

До спеціалізованої вченої ради ДФ 41.086.081
Національного університету
«Одеська юридична академія»
65009, м. Одеса, вул. Фонтанська дорога, 23

ВІДГУК

**офіційного опонента –
кандидата юридичних наук Плотнікова Олексія Вікторовича
на дисертацію Музики Вікторії Василівни на тему:
«Атрибуція кібератак проти об'єктів критичної інфраструктури:
визначення основних проблем та шляхів їх вирішення»,
подану на здобуття наукового ступеня доктора філософії за спеціальністю
081 «Право»**

Актуальність теми наукового дослідження. З появою кіберпростору порушення норм внутрішньодержавного та міжнародного права вийшло на принципово новий рівень. Держави почали не тільки нарощувати свою кіберспроможність для захисту національних інтересів від різноманітних кібероперацій з деструктивним потенціалом, а й використовувати можливості кіберпростору з метою досягнення геополітичних цілей.

Наразі саме об'єкти критичної інфраструктури є основною ціллю кібератак, що підтверджується висновками Групи урядових експертів ООН щодо заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки. Відсутність розуміння щодо того, чи застосовується міжнародне право в кібердомені та як має здійснюватися процес атрибуції кібератак проти таких об'єктів в сукупності призвели до зростання кількості кібератак та їх тривалого толерування як «прийнятного відхилення».

В епоху безпрецедентних загроз для міжнародного миру й безпеки та взаємної уразливості сильних і слабких держав особливої значимості набуває неухильне виконання всіма суб'єктами міжнародного права міжнародно-правових зобов'язань. Попри відсутність *lex specialis*, міжнародне право застосовується до кіберпростору. Таким чином, кібератаки проти об'єктів

критичної інфраструктури, що призвели до порушення договірних та звичаєвих зобов'язань повинні атрибутуватися відповідальним державам.

Процес атрибуції кібератак є досить складним і неоднозначним, тому спричинює гострі дискусії в теорії та на практиці міжнародного права. Практика свідчить про необхідність здійснення технічної та політичної атрибуції як передумови здійснення атрибуції в розумінні Статей про відповідальність держав за міжнародно-протиправні діяння 2001 року.

Вище зазначені обставини вказують на високий рівень актуальності дисертаційного дослідження.

Особливої актуальності дослідженню додають постійні кібератаки, зокрема проти об'єктів критичної інфраструктури України. Варто відмітити, що дисертанта комплексно підійшла до атрибуції кібератак проти систем електропостачання України в 2015 та 2016 роках в контексті збройного конфлікту, продемонструвавши важливість оцінки наявних політичних та технічних індикаторів в процесі атрибуції кібератак.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації. Дисертаційне дослідження характеризується комплексним і глибоким підходом до предмету дослідження.

Обґрунтованість положень, сформульованих у дисертації, підтверджується критичним аналізом значного масиву джерел різноманітного спрямування (юридичного, технічного, методологічного, порівняльно-правового), які дають можливість системно осягнути питання, пов'язані з процесом атрибуції кібератак проти об'єктів критичної інфраструктури.

На сторінках дисертації авторка коректно веде полеміку з іншими науковцями, належно аргументуючи власну позицію, а також доречно звертається до національного законодавства та різних форм *opinio juris* іноземних держав, формулюючи на підставі відповідних кореляцій висновки щодо особливостей атрибуції кібератак проти об'єктів критичної інфраструктури та категоризації об'єктів як таких, що входять в поняття «критична інфраструктура».

Зроблені дисертанткою висновки та сформульовані пропозиції, які загалом є переконливими, ґрунтуються також на системному аналізі звітів міжнародних експертів (ООН, НАТО, ОБСЄ), заявах, стратегіях та односторонніх деклараціях держав.

Список використаних джерел свідчить про опрацювання значної кількості актуальних джерел, серед яких значне місце належить англомовним першоджерелам.

Високий ступінь вірогідності та наукової обґрунтованості результатів виконаного дослідження також забезпечено завдяки використанню відповідного методологічного апарату, який детально розкрито у вступній частині (с. 18-19).

