«ЗАТВЕРДЖУЮ»
В.о. ректора Національного університету «Одеська юридична академія»
д.ю.н., професор М. Р. Аракелян

«24» листопада 2021 р.

ВИСНОВОК

Національного університету «Одеська юридична академія» про наукову новизну, теоретичне та практичне значення результатів дисертації Музики Вікторії Василівни на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», поданої на здобуття ступеня доктора філософії за спеціальністю 081 «Право», затвердженої Вченою радою Національного університету «Одеська юридична академія» «02» грудня 2020 року (Протокол № 3)

ВИТЯГ

з протоколу засідання фахового семінару кафедри міжнародного та європейського права та кафедри права інтелектуальної власності та патентної юстиції Національного університету «Одеська юридична академія» від «24» листопада 2021 року № 3

ПРИСУТНІ:

декан факультету міжнародно-правових відносин к.ю.н. Неугодніков А.О., д.ю.н., професор Аракелян М. Р., д.ю.н., професор Бігняк О. В., д.ю.н., професор Бехруз Х. Н., д.ю.н., професор Сурілова О.О., д.ю.н., професор Бабін Б.В., д.ю.н., професор Харітонова О. І., к.ю.н, доцент Бєлогубова О. О., к.ю.н, доцент Мануїлова К. В., к.ю.н, доцент Грушко М. В., к.ю.н, доцент Чайковський Ю. В., к.ю.н., доцент Канєнберг-Сандул О. К., к.ю.н, доцент Пасечник О. В., к.ю.н., доцент Дронов В. Ю., к.ю.н., доцент Гриб Г. М., к.ю.н., доцент Цибульська О. Ю., к.ю.н., доцент Рябошапченко В.А., к.ю.н., доцент Форманюк В. В., к.ю.н., доцент Харитонов Р.Ф., к.ю.н., доцент Федорова Т.С., доктор філософії, доцент Войтович П. П., асистент Владишевська В. В., асистент Гребенюк Д. О., лаборант Рудецька П. А, дисертант Музика В. В.

З присутніх 6 докторів юридичних наук, 14 кандидатів юридичних наук, один доктор філософії та 2 асистенти – фахівців з проблем поданої на розгляд дисертації.

ПОРЯДОК ДЕННИЙ:

Обговорення дисертаційного дослідження здобувачки кафедри міжнародного та європейського права Музики Вікторії Василівни за темою: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», поданої на здобуття ступеня доктора філософії зі спеціальності 081 «Право».

СЛУХАЛИ:

Доповідь здобувачки ступеня вищої освіти доктора філософії Вікторії Василівни Музики на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», поданої на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 «Право».

Обґрунтовуючи вибір теми дисертаційного дослідження, здобувачка зазначила, що об'єкти критичної інфраструктури та їх захист знаходяться в повістці багатьох держав світу з початку двадцять першого століття. Теракти 11 вересня 2001 року в Сполучених Штатах Америки та теракти 2004 і 2005 років на території країн-членів Європейського Союзу стали тим індикатором, який підкреслив важливість критичної інфраструктури, від нормального функціонування якої залежить безпека та добробут держави і людей. Водночас, якщо на початку 2000-х років до атак на об'єкти критичної інфраструктури вдавалися недержавні актори, то виникнення кіберпростору, а з ним і кібератак, відкрило нові можливості для держав, а саме – щодо переслідування своїх геополітичних інтересів шляхом використання кібератак з руйнівним потенціалом.

На підтвердження своєї позиції здобувачка згадала кібератаки на американську греблю у 2013 році, німецький металургійний комбінат у 2014 році, українські системи електроенергетики у 2015 та 2016 роках, Національну службу охорони здоров'я у Великобританії у 2017 році, системи приладів безпеки Саудівської Аравії в 2017 році, постачальника електроенергії в Південній Африці, індійський атомний завод у 2019 році та найбільшу трубопровідну систему США у 2021 році, що, на її думку, представляють лише незначний перелік кібератак проти об'єктів критичної інфраструктури. Дисертантка зазначила, що кількість кібератак буде постійно зростати, а з ними і складність їх реалізації та серйозність наслідків. Такий висновок вона пов'язує з тривалим толеруванням та сприйняттям більшості кібератак в якості нового «нормально», що викликано відсутністю атрибуції кібератак для цілей притягнення держав до відповідальності. Більш того, з урахуванням постійного розвитку штучного інтелекту в недалекому майбутньому, як зазначила дисертантка, цілком справедливо можна очікувати на масштабні та серйозні гуманітарні наслідки кібератак проти критичної інфраструктури. Стійкості та безпеці таких об'єктів загрожують не тільки кібератаки з боку державних, а й недержавних акторів. Також можна очікувати на терористичні кібератаки, серед пріоритетних об'єктів яких виділяють об'єкти атомної енергетики, залізничну та авіаінфраструктури, системи

водопостачання, небезпечні біологічні та хімічні об'єкти. Відтак, держави повинні гарантувати те, що їх кіберінфраструктура не використовується такими акторами для завдання шкоди об'єктам критичної інфраструктури третіх держав.

В.В. Музика висловила думку про те, що всі кібератаки проти об'єктів критичні інфраструктури, за якими стоїть держава, повинні їй атрибутуватись в цілях попередження та стримування росту таких кібератак, незалежно від того, здійснювалися вони державними агентами, під керівництвом або контролем держави чи недержавними акторами, які використовують кіберінфраструктуру держави, що не проявила необхідної обачності. Водночас для вирішення питання з атрибуцією потрібно сформувати єдиний підхід до поняття «критична інфраструктура». Оскільки в міжнародному праві відсутнє конвенційне визначення критичної інфраструктури, критерії ідентифікації об'єктів, що охоплюються цим поняттям, відсутня також ясність щодо того, як потрібно здійснювати атрибуцію кібератак проти об'єктів критичної інфраструктури і розуміння необхідності відходу від децентралізованого процесу атрибуції, що зумовлено природою та особливостями кіберпростору. Все це в сукупності, на думку дисертанта, визначає актуальність даного дисертаційного дослідження.

Дисертантка також зазначила, що починаючи з 2007 року, держави йдуть альтернативним шляхом, і замість юридичної атрибуції, яка є одним із елементів міжнародно-протиправного діяння, здійснюють публічну (політичну) атрибуцію, яка лише в незначній мірі стримувала зростання кібератак, допоки вони не стали більш складними та «вишуканими». Атрибуція поведінки державі в цілому створює ряд складнощів, особливо коли держава використовує проксі. В кіберконтексті атрибуція кібератак іноді ускладняється відсутністю у постраждалої держави можливості та ресурсів самостійно здійснити коректну атрибуцію, а також розуміння того як звичаєві норми щодо атрибуції застосовуються в кіберконтексті та чи існуюче міжнародно-правове регулювання є достатнім для атрибуції.

Наявні дослідження у міжнародній та національній доктрині здебільшого стосуються питань атрибуції кібератак в загальному та практики їх публічної атрибуції. Проте, відсутність комплексного дослідження, яке б аналізувало підходи держав до розуміння того, як існуючі норми міжнародного право застосовується до кібератак проти об'єктів критичної інфраструктури і як такі атаки повинні атрибутуватися, а також виробленої позиції щодо поняття критична інфраструктура та можливих шляхів вирішення проблемних аспектів, пов'язаних з атрибуцією, зумовлює потребу дослідження обраної тема. Нарешті, кібератаки проти систем електроенергосистем України у 2015 та 2016 роках в контексті збройного конфлікту на Сході України актуалізують необхідність здійснення дослідження атрибуції кібератак для захисту інтересів України в юридичній площині.

Що стосується основних висновків, то здобувачем зазначено, що для здійснення атрибуції кібератак потрібно чітко розмежовувати дії, які порушують міжнародно-правові зобов'язання від тих, які не призводять до порушень. Оскільки щодо

кіберпростору відсутнє *lex specialis*, існує необхідність у встановленні того, як існуючі міжнародні зобов'язання повинні тлумачитись та застосовуватись до конкретних кібероперацій. Принципова позиція автора полягає в переконаності, що державам не вдасться прийняти юридично обов'язковий документ щодо застосування міжнародного права в кіберпросторі за прикладом Талліннських керівництв. З урахуванням того, що технології постійно розвиваються, навіть у випадку розробки тексту такого інструменту, існує досить високий ризик того, що він стане чимось більше, ніж проект статей. Звичаєві норми, навпаки, знаходяться в процесі формування. Ряд держав вже висловили позиції щодо інтерпретації та застосування існуючих норм міжнародного права в кіберпросторі. Відтак, було проаналізовано *opinio juris*, що, як правило, може компенсувати недостатньо розвинену або непослідовну практику держав щодо формування міжнародних звичаїв. Аналіз заяв, декларацій та воєнних доктрин дозволяє встановити «межі» відповідальної поведінки в кіберпросторі, розуміння того, якими держави бачать існуючі зобов'язання та що вкладають в їх зміст. Це дозволило визначити які міжнародно-протиправні діяння розглядаються в якості кібератак та можуть атрибутуватись державі.

В роботі представлено висновки щодо необхідності здійснення технічної та політичної атрибуції, які є передумовами встановлення юридичної атрибуції як елементу міжнародно-протиправного діяння. Обґрунтовано важливість здійснення централізованої та децентралізованої атрибуції для уникнення помилкових висновків, які здійснювалися б паралельно або у тісній співпраці в межах спеціалізованого органу.

