DOI: 10.33498/louu-2020-12-100

Ліліана Тимченко

кандидатка юридичних наук, доцентка,
доцентка кафедри міжнародних відносин
та міжнародного права
Київського університету імені Бориса Грінченка
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0002-4433-1077
Researcher ID: http://ResearchID.co/l.tymchenko
l.tymchenko@kubg.edu.ua

Марта Яцишин

кандидатка юридичних наук,
директорка ГО "Українська академія кібербезпеки"
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0002-6013-7098
martayatsyshyn@gmail.com

УДК 341.48/.49

МІЖНАРОДНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ЗА ТЕРОРИСТИЧНІ ТА КІБЕРТЕРОРИСТИЧНІ ДІЇ В УКРАЇНІ

Анотація. Агресія Російської Федерації (РФ) проти України, розпочата у 2014 р., призвела до нищівних наслідків. Перебуваючи в умовах гібридного конфлікту, Україна стала середовищем здійснення різноманітних атак, зокрема терористичних і кібертерористичних.

Встановлення обставин кожного конкретного інциденту та притягнення до відповідальності РФ є першочерговим завданням для підтримання міжнародної безпеки, зниження рівня світової терористичної загрози, а також відновлення миру і справедливості в Україні.

Метою статті є визначення та комплексний аналіз можливостей притягнення РФ до міжнародно-правової відповідальності за терористичні та кібертерористичні дії в Україні відповідно до чинних норм міжнародного права.

Докази причетності РФ до організації та підготовки незаконних збройних формувань для вчинення на території України терористичних актів є численними. Вони перебувають у розпорядженні правоохоронних органів України, Казахстану, Чехії, обговорюються у межах роботи органів міжнародних міжурядових організацій, розміщені на відкритих інформаційних майданчиках засобів масової інформації. Вчені у своїх наукових працях вдало підсумували свідчення, на підставі яких можна зробити однозначний висновок про відповідальність РФ за скоєння терористичних

дій і за причетність до них, встановлений зв'язок терористичних угруповань "Донецької Народної Республіки" та "Луганської Народної Республіки" з російською владою.

Варто окремо відзначити інтенсифікацію кібератак на території України, починаючи з 2014 р., за участю, сприяння і фінансування РФ. Фактичні підстави притягнення РФ до міжнародно-правової відповідальності за кібертерористичні акти на території України можна розглядати з позиції порушення зобов'язань, встановлених міжнародними договорами у сфері протидії тероризму. Відсутність безпосередніх вказівок на конкретні кібератаки, які відбувалися на території України, у позовній заяві Уряду України до Міжнародного суду ООН від 16 січня 2017 р. про порушення Російською Федерацією зобов'язань за Міжнародною конвенцією про боротьбу з фінансуванням тероризму від 9 грудня 1999 р. та за Міжнародною конвенцією про ліквідацію всіх форм расової дискримінації від 21 грудня 1965 р. (Україна проти Російської Федерації), а також у матеріалах справи, що перебувають у публічному доступі, обумовлено загальною невизначеністю засад застування норм міжнародного права до кіберпростору.

Беззаперечними є факти здійснення кібератак на території України саме з російської інформаційної інфраструктури, а також за участю Збройних сил Російської Федерації, що підтверджується у заявах багатьох держав, рішеннях міжнародних організацій, зокрема і Європейського Союзу. Держава зобов'язана не надавати свідомого дозволу для використання кібернетичної інфраструктури, яка перебуває на її території або під її контролем, для здійснення негативних і незаконних дій проти іншої держави. Ба більше, держава зобов'язана вжити всіх необхідних та ефективних заходів, аби зупинити таку протиправну діяльність.

РФ заперечує наявність підстав для відповідальності за вчинені терористичні та кібертерористичні дії. Завдання України – продовжити розслідування справ, інтенсифікувати розпочаті провадження, вести пропагандистську (роз'яснювальну) роботу у межах міжнародних організацій, через двосторонні перемовини, розповсюдження знань на рівні суспільства.

Визначення способів притягнення РФ до міжнародно-правової відповідальності за здійснені терористичні і кібертерористичні атаки на території України є важливою умовою для відновлення справедливості, відшкодування завданих збитків, а також елементом розвитку державного контуру безпеки, зокрема й кібернетичної.

Ключові слова: міжнародно-правова відповідальність; тероризм; терористичний акт; кібертероризм; кібератака; Російська Федерація; Україна.

Дії держави, які не є обумовленими проголошенням війни, але завдають шкоди мирному існуванню суверенної держави, її політичній незалежності, безпеці її населення та залякують його, загрожують його життю і добробуту, розглядаються суспільно-політичними науками як терористичні. З плином часу може змінюватися характер, межі, механізми та інструментарій їхнього здійснення. Вони можуть впливати на об'єкти інфраструктури безпосередньо у фізичному просторі, а також через використання комп'ютерних систем і комунікаційних мереж у віртуальному кібернетичному середовищі. Проте метою таких дій завжди залишатиметься прагнення посіяти страх, аби "вивести" суспільство із

нормального життєвого ритму. Інакше кажучи, терористичні дії мають намір зламати суспільний стрижень, який у сучасних умовах базується на цінностях демократії, верховенства права і прав людини, передбачає успішне просування ринкової економіки, стійкий розвиток та екологічне мислення населення.

Істинно демократична, правова, соціальна держава *a priori* не має наміру принизити, зламати, знищити позицію іншого рівного учасника міжнародно-правових відносин. Вона буде просувати національні інтереси через компромісні заходи і домовленості, співробітництво і спільний розвиток.

Російська Федерація (далі – РФ) із самого початку свого існування демонструвала неповагу до суб'єктів міжнародно-правових відносин, відмову від політики невтручання у внутрішні справи держав і прагнення до експансії територій найближчих сусідів.