Постановка завдань, визначення об'єкта, предмета та мети наукового пошуку має чіткий і зрозумілий вигляд, та цілком відповідає загальним вимогам. Завдання та мета наукової праці автором загалом досягнуті.

Достовірність і новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації не викликає сумнівів та полягає, насамперед, у тому, що дисертаційна робота є першим у національній науці спеціальним комплексним монографічним дослідженням атрибуції кібератак проти об'єктів критичної інфраструктури, що встановлює основні складнощі та можливі шляхи їх вирішення задля забезпечення відповідальної поведінки держав в кіберпросторі.

До положень дисертації, які, безспірно, характеризуються елементом новизни, та, на мій погляд, допомагають вирішити ряд важливих теоретичних і практичних проблем, належать, зокрема, такі результати дослідження:

1. Заслугує на увагу аналіз різних форм *opinio juris* держав щодо застосування міжнародного права в кіберпросторі щодо міжнародно-протиправної поведінки в кіберпросторі, яка вимагає атрибуції, визначення спільного та відмінного у існуючих підходах та баченні перспектив міжнародно-правового регулювання кібератак та їх атрибуції.

2. Логічною та слушною є позиція дисертантки щодо комплексного підходу до атрибуції кібератак проти об'єктів критичної інфраструктури, яка, на її думку, вимагає здійснення технічної, політичної та юридичної атрибуції як нероздільної тріади при встановленні відповідальності держави за міжнародно-протиправні діяння держав в кіберпросторі.

3. Слід підтримати намагання авторки відокремити міждержавні об'єкти критичної інфраструктури, що спільно використовуються декількома державами, в самостійну категорію, а також вироблення раціонального підходу до категоризації об'єктів як критично важливих, який попри орієнтованість на національні пріоритети, виключав би можливі зловживання дискрецією в питаннях категоризації.

4. Цікавою є ідея перенесення практики Європейського Союзу щодо забезпечення кіберстійкості критичної інфраструктури, зокрема використання можливостей розробленого в ЄС інструментарію кібердипломатії на універсальному рівні (з певними модифікаціями щодо характеру санкцій та атрибуції кібератак).

5. Особливу цінність становить атрибуція кібератак проти систем електропостачання України в контексті збройного конфлікту на Донбасі з урахуванням наявних технічних та політичних індикаторів, що підтверджує необхідність врахування загального контексту, мотивації, використаних ресурсів та інших релевантних факторів.

Результати дослідження мають не лише наукове, а й практичне значення. Одержані автором висновки можуть бути використані у нормотворчій сфері, а також у правозастосовній діяльності. Окремі положення дисертації можуть бути використані при написанні відповідних розділів підручників і навчальних посібників; при викладанні навчальних курсів та спецкурсів, а також у науково-дослідній роботі.

Основні положення дисертації висвітлено дисертанткою в 11 наукових публікаціях, 3 з яких опубліковано у вітчизняних наукових фахових виданнях, що входять до затвердженого переліку, 1 – в іноземному виданні, 1 –

колективній монографії (розділ), 6 тез доповідей на науково-практичних конференціях. Це відповідає вимогам п. 11 Тимчасового порядку присудження ступеня доктора філософії, затвердженому Постановою Кабінету Міністрів України від 06 березня 2019 р. № 167 (зі змінами).

Оцінка змісту дисертації. Структурно дисертація складається із переліку умовних позначень, вступу, трьох розділів, що містять 11 підрозділів, висновків, списку використаних джерел та додатків.

Структура дослідження повністю відповідає окресленій меті та завданням, що дозволило здобувачці наукового ступеню найбільш повно охопити предмет дослідження, а опоненту – прослідкувати авторський задум, краще зрозуміти логіку та послідовність сформульованих в роботі висновків. Дисертантка у повному обсязі виконала вимоги, які висуваються МОН України до цього виду наукових праць.

У вступі обґрунтовано актуальність теми дисертаційного дослідження, розкривається зв'язок роботи з науковими програмами, планами, темами, визначаються мета, завдання, об'єкт, предмет і методи дослідження, науково-теоретична основа, нормативно-правова і емпірична база, характеризується наукова новизна та практичне значення одержаних результатів, подається інформація про апробацію результатів дослідження та структура дисертації.