В роботі також обґрунтовано потребу розробки та прийняття юридично обов'язкового міжнародного інструменту, який би безпосередньо стосувався атрибуції кібератак проти об'єктів критичної інфраструктури, включав би відповідні поняття та встановлював права та зобов'язання у випадку того, коли кібернетичні атаки кваліфікуються як «застосування сили» чи «збройна атака». Разом з тим, вважається за доцільне, щоб в рамках режиму, створеного даним інструментом, передбачалось функціонування міжнародного органу із здійснення атрибуції, який включав би державних та недержавних суб'єктів.

Вперше проведено комплексний аналіз кібератак проти систем енергопостачання України у 2015 та 2016 роках в контексті збройного конфлікту на Сході України, що підкреслює необхідність оцінки як технічних, так і політичних індикаторів при атрибуції кібератак, особливо в контексті збройного конфлікту. Дослідження кібератак 2015 та 2016 років проти України ілюструє їх небезпеку для об'єктів критичної інфраструктури та демонструє важливість вивчення загального контексту, в якому були здійснені кібератаки, керуючись висновками міжнародних місій, які здійснюють моніторинг за збройними діями.

У дисертації сформульовані й інші теоретично обґрунтовані висновки та положення щодо атрибуції кібератак проти об'єктів критичної інфраструктури.

Структура та обсяг дисертації зумовлені метою і логікою дослідження та складаються з анотації державною та англійською мовами, вступу, трьох розділів, що містять 10 підрозділів, висновків та списку використаних джерел.

По закінченню доповіді Музики В.В. присутніми були поставлені наступні **запитання:**

К.ю.н., доцент Мануїлова К.В.:

У формулюванні теми, розділів (підрозділів) Ви використовуєте концепцію атрибуція. Мова про атрибуцію поведінки державі в розумінні Статей про відповідальність держав 2001 року?

В. В. Музика відповіла:

Так, дане поняття в назві теми, розділів та підрозділів я використовую в класичному розумінні Статей про відповідальність держав 2001 року, які містять звичаєві норми щодо атрибуції поведінки держави. Водночас з урахуванням того, що в *opinio juris* держав щодо атрибуції кібератак державі робиться акцент на врахуванні технічних та політичних індикаторів, поряд з юридичною атрибуцією кібератак я згадую технічну та юридичну, намагаючись зберігати розуміння щодо їх відмінності та потребі в інтегральному підході до них.

К.ю.н., доцент Бєлогубова О.О. :

Якою є офіційна позиція спеціалізованих органів/установ щодо врахування технічних та політичних індикаторів при здійсненні атрибуції кібератак?

В. В. Музика відповіла:

Досліджуючи доповіді Групи урядових експертів 2010, 2013, 2015 років, варто визнати, що вона всіляко уникали деталізації практичних аспектів атрибуції. Водночас параграф 24 Доповіді Групи урядових експертів, що увійшов в Резолюцію Генеральної Асамблеї ООН від 14 липня 2021 року, свідчить про визнання необхідності врахування технічних та політичних індикаторів при зловмисному використанні ІКТ. Так, наприклад, там наголошувалося, що постраждала держава повинна враховувати всі аспекти при оцінці інциденту, а саме: аспекти, підкріплені фактами, які можуть включати технічні характеристики інциденту; сферу охоплення, масштаби та вплив; більш широкий контекст, включаючи вплив інциденту на міжнародний мир і безпеку; і результати консультацій між зацікавленими державами.

Д.ю.н., професор Бехруз Х.Н.:

Як щодо міжнародних експертів Талліннського керівництва, яке містить норми щодо застосування міжнародного права до кібероперацій. Чи розглядається в ньому питання атрибуції кібератак і які фактори, на думку експертів, повинні чи можуть враховуватися під час атрибуції?

В. В. Музика відповіла:

На мою думку, Талліннське керівництво частково сприяло утвердженню ідеї необхідності здійснювати технічну та політичну атрибуцію. В коментарях до норм Керівництва 2017 року експерти зазначають, що часто атрибуція здійснюється в

різних контекстах та ситуаціях. Зокрема, в контексті односторонніх заходів самодопомоги реальність така, що держави повинні здійснити *ex ante* атрибуцію кібероперації іншій державі, перед тим як відреагувати. Хоча такі рішення можуть підлягати розгляду *post factum* із застосуванням стандартів, встановлених судовим або іншим органом, на практиці держава може зіткнутися з ситуацією, на яку їй, можливо, доведеться реагувати в надзвичайно короткий період часу, не звертаючись до повного спектру інформації, яка може бути доступна в поза межами кіберконтексту.

Стосовно *ex ante* атрибуції кібероперацій, Міжнародна група експертів погодилася, що, як правило, держави повинні діяти так, як діяли б розумні держави («*reasonable states*») в тих самих або подібних обставинах, при потребі реагувати на них. Розумність завжди залежить від контексту. І визначається такими факторами, як, серед іншого, надійність, кількість, безпосередність, характер (наприклад, технічні дані, людський інтелект) і специфічність відповідної доступної інформації, якщо розглядати її у світлі супутніх обставин і важливості права, що підлягає застосуванню. На думку експертів, ці фактори необхідно розглядати в їх сукупності.

Д.ю.н., професор Сурілова О.О.:

В роботі Ви виділяєте об'єкти критичної інфраструктури національного значення, чи розглядали Ви можливість визначення міжнародних об'єктів критичної інфраструктури та атрибуцію кібератак проти них?

В. В. Музика відповіла:

Так, в своїй роботі я згадую об'єкти інфраструктури, що обслуговують декілька держав, зокрема технічну інфраструктуру, необхідну для забезпечення загальнодоступності та надійності Інтернету. Адже така інфраструктура може мати вирішальне значення для міжнародної торгівлі, фінансових ринків, глобального транспорту, зв'язку, охорони здоров'я чи гуманітарної діяльності. Відтак, в дисертаційному дослідженні я не обмежуюсь об'єктами критичної інфраструктури, що знаходяться в межах юрисдикції держави та мають національне значення.

К.ю.н., доцент Чайковський Ю.В. :

В свої роботі Ви згадували про те, що кібератаки можуть призвести до різних наслідків. У зв'язку з цим виникає питання – чи впливають наслідки кібератак на рішення держави щодо їх атрибуції? Якщо так, то як саме?

В. В. Музика відповіла:

Проаналізувавши практику держав, я з впевненістю можу відповісти позитивно на це питання. Так, наприклад, коли зловмисникам не вдається реалізувати весь деструктивний потенціал кібератак і певні кібератаки мають незначний, майже невідчутній ефект – держави утримуються від атрибуції кібератак. В першу чергу, від ідеї юридичної атрибуції, а іноді – і від публічної атрибуції.

Якщо ж все-таки наслідки кібератаки відчутні, мають регіональний чи глобальний масштаб, як це було у випадку з кібератакою «NotPetya», держави одразу здійснюють технічну та публічну атрибуцію. При цьому, така атрибуція має

наростаючий колективний характер. До юридичної атрибуції наразі держави не вдавались, але все ж відмінності в реагуванні можна виділити при різних наслідках кібератак.

К.ю.н., доцент Рябошапченко А.О.:

Можливо тоді взагалі не потрібно здійснювати атрибуцію кібератак, які не мали серйозних наслідків?

В. В. Музика відповіла:

Це може видатися привабливим рішенням, особливо в розрізі часто обмежених людських та фінансових ресурсів, що необхідні для атрибуції кібератак. Проте, я вважаю, що таке рішення не є правильним.

Згідно з Талліннським керівництвом, кібератака – це завжди кібероперація, наступальна або оборонна, що цілком очікувано може призвести до завдання трав чи смерті особам або шкоди чи знищення об'єктів. Відтак, толерувати такі кібератаки та сприймати їх як «незначну девіацію» чи «сучасну норму» не потрібно. Водночас, якщо така кібератака мала на меті завдання незначної шкоди об'єктам комп'ютерної системи і в силу своєї природи потенційно не могла призвести до знищення (повного чи часткового) або завдання серйозної шкоди людям, то я погоджусь з тим, що атрибуція може здійснюватися на національному, а не міжнародному рівні.

Д.ю.н., професор Бабін Б.В.:

Скажіть, будь ласка, ким саме має бути врегульовано питання атрибуції кібератак. Чи розглядаєте Ви роль таких організацій як Міжнародний союз електрозв'язку, ІКАО тощо?

В. В. Музика відповіла:

Ідея атрибуції кібератак спеціалізованими установами, які мають технічних експертів, що можуть оцінити втручання і його потенційні наслідки в об'єкт критичної інфраструктури, в цілому, може мати місце. Але в силу різних національних пріоритетів держав і підходів до категоризації об'єктів як критично важливих – ми справедливо можемо зазначати, що на міжнародному чи регіональному рівні відсутні спеціалізовані установи, які б могли охопити всі потенційно можливі об'єкти критичної інфраструктури. Водночас я вважаю, що після загального визнання норм відповідальної поведінки в кіберпросторі, що вироблені в рамках першого комітету Генеральної Асамблеї ООН, має слідувати створення автономного спеціалізованого механізму щодо атрибуції кібератак та можливо навіть інших зловмисних ІКТ-інцидентів.

К.ю.н., доцент Грушко М.В.:

Щодо об'єктів критичної інфраструктури, хто має визначати які саме об'єкти входять в це поняття? І чи пропонуєте Ви власне визначення об'єктів критичної інфраструктури?