У лютому-березні 2014 р. Росія розпочала масштабні агресивні дії проти України, захопивши Крим і створивши (контрольовані, керовані та фінансовані спецслужбами РФ) озброєні бандитські формування "Донецька Народна Республіка" (далі – "ДНР") і "Луганська Народна Республіка" (далі – "ЛНР")[1]. До сьогодні РФ не визнає їх злочинними, зневажаючи норми міжнародного права та положення національного законодавства України, ігноруючи вимоги української держави, нехтуючи оцінками більшості держав світового співтовариства. Свідчення причетності Росії до терористичних дій в Україні розглядаються міжнародними судовими установами, підтверджуються авторитетними міжурядовими організаціями. Незважаючи на обґрунтовані звинувачення у порушеннях норм міжнародного права, РФ продовжує активно втручатися прямо або опосередковано у справи України.

Якими будуть наслідки такої поведінки РФ? Чи буде міжнародне співтовариство миритися із терористичною діяльністю постійного члена Ради Безпеки Організації Об'єднаних Націй (далі – ООН)? Як міжнародне співтовариство має протистояти державі-агресорці, аби зупинити руйнування системи міжнародного права?

Закон України "Про боротьбу з тероризмом"[2] чітко визначає поняття "тероризм", "терористичний акт", "активи, що пов'язані з фінансуванням тероризму та стосуються фінансових операцій, зупинених відповідно до рішення, прийнятого на підставі резолюцій Ради Безпеки ООН", "технологічний тероризм", "терористична діяльність", "фінансування тероризму", "міжнародний тероризм". Український законотворець сфор-

[1] Про відсіч збройній агресії Російської Федерації та подолання її наслідків: Заява Верховної Ради України, схвалена Постановою Верховною Радою України від 21 квітня 2015 р. № 337-VIII <https://zakon.rada.gov.ua/laws/show/337-19#Text> (дата звернення: 10.10.2020).

[2] Про боротьбу з тероризмом: Закон України від 20 березня 2003 р. № 638-IV <https://zakon.rada.gov.ua/laws/show/638-15/ed20180729#n12> (дата звернення: 10.10.2020).

мулював наведену термінологію, базуючись на нормах міжнародно-правового законодавства, а саме на положеннях Європейської конвенції про боротьбу з тероризмом[3], Міжнародної конвенції про боротьбу з бомбовим тероризмом[4], Міжнародної конвенції про боротьбу з фінансуванням тероризму[5] та інших міжнародних договорів, користуючись розумінням позицій, сформульованих у доктрині авторитетних світових терологів.

Відповідно до положень абзацу 5 ч. 1 ст. 1 Закону України "Про боротьбу з тероризмом" до числа дій РФ, які підпадають під кваліфікацію "терористична діяльність", необхідно віднести:

1. Планування, організацію, підготовку та реалізацію терористичних актів.
2. Підбурювання до вчинення терористичних актів, насильство 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 і поширення ідеології тероризму.
6. Фінансування та інше сприяння тероризму.

У Законі України "Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях" відзначено:

> <…> збройна агресія Російської Федерації розпочалася з неоголошених і прихованих вторгнень на територію України підрозділів збройних сил та інших силових відомств Російської Федерації, а також шляхом організації та підтримки терористичної діяльності[6].

Дії, які з метою досягнення політичних цілей залякують населення, створюють небезпеку для його життя і здоров'я, внаслідок яких була спричинена значна шкода, відповідно кваліфікуються як терористичні акти. Таких дій дотепер за безпосередньою участю Росії скоєно чимало, зокрема:

– 6 червня 2014 р. на території Донецької області був збитий літак АН-30;

[3] Європейська конвенція про боротьбу з тероризмом (ETS № 90) від 27 січня 1977 р. <https://zakon.rada.gov.ua/laws/show/994_331#Text> (дата звернення: 10.10.2020).
[4] Міжнародна конвенція про боротьбу з бомбовим тероризмом від 15 грудня 1997 р. <https://zakon.rada.gov.ua/laws/show/995_374#Text> (дата звернення: 10.10.2020).
[5] Міжнародна конвенція про боротьбу з фінансуванням тероризму від 9 грудня 1999 р. <https://zakon.rada.gov.ua/laws/show/995_518#Text> (дата звернення: 10.10.2020).
[6] Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях: Закон України від 18 січня 2018 р. № 2268-VIII <https://zakon.rada.gov.ua/laws/show/2268-19/ed20180118#n24> (дата звернення: 10.10.2020).

– 14 червня 2014 р. унаслідок обстрілу із зенітної установки та великокаліберного кулемета під час посадки в аеропорту "Луганськ" був збитий військово-транспортний літак Іл-76 Повітряних Сил Збройних Сил України, внаслідок чого 49 військових загинули;

– 17 липня 2014 р. російським зенітно-ракетним комплексом "Бук" було збито авіалайнер цивільної авіації "Малайзійських авіаліній" *Boeing 777*, який рухався маршрутом з Амстердаму до Куала-Лумпур, унаслідок чого загинуло 283 пасажири та 15 членів екіпажу.

Оцінку терористичній діяльності РФ проти України намагаються надати судові установи та міжнародні міжурядові інституції.

16 січня 2017 р. у Міжнародному суді ООН за заявою Уряду України про порушення Російською Федерацією зобов'язань за Міжнародною конвенцією про боротьбу з фінансуванням тероризму від 9 грудня 1999 р. та за Міжнародною конвенцією про ліквідацію всіх форм расової дискримінації від 21 грудня 1965 р. (Україна проти Російської Федерації)[7], було розпочато провадження щодо визначення протиправності дій РФ, яка 'через свої державні органи, державних агентів й інших осіб та суб'єктів, що здійснюють державні повноваження, та через інших агентів діючи за її вказівкою або під її керівництвом і контролем', постачала кошти незаконним збройним формуванням, не вживала відповідні заходи для виявлення, заморожування та вилучення коштів, що використовуються для допомоги незаконним збройним формуванням, які брали участь у терактах в Україні; не розслідувала, не притягувала до кримінальної відповідальності або не екстрадувала осіб, винних у перелічених діях (*Relief Sought under the Terrorism Financing Convention*, п. 134)[8].