Розділ 1 «Кібератаки як міжнародно-протиправні діяння в кіберпросторі: визначення поведінки, що вимагає атрибуції» складається з трьох підрозділів, у яких послідовно проаналізовано природу та сутнісні характеристики кібератак, застосування наявного міжнародно-правового регулювання до кібератак і аналіз *opinio juris* та практики держав щодо міжнародно-протиправної поведінки в кіберпросторі, яка повинна атрибутуватись державам.

В підрозділі 1.1 дисертанткою зазначається, що кібератаки можуть здійснюватися проти різних компонентів фізичного, логічного та соціального рівнів кіберпростору, які майже завжди знаходяться в межах території держав. Встановлено, що собою представляють кібератак та як співвідносяться з такими поняттями як «кібероперація» та кіберексплуатація. Таке розмежування є

позитивним, оскільки дисертантка пояснює взаємозв'язок між успішною кібератакою та кіберексплуатацією, що їй передує, та вибудовує розуміння читача щодо того, чому в подальшому буде враховуватися публічна атрибуція деяких випадків кіберексплуатації.

В підрозділі 1.2 дається оцінка звичаєвих та договірних норм міжнародного права до кібератак, і найголовніше – підкреслюються проблеми щодо визнання застосування спеціальних міжнародно-правових режимів. Дисертантка наголошує, що «кібератаки не є однорідними за своєю природою та наслідками. Неоднорідним є і саме міжнародне право, яке представляє систему, що об'єднує норми в галузі, інститути та спеціальні міжнародно-правові режими». В подальшому надається класифікація кібератак, до яких застосовуються різні правові режими та які, на думку авторки, визначатимуть особливості здійснення процесу атрибуції.

Цінним з позиції доктрини міжнародного права є підрозділ 1.3, що розкриває *opinio juris* та практику держав щодо застосування міжнародного права до кіберпростору та в значній мірі ґрунтується на аналізі першоджерел (заяв, односторонніх декларацій, воєнних стратегій держав). Дисертантка демонструє, що попри висновок Групи урядових експертів у 2013 та 2015 роках про застосування норм міжнародного права в кіберпросторі, держави по-різному підходять до інтерпретації та застосування норм міжнародного права. В окремих випадках практика держав також свідчить про відхилення від офіційної позиції. Разом з тим, аналіз конститутивних елементів міжнародного звичаю дозволяє чітко простежити позицію дисертантки, що полягає в підтримці ідеї формування та ідентифікації звичаєвих норм в кібердоміні. При цьому, дисертантка досить стримано підходить до ідеї розробки спеціального інструменту щодо застосування міжнародного права до кібератак, що, на думку дисертантки, ризикує стати «ще одним «проектом статей» в силу швидкого розвитку інформаційних технологій, які завжди випереджають позитивне міжнародне право».

Другий розділ дисертації розпочинається встановленням змісту поняття «критична інфраструктура», що є центральним в межах атрибуції кібератак. Авторка зважено підходить до поставленого завдання, критично підходячи до порівняльно-правового аналізу національного законодавства. Наприклад, дисертантка не погоджується з підходом США, які до об'єктів критичної інфраструктури зараховують зоопарки, мотелі, конференц-центри тощо, наголошуючи, що такий підхід є не виправдано широким. Наголошується на необхідності розробки підходу, який враховував би критичність об'єктів для конкретних держав, а також базувався би на критично важливих функціях, як це зроблено в законодавстві Франції чи законопроектів України «Про критичну інфраструктуру». Пропонується виділити транснаціональні (міждержавні) об'єкти в окрему категорію, що є цілком прийнятним, оскільки порушення чи знищення таких об'єктів може призвести до серйозних людських втрат, помітного впливу на економіку, політичне та соціальне функціонування держав та їх безпеку.

Підрозділи 2.2, 2.3 та 2.4 в сукупності розкривають особливості атрибуції кібератак проти об'єктів критичної інфраструктури. По-перше, стандарти атрибуції, що містяться в Статях про відповідальність держав та Талліннському керівництві 2.0, застосовуються до кібератак проти об'єктів критичної інфраструктури. В контексті кібератак, в першу чергу, у фокус аналізу потрапляє атрибуція державі поведінки її органів, поведінки індивідів чи юридичних осіб, що уповноважені здійснювати елементи урядових функцій, та поведінки осіб чи групи осіб, що діють під керівництвом чи контролем держави.