В. В. Музика відповіла:

Слідуючи позиції Групи урядових експертів від 2021 року, кожна держава самостійно визначає, які об'єкти інфраструктури або сектори, що знаходяться в

межах її юрисдикції, можна категоризувати як критично важливі. При цьому, таке рішення має прийматися відповідно до національних пріоритетів і методів визначення об'єктів критично важливої інфраструктури.

Одразу зазначу своє частково негативне відношення до такого підходу, який може призвести до того, що майже всі наявні об'єкти в межах своєї юрисдикції держава буде відносити до об'єктів критичної інфраструктури. Показовим в цьому плані є приклад США. Наразі в США визначено 16 секторів критичної інфраструктури, серед яких, сектор комерційних об'єктів – об'єкти, які приваблюють натовпи людей для здійснення покупок, ведення бізнесу, розваг чи проживання. Визначені також конкретні об'єкти в межах цього підсектору – конференц-центри, мотелі, казино зоопарки тощо. Попри загальну важливість цих об'єктів, я не можу погодитися з тим, що вони є критично важливими об'єктами інфраструктуру. Тому я пропоную власний підхід до поняття «об'єкти критичної інфраструктури»

Доктор філософії в галузі права, доцент Войтович П. П.:

Чи розглядаєте Ви за можливе обмежити перелік таких об'єктів, створивши певним чином закритий і вичерпний перелік об'єктів критичної інфраструктури?

В. В. Музика відповіла:

Насправді, в своїй роботі я пропоную зберігати досить гнучний підхід, який би дозволяв оцінювати спрямованість таких об'єктів на забезпечення життєво важливих функцій, послуг та діяльності суспільства. Щодо створення вичерпного списку – вважаю, що це не є ні необхідним, ні можливим. Все-таки держави досить різні, а також різні їх можливості – відтак, пріоритети. Я погоджуюсь з висновком Групи урядових експертів, що загалом саме держави мають здійснювати категоризацію об'єктів в якості об'єктів критичної інфраструктури. Але має бути певне обмеження від надмірно інклюзивного підходу держав, а значить – від потенційно можливих зловживань з їх боку.

К.ю.н., доцент Цибульська О.Ю:

В першому розділі Ви значну увагу приділяєте аналізу *opinio juris* держав щодо застосування міжнародного права до кібероперацій, зокрема до кібератак? Можете пояснити необхідність такого аналізу.

В. В. Музика відповіла:

Так, звичайно. По-перше, відзначу, що це робиться з ціллю встановити як держави бачать процес здійснення атрибуції кібератак. Для досягнення мети роботи мені було важливо встановити, чи вважають держави за необхідне здійснювати технічну, політичну та юридичну атрибуцію, і також їх позицію щодо інтерпретації та застосування норм щодо відповідальності держав за міжнародно-протиправні діяння до кібератак.

По-друге, існувала необхідність встановити, яку саме поведінку (дії та бездіяльність) в кіберпросторі вони розглядають в якості протиправної та такої, що вимагає атрибуції. І взагалі, чи застосовується міжнародне право, на їх думку в кіберпросторі, і якщо так, то в якій мірі.

Д.ю.н., професор О. І. Харітонова:

Чому Ви використовуєте саме категорію *opinio juris* замість вказівки на те, що мова про позиції держав, виражені в їх заявах, деклараціях?

В. В. Музика відповіла:

Такий вибір не є випадковим. Використанням категорії «*opinio juris*» я хочу вже в самій назві підрозділу підвести до своєї позиції щодо формування звичаєвих норм в даній сфері. Вважається, що, будучи одним із конститутивних елементів звичаю, *opinio juris* може компенсувати недостатньо розвинуту або непослідовну практику держав щодо формування міжнародних звичаїв. Звісно заяви, декларації та воєнні доктрини мають орієнтуючий, а не визначальний характер, але на стадії формування норм, що діють в кіберпросторі, аналіз *opinio juris* дозволяє встановити «межі» відповідальної поведінки в кіберпросторі, розуміння того, якими держави бачать існуючі зобов'язання та що вкладають в їх зміст.

В найближчому майбутньому прийняття міжнародного юридично обов'язкового інструменту щодо застосування міжнародного права в кіберпросторі є маловірогідним. Тому в свої роботі я більше схиляюсь до формування звичаєвих норм щодо атрибуції міжнародно-противних діянь (зокрема кібератак) в кіберпросторі, які матимуть характер *lex specialis* по відношенню до загальних норм атрибуції поведінки державі, що містяться в Статтях про відповідальність держав 2001 року.

Після відповідей на запитання було озвучено висновок наукового керівника – **доктора юридичних наук, професора, завідувача кафедри міжнародного та європейського права Національного університету «Одеська юридична академія» - Бігняка Олександра Валентиновича**.

1. Оцінка роботи здобувача у процесі підготовки дисертації.

У процесі підготовки дисертації В.В. Музика виконала індивідуальний план наукової роботи та індивідуальний навчальний план у повному обсязі. Всі заплановані види робіт були виконані своєчасно. Здобувач плідно співпрацював з науковим керівником протягом усього терміну навчання в аспірантурі Національного університету «Одеська юридична академія».

2. Актуальність теми дисертаційного дослідження.

Здійснені кібернетичні атаки демонструють, що пріоритетними об'єктами кібератак є об'єкти атомної енергетики, системи управління електропостачанням, авіа- та залізничним транспортом, потужні сховища стратегічних видів сировини, системи водопостачання, хімічні й біологічні об'єкти, тобто об'єкти критичної інфраструктури держави. В силу того, що такі об'єкти забезпечують нормальне функціонування держави та суспільства, актуальним є встановлення основних проблем атрибуції кібернетичних атак та шляхів їх вирішення.

Необхідність здійснення атрибуції кібератак викликана і тим фактом, що кіберпростір разом з іншими фізичними просторами уже визнано одним з можливих театрів воєнних дій. Спроможність держави захищати національні інтереси в

кіберпросторі розглядається як важлива складова кібербезпеки, але важливо не лише забезпечувати захист та стійкість критичної інфраструктури від кібератак, а й атрибутувати такі кібератаки державним та недержавним акторам для формування культури відповідальної поведінки в кіберпросторі, а, отже, стримування росту кібератак проти таких об'єктів.

Особливої актуальності дослідженню надає той факт, що критична інфраструктура України неодноразово ставала жертвою кібератак, але на їх на загальному фоні виділяються ті, що були здійснені в контексті збройного конфлікту на Сході України та мали руйнівний потенціал, враховуючи те, що могли призвести до серйозних гуманітарних наслідків.

З урахуванням розвитку технологій штучного інтелекту в найближчі 5-10 років масштаби та наслідки таких втручань, імовірно, зростатимуть. Отже, потреба в атрибуції кібератак проти критичної інфраструктури не викликає сумнівів та вимагає вироблення підходів до вирішення основних проблем, що до сьогодні зупиняють держави атрибутувати такі кібератаки та притягнути державу до відповідальності на міжнародному рівні.

3. Зв'язок роботи з науковими програми, темами, планами.

Дисертаційне дослідження здійснювалося в рамках науково-дослідної програми кафедри міжнародного та європейського права Національного університету «Одеська юридична академія» на 2016-2020 роки за темою «Міжнародне право в період трансформації міжнародного правопорядку та захист національних інтересів України» як складова загальної теми науково-дослідної роботи НУ «ОЮА» «Стратегія інтеграційного розвитку України: правовий та культурний вимір» ДРН 0116U001842.

4. Наукова новизна отриманих результатів.

Наукова новизна одержаних результатів дослідження полягає в тому, що вперше в українській правовій науці здійснено цілісне дослідження процесу атрибуції кібератак проти об'єктів критичної інфраструктури держави, а саме:

– здійснено детальний аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі, визначено спільне та відмінне у існуючих підходах та баченні перспектив міжнародно-правового регулювання кібернетичних атак;

– встановлено зміст поняття «критична інфраструктура», окреслено сектори (сукупність об'єктів критичної інфраструктури), які, на думку, більшості держав входять в поняття «критична інфраструктура»;

– обґрунтовано необхідність прийняття поняття, яке включало б рівні критичності та дозволяло зберігати гнучкість при оцінці того, чи конкретний об'єкт може підпадати під поняття критичного;

– здійснено атрибуції кібератак проти системи електроенергетики України в контексті збройного конфлікту на Донбасі, з урахуванням не тільки технічних індикаторів, які оцінювались державними та недержавними акторами, а й політичних

індикаторів (оцінка мотивації, стратегічних інтересів, технічних показників, рівня близькості між державними та недержавними акторами, а також географічної локації);

– комплексно досліджено атрибуцію, яка у випадку з кібератаками вимагає здійснення технічної, політичної та юридичної атрибуції як нероздільної тріади при встановленні відповідальності держави;

– подальшого розвитку набули ідеї щодо створення спеціального механізму, який би здійснював технічну атрибуцію кібератак з метою уникнення помилкової атрибуції внаслідок спуфінгу та вирішення проблеми обмежених людських та технічних ресурсів постраждалих держав;

– обґрунтовано необхідність співпраці між державою та приватними суб'єктами для обміну інформацію щодо існуючих вразливостей та кращих практик технічної атрибуції кібератак;

– теоретично обґрунтовано потребу розробки та прийняття юридично обов'язкового міжнародного інструменту, який би безпосередньо стосувався атрибуції кібератак проти об'єктів критичної інфраструктури та включав відповідні поняття та встановлював права та зобов'язання у випадку того, коли кібернетичні атаки кваліфікуються як «застосування сили» чи «збройна атака».