Причетність до терористичних дій РФ опосередковано доказується судами різних держав. Так, зокрема, за повідомленнями казахстанського інформаційного порталу "Медіазона" від 22 травня 2020 р. Суд № 2 міста Костанай у кримінальних справах притягнув до відповідальності за ст. 172 (участь в іноземних збройних конфліктах) Кримінального кодексу Республіки Казахстан казахстанця Є. Щербака. Привертають увагу зізнання депутата російської Державної думи С. Шаргунова, який оплатив Є. Щербаку адвоката: 'З Росії, яка його поманила на війну всім блиском і шумом своїх телеекранів, Євгенія видали в Казахстан. Хоча він благав надати йому притулок. І вже, звичайно, ніхто не турбувався подальшою долею відданого'[9].

[7] Міжнародна конвенція про ліквідацію всіх форм расової дискримінації від 21 грудня 1965 р. <https://zakon.rada.gov.ua/laws/show/995_105#Text> (дата звернення: 10.10.2020).

[8] Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of all forms of Racial Discrimination (Ukraine v. Russian Federation) <https://www.icj-cij.org/public/files/case-related/166/166-20170116-APP-01-00-EN.pdf> (accessed: 10.10.2020).

[9] 'Казахстанца, воевавшего на стороне сепаратистов в Донбассе, приговорили к 4,5 годам лишения свободы' (*Медиазона,* 22.05.2020) <https://mediazona.ca/news/2020/05/22/dnr-deported-2> (дата звернення: 10.10.2020).

Інформаційні агенції, посилаючись на авторитетні джерела, вказують на факт підготовки бойовиків на території РФ та під її фінансовим патронатом. Із посиланням на матеріали Генеральної прокуратури України Балканська редакція "Радіо Вільна Європа" повідомляла про свідоме залучення іноземних громадян до агресивних бойових дій проти України на території Донецької та Луганської областей у складі нелегальних озброєних формувань, створених РФ та їй підпорядкованих[10].

За повідомленнями українського видання "Європейська правда" з посиланням на чеські "*Novinky*" від 22 вересня 2020 р. у Чехії був засуджений за участь в організованій злочинній групі на сході України громадянин Білорусі О. Фадєєв[11]. Голова кримінальної палати Л. Чихларжова зауважила, що спочатку О. Фадєєв був звинувачений у тероризмі. 'Не вдалося довести, що підсудний був особою, яка брала активну участь у бойових діях і стріляла у військовослужбовців української армії', – зазначила суддя, додавши, що чоловік імовірніше за все займав тільки допоміжні позиції і не брав участі в активних боях[12].

Про підозру в участі у терористичній організації (ч. 1 ст. 258[3] Кримінального кодексу України, далі – КК України)[13] було повідомлено 28 особам (дев'ять – громадяни України), які за результатами слідства визнані причетними до активної участі в бойових діях на території Донецької та Луганської областей у складі терористичних організацій "ЛНР" і "ДНР". 11 серпня 2020 р. Офіс Генерального прокурора України в запиті до Генеральної прокуратури Республіки Білорусь вимагав видати цих осіб, які 29 липня 2020 р. були затримані правоохоронними органами Білорусі[14].

Наведені факти – лише поодинокі докази причетності РФ до організації та підготовки незаконних збройних формувань для вчинення на території України терористичних актів. Таких доказів є значно більше в розпорядженні українських правоохоронних органів, а також незалежних міжнародних інформаційних агенцій, які займаються розслідуванням терористичних дій, скоєних на території України (зокрема, варто назвати розслідування факту збиття літака рейсу MH17 Малайзійських авіаліній Глобальною мережею журналістів-розсліду-

[10] М Рамач, 'Бойовик, засуджений у Сербії, знову воює на Донбасі' (*Радіо Свобода,* 20.10.2018) <https://www.radiosvoboda.org/a/29554393.html> (дата звернення: 10.10.2020).

[11] 'У Чехії білоруса посадили на 4,5 роки за допомогу сепаратистам Донбасу' (*Європейська правда,* 22.09.2020) <https://www.eurointegration.com.ua/news/2020/09/22/7114573> (дата звернення: 11.10.2020).

[12] Такм само.

[13] Кримінальний кодекс України: Закон України від 5 квітня 2002 р. № 2341-III <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 11.10.2020).

[14] 'Офіс Генпрокурора направив до Генпрокуратури Республіки Білорусь запити про видачу 28 учасників збройного конфлікту на Донбасі' (*Офіс Генерального Прокурора,* 12.08.2020) <https://www.gp.gov.ua/ua/news?_m=publications&_t=rec&id=278570> (дата звернення: 11.10.2020).

вачів, *Bellingcat – Global Investigative Journalists Network*[15]). 6 т доказів проти Росії, 17 тис. сторінок передала Україна до Міжнародного суду ООН лише в червні 2018 р. У цих документах – численні аудіоматеріали і відеодокази теракту проти "Боїнга" Малайзійських авіаліній та обстрілів житлових кварталів Маріуполя у січні 2015 р., свідчення про окремі епізоди фінансування росіянами тероризму[16].

Серйозну стурбованість щодо продовження присутності російських військ на сході України і припливу передової зброї та "добровольців" із РФ висловлювала Парламентська Асамблея Ради Європи[17]. А у вересні 2020 р. на Антитерористичній конференції Організації з безпеки і співробітництва в Європі "Ефективне партнерство проти тероризму, насильницького екстремізму та радикалізації, що призводять до тероризму", яка відбувалася в онлайн-форматі у Відні, учасники засудили політику РФ, спрямовану на підтримку, фінансування і координацію діяльності терористичних формувань на тимчасово окупованих територіях[18].

