ВІДГУК

офіційного опонента доктора юридичних наук, професора Оксіня Віталія Юрійовича на дисертаційне дослідження Колесника Олександра Олександровича на тему: «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід», подане на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право»

Актуальність теми дослідження. Актуальність дисертаційного дослідження Колесника Олександра Олександровича не викликає сумнівів і безпосередньо зумовлена умовами повномасштабної збройної агресії Російської Федерації проти України, трансформацією характеру сучасних воєн та переходом гібридного протиборства у затяжну фазу. За таких обставин кіберпростір набуває статусу повноцінного театру стратегічних дій, де кібератаки за масштабом і наслідками співвідносяться з традиційними воєнними засобами. Це об'єктивно висуває проблему забезпечення кібербезпеки у ранг ключового системоутворювального компонента національної безпеки, що визначає стабільність функціонування державних інститутів, стійкість критичної інфраструктури, захист інформаційних ресурсів і збереження суспільної довіри до публічної влади.

Проблематика, обрана дисертантом, органічно вписується в сучасний науковий дискурс публічного права та права національної безпеки з урахуванням міжнародно-правових стандартів, водночас істотно виходячи за межі суто теоретичного аналізу. У роботі акцент зроблено не лише на дефінітивному та концептуальному осмисленні феномену кібербезпеки, а й на практичних механізмах побудови цілісної національної системи кіберзахисту, формуванні моделі колективної кіберстійкості та гармонізації українських підходів із євроатлантичними стандартами управління кіберризиками. Особливої ваги набуває звернення до питань інституційної архітектури сектору безпеки й оборони, ролі координаційних органів, а також державно-приватної взаємодії як необхідної умови ефективної протидії кіберагресії.

Вибір напряму дослідження є належно вмотивованим як у теоретико-методологічному, так і в прикладному вимірах. Цілком обґрунтовано дисертант виходить із того, що за видимою адаптивністю національної системи кібербезпеки приховані суттєві інституційні й нормативно-правові вразливості: фрагментарність правового регулювання, розпорошеність повноважень між суб'єктами сектору безпеки, відсутність єдиного центру координації та дефінітивна невизначеність ключових понять («кібербезпека», «кіберзахист», «кіберстійкість»). Саме ці диспропорції, які ускладнюють формування цілісної системи державного управління у сфері кібербезпеки та сталих механізмів колективної кіберстійкості, потребують комплексного системно-правового осмислення, що й становить предмет дисертаційного пошуку.

Тематика дослідження безпосередньо кореспондує зі стратегічним курсом України на європейську та євроатлантичну інтеграцію, виконанням Угоди про асоціацію з ЄС, Стратегії національної безпеки України та Стратегії кібербезпеки України. Звернення автора до проблем гармонізації національної моделі кіберзахисту з acquis ЄС і нормативно-організаційними стандартами НАТО (зокрема, до положень NIS2, DORA, CRA та відповідних європейських підходів до ризик-орієнтованого управління, інцидент-репортингу, сертифікації та спільного реагування) свідчить про глибоке розуміння ним системних засад сучасної політики кібербезпеки. Дисертант демонструє здатність поєднувати національний контекст із вимогами європейських та міжнародних режимів у сфері цифрової безпеки.

Наукова цінність роботи полягає також у зосередженні на відносно недостатньо розробленому у вітчизняній правовій науці сегменті – правових механізмах державно-приватної взаємодії у сфері кібербезпеки, включно з інституціоналізацією форматів на кшталт ISAC/CSIRT, розробленням процедур обміну інформацією, атрибуції кібератак та забезпеченням належної обачності (due diligence) у транскордонних кіберінцидентах. Колесник Олександр Олександрович слушно наголошує, що ефективне реагування на кіберагресію потребує не лише оновлення законодавства, а й побудови стійкої

системи партнерства між державою, бізнесом і громадянським суспільством на засадах довіри, прозорості, спільної відповідальності та технологічної сумісності.

Таким чином, актуальність обраної теми не викликає жодних сумнівів. Вона адекватно відображає виклики сучасного етапу гібридної війни проти України, відповідає стратегічним орієнтирам державної політики у сфері національної безпеки та євроінтеграції, а також сприяє поглибленню теоретико-методологічних і прикладних засад правового забезпечення кібербезпеки та кіберстійкості України в умовах глобальної цифрової взаємозалежності.

Оцінка наукового рівня дисертації і наукових публікацій здобувача. Вивчення дисертаційного дослідження Колесника Олександра Олександровича та його наукових напрацювань засвідчує високий рівень теоретичної підготовки здобувача, логічність побудови й послідовність викладу матеріалу. Автор чітко визначив мету, об’єкт, предмет і завдання дослідження, забезпечивши їхню внутрішню методологічну узгодженість та повну кореляцію з обраною тематикою – кібербезпекою як складовою сучасної архітектури національної та міжнародної безпеки України. Структура дисертації вирізняється цілісністю, логікою розгортання наукового аналізу від теоретико-методологічних засад до прикладних рекомендацій, а також завершеністю кожного розділу, що свідчить про зріле розуміння здобувачем предмета дослідження, уміння працювати з великим обсягом нормативного, доктринального й аналітичного матеріалу та сформований науковий стиль мислення.