5. Наукове та практичне значення дослідження.

Практичне значення одержаних результатів полягає у тому, що сформовані в дисертації висновки та пропозиції можуть бути використані у: 1) науково-дослідній сфері – з метою подальшого розвитку доктринальних досліджень, що пов'язанні з питаннями відповідальності держав за міжнародно-протиправні діяння, пов'язані із застосуванням кіберпростору, а також питань атрибуції кібератак проти об'єктів критичної інфраструктури держав; 2) нормотворчій діяльності – в процесі підготовки та удосконалення законодавчих та підзаконних актів, що стосуються захисту та стійкості критичної інфраструктури від кібернетичних атак; 3) правозастосовчій діяльності – для забезпечення єдиного підходу до застосування міжнародних звичаєвих норм про атрибуцію міжнародно-правових діянь до кібератак проти об'єктів критичної інфраструктури; 4) науково-методичній роботі – при підготовці навчальних посібників та підручників з міжнародного права, при читанні курсів міжнародного права, розробці спецкурсів, що пов'язані з питаннями відповідальності держав та забезпеченні кіберстійкості критичної інфраструктури в контексті міжнародної безпеки; 5) начальному процесі – для вивчення дисциплін «Міжнародне право», «Міжнародне право відповідальності держав», «Міжнародне гуманітарне право», «Міжнародне право безпеки»; 6) правовиховній – для підвищення рівня правової культури населення, формування правосвідомості студентів правничих закладів вищих закладів та факультетів.

6. Повнота викладення матеріалу дисертації в наукових публікаціях.

Основні результати дисертації висвітлено у 11 публікаціях, серед яких: 4 наукові статті у фахових виданнях (з них три видання вітчизняні і одне іноземне), 1

колективній монографії (розділ) та 6 збірниках матеріалів всеукраїнських/міжнародних науково-практичних конференцій. Аналіз наукових робіт здобувача, що вказані у списку опублікованих праць за темою дисертації, дає можливість стверджувати, що опубліковані роботи повною мірою відображають основні положення та висновки дослідження.

7. Ступінь обґрунтованості наукових положень.

Обґрунтованість наукових положень, висновків і рекомендацій забезпечується логікою подання матеріалу дисертаційної роботи, послідовністю розв'язання поставлених завдань, репрезантативністю джерельної бази та широкою апробацією результатів, висновками та пропозиціями, які представлені в розділах дисертаційного дослідження, загальних висновках дисертації.

Достовірність отриманих висновків підтверджено використанням теоретичних та емпіричних методів, тривалістю дослідно-експериментальної роботи, а також актуальних іноземних та вітчизняних джерел.

8. Структура та зміст дисертації, її завершеність та відповідність установленим вимогам щодо оформлення.

Структурні компоненти дослідження, а саме: анотації, вступ, 3 розділи, 10 підрозділів, висновки до розділів, загальні висновки, список використаних джерел, – пов'язані внутрішньою логікою і послідовністю викладу. Робота відзначається також логічністю викладу, чіткістю аргументації. Аналіз наукового апарату засвідчив відповідність вимогам кваліфікаційного наукового дослідження.

У вступі обґрунтовано актуальність дослідження на основі аналізу нормативних документів та визначених суперечностей, коректно визначено мету, об'єкт, предмет, завдання дослідження; вказано на зв'язок роботи з науковими програмами, планами, темами, представлено інформацію про результати наукового пошуку та відомості щодо його апробації; обсяг і структуру дослідження; охарактеризовано новизну, теоретичне і практичне значення дослідження.

В першому розділі здобувачем встановлено, що собою представляють кібератаки та що розглядається в якості об'єкта кібератаки, здійснено розмежування із суміжними поняттями: «кібернетичні операції», «кіберексплуатаці», «збройний напад», «використання сили». Проаналізовано *opinio juris*, що дозволило визначити які міжнародно-протиправні діяння розглядаються в якості кібератак та можуть атрибутуватись.

В другому розділі досліджено становлення та процес модифікації поняття «критична інфраструктура» в національному законодавстві держав. Обґрунтовано необхідність прийняття на міжнародному рівні поняття, яке дозволило б зберігати гнучкість, враховуючи різноманітність держав. Визначено, що процес атрибуції охоплює здійснення технічної, політично (публічної) та юридичної атрибуції, що фактично визначає особливість здійснення атрибуції міжнародно-протиправних діянь (кібератак) в кіберпросторі.

В цьому розділі також розкрито особливість застосування правил атрибуції в кіберпросторі і здійснено комплексний аналіз кібератак проти систем енергопостачання України у 2015 та 2016 роках в контексті збройного конфлікту на Сході України.

В третьому розділі досліджено існуючі та потенційно можливі шляхи вирішення проблем, пов'язаних з атрибуцією кібератак проти об'єктів критичної інфраструктури, зокрема можливості інституційної співпраці держави та приватних компаній ІТ-компаній чи компаній, що займаються питаннями кібербезпеки, а також досліджено перспективи розгляду міждержавного спору за результатами якого можна заповнити існуючі прогалини. Досліджено особливості кібердипломатії ЄС та практику атрибуції кібератак цим наднаціональним інтеграційним об'єднанням.

Логічним завершенням дослідження є обґрунтовані відповідно до завдань загальні висновки.

Список використаних джерел вміщує перелік опрацьованої літератури.

Дисертація оформлена згідно з чинними вимогами.

9. Загальний висновок.

Дисертаційне дослідження Музики Вікторії Василівни «Атрибуція кібератак проти об'єктів критичної інфраструктури держави: визначення основних проблем та шляхів їх вирішення» на здобуття ступеня доктора філософії з галузі знань 08 «Право», за спеціальністю 081 «Право» за актуальністю, науково-теоретичним рівнем, новизною постановки та розв'язанням проблем, практичним значенням відповідає вимогам Постанови КМА від 24 липня 2013 р. № 567 «Порядок присудження наукових ступенів», та Постанови КМА від 6 березня 2019 р. № 167 «Про присудження ступеня доктора філософії».

В обговоренні дисертаційного дослідження взяли участь:

К.ю.н., доцент О. К. Канєнберг-Сандул відмітила, що робота є ґрунтовним науковим дослідженням, яке має значну актуальність, містить ґрунтовно розкриті питання, правильні, логічні та значимі висновки. Зазначила, що дисертація В.В. Музики на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення» може бути рекомендована до захисту у разовій спеціалізованій вченій раді.

К.ю.н., доцент Р. Ф. Харитонов відмітил високий науковий рівень дослідження, його актуальність та повноту зроблених висновків. Визначив дискусійні моменти, зокрема щодо необхідності створення спеціального міжнародного механізму щодо атрибуції кібератак. Проте зазначив, що ці зауваження не впливають на високу оцінку дослідження. Нарешті, вказав, що дисертація В.В. Музики на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення» може бути рекомендована до захисту у разовій спеціалізованій вченій раді.

К.ю.н., доцент О. О. Бєлогубова у своєму виступі підтримала попередніх доповідачів, акцентувала увагу на глибокому змісті авторських визначень і висновків. Відзначила, що дисертаційне дослідження є теоретично і практично значущим. Підкреслила, що в процесі доповіді головних положень дисертаційного дослідження, а також під час відповідей на запитання членів кафедри міжнародного та європейського права Національного університету «Одеська юридична академія», В.В. Музика продемонструвала опрацювання значної кількості джерел, на підставі яких була підготовлена дисертаційна робота, вміння узагальнювати, аналізувати, формулювати власні висновки. Відзначила, що дисертація В.В. Музики на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», подана на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 «Право», може бути рекомендована до захисту у разовій спеціалізованій вченій раді.

Д.ю.н., професор Бехруз Х.Н. надав високу оцінку дисертації, кількості та характеру досліджених у ній питань, вдалості і значущості для науки висновків, виваженості пропозицій. Відзначив, що дисертантка здійснила ретельне вивчення питання атрибуції кібератак проти об'єктів критичної інфраструктури. Вказав, що дисертація В.В. Музики на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», подана на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 «Право», може бути рекомендована до захисту у разовій спеціалізованій вченій раді.

Д.ю.н., професор О. І. Харітонова зазначила, наскільки робота зацікавила всіх присутніх. Вказала на те, що такі дисертації є дуже важливими для продовження певного дискурсу, який ми сьогодні спостерігаємо. Ми бачимо, як міжнародне право розширює свою сферу, а дисертаційне дослідження В. В. Музики є прекрасним доказом цьому. Зокрема, про це свідчить аналіз доповідей Групи урядових експертів та Відкритої робочої в рамках першого комітету Генеральної Асамблеї ООН, мандат яких пов'язаний з визначення норм відповідальної поведінки в кіберпросторі. Звичайно, ця робота представляє науковий інтерес з урахуванням того, що В. В. Музика накопичила значний матеріал, який забезпечить активне впровадження дисертаційного дослідження у навчальну та наукову діяльність, і що характеризує роботу як актуальне та затребуване наукове дослідження.

У підсумку, зазначила, що дисертація В. В. Музики на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», подана на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 «Право», може бути рекомендована до захисту у разовій спеціалізованій вченій раді.