Вчені в своїх наукових працях вдало підсумовували свідчення, на підставі яких можна зробити однозначний висновок про відповідальність РФ за скоєння терористичних дій і за причетність до них, встановлений зв'язок терористичних угруповань "ДНР" і "ЛНР" із російською владою. У праці О. Задорожнього та Т. Короткого перелічені, зокрема, такі факти:

1) призначення керівників цих організації серед кадрових офіцерів російських спецслужб (І. Гіркін, О. Бородай, В. Антюф'єєв та інші);

2) поставка бойовиками РФ великої кількості зброї, включаючи важку зброю;

3) фінансування російською владою "збройних сил" у "ДНР" і "ЛНР";

4) підготовка бойовиків у Росії;

5) забезпечення бойовиків "зеленими коридорами" на кордоні України;

6) телефонні розмови керівників бойовиків зі своїми "кураторами" у Федеральній службі безпеки та Головному розвідувальному управлінні Росії, які були перехоплені Службою безпеки України;

7) відкриття у Росії низки "місій" "ДНР" і "ЛНР", керованих російською владою;

8) зустрічі з представниками лідерів терористів з оточення В. Путіна;

[15] 'Case Studies: Tags: MH 17' *(Bellingcat)* <https://www.bellingcat.com/category/resources/case-studies/?fwp_tags=mh17> (accessed: 10.10.2020).

[16] С Сидоренко, 'Шість тонн доказів проти Росії: що передала Україна до Міжнародного суду ООН' (*Європейська правда,* 12.06.2018) <www.eurointegration.com.ua/articles/2018/06/12/7083003> (дата звернення: 11.10.2020).

[17] Consideration of the annulment of the previously ratified credentials of the delegation of the Russian Federation (follow-up to paragraph 16 of Resolution 2034 (2015)) Report. Doc. 13800. 04 June 2015 <https://pace.coe.int/en/files/21801/html> (accessed: 10.10.2020).

[18] Інформація оприлюднена на сайті Міністерства закордонних справ України. Див.: 'Делегація України бере участь у антитерористичній конференції ОБСЄ' (*Міністерство закордонних справ України,* 15.09.2020) <https://mfa.gov.ua/news/delegaciya-ukrayini-bere-uchast-u-antiteroristichnij-konferenciyi-obsye> (дата звернення: 01.11.2020).

9) визнання Росією "ДНР" як незалежної держави (27 червня 2014 р.);

10) пряме та неодноразове визнання впливу В. Путіна на сепаратистів в Україні[19].

Крім наведених фактів, слід окремо відзначити інтенсифікацію кібератак на території України з 2014 р. Так, група *CERT-UA (Computer Emergency Response Team of Ukraine)* при Державній службі спецзв'язку в 2014 р. виявила 216 кібератак ззовні, а у 2015 р. це число збільшилося в півтора рази. За інформацією, оприлюдненою Радою національної безпеки і оборони України, у 2020 р. в Україні було зафіксовано близько 1 млн кібератак.

У переважній більшості об'єктами DDoS-атак, нападів на вебсайти та інфікування шкідливими програмами, починаючи з 2014 р., були державні органи, установи та організації, а програмні коди, які використовувалися при цьому (наприклад, *BlackEnergy, KillDisk, Petya/NotPetya, BadRabbit*), потребували висококваліфікованих знань і значних матеріальних затрат.

Такого рівня операції могли бути здійснені лише організованою злочинною групою за участю та (або) фінансування іноземної держави. Засоби масової інформації часто пов'язують вчинення цих кібератак на території України з діяльністю російських злочинних угруповань, таких як *CyberBerkut*, так звані *APT29* (також відома як *Cozy Bear, Cozy Duke*), *APT28* (також відома як *Sofacy Group, Tsar Team, Pawn Storm, Fancy Bear*)[20], *Sandworm* (також відомий як *Sandworm Team, BlackEnergy Group, Voodoo Bear, Quedagh, Olympic Destroyer і Telebots*)[21]. У жовтні 2020 р. видання *The Washington Post* опублікувало позов США проти шести офіцерів Головного управління розвідки Генерального штабу Збройних сил Російської Федерації *(Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation)* з обвинуваченням у здійсненні найбільших кібернетичних атак у світі, зокрема й кібератак 2015–2017 рр. на території України[22].

---

[19] O Zadorozhny, T Korotkyi, 'Legal Assessment of the Russian Federation's Policy in the Context of the Establishment and Activities of Terrorist Organizations "Donetsk People's Republic" ("DPR") and "Lugansk People's Republic" ("LPR") in Eastern Ukraine' [2015] 2 (1) Evropský Politický A Právní Diskurz 8–18.

[20] 'Найбільші кібератаки проти України з 2014 року. Інфографіка' (*Новое время,* 08.07.2017) <https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html> (дата звернення: 11.10.2020).

[21] Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN> (accessed: 11.10.2020); Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125&from=EN> (accessed: 11.10.2020).

[22] Див.: *Anne Applebaum,* 'Opinion: Russian hackers were caught in the act – and the results are devastating' *(The Washington Post)* <https://www.washingtonpost.com/opinions/global-opinions/russian-hackers-were-caught-in-the-act--and-the-results-are-devastating/2018/10/05/5e72495a-c8b5-11e8-b1ed-1d2d65b86d0c_story.html> (accessed: 11.10.2020).