По-друге, підкреслюється необхідність здійснення технічної та політичної атрибуції, що, серед іншого, розкривають особливості процесу атрибуції кібератак проти об'єктів критичної інфраструктури.

На увагу заслуговує також розвиток ідеї щодо можливості перенесення обов'язку проявляти необхідну обачність з первинних до вторинних норм відповідальності держав.

Підрозділ 2.5 містить комплексне дослідження кібератак проти об'єктів критичної інфраструктури України в контексті збройного конфлікту на сході України та їх атрибуцію на підставі технічних та політичних індикаторів. Дисертантка доводить необхідність врахування загального контексту, мотивації, використаних ресурсів та інших індикаторів. Достовірність висновків знаходить підтвердження в рішенні Ради ЄС, яке фактично публічно атрибутує кібератаки 2015 та 2016 років Російській Федерації, накладаючи кіберсанкції на Головне управління Збройних Сил РФ та його співробітників, чия причетність до кібератак була встановлена.

Третій розділ є логічним завершенням двох попередніх, що містить практичні пропозиції щодо вирішення проблеми атрибуції кібератак, що часто зумовлена відсутністю у постраждалих держав необхідних людських та технічних ресурсів.

Підрозділ 3.1 стосується співпраці з приватним сектором в межах спеціального механізму атрибуції кібератак. Така співпраця є логічною та виражає прагнення як урядового, так і приватного секторів. Положення дисертації свідчать про те, що взаємодія вже відбувається, але дисертантка наполягає на створенні спеціалізованого механізму, який би займався здійсненням атрибуції кібератак. Розглядаються різні варіанти співпраці, зокрема пропозиції щодо не передбачають включення державних агентів в склад такого механізму. Разом з тим, дисертантка зупиняється на більш прийнятній пропозиції, оскільки в розпорядженні держави знаходяться релевантні відомості і часто саме держави можуть розкрити особливості політичного, соціального та економічного контексту, що мають значення в ході атрибуції кібератак проти об'єктів критичної інфраструктури.

Цікавим та цінним є розділ присвячений інтегральній моделі взаємодії ЄС, яка, серед іншого, передбачає інструментарій кібердипломатії. Наразі Європейський Союз першим почав застосовувати кіберсанкції до кібератак, що становлять зовнішню загрозу. Дисертантка зазначає, що міжнародна спільнота може перейняти досвід та практику ЄС щодо співпраці з різним акторами з

ціллю встановлення джерела кібератаки (атрибуції), а також може вдатися до застосування кіберсанкцій в межах ООН, замінивши вибіркові (індивідуальні) кіберсанкції на секторальні з метою підвищення їх ефективності. Така ідея є не тільки цікавою, а й характеризується практичною цінністю, оскільки секторальні санкції та публічна атрибуція кібератак державі в межах ООН в сукупності сприятимуть підвищенню відповідальної поведінки в кіберпросторі.

Завершує третій розділ підрозділ щодо розгляду міждержавного спору. Дисертантка виходить з того, що розгляд спору щодо кібератак проти об'єктів критичної інфраструктури сприятиме вирішенню низки практичних проблем. Аналізуються стандарти доказування, які Суд потенційно може застосовувати до різних кібератак, різні групи доказів тощо, а також встановлюються переваги такого сценарію.

У висновках сформульовано найбільш суттєві, на думку дисертантки, результати та положення дослідження.

Зауваження щодо змісту дисертації. Не зупиняючись на досягненнях та позитивних моментах виконаної дисертаційної роботи, загалом позитивно оцінюючи рецензовану працю, необхідно звернути увагу на окремі протиріччя та дискусійні положення, які, на мій погляд, потребують або додаткової аргументації, або спеціальних роз'яснень під час захисту дисертації, а саме:

1. Розглядаючи природу та сутнісні характеристики кібератак, дисертантка пояснює суміжні з поняттям «кібератака» категорії (зокрема, кібероперація, кіберексплуатації тощо). Разом з тим, в підрозділі 1.1 не розкривається зміст поняття «кіберінцидент», яке в подальшому згадується при аналізі позиції Швейцарії в підрозділі 1.3.