Після цього, слово було надано **рецензентам** наукової праці доктору юридичних наук, професору О. О. Суріловій та кандидату юридичних наук, доценту М. В. Грушко:

Д.ю.н., професор О. О. Сурілова відзначила, що звернення В. В. Музики до проблематики атрибуції кібератак проти об'єктів критичної інфраструктури представляє особливий науковий інтерес.

Майже всі аспекти повсякденного життя пов'язані з нормальним функціонуванням об'єктів критичної інфраструктури. За останнє десятиліття кількість кібератак на ці об'єкти збільшилась в рази, як і кількість суб'єктів, що вдаються до таких атак задля досягнення своїх цілей. Ситуація толерування кібератак, без перенесення в юридичну площину, в недалекому майбутньому може призвести до серйозних гуманітарних наслідків, де міста будуть відключені від води чи електроенергії, а економіка – знаходитиметься під серйозною загрозою. Відтак, не тільки добробут населення, але й життєздатність держави як суб'єкта міжнародного права може залежати від спроможності реагувати на кібератаки проти об'єктів критичної інфраструктури. Для того, щоб попередити можливі серйозні наслідки, спричинені кібератаками, і сприяти міжнародному миру та безпеці, важливо утвердити відповідальну поведінку держав в кіберпросторі. Досягнення цієї цілі складно уявити без атрибуції кібератак, що є предметом даного дослідження.

Атрибуція є процесом віднесення певного міжнародно-протиправного діяння до його джерела, яке допомагає встановити, хто саме стоїть за кібератакою. Атрибуція є важливою, оскільки вона визначає технічні, політичні і правові дії держави, об'єкти критичної інфраструктури якої постраждали від кібератаки. При цьому, в кіберконтексті атрибуція часто створює ряд викликів, пов'язаних з проблемою анонімності, можливістю фальсифікації даних, багатоетапним характером кібератак і невибірковістю кіберінструментів. До цього слід додати необхідні людські та технічні ресурси, тривалі часові масштаби та пов'язані з цим вимоги до атрибуції. Атрибуція кібератак державі сприймається з особливим трепетом, оскільки некоректна атрибуція може призвести до серйозних наслідків. Наразі держави дещо змінили свій підхід, продемонструвавши свою здатність публічно атрибутувати кібератаки державам, які за ними стоять. Втім, юридична атрибуція кібератак для притягнення держав до відповідальності жодного разу не застосовувалася. Насамперед це пов'язано з відсутністю ясності щодо того, як повинна здійснюватися атрибуція кібератак, що разом з відсутністю поняття «критична інфраструктура» визначають актуальність даного дослідження. Відтак, звернення В.В. Музики до проблематики атрибуції кібератак проти об'єктів критичної інфраструктури представляє особливий науковий інтерес.

Аналіз тексту дисертаційного дослідження свідчить про дисертабельність обраної теми та наявну наукову новизну. Здобувачка проаналізувала природу кібернетичних атак, позиції держав щодо того, які міжнародно-протиправні діяння повинні атрибутуватися державі і застосування звичаєвих норм щодо атрибуції поведінки державі в кіберконтексті. Також було встановлено основні складнощі, що виникають в ході атрибуції кібератак та запропоновано конкретні шляхи їх подолання.

В роботі містяться оригінальні положення та висновки, що мають елементи наукової новизни та можуть бути винесені на публічну дискусію під час публічного захисту. Зокрема, науковий інтерес привертає обґрунтування ідеї створення міжнародного механізму з мандатом на здійснення атрибуції кібератак. Дисертант аналізує наявні пропозиції, які, зокрема, заперечують залучення представників приватного сектору або державних агентів до роботи цього органу та пояснює переваги їх співпраці в рамках такого органу.

Серед важливих переваг дисертаційного дослідження, які визначають його актуальність для України та новизну, варто зазначити аналіз кібератак 2015 та 2016 років проти об'єктів критичної інфраструктури України (систем електроенергетики). Представлений підрозділ є першим комплексним дослідженням даних кібератак в контексті збройного конфлікту на Сході України. Крім того, підрозділ щодо України цікавий тим, що для цілей атрибуції здобувачка робить посилання на наявні технічні та політичні індикатори, що є важливими при здійсненні технічної та політичної атрибуції.

Теоретичні та практичні аспекти дисертаційного дослідження В.В. Музики, що викладені в роботі, загалом можуть бути використані при читанні таких дисциплін як «Міжнародне право», «Міжнародне гуманітарне право», «Право відповідальності», «Міжнародна безпека» тощо.

Висновки і положення дисертації апробовані в ході ряду всеукраїнських та міжнародних наукових та науково-практичних конференцій, а також висвітлені у вітчизняних та міжнародних фахових журналах і розділі колективної монографії.

Текст дисертації справляє досить позитивне враження та свідчить про високий рівень проведеного дослідження. Водночас, як будь-яка дисертаційна робота, рецензоване дослідження не позбавлене окремих недоліків та дискусійних положень:

1. З методологічної точки зору вкрай актуальним є питання термінології, що використовується. У формулюваннях теми, назв розділів (підрозділів) використовується визначення «атрибуція», хоча в перекладі з російської, яка є офіційною мовою Організації Об'єднаних Націй, доречніше використовувати «присвоєння поведінки державі» замість «атрибуція поведінки державі».

2. Дисертаційне дослідження здобувачки, серед іншого, акцентує увагу на технічних індикаторах та технічній атрибуції, що є категоріями відокремленими від юридичної атрибуції. З урахуванням цього хотілось би зрозуміти позицію автора щодо доцільності розгляду технічних аспектів в контексті правового дослідження. Та чому, на її погляд, технічна атрибуція має здійснюватися? Чи є на міжнародному рівні приклади органів, які наразі здійснюють технічну експертизу/оцінку, і які можуть використовуватися в якості моделі?

3. В Розділі 3 здобувачка розглядає інструменти кібердипломатії, зокрема кіберсанкції Європейського Союзу. На мій погляд, доречним буде розглянути можливість застосування кіберсанкцій в межах ООН задля забезпечення стабільності та безпеки на міжнародному та регіональному рівнях.

4. Дисертант аналізує кібератаки проти українських об'єктів критичної інфраструктури, підкреслюючи, що тривалий час, а саме до 30 липня 2020 року ці кібератаки не отримали належної уваги з боку міжнародної спільноти. У цьому зв'язку, доречно додати про те, чи може Україна перенести дані питання в юридичну площину для атрибуції кібератак Російській Федерації, зокрема в межах наявних чи потенційно можливих судових розглядів в міжнародних інстанціях.

5. В Розділі 3 наявні незначні граматичні та стилістичні помилки. Відтак, роботу потрібно ще раз уважно перечитати і усунути наявні помилки.

Загалом здобувачці вдалося висвітлити основні питання теми і підготувати цілісне наукове дослідження, що відповідає вимогам до дисертаційних досліджень. Зазначені зауваження переважно мають дискусійних характер та не впливають на загальне позитивне враження від роботи в цілому.

К.ю.н., доцент М. В. Грушко зазначила, що робота містить ряд нових наукових результатів і положень, висунутих для публічного захисту. Робота грамотно структурована, має внутрішню єдність, і свідчить про вирішення поставлених дисертанткою завдань. Робота в цілому має наукове значення для теорії і практики міжнародного права.

Підтримання і зміцнення міжнародного правопорядку в значній мірі залежить від встановлення відповідальності за міжнародно-протиправні діяння, одним із елементів якого є атрибуція протиправної поведінки державі. Концепція атрибуції поведінки державі завжди знаходилась в центрі уваги міжнародної спільноти, але наразі зростаюча роль інформаційно-комунікаційних технологій вимагає її переосмислення задля подолання безкарності в кіберпросторі.

Кількість кібератак, середовищем здійснення яких є кіберпростір, значно зросла за останнє десятиліття. Кібератаки стали одним із основних інструментів досягнення геополітичних цілей в кіберпросторі, оскільки при залученні порівняно незначних ресурсів, тривалій анонімності в кіберпросторі і толеруванні кібератак, держави могли вдатися до міжнародно-протиправних діянь без страху бути притягнутими до відповідальності. Серйозним викликом є факт того, що кібератаки використовуються проти об'єктів критично важливої інфраструктури, яка забезпечує нормальне функціонування держави та від якої залежить добробут населення. Саме це зумовлює необхідність подолання основного виклику, пов'язаного з їх атрибуцією, і винесенням даного питання в юридичну площину.

З урахуванням цього, звернення В.В. Музики до проблематики атрибуції кібератак проти об'єктів критичної інфраструктури представляє особливий науковий інтерес.

Текст дисертації свідчить про те, що здійснене дисертаційне дослідження характеризується дисертабельністю обраної теми та науковою новизною. Здобувачкою проаналізовано та встановлено, як держави бачать здійснення атрибуції в силу особливої природи та характеристик кіберпростору, визначено роль технічних та політичних індикаторів при здійсненні атрибуції, а також важливість здійснення

технічної, політичної та юридичної атрибуції кібератак для встановлення держав, відповідальних за такі кібератаки та для подальшого їх притягнення до міжнародно-правової відповідальності.