Відповідно до оприлюднених офіційних заяв відповідальність за розроблення і використання вірусу *Petya/NotPetya* офіційно покладають на РФ, а саме її військові сили Велика Британія[23], Канада[24], Нова Зеландія[25], США[26], а також уряди Данії[27] та України[28]. 30 липня 2020 р. Радою Європейського Союзу (далі – ЄС) було прийнято рішення *(CFSP)* 2020/1127 і регламент (EU) 2019/796 про обмежувальні заходи проти кібератак, що загрожують Союзу або його державам-членам[29], на основі яких було встановлено санкції щодо Головного центру спеціальних технологій Головного управління Генерального штабу Збройних сил Російської Федерації *(Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation)*, який визначається відповідальним за кібератаки, що вчинялися за межами ЄС і являли собою зовнішню загрозу для Союзу, його членів і третіх держав, включно з кібератаками *NotPetya* чи *EternalPetya* у червні 2017 р. і нападами, спрямованими на енергосистему України взимку 2015 і 2016 рр.

Враховуючи все зазначене вище, притягнення РФ до міжнародно-правової відповідальності за кібернетичні атаки, вчинені на території України, є також можливим, однак низка питань щодо застосовності конкретних норм міжнародного публічного права потребує конкретизації.

Міжнародно-правова відповідальність держави настає за умови, якщо остання здійснила міжнародне правопорушення, що виражається в дії або бездіяльності її органів або посадових осіб, яке порушує міжнародно-правові зобов'язання. Це положення закладено в основу проєкту Статей про відповідальність держав за міжнародні протиправні дії 2001 р. Таким чином, держава має нести відповідальність за певні діяння лише у тому випадку, якщо вони порушують чинну норму міжнародного права, а також можуть бути атрибутовані конкретній державі.

З огляду на це фактичні підстави притягнення РФ до міжнародно-правової відповідальності за кібернетичні атаки на території України

[23] 'Russian military 'almost certainly' responsible for destructive 2017 cyber attack' (*National Cyber Security Centre,* 14.02.2018) <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> (accessed: 11.10.2020).

[24] 'CSE Statement on the NotPetya Malware' (*Government of Canada,* 15.02.2018) <https://www.cse-cst.gc.ca/en/media/2018-02-15> (accessed: 10.10.2020).

[25] 'New Zealand joins international condemnation of NotPetya cyber-attack' (*Government Communications Security Bureau,* 16.02.2018) <https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack> (accessed: 11.10.2020).

[26] 'Statement from the Press Secretary' (*The White House,* 15.02.2018) <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25> (accessed: 12.10.2020).

[27] 'Claus Hjort: Rusland stod bag cyberangreb mod Mærsk' (*Berlingske,* 15.02.2018) <https://www.berlingske.dk/virksomheder/claus-hjort-rusland-stod-bag-cyberangreb-mod-maersk> (accessed: 11.10.2020).

[28] 'СБУ встановила причетність спецслужб РФ до атаки вірусу-вимагача Petya.A' (*Укрінфо,* 01.07.2017) <https://www.ssu.gov.ua/ua/news/1/category/21/view/3660#.37yT3eBD.dpbs> (дата звернення: 10.10.2020).

[29] Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (n 21); Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (n 21).

можна розглядати з позиції порушення зобов'язань, встановлених міжнародними договорами у сфері протидії тероризму.

Основними міжнародними джерелами щодо протиправних діянь, вчинених у кібернетичному просторі, станом на сьогодні залишаються спеціальні міжнародні конвенції у сфері протидії кіберзлочинності, насамперед Конвенція про кіберзлочинність[30], прийнята у 2001 р. у межах Ради Європи. Однак такі конвенції не орієнтовані на боротьбу з тероризмом, а тому не встановлюють відповідальності за кібертерористичні дії.

Водночас кібернетичні атаки можна кваліфікувати як терористичні акти, сприяння чи підготовку для здійснення останніх у випадку, якщо наслідки кібератак будуть зіставні з дефініціями тероризму відповідно до Міжнародної конвенції про боротьбу з фінансуванням тероризму. Такий підхід використано, зокрема, у рекомендації Комітету Конвенції про кіберзлочинність Ради Європи № 11 "Тероризм"[31]. І хоча РФ не є її учасницею, Міжнародна конвенція про боротьбу з фінансуванням тероризму є чинною на території РФ із 27 грудня 2002 р.

Закон України "Про основні засади забезпечення кібербезпеки України" передбачає поняття "кібертероризм", що визначається як: 'терористична діяльність, що здійснюється у кіберпросторі або з його використанням'[32]. Враховуючи поняття "технологічний тероризм", включене до Закону України "Про боротьбу з тероризмом", кібертерористичними актами РФ на території України можна вважати будь-які

> кримінальні правопорушення, вчинені з терористичною метою із застосуванням комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру[33].

Необхідно також зазначити, що ані у позовній заяві Уряду України до Міжнародного суду ООН від 16 січня 2017 р. про порушення Російською Федерацією зобов'язань за Міжнародною конвенцією про боротьбу з фінансуванням тероризму від 9 грудня 1999 р. та за Міжнародною конвенцією про ліквідацію всіх форм расової дискримінації від 21 грудня 1965 р. (Україна проти Російської Федерації), ані в матеріалах справи,

[30] Конвенція про кіберзлочинність від 23 листопада 2001 р. <https://zakon.rada.gov.ua/laws/show/994_575#Text> (дата звернення: 10.10.2020).
[31] T-CY Guidance Note № 11 Aspects of Terrorism covered by the Budapest Convention, Adopted by the 16th Plenary of the T-CY <https://rm.coe.int/16806bd640> (accessed: 12.10.2020).
[32] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 15.10.2020).
[33] Про боротьбу з тероризмом (н 2).

що перебувають у публічному доступі, прямо не вказуються відповідні кібератаки, які відбувалися на території України[34].

