-який прояв терористичної діяльності, акт кібертероризму має чітко обмежений перелік цілей, заради досягнення яких він вчиняється. Вважаємо, що такі цілі, як порушення громадської безпеки, залякування населення, провокація воєнного конфлікту, міжнародного ускладнення, вплив на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, привернення уваги громадськості до певних політичних, релігійних, ідеологічних чи інших поглядів винного (терориста), мають обов'язково віднайти своє закріплення у відповідній статті. Саме за цими цілями акт кібертероризму можливо відмежувати від технологічної диверсії, кібершпигунства чи злочинів загальнокримінального спрямування.

5. Впровадження кримінальної відповідальності за вчинення злочину «кібертероризм» може потягнути за собою порушення архітектури інституту злочинів терористичного характеру, оскільки призведе до необхідності розділення цих складів по категоріях «загального виду терористичної діяльності», «інформаційного тероризму» та «кібертероризму» як технологічного виду інформаційного тероризму. Окремі форми об'єктивної сторони цих складів злочинів чи способи їх вчинення можуть бути пере-

розподілені між різними статтями, що передбачають кримінальну відповідальність за ті чи інші форми терористичної діяльності.

Додатково наголосимо на необхідності посилення кримінально-правового захисту об'єктів критичної інфраструктури, який у світлі прийняття окремих нормативно-правових актів (постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», постанова Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури») набуває особливого значення. При цьому кримінальна відповідальність за неправомірний вплив на такі об'єкти та акт кібертероризму проти такого об'єкта мають бути чітко диференційовані за відповідними ознаками суб'єктивної сторони терористичного акту та відповідними формами об'єктивної сторони, які у разі вчинення акту кібертероризму мають активний та цілеспрямований характер.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коржанский Н.И. Объект и предмет уголовно-правовой охраны. М.: Юридическая литература, 1980. 248 с.
2. Жалинский, А.Э. Уголовное право в ожидании перемен: теоретико- инструментальный анализ. М.: Проспект, 2009. 400 с.
3. Нечаев А.Д. Концептуальные основы и теоретическое моделирование криминализации и декриминализации: дис. … канд. юрид. наук. Саратов, 2017. 331 с.
4. Рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», введене в дію Указом Президента України від 15 березня 2016 року № 96/2016. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT.
5. Пояснювальна записка до проєкту Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм». URL: https://ips.ligazakon.net/document/GH1VR68A?an=4.
6. Brenner S. W. Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J. 1 (2004).
7. Stein A.R. Symposium: Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision. 98 Nw. U.L. Rev. 411 (2004).
8. Кубишкін О.В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави. URL: http://pravolib.pp.ua/informatsionnyiyterrorizm-15103.html.
9. Родіонова Т.В. Місце вчинення злочину за кримінальним правом України: дис. … канд. юрид. наук. Одеса, 2018. 247 с.
10. Мороз В.Г. Поняття місця вчинення злочину як ознаки об'єктивної сторони злочину // Юридична наука. 2014. № 5. С. 122-136.
11. Самойленко О. А. Сутність злочинів, учинених із використанням обстановки кіберпростору // National law journal: teory and practice (Молдова). 2017. № 6, ч. 2. С. 129-132.
12. Діордіца І.В. Кримінальне право України: [посібник для підготовки до іспитів]. К. : О.С. Ліпкан, 2010. 288 с.
13. Коржанський М.Й. Уголовне право України. Загальна частина: [курс лекцій]. К. : Наукова думка; Українська видавнича група, 1996. 336 с.
14. Астахова О. О. Поняття обстановки вчинення злочину як ознака об'єктивної сторони злочину // Юридична наука. 2015. № 3. С. 49-67.

15. Ковлагина Д.А. Информационный терроризм: понятие, уголовно- правовые и иные меры противодействия: дис. … канд. юрид. наук. Саратов, 2016. 270 с.
16. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 27.10.2020). URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.
17. Уголовный Закон Латвии, принятый Сеймом 17 июня 1998 года и обнародованный Президентом государства 8 июля 1998 года (С изменениями, внесенными по состоянию на 20 июня 2019 года). URL: https://lawyer-khroulev.com/wp-content/uploads/2019/09/ugolovnij-zakon- latvii.pdf.
18. Капитонова Е. А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2 (34). С. 29–41.