В роботі містяться оригінальні положення та висновки, що мають елементи наукової новизни та можуть бути винесені на публічну дискусію під час публічного захисту. Зокрема, цікавим є обґрунтування необхідності прийняття поняття «критична інфраструктура», яке б дозволяло зберігати автономність та гнучкість при оцінці того, чи конкретний об'єкт може підпадати під категоризацію як критичний. Крім того, на увагу заслуговують пропозиції щодо створення спеціального правового режиму, в рамках якого б функціонував спеціальний механізм щодо атрибуції кібератак. Ця пропозиція цікава тим, що здобувачка хоче об'єднати зусилля держав та приватного сектору та створити міжнародний механізм, уповноважений на здійснення технічної, політичної та юридичної атрибуції.

В силу наявності збройного конфлікту на території України також важливо, що здобувачка розглянула кібератаки 2015 та 2016 років безпосередньо в контексті подій, що мали місце в ході збройного конфлікту на Сході України, цим самим продемонструвавши взаємодоповнюваність політичних та технічних індикаторів в процесі атрибуції кібератак.

Теоретичні аспекти дисертаційного дослідження, викладені в роботі, можуть бути використані при читанні курсів з міжнародного права, права відповідальності, міжнародного гуманітарного права та права безпеки.

Звертає увагу значна кількість опублікованих здобувачем праць за темою дослідження. Висновки і положення дисертації апробовані на багатьох конференціях, висвітлені в фахових журналах, колективній монографії та іноземному журналі.

Загалом текст дисертації справляє досить позитивне враження та свідчить про високий рівень підготованого дисертаційного дослідження. Водночас, як будь-яка дисертаційна робота, рецензоване дослідження не позбавлене окремих недоліків та дискусійних положень:

1. В Розділі 1 та Розділі 2 здобувачка згадує перспективи розробки та прийняття спеціального міжнародного інструменту. Втім, відношення автора до такого інструменту, як видається, є різним. Якщо мова про два різні інструменти – щодо застосування міжнародного права до кібероперацій і безпосередньо щодо атрибуції кібератак (технічної, політичної та юридичної) – доречним буде уточнити це в тексті і провести більш чітке розмежування.

2. В другому розділі згадується технічна та політична атрибуція кібератак, які не є традиційними для атрибуції міжнародно-правових діянь в межах права відповідальності держав. Автор робить акцент на їх послідовному та інтегральному здійсненні, але виникає питання, чи завжди це необхідно. Зокрема, з урахуванням суверенної волі держав – чи можуть вони обмежитись здійсненням виключно технічної чи політичної атрибуції? І якщо так, то які переваги в здійсненні юридичної атрибуції?

3. Здобувачка загалом досить детально зазначає, які об'єкти мають відноситись до об'єктів критичної інфраструктури, аналізуючи категоризацію таких об'єктів відповідно до національного законодавства держав світу та згадок і прикладів таких об'єктів в доповідях Групи урядових експертів та Відкритої робочої групи від 2021 року. Втім, відкритим залишається питання, чи потрібно такі об'єкти поділяти на об'єкти цивільної та військової критичної інфраструктури (як це часто робить Міжнародний Комітет Червоного Хреста), і яку роль атрибуція відіграватиме в ході збройного конфлікту. Хотілось би, щоб здобувачка розкрила цей аспект в своєму дослідженні.

4. Описуючи можливу співпрацю з приватним сектором, дисертант згадує ряд позитивних прикладів децентралізованої атрибуції кібератак приватним сектором. Втім, містяться згадки про досить неточні звіти, підготовка яких без перевірки наявної інформації свідчить про непрофесіоналізм та відсутність розуміння наслідків у випадку встановлення причетності держави до кібероперацій проти іншої держави. Зокрема, мова про звіт компанії CrowdStrike «Використання шкідливого програмного забезпечення групи «Fancy Bear»для платформи Android з ціллю відстеження української польової артилерії» від 22 грудня 2016 року. На погляд здобувача, чи не потрібно все-таки схилитися до позиції щодо того, що спеціальний механізм атрибуції кібератак, який, як дисертант зазначає, має бути створений для здійснення атрибуції кібератак, не повинен включати представників приватного сектору. Або, в протилежному випадку, їх участь в цьому органі має бути максимально обмеженою з урахуванням відсутності відповідальності.

5. Формальним зауваженням є наявність в роботі незначних граматичних та стилістичних помилок. Роботу потрібно ще раз уважно перечитати.

Водночас, як зазначив рецензент, здобувачці вдалося висвітлити основні питання теми і підготувати цілісну наукову роботу, що відповідає вимогам, які пред'являються до дисертаційних досліджень. Зазначені зауваження переважно мають дискусійних характер та не впливають на загальне позитивне враження від роботи в цілому.

УХВАЛИЛИ:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Музики Вікторії Василівни «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення».

2. Констатувати, що за актуальністю, ступенем новизни, обґрунтуванням, науковою та практичною цінністю здобутих результатів дисертація В. В. Музики відповідає спеціальності 081«Право» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами і доповненнями від 03 березня 2019 року № 283),

п. 10 Тимчасового порядку присудження ступеня доктора філософії затвердженого постановлю Кабінету міністрів України від 06 березня 2019 р. № 167.

3. Рекомендувати дисертацію В. В. Музики на тему «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення» до захисту на здобуття ступеня доктора філософії у разовій вченій раді за спеціальністю 081 «Право».

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення дисертації Музики Вікторії Василівни на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», поданої на здобуття ступеня доктора філософії за спеціальністю 081 «Право»

Обґрунтування вибору теми дослідження. Об'єкти критичної інфраструктури та їх захист знаходяться в повістці багатьох держав світу з початку двадцять першого століття. Теракти 11 вересня 2001 року в Сполучених Штатах Америки та теракти 2004 і 2005 років на території країн-членів Європейського Союзу стали тим індикатором, який підкреслив важливість критичної інфраструктури, від нормального функціонування якої залежить безпека та добробут держави і людей. Але якщо атаки на об'єкти критичної інфраструктури на початку 2000-х років були «іграшкою страху» в руках недержавних акторів, то виникнення кіберпростору, а з ним і кібератак, відкрило нові можливості для держав, а саме – переслідування своїх геополітичних інтересів шляхом використання кібератак з руйнівним потенціалом.

Кібератаки на американську греблю у 2013 році, німецький металургійний комбінат у 2014 році, українські системи електроенергетики у 2015 та 2016 роках, Національну службу охорони здоров'я у Великобританії у 2017 році, системи приладів безпеки Саудівської Аравії в 2017 році, постачальника електроенергії в Південній Африці, індійський атомний завод у 2019 році та найбільшу трубопровідну систему США у 2021 році – лише незначний перелік кібератак проти об'єктів критичної інфраструктури. І, як видається, це лише початок. Тривале толерування та сприйняття більшості кібератак в якості нового «нормально», що є наслідком відсутності необхідної атрибуції кібератак для цілей притягнення держав до відповідальності, лише сприяли їх зростанню. Більш того, з урахуванням постійного розвитку штучного інтелекту в недалекому майбутньому цілком справедливо можна очікувати на масштабні та серйозні гуманітарні наслідки кібератак проти критичної інфраструктури. Стійкості та безпеці таких об'єктів загрожують не тільки кібератаки з боку державних, а й недержавних акторів. В найближче десятиліття варто очікувати на терористичні кібератаки, серед пріоритетних об'єктів яких виділяють об'єкти атомної енергетики, залізничну та авіаінфраструктури, системи водопостачання, небезпечні біологічні та хімічні об'єкти. Відтак, держави повинні гарантувати те, що

їх кіберінфраструктура не використовується такими акторами для завдання шкоди об'єктам критичної інфраструктури третіх держав.

Всі кібератаки проти об'єктів критичні інфраструктури, за якими стоїть держава, повинні їй атрибутуватись в цілях попередження та стримування росту таких кібератак, незалежно від того, здійснювалися вони державними агентами, під керівництвом або контролем держави чи недержавними акторами, які використовують кіберінфраструктуру держави, що не проявила необхідної обачності. Водночас для вирішення питання з атрибуцією потрібно сформувати єдиний підхід до поняття «критична інфрастуктура». Наразі в міжнародному праві відсутнє конвенційне визначення критичної інфраструктури, критерії ідентифікації об'єктів, що охоплюються цим поняттям. Відсутня також ясність щодо того, як потрібно здійснювати атрибуцію кібератак проти об'єктів критичної інфраструктури і розуміння необхідності відходу від децентралізованого процесу атрибуції, що зумовлене природою та особливостями кіберпростору. Все це в сукупності визначає актуальність даного дисертаційного дослідження.

Починаючи з 2007 року, держави йдуть альтернативним шляхом, і замість юридичної атрибуції, яка є одним із елементів міжнародно-протиправного діяння, здійснюють публічну (політичну) атрибуцію, яка лише в незначній мірі стримувала зростання кібератак, допоки вони не стали більш складними та «вишуканими». Атрибуція поведінки державі в цілому створює ряд складнощів, особливо коли держава використовує проксі. В кіберконтексті атрибуція кібератак іноді ускладняється відсутністю у постраждалої держави можливості та ресурсів самостійно здійснити коректну атрибуцію, а також розуміння того як звичаєві норми щодо атрибуції застосовуються в кіберконтексті та чи існуюче міжнародно-правове регулювання є достатнім для атрибуції, а, отже, притягнення держави до відповідальності за кібератаки та спричинені ними наслідки.