Ця ситуація могла скластися з огляду на те, що питання застосовування норм міжнародного права щодо кібернетичного простору на сьогодні все ще залишається дискусійним. Розроблення загальних правил відповідальності держав за їхні діяння у кіберпросторі перебуває на поряду денному в ООН із 1998 р., але досі не має успіху[35], зокрема через припинення роботи п'ятої групи урядових експертів ООН у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки у зв'язку з відсутністю консенсусу щодо застосування права на самооборону і міжнародного гуманітарного права щодо протиправного використання інформаційно-комунікаційних технологій. Робота ООН у цьому напрямі була відновлена лише в жовтні 2018 р., коли Генеральна Асамблея ООН прийняла дві резолюції про створення двох груп: Відкритої робочої групи, ініційованої РФ[36], і Групи урядових експертів, ініційованої США[37]. Вони наразі провадять консультації і дослідження, а звітуватимуть у 2021 р.

Найбільш проблематичним в умовах віртуального кібернетичного простору є встановлення зв'язку між державою та конкретною кібератакою. Так, розвиваючи положення розділу II Проєкту Статей про відповідальність держав за протиправні діяння, Талліннський посібник із застосування міжнародного права до кібервоєн (далі – Талліннський посібник) передбачає умови, на основі яких може бути встановлено зв'язок певного протиправного діяння у кіберпросторі з конкретною державою:

1) воно вчинене органами влади цієї держави;

2) воно вчинене недержавними установами, які відповідно до національного законодавства здійснюють владні повноваження держави;

3) воно вчинене приватними особами за безпосереднього керування державою;

4) воно вчинене приватними особами, щодо яких держава здійснює "ефективний контроль";

5) воно вчинене приватними особами, яким надавалася підтримка, захист, фінансування цієї держави[38].

[34] Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination (Ukraine v. Russian Federation) (n 8).

[35] 'Developments in the field of information and telecommunications in the context of international security' *(United Nations)* <https://www.un.org/disarmament/ict-security> (accessed: 12.10.2020).

[36] Resolution adopted by the General Assembly A/RES/73/27 on 5 December 2018 <https://undocs.org/A/RES/73/27> (accessed: 12.10.2020).

[37] Resolution adopted by the General Assembly A/RES/73/266 on 22 December 2018 <https://undocs.org/A/RES/73/266> (accessed: 12.10.2020).

[38] The Tallin Manual on International Law applicable to Cyber Warfare, Prepared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence <http://csef.ru/media/articles/3990/3990.pdf> (accessed: 10.10.2020).

Додатковим критерієм для встановлення міжнародно-правової відповідальності держави за протиправні дії у кібернетичному просторі може бути здійснення протиправних діянь із кіберінфраструктури, розташованої на території відповідної держави. Однак, як зазначається у Звіті групи міжурядових експертів ООН у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки 2015 р.[39] і Талліннському посібнику, однієї вказівки на той факт, що незаконна діяльність була розпочата або відбувалась через інформаційно-комунікаційну інфраструктуру у цій державі, не є переконливим доказом для атрибуції цих дій державі.

Водночас слід зауважити, що у міжнародному праві фактично сформувався позитивний обов'язок держави забезпечувати, щоб з її території не здійснювалися атаки проти інших держав чи організацій[40]. Зокрема, у справі *Corfu Channel*[41] Міжнародний суд ООН визначив, що відповідно до ст. 74 Статуту ООН принцип добросусідства включає обов'язок держав не дозволяти використовувати власну територію для дій, що суперечать правам інших держав[42]. Принцип "не завдавати шкоди", також закріплений у положеннях Стокгольмської декларації[43] і Ріо декларації[44], був застосований і під час розгляду справ *Trail Smelter*[45] та *Lac Lanoux*[46]. Зобов'язання запобігати протиправній діяльності, що походить із території держави, підтверджено у справі *ICJ case Namibia*[47], а зобов'язання забезпечувати безпеку власної території і не визнавати результати протиправних дій – у справі *ICJ case Tehran*[48].

Таким чином, можна стверджувати, що держава зобов'язана не надавати свідомого дозволу для використання кібернетичної інфраструктури, яка перебуває на її території або під її контролем, для здійснення

[39] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 22 July 2015 <https://undocs.org/A/70/174> (accessed: 18.10.2020).
[40] M Kettemann, 'Ensuring Cybersecurity Through International Law' [2017] 69 (2) Revista Española De Derecho Internacional 281–90.
[41] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) <https://www.icj-cij.org/en/case/1> (accessed: 10.10.2020).
[42] Summary of relevant aspects of Corfu Channel Case (MERITS) <https://www.iilj.org/wp-content/uploads/2016/08/Summary-of-and-extract-from-Corfu-Channel-Case-United-Kingdom-v.-Albania.pdf> (accessed: 10.10.2020).
[43] Декларація Конференції Організації Об'єднаних Націй з проблем оточуючого людину середовища від 16 червня 1972 р. <https://zakon.rada.gov.ua/laws/show/995_454#Text> (дата звернення: 15.10.2020).
[44] Декларація Ріо-де-Жанейро щодо навколишнього середовища та розвитку від 14 червня 1992 р. <https://zakon.rada.gov.ua/laws/show/995_455#Text> (дата звернення: 15.10.2020).
[45] Trail smelter case (United States, Canada) 16 April 1938 and 11 March 1941 <https://www.informea.org/sites/default/files/court-decisions/Trail%20Smelter%20Case.pdf> (accessed: 10.10.2020).
[46] Lake Lanoux Arbitration (France v. Spain), Nov 16, 1957 <https://www.informea.org/sites/default/files/court-decisions/COU-143747E.pdf> (accessed: 10.10.2020).
[47] Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970) <https://www.icj-cij.org/en/case/53> (accessed: 10.10.2020).
[48] United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) <https://www.icj-cij.org/en/case/64> (accessed: 10.10.2020).