REFERENCES

1. Korzhanskiy, N.I. (1980). *Ob'yekt i predmet ugolovno-pravovoy okhrany* [*Object and subject of criminal law protection*]. Moscow: Yuridicheskaya literatura [in Russian].
2. Zhalinskiy, A.E. (2009). *Ugolovnoye pravo v ozhidanii peremen: teoretiko- instrumental'nyy analiz* [*Criminal law in anticipation of changes: theoretical and instrumental analysis*]. Moscow: Prospekt [in Russian].
3. Nechayev, A.D. (2017). Kontseptual'nyye osnovy i teoreticheskoye modelirovaniye kriminalizatsii i dekriminalizatsii [Conceptual foundations and theoretical modeling of criminalization and decriminalization]. *Candidate's thesis.* Saratov [in Russian].
4. Rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 27 sichnya 2016 roku «Pro Stratehiyu kiberbezpeky Ukrayiny» [Decision of the National Security and Defense Council of Ukraine «On the Cyber Security Strategy of Ukraine»]. from https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT. [in Ukrainian].
5. Poyasnyuval'na zapyska do proektu Zakonu Ukrayiny «Pro vnesennya zmin do Kryminal'noho kodeksu Ukrayiny shchodo vstanovlennya vidpovidal'nosti za kiberteroryzm» [Explanatory note to the draft Law of Ukraine «On Amendments to the Criminal Code of Ukraine on Establishing Liability for Cyberterrorism»]. *ips. ligazakon.net*. Retrieved from https://ips.ligazakon.net/document/GH1VR68A?an=4 [in Ukrainian].
6. Brenner, S. W. (2004). Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J. vol.1 [in English].
7. Stein, A.R. (2004). Symposium: Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision. 98 Nw. U.L. Rev. 411 p [in English].
8. Kubyshkin, O.V. Mizhnarodno-pravovi problemy zabezpechennya informatsiynoyi bezpeky derzhavy [International legal problems of information security of the state]. (n.d.).*pravolib.pp.ua.* Retrieved from http://pravolib.pp.ua/informatsionnyiyterrorizm-15103.html. [in Ukrainian].
9. Rodionova, T.V. (2018). Mistse vchynennya zlochynu za kryminal'nym pravom Ukrayiny [The place of commission of a crime under the criminal law of Ukraine]. *Candidate's thesis.* Odessa [in Ukrainian].
10. Moroz, V.H. (2014). Ponyattya mistsya vchynennya zlochynu yak oznaky ob"yektyvnoyi storony zlochynu [The concept of crime scene as a sign of the objective side of the crime]. *Yurydychna nauka - Legal science*, 5, 122-136 [in Ukrainian].
11. Samoylenko, O. A. (2017). Sutnist' zlochyniv, uchynenykh iz vykorystannyam obstanovky kiberprostoru [The essence of crimes committed with the use of cyberspace]. *National law journal: teory and practice (Moldova), 6*, 129-132 [in Ukrainian].
12. Diorditsa, I.V. (2010). *Kryminal'ne pravo Ukrayiny* [*Criminal law of Ukraine*]. Kyiv: O.C. Lipkan [in Ukrainian].

13. Korzhans'kyy, M.Y. (1996). *Uholovne pravo Ukrayiny. Zahal'na chastyna [Criminal law of Ukraine. General part].* Kyiv: Naukova dumka; Ukrayins'ka vydavnycha hrupa [in Ukrainian].
14. Astakhova, O. O. (2015). Ponyattya obstanovky vchynennya zlochynu yak oznaka ob'yektyvnoyi storony zlochynu [The concept of the situation of the crime as an element of the objective side of the crime]. *Yurydychna nauka - Legal science, 3,* 49-67 [in Ukrainian].
15. Kovlagina, D.A. (2016). Informatsionnyy terrorizm: ponyatiye, ugolovno- pravovyye i inyye mery protivodeystviya [Information terrorism: concept, criminal law and other countermeasures]. *Candidate's thesis.* Saratov [in Russian].
16. Ugolovnyy kodeks Rossiyskoy Federatsii [The Criminal Code of the Russian Federation]. (n.d.). *http://www.consultant.ru.* Retrieved from http://www.consultant.ru/document/cons_doc_LAW_10699/ [in Russian].
17. Ugolovnyy Zakon Latvii [The Criminal Law of Latvia]. (n.d.). *lawyer-khroulev.com*. Retrieved from https://lawyer-khroulev.com/wp-content/uploads/2019/09/ugolovnij-zakon-latvii.pdf. [in Russian].
18. Kapitonova, Ye. A. (2015). Osobennosti kiberterrorizma kak novoy raznovidnosti terroristicheskogo akta [Features of cyber terrorism as a new type of terrorist act]. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Obshchestvennyye nauki - Proceedings of higher educational institutions. Volga region. Social Sciences, 2 (34),* 29–41 [in Russian].