Наявні дослідження у міжнародній та національній доктрині здебільшого стосуються питань атрибуції кібератак в загальному та практики їх публічної атрибуції. Проте, відсутність комплексного дослідження, яке б аналізувало підходи держав до розуміння того, як існуючі норми міжнародного право застосовується до кібератак проти об'єктів критичної інфраструктури, а також виробленої позиції щодо поняття критична інфраструктура та можливих шляхів вирішення проблемних аспектів, пов'язаних з атрибуцією, зумовлює потребу дослідження обраної тема. Нарешті, кібератаки проти систем електроенергосистем України у 2015 та 2016 роках в контексті збройного конфлікту на Сході України актуалізують необхідність здійснення дослідження атрибуції кібератак для захисту інтересів України в юридичній площині.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано в рамках наукових досліджень Національного університету «Одеська юридична академія» «Стратегія інтеграційного розвитку України: правовий і культурний вимір» на 2016-2020 рр. (державний реєстраційний номер

0116U001842), а також плану науково-дослідницької роботи кафедри міжнародного та європейського права Національного університету «Одеська юридична академія» «Міжнародне право і період трансформації міжнародного правопорядку та захист національних інтересів України» на 2016-2020 рр.

Теоретичну основу дослідження становлять наукові положення, які містяться в роботах таких вчених, як К. Айхенсен, Д. Альперовіч, С.С. Андрейченко, Дж. Буттігідж, Д. Вагнер, Дж. К. Вольтаг, Н. В. Галлагхер, А. Гавріловіч, Л. Гісел, М. В. Грушко, К. В. Дам, Д. Джонсон, Е. Корзак, С. Лін, С. Калтагіроне, Н. Карнієвіч, Д. Кларк, О. Климчук, С. І. Кондратов, Дж. Кроуфорд, А. Кляйнер, Е. Луїджф, К. Мачак, П. Мейер, Г. Навін, Ф. Німанн, В. А. Овенс, Д. Пост, М. Сасолі, Р. Сетола, Б. Сміт, Дж. Ставрідіс, О. О. Сурілова,А. Расселл, Ш. Розен, Т. Роденхойсер, М. Росіні, М. Теохаруду, Н. Томпсон, Р. Хенг, Т. Хітченс, Н. Цагоріас, С. Чарней, Б. Швайцер, М. Шмідт, Р. Шондорф та інших.

Мета і завдання дослідження. Мета дисертації полягає в дослідженні питань атрибуції кібератак проти об'єктів критичної інфраструктури з ціллю встановлення основних проблем, які формують перепони на шляху здійснення юридичної атрибуції. Для досягнення цієї мети, на виконання було поставлено такі завдання:

- визначити природу та сутнісні ознаки кібернетичних атак, а також їх співвідношення з суміжними поняттями, такими як «кібероперації», «кіберексплуатації», «застосування сили», «збройний конфлікт»;
- встановити які норми міжнародного права та як можуть бути порушені в кіберпросторі та, відповідно, вимагають атрибуції в межах права відповідальності держав;
- прослідкувати та проаналізувати *opinio juris* держав щодо ключових питань застосування міжнародного права до кібератак та їх атрибуції;
- визначити, які об'єкти, згідно з позицією держав, входять в поняття «критична інфраструктура», враховуючи відсутність конвенційного поняття «критична інфраструктура»;
- охарактеризувати особливості застосування звичаєвих правил атрибуції міжнародно-протиправних діянь до кібератак;
- встановити відмінності між політичною, технічною та юридичною атрибуціями кібератак, потребою у їх інтегральному здійсненні;
- дослідити питання атрибуції кібернетичних атак у випадку порушення обов'язку необхідної обачності (*due diligence*);
- проаналізувати кібератаки проти об'єктів критичної інфраструктури України в контексті збройного конфлікту на Сході України та практичні аспекти їх атрибуції;
- визначити специфіку атрибуції кібератак в Європейському Союзі, шляхи підвищення стійкості об'єктів критичної інфраструктури шляхом застосування кіберсанкцій;

- оцінити перспективи розгляду міждержавної скарги щодо кібератак проти об'єктів критичної інфраструктури, яка б могла допомогти заповнити прогалини у досліджуваній проблематиці.

Об'єкт дослідження – міжнародні правовідносини, пов'язані зі встановленням відповідальності держав за кібератаки, що представляють міжнародно-протиправне діяння в кіберпросторі.

Предмет дослідження – процес атрибуції кібератак проти об'єктів критичної інфраструктури як один із елементів міжнародно-протиправного діяння.

Методи дослідження. Герменевтичний метод є ключовим при здійсненні дисертаційного дослідження. Цей метод допоміг здійснити інтерпретацію юридичних та технічних текстів для встановлення розуміння та осягнення понять, категорій та процесів, що є центральними при дослідженні проблеми атрибуції кібератак проти об'єктів критичної інфраструктури (підрозділи 1.1., 1.2., 2.1, 2.2., 2.3.). Порівняльно-правовий метод використаний для здійснення компаративних досліджень підходів держав до застосування міжнародного права в кіберпросторі, встановлення розуміння та змісту поняття критична інфраструктура та об'єктів, які, на думку держав, входять в дане поняття (підрозділ 2.1.).

В першому розділі чітко простежується використання аксіологічного, цивілізаційного та антропологічного підходів. Аксіологічний підхід допоміг розкрити цінність атрибуції як одного із елементів міжнародно-протиправного діяння, необхідного для встановлення відповідальності держави, а також цінність існуючих норм міжнародного права, порушення яких в кіберпросторі сприймається членами міжнародної спільноти як такі що потребують подальшої атрибуції для цілей відповідальності держав та встановлення справедливості (підрозділ 1.2, 1.3). Використання цивілізаційного та антропологічного підходів дозволило розглядати процес атрибуції як міжцивілізаційну та загальнолюдську цінність (підрозділ 1.2., 2.2., 2.3., 3.1., 3.2.).

В другому розділі історико-правовий підхід допоміг простежити виникнення та еволюцію такого поняття як критична інфраструктура та нормативного змісту, яким держави наповнюють це поняття (підрозділ 2.1). Цивілізаційний підхід на основі лінійно-стадіальної моделі допоміг підкресли перехід від менш прогресивної до більш прогресивної атрибуції – від атрибуції міжнародно-протиправних діянь, що вчиняються в межах традиційних просторів (кінетичного світу) до атрибуції міжнародно-протиправних діянь, що пов'язанні з віртуальним простором, а саме – кіберпростором (підрозділ 2.2, 2.3.).

Основним підходом, що є наріжним камнем третього розділу є прогностичний метод, який сприяв встановленню перспектив щодо вирішення практичних проблем атрибуції кібератак (підрозділи 3.1., 3.2., 3.3.).

Наукова новизна одержаних результатів. Дисертація є першим дослідженням комплексного характеру, що розкриває практичні аспекти процесу атрибуції

кібернетичних атак проти об'єктів критичної інфраструктури, окреслює основні проблеми та шляхи їх вирішення. У дисертації виконано наступне:

вперше

комплексно досліджено атрибуцію кібератак, яка загалом вимагає здійснення технічної, політичної та юридичної атрибуції як нероздільної тріади при встановленні відповідальності держави за міжнародно-протиправні діяння держав в кіберпросторі;

здійснено аналіз opinio juris держав щодо застосування міжнародного права в кіберпросторі, визначено спільне та відмінне у існуючих підходах та бачення перспектив міжнародно-правового регулювання кібернетичних атак та їх атрибуції;

встановлено зміст поняття «критична інфраструктура» і визначено сектори (сукупність об'єктів критичної інфраструктури), які, на думку, більшості держав входять в дане поняття;

запропоновано виділити об'єкти критичної інфраструктури, які використовуються спільно декількома державами в окрему категорію – транснаціональні (міждержавні) об'єкти критичної інфраструктури в силу спільного інтересу держав в забезпеченні їх кіберстійкості та залежності від їх функціонування;

здійснено атрибуцію 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;

встановлено перспективи подолання практичних проблем атрибуції кібератак на прикладі інтегральної моделі взаємодії в Європейському Союзі: державно-приватної співпраці та застосування інструментарію кібердипломатії на універсальному рівні;

проаналізовано перспективи розгляду міждержавного спору щодо відповідальності за кібератаки проти об'єктів критичної інфраструктури держави як варіант подолання проблем атрибуції на практиці.

удосконалено:

розуміння застосування звичаєвих норм атрибуції до кібератак, що здійснюються проти об'єктів критичної інфраструктури держави;

ідеї розвитку здійснення централізованої та децентралізованої атрибуції кібернетичних кібератак проти об'єктів критичної інфраструктури з урахуванням наявних політичних та технічних індикаторів;

наукові ідеї щодо створення спеціального механізму, який би здійснював технічну та політичну атрибуцію кібератак з метою уникнення помилкової атрибуції та вирішення проблеми обмежених людських та технічних ресурсів постраждалих держав;

розуміння процесу політичної атрибуції кібератак, яке ґрунтується на оцінці мотивації, стратегічних інтересів, технічних показників, рівня близькості між державними та недержавними акторами, географічної локації та інших важливих індикаторів.