негативних і незаконних дій проти іншої держави. Ба більше, держава зобов'язана прийняти всі необхідні й ефективні заходи, щоб зупинити таку протиправну діяльність. Більшість кібератак на території України походили саме з російської інформаційної інфраструктури. Для прикладу, за заявою міністра енергетики України, опублікованою у *Reuters*, атаку на енергосистему України у 2015 р. слід позиціонувати з російською стороною[49]. А за даними Служби безпеки України, розслідування кібератак на "Прикарпаттяобленерго", "Київобленерго", "Чернівціобленерго" та "Хмельницькобленерго" із залученням міжнародних експертів із кібербезпеки було виявлено шкідливе програмне забезпечення типу *BlackEnergy* та встановлено віддалений несанкціонований доступ із території РФ[50].

Слід також враховувати, що кібератаки на території України здійснювалися паралельно зі збройним конфліктом між Україною та РФ. Відповідно до положень Талліннського посібника, а також окремих доктринальних підходів, зокрема Дж. Валух та О. Гамулак[51], кібероперації, що здійснюються у контексті збройного конфлікту, мають бути об'єктом регулювання міжнародного гуманітарного права. Тому для встановлення міжнародно-правової відповідальності щодо таких дій мають застосовуватися норми *jus in bello.*

Водночас кваліфікація ситуації на сході України та в Автономній Республіці Крим як міжнародного збройного конфлікту визначена звітами про дії щодо попереднього розслідування Офісу Прокурора Міжнародного кримінального суду за 2016 і 2017 рр. Проаналізувавши значний обсяг інформації, що стосується передбачуваних злочинів, які відбувалися під час цього конфлікту, Канцелярія Прокурора не досліджувала і не розглядала кібернетичні атаки, які здійснювалися на території України з 2014 р.

Висновки. Отже, РФ заперечує наявність підстав для відповідальності за вчинені терористичні та кібертерористичні дії. Завдання України – продовжити розслідування справ, інтенсифікувати розпочаті провадження, вести пропагандистську (роз'яснювальну) роботу у межах міжнародних організацій, через двосторонні перемовини, розповсюдження знань на рівні академічного суспільства.

Визначення способів притягнення РФ до міжнародно-правової відповідальності за здійснені терористичні і кібертерористичні атаки на території України є важливою умовою для відновлення справедливості,

[49] P Potilyuk, 'Ukraine Sees Russian Hand in Cyber Attacks Against Power Grid' (*Reuters,* 16.02.2016) <http://www.reuters.com/article/us-ukrainecybersecurity-idUSKCN0VL18E> (accessed: 10.10.2020).

[50] Н Прудка, 'Кібервійна проти України. Перші жертви і висновки' (*Главком,* 08.04.2016) <https://glavcom.ua/publications/334262-kibervijna-proti-ukrajini.-pershi-zhertvi-i-visnovki.html> (дата звернення: 10.10.2020).

[51] S Sayapin and E Tsybulenko, *The use of force against Ukraine and International Law* (Springer 2018) 465.

відшкодування завданих збитків, а також елементом розвитку державного контуру безпеки, зокрема й кібернетичної, і розбудови кіберщита від гібридних агресій.

REFERENCES

Bibliography

Authored books

1. Sayapin S and Tsybulenko E, *The use of force against Ukraine and International Law* (Springer 2018) (in English).

Journal articles

2. Kettemann M, 'Ensuring Cybersecurity Through International Law' [2017] 69 (2) Revista Española De Derecho Internacional 281–90 (in English).
3. Zadorozhny O and Korotkyi T, 'Legal Assessment of the Russian Federation's Policy in the Context of the Establishment and Activities of Terrorist Organizations "Donetsk People's Republic" ("DPR") and "Lugansk People's Republic" ("LPR") in Eastern Ukraine' [2015] 2 (1) Evropský Politický A Právní Diskurz 8–18 (in English).

Websites

4. 'Case Studies: Tags: MH 17' *(Bellingcat)* <https://www.bellingcat.com/category/resources/case-studies/?fwp_tags=mh17> (accessed: 10.10.2020) (in English).
5. 'Claus Hjort: Rusland stod bag cyberangreb mod Mærsk' (*Berlingske,* 15.02.2018) <https://www.berlingske.dk/virksomheder/claus-hjort-rusland-stod-bag-cyberangreb-mod-maersk> (accessed: 11.10.2020) (in German).
6. 'CSE Statement on the NotPetya Malware' (*Government of Canada,* 15.02.2018) <https://www.cse-cst.gc.ca/en/media/2018-02-15> (accessed: 10.10.2020) (in English).
7. 'Developments in the field of information and telecommunications in the context of international security' *(United Nations)* <https://www.un.org/disarmament/ict-security> (accessed: 12.10.2020) (in English).
8. 'New Zealand joins international condemnation of NotPetya cyber-attack' (*Government Communications Security Bureau,* 16.02.2018) <https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack> (accessed: 11.10.2020) (in English).
9. 'Russian military 'almost certainly' responsible for destructive 2017 cyber attack' (*National Cyber Security Centre,* 14.02.2018) <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> (accessed: 11.10.2020) (in English).
10. 'Statement from the Press Secretary' (*The White House,* 15.02.2018) <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25> (accessed: 12.10.2020) (in English).
11. Potilyuk P, 'Ukraine Sees Russian Hand in Cyber Attacks Against Power Grid' *(Reuters,* 16.02.2016) <http://www.reuters.com/article/us-ukrainecybersecurity-idUSKCN0VL18E> (accessed: 10.10.2020) (in English).
12. 'Delehatsiia Ukrainy bere uchast u antyterorystychnii konferentsii OBSIe' (*Ministerstvo zakordonnykh sprav Ukrainy,* 15.09.2020) <https://mfa.gov.ua/news/delegaciya-ukrayini-bere-uchast-u-antiteroristichnij-konferenciyi-obsye> (accessed: 01.11.2020) (in Ukrainian).