2. Положення дисертації містять твердження про формування звичаєвих норм міжнародного права. З цим можна погодитися, оскільки міжнародні договори, як правило, не завжди слідують появі нових технологій або це відбувається після їх тривалого використання. Наприклад, жодного договору, який би регулював військові операції в повітряному просторі, не існує, хоча повітряній війні вже понад сто років. Парадигматичними

прикладом є конвенції, що регулюють такі види зброї, як протипіхотні наземні міни та касетні боєприпаси, що були прийняті через десятиліття після першого застосування цих видів озброєнь і які досі є предметом багатьох суперечок.

Попри встановлення заперечень з боку низки держав, дисертантка не згадує доктрину «наполегливого заперечувача» (*persistent objector*). Тому хотілось би почути позицію авторки щодо застосування даної доктрини до звичаєвих кібернорм та наслідки такого застосування.

3. Дисертантка наполягає на комплексному здійсненні атрибуції кібератак, що охоплює технічну та політичну атрибуцію кібератак, логічним завершенням яких, на її переконання, є здійснення юридичної атрибуції. В підрозділі 1.2 також зазначається, що наслідки кібератак визначатимуть процес атрибуції. Так, наприклад, зазначається, що «у випадку звернення до односторонніх заходів самопомоги в рамках *jus ad bellum* державам потрібно здійснити атрибуцію *ex ante* в короткі строки, яка буде відрізнятися від атрибуції *post factum*». У зв'язку з цим, хочеться почути позицію автора щодо доцільності здійснення технічної, політичної та юридичної атрибуції всіх кібератак проти об'єктів критичної інфраструктури.

4. В підрозділі 3.1 дисертантка заперечує можливість створення спеціалізованого механізму, який не передбачає участь держав в процесі здійснення атрибуції, посилаючись на необхідність оцінки політичних індикаторів та задля пришвидшення процесу атрибуції. Така позиція є зрозумілою, але до оцінки політичних індикаторів можуть залучатися науковці, представники громадськості постраждалої держави тощо. З одного боку, це вирішить проблему участі держави як потенційно зацікавленої сторони, з іншого – процес атрибуції протікатиме швидше.

5. Дисертантка пропонує адаптувати інструментарій кібердипломатії з метою підвищення його ефективності та подальшого використання на універсальному рівні. Враховуючи тривалість та складність досягнення консенсусу в межах діяльності ООН, хотілось би почути позицію здобувачки

щодо можливості застосування, наприклад, кіберсанкцій Україною, критична інфраструктура якої часто стає ціллю кібератак.

Водночас варто зазначити, що висловлені критичні коментарі носять дискусійний характер і не стосуються основних, концептуальних положень дисертації. Таким чином, вони не впливають на загальну позитивну оцінку дисертаційного дослідження.

Наведене дозволяє дійти висновку, що дисертаційне дослідження В.В. Музики «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», подане на здобуття освітньо-наукового ступеня доктора філософії за спеціальністю 081 «Право», за змістом, обсягом, науковою новизною, теоретичним і практичним значенням відповідає вимогам Тимчасового порядку присудження ступеня доктора філософії, затвердженого Постановою Кабінет Міністрів України від 06 березня 2019 р. № 167 (зі змінами).

Отже, авторка дисертаційного дослідження, Вікторія Василівна Музика, набула теоретичних знань, умінь, навичок та інших компетентностей, достатніх для продукування нових ідей, розв'язання комплексних проблем у галузі професійної діяльності, оволоділа методологією наукової та педагогічної діяльності, а також здійснила власне оригінальне дослідження, результати якого мають наукову новизну, теоретичне та практичне значення (п. 3 та пп. 9-15 Тимчасового Порядку).

У підсумку слід зазначити, що за результатами публічного захисту здобувачка наукового ступеня, Музика Вікторія Василівна, заслуговує на присудження їй наукового ступеня доктора філософії за спеціальністю 081 «Право».

Офіційний опонент
кандидат юридичних наук,
старший юрист ГО «Десяте квітня»



О. В. Плотніков

ВІДПОВІДАЄ
ОРИГІНАЛУ