набули подальшого розвитку:

положення щодо атрибуції кібератак, об'єктом яких є критична інфраструктура держави;

наукові ідеї щодо застосування міжнародного права до кібератак, зокрема звичаєвих норм атрибуції поведінки державі, що містяться в Статтях про відповідальність держав за міжнародно-протиправні діяння 2001 року;

ідеї перенесення обов'язку проявляти необхідну турботу (due diligence), який не є стандартом для атрибуції поведінки державі, з основних до похідних норм відповідальності держав, враховуючи важливість атрибуції кібератак проти об'єктів критичної інфраструктури

обґрунтування необхідності врахування технічних та політичних індикаторів при здійсненні атрибуції кібератак, що часто є взамокомпенсуючими та у своїй сукупності дозволяють звести до мінімуму помилку у встановленні джерела кібератаки;

необхідність співпраці між державою та приватним сектором для обміну інформацією щодо існуючих вразливостей та кращих практик технічної атрибуції кібератак;

теоретично обґрунтовано потребу розробки та прийняття юридично обов'язкового міжнародного інструменту, який безпосередньо би стосувався атрибуції кібератак проти об'єктів критичної інфраструктури, включав відповідні поняття та встановлював права та зобов'язання у випадку того, коли кібернетичні атаки кваліфікуються як «застосування сили» чи «збройна атака».

Практичне значення одержаних результатів полягає у тому, що сформовані в дисертації висновки та пропозиції можуть бути використані у:

науково-дослідній сфері – з метою подальшого розвитку доктринальних досліджень, що пов'язанні з питаннями відповідальності держав за міжнародно-протиправні діяння, пов'язані із застосуванням кіберпростору, а також питань атрибуції кібератак проти об'єктів критичної інфраструктури держав;

нормотворчій діяльності – в процесі підготовки та удосконалення законодавчих та підзаконних актів, що стосуються захисту та стійкості критичної інфраструктури від кібернетичних атак;

правозастосовчій діяльності – для забезпечення єдиного підходу до застосування міжнародних звичаєвих норм про атрибуцію міжнародно-правових діянь до кібератак проти об'єктів критичної інфраструктури;

науково-методичній роботі – при підготовці навчальних посібників та підручників з міжнародного права, при читанні курсів міжнародного права, розробці спецкурсів, що пов'язані з питаннями відповідальності держав та забезпеченні кіберстійкості критичної інфраструктури в контексті міжнародної безпеки;

навчальному процесі – для вивчення дисциплін «Міжнародне право», «Відповідальність в міжнародному праві», «Міжнародне гуманітарне право», «Міжнародне право безпеки»;

правовиховній – для підвищення рівня правової культури населення, формування правосвідомості студентів правничих закладів вищих закладів та факультетів.

Апробація результатів дослідження. Дисертацію обговорено та виконано на кафедрі міжнародного та європейського права Національного університету «Одеська юридична академія». Результати дисертаційного дослідження доповідалися на очних та заочних науково-практичних конференціях та семінарах, а саме: «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру» (м. Одеса, 21 травня 2021 року); «Право і суспільство: актуальні питання і перспективи розвитку» (м. Полтава, 10 грудня 2020 року); «Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe» (м. Рига, Латвія, 20 листопада 2020 року); «Права людини – пріоритет сучасної держави» (м. Одеса, 10 грудня 2020 р.); «Правова система України в умовах новітніх викликів міжнародного порядку» (м. Одеса, 20 травня 2020 р.); «Правове життя сучасної України» (м. Одеса, 15 трав. 2020 р.).

У процесі здійснення дослідження авторка брала участь у фахових обговореннях, круглих столах, семінарах присвячених сучасним проблемам міжнародного права. Зокрема, у 26 червня 2020 року авторка долучилась до міжкафедрального семінару, в якому брали участь аспіранти та науковців кафедри міжнародного та європейського права. 23 червня 2021 року результати дослідження представленні в ході семінару, присвяченого актуальним питанням міжнародного права, в рамках модулю Жана Моне на базі НУ «ОЮА».

Публікації. Основні наукові результати дисертації висвітлені в 4 наукових публікаціях, а також одному розділі колективної монографії, що в сукупності розкривають основний зміст дисертації.

Структура та обсяг дисертації. Дисертація складається із анотації, вступу, трьох розділів, які містять 11 підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 219 сторінок, у тому числі основного тексту – 167 сторінок. Список використаних джерел налічує 251 найменування.

Список публікацій здобувача за темою дисертації та відомості про апробацію матеріалів дисертації:

***Наукові праці, в яких опубліковані основні наукові результати дисертації*:**

1. Музика В.В. Кібератаки та міжнародне право: природа та аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі : колект.

моногр. «Проблеми публічного та приватного права» / за заг. ред. Н. В. Мішиної. 2021. С. 309-342.

2. Музика В.В. Проблема атрибуції кібератак проти об'єктів критичної інфраструктури та шляхи її вирішення в міжнародному праві. *Юридичний вісник*. № 4. 2020. С. 164-171. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/1985/2080.
3. Muzyka V. Analysis of cyber-attacks on Ukrainian power grid systems in the context of armed conflict in Donbas. *Constitutional State*. № 39. 2020. С. 78-85. URL: http://pd.onu.edu.ua/article/view/212983/214967.
4. Muzyka V. New wine in old bottles: applicability of the rules on attribution to cyberattacks committed against objects of critical infrastructure. *Law Review of Kyiv University of Law*. № 3. 2020. С. 388-391. URL: https://chasprava.com.ua/index.php/journal/article/view/419/400.

Наукові праці у періодичних наукових виданнях інших держав:

1. Музика В.В. Політика ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки. *Evropský politický a právní diskurz*. 2021. Том 8 (1). С. 46-51. URL: https://eppd13.cz/wp-content/uploads/2021/2021-8-1/9.pdf.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Музика В.В. До питання про відсутність поняття «критична інфраструктура» в міжнародному праві. Матеріали міжнародної конференції : Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (21 травня 2021 року). Одеса, 2021. С. 359-362.
2. Музика В.В. Відповідальність держав за порушення обов'язку належної обачності (due diligence) в кіберпросторі. Право і суспільство: актуальні питання і перспективи розвитку : Матеріали V Міжнародної науково-практичної конференції Частина I (10 грудня 2020 року). Полтава, 2020. С. 107-110.
3. Muzyka V. Attribution of cyberattacks committed through cyber infrastructure of a third state and due diligence obligation. Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe : International Scientific Conference. Baltija Publishing. (20 November 2020). Riga, Latvia. 2020. P. 111-114.
4. Muzyka V. Human dimension of cyberoperations. Права людини – пріоритет сучасної держави : збір. матер. наук.-прак. конф. (м. Одеса, 10 грудня 2020 р.). Херсон : Видавничий дім «Гельветика», 2020. С. 179-182.
5. Muzyka Viktoriia V. Cyber-attacks attribution and EU collective cyber sanctions as a way to respond to cyber threats from outside the Union. Правова система України

в умовах новітніх викликів міжнародного порядку : матеріали науково-практичної заочної конференції (м. Одеса, 20 травня 2020 р.) / за ред. М. Р. Аракеляна. Херсон : Видавничий дім «Гельветика», 2020. С. 63-65.

6. Muzyka Viktoriia V. Public Attribution of Cyber-Attacks: Toward a New Approach in International Law. Правове життя сучасної України : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Видавничий дім «Гельветика», 2020. Т. 3. С. 46-49.

Характеристика особистості здобувача. Музика В. В. здобула другий (магістерський) рівень вищої юридичної освіти. У 2015 році закінчила Національний університет «Одеська юридична академія» та отримала диплом з відзнакою за ступенем вищої освіти «бакалавр» за спеціальністю 081 «Право». У 2017 році закінчила магістратуру Національного університету «Одеська юридична академія», отримала диплом з відзнакою та здобула кваліфікацію: ступінь вищої освіти магістр, спеціальність «Право». З вересня 2017 року – аспірант кафедри міжнародного та європейського права Національного університету «Одеська юридична академія» денної форми навчання. Володіє українською, російською, англійською мовами. Має 4 наукові статті, опубліковані у фахових виданнях, перелік яких затверджений МОН України, з них 1 наукова стаття у періодичному науковому виданні іншої держави, які входять до Організації економічного співробітництва та розвитку та/або Європейського Союзу, а також розділ в колективній монографії. Додатково положення дослідження відображені у 6 тезах доповідей на всеукраїнських та міжнародних науково-практичних конференціях.

Особистий внесок автора. Дисертаційна робота є власним авторським дослідженням, у якому наукові положення, висновки та пропозиції обґрунтовано самостійно в результаті опрацювання значної кількості наукових джерел. Ідеї та розробки, що належать співавторам не використовувались.

Оцінка мови та стилю дисертації. Мова та стиль написання дисертації відповідають прийнятному у науковій літературі та відповідають встановленим вимогам, які висуваються до наукової праці такого рівня, що забезпечує легкість та доступність сприйняття дисертації.

У результаті попередньої експертизи дисертації В. В. Музики та повноти основних результатів дослідження.

УХВАЛИЛИ:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Музики Вікторії Василівни на тему: «Атрибуція кібератак проти об’єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення», представленої на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

2. Констатувати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Музики Вікторії Василівни відповідає спеціальності 081 «Право» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами і доповненнями від 03 квітня 2019 року № 283), п. 10 Тимчасового порядку присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 06 березня 2019 року № 167.
3. Рекомендувати дисертацію Музики Вікторії Василівни на тему: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення» до захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 081 «Право».

Рецензент:
доктор юридичних наук, професор
професор кафедри міжнародного та
європейського права Національного
університету «Одеська юридична академія» О. О. Сурілова

Рецензент:
кандидат юридичних наук, доцент
доцент кафедри міжнародного та
європейського права Національного
університету «Одеська юридична академія» М. В. Грушко