13. 'Kazakhstantsa, voevavsheho na storone separatystov v Donbasse, pryhovoryly k 4,5 hodam lyshenyia svobody' (*Medyazona,* 22.05.2020) <https://mediazona.ca/news/2020/05/22/dnr-deported-2> (accessed: 10.10.2020) (in Ukrainian).
14. 'Naibilshikiberataky proty Ukrainy z 2014 roku. Infohrafika' (*Novoe vremia,* 08.07.2017) https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html (accessed: 11.10.2020) (in Ukrainian).
15. 'Ofis Henprokurora napravyv do Henprokuratury Respubliky Bilorus zapyty pro vydachu 28 uchasnykiv zbroinoho konfliktu na Donbasi' (*Ofis Heneralnoho Prokurora,* 12.08.2020) <https://www.gp.gov.ua/ua/news?_m=publications&_t=rec&id=278570> (accessed: 11.10.2020) (in Ukrainian).
16. 'SBU vstanovyla prychetnist spetssluzhb RF do ataky virusu-vymahacha Petya.A' (*Ukrinfo,* 01.07.2017) <https://www.ssu.gov.ua/ua/news/1/category/21/view/3660#.37yT3eBD.dpbs> (accessed: 10.10.2020) (in Ukrainian).
17. 'U Chekhii bilorusa posadyly na 4,5 roky za dopomohu separatystam Donbasu' (*Ievropeiska pravda,* 22.09.2020) <https://www.eurointegration.com.ua/news/2020/09/22/7114573> (accessed: 11.10.2020) (in Ukrainian).
18. Prudka N, 'Kiberviina proty Ukrainy. Pershi zhertvy i vysnovky' (*Hlavkom,* 08.04.2016) <https://glavcom.ua/publications/334262-kibervijna-proti-ukrajini.-pershi-zhertvi-i-visnovki.html> (accessed: 10.10.2020) (in Ukrainian).
19. Ramach M, 'Boiovyk, zasudzhenyi u Serbii, znovu voiuie na Donbasi' (*Radio Svoboda,* 20.10.2018) <https://www.radiosvoboda.org/a/29554393.html> (accessed: 10.10.2020) (in Ukrainian).
20. Sydorenko S, 'Shist tonn dokaziv proty Rosii: shcho peredala Ukraina do Mizhnarodnoho sudu OON' (*Ievropeiska Pravda,* 12.06.2018) <www.eurointegration.com.ua/articles/2018/06/12/7083003> (accessed: 11.10.2020) (in Ukrainian).

Liliana Tymchenko
Marta Yatsyshyn

INTERNATIONAL LEGAL RESPONSIBILITY OF THE RUSSIAN FEDERATION FOR TERRORIST AND CYBERTERRORIST ACTIONS IN UKRAINE

Abstract. The aggression of the Russian Federation against Ukraine, launched in 2014, led to destructive consequences. In particular, being in a hybrid conflict, Ukraine has become an environment for various attacks, including terrorist and cyber-terrorist.

Establishing the truth circumstances of each specific incident and bringing Russia to justice is a priority to maintain international security, reduce the level of the global terrorist threat, and restore peace and justice in Ukraine.

In light of the urgency and importance of this problem, the purpose of this article is to identify and comprehensively analyse the possibility of bringing the Russian Federation to international legal responsibility for terrorist and cyberterrorist activities in Ukraine in accordance with applicable international law.

There are numerical evidences that the Russian Federation is responsible for organizing and preparing illegal abductions to commit terrorist acts in the territory of Ukraine. Such proves are at the disposal of authorized law enforcement agencies of Ukraine, Kazakhstan, Czech Republic, negotiated within the framework of the international intergovernmental organizations, published in well-known media. Academics summarized testimonies in their scientific works and on the bases of it is possible to make an unambiguous conclusion that

the Russian Federation is responsible for committing terrorist acts and for involvement in them; the connection of terrorist groups of DNR and LNR with the Russian authorities is also established.

It is worth to note that since 2014 there has been an intensification of cyberattacks in Ukraine with the participation, assistance and funding of the Russian Federation. The factual grounds for bringing the Russian Federation to international legal responsibility for cyberterrorist acts on the territory of Ukraine can be considered from the standpoint of violation of obligations established by international treaties in the field of counter-terrorism.

Lack of direct reference to specific cyberattacks, that took place on the territory of Ukraine, in the statement of claim of the Government of Ukraine to the UN International Court of Justice of January 16, 2017 on violation by the Russian Federation of obligations under the International Convention for the Suppression of the Financing of Terrorism of December 9, 1999 and the International Convention on the Elimination of All Forms of Racial Discrimination of December 21, 1965 (Ukraine v. the Russian Federation), as well as in the materials of the case that are publicly available, due to the general uncertainty of international law applicability in cyberspace.

There are undeniable facts of cyberattacks commitment on the territory of Ukraine through the Russian cyber infrastructure, as well as with the participation of the Armed Forces of the Russian Federation, which is confirmed in the statements of many states, decisions of international organizations, including the EU. However, a state is obliged not to give conscious permission to use cyber infrastructure located on its territory or under its control to commit negative and illegal actions against another state. Moreover, the state is obliged to take all necessary and effective measures to stop such illegal activities.

Russian Federation denies the existence of grounds for liability for terrorist and cyberterrorist acts. The task of Ukraine is to continue the investigation of cases, to intensify the initiated proceedings, to conduct propaganda (explanatory) work within the framework of international organizations, through bilateral negotiations, dissemination of knowledge at the level of academic society.

Determining ways to bring the Russian Federation to international legal responsibility for terrorist and cyber-terrorist attacks on the territory of Ukraine is an important condition for restoring justice, compensation for losses, as well as an element of the development of the state security circuit, including cybersecurity.

KEYWORDS: international legal responsibility; terrorism; terrorist act; cyberterrorism; cyberattack; Russian Federation; Ukraine.