Робота характеризується виваженим і методологічно коректним поєднанням загальнонаукових, міждисциплінарних і спеціально-юридичних методів пізнання. Дисертант послідовно застосовує діалектичний метод для розкриття кібербезпеки як динамічного соціотехнічного явища в умовах гібридної агресії, методи аналізу та синтезу – для виокремлення й інтеграції нормативних, інституційних, технологічних та організаційних компонентів національної системи кіберзахисту. Формально-юридичний та логіко-

семантичний методи забезпечили системний аналіз законодавчої бази України в галузі кібербезпеки й уточнення понятійно-категоріального апарату дослідження; системно-структурний та функціональний підходи використано для моделювання архітектури сектору кібербезпеки та механізмів публічного управління. Порівняльно-правовий та історико-правовий методи дали змогу обґрунтовано зіставити національну модель з євроатлантичними підходами (ЄС, НАТО) та простежити еволюцію української системи кіберзахисту, а метод правового прогнозування – сформулювати концептуальні пропозиції щодо її подальшого розвитку. Таке методологічне поєднання забезпечило глибоке, багатовимірне й внутрішньо узгоджене осмислення феномену кібербезпеки, кіберагресії та державно-приватної взаємодії.

Джерельна база дисертації є репрезентативною та відзначається високим рівнем різноплановості. У роботі широко використано міжнародні договори та документи універсального й регіонального рівнів (ООН, ОБСЄ, Рада Європи, ЄС, НАТО), чинне законодавство України у сфері національної безпеки, кібербезпеки та критичної інфраструктури, стратегічні й концептуальні акти у галузі цифрового розвитку, а також релевантні акти права ЄС, що регулюють кіберзахист, управління кіберризиками та захист критичних послуг. Значне місце посідають аналітичні матеріали національних і міжнародних інституцій, доктринальні джерела вітчизняних та зарубіжних учених з питань кіберправа, міжнародно-правових стандартів у сфері кібербезпеки, інформаційної безпеки та публічного управління. Такий добір свідчить про ґрунтовність і системність опрацювання матеріалу, відповідність дослідження сучасним вимогам академічної доброчесності й уміння здобувача здійснювати критичний аналіз наукових підходів, виявляти дискусійні положення та формулювати власні аргументовані висновки.

Основні положення дисертації належно апробовано у фахових статтях та виступах здобувача на науково-практичних конференціях, що охоплюють ключові напрями дослідження. Зокрема, у працях 2022–2025 років Колесник О. О. послідовно розкривав питання формування поняття кібербезпеки, міжнародно-правових принципів регулювання кіберпростору,

правових та інституційних засад національної системи кіберзахисту, а також впливу війни на трансформацію української моделі кібербезпеки. До таких публікацій належать матеріали конференцій і статті у фахових юридичних виданнях, де автор аналізує дефінітивні підходи, міжнародні стандарти та українську практику кіберзахисту.

Наведені роботи свідчать про системність і цілісність наукового пошуку здобувача, послідовне розгортання тематики дисертації в науковому просторі та позитивне сприйняття його результатів фаховою спільнотою. Таке коло апробацій підтверджує практичну значущість отриманих висновків і їх відповідність сучасним потребам розвитку правового й інституційного забезпечення кібербезпеки України.

Новизна представлених теоретичних результатів та повнота їх відображення у публікованих працях. Дисертаційне дослідження Колесника Олександра Олександровича є одним із перших в Україні комплексних наукових досліджень, у якому кібербезпека розглядається як інтегральний елемент сучасної архітектури національної та міжнародної безпеки в умовах гібридної війни. Робота поєднує ґрунтовний теоретико-правовий аналіз із розробленням прикладних рекомендацій щодо вдосконалення правового регулювання, інституційного забезпечення та механізмів державно-приватної взаємодії в сфері кіберзахисту, а також адаптації української моделі до євроатлантичних стандартів. За результатами дослідження сформульовано низку нових наукових положень, що становлять особистий внесок здобувача у розвиток національної доктрини кіберправа та публічно-правових механізмів забезпечення кібербезпеки держави.

Зокрема, уперше запропоновано інтегральне авторське визначення поняття «кібербезпека», яке поєднує технічні, правові, організаційні та етичні компоненти та відображає її як стан і безперервний процес стійкого, правомірного та безпечного функціонування цифрового середовища. Важливими науковими новаціями є розроблення ієрархічної моделі референтних об’єктів кіберзахисту, що дозволяє уніфікувати предметне поле кібербезпеки, а також створення оригінальної типології кіберагресії за

моделлю «цілі – інструменти – очікувані ефекти», яка забезпечує комплексне та порівнюване дослідження кіберінцидентів. Значним внеском є розроблення методологічних підходів до аналізу кібератак, що сприяють підвищенню обґрунтованості аналітичних висновків та їх юридичної придатності. Вперше також представлено системну модель адаптації євроатлантичних підходів до національної правової системи, яка охоплює кодифікаційний, гармонізаційний, інституційний та концептуально-принциповий рівні.

У межах дисертації суттєво удосконалено теоретико-методичний апарат дослідження кібербезпеки, поглиблено концепцію кіберстійкості як динамічного циклу реагування, відновлення та навчання, конкретизовано підхід до правової кваліфікації кібероперацій з урахуванням міжнародного гуманітарного та звичаєвого права, а також розширено методологію аналізу національної кіберстійкості через матричну модель «вразливість – прояви – напрями вдосконалення». Подальший розвиток отримали національно-правові засади кібербезпеки, концепція кіберагресії як елементу гібридної війни, а також підходи до формування проактивної моделі кіберзахисту та державно-приватного партнерства.

Наукова обґрунтованість отриманих результатів, наукових положень, висновків і рекомендацій, сформульованих у дисертації. Наукові результати, отримані Колесником Олександром Олександровичем, відзначаються високим рівнем обґрунтованості, логічною завершеністю та внутрішньою цілісністю. Вони спираються на ґрунтовний теоретико-правовий аналіз феномену кібербезпеки як складової архітектури національної та міжнародної безпеки, багаторівневе дослідження національного законодавства України, міжнародно-правових актів ООН, ОБСЄ, Ради Європи, ЄС і НАТО, а також на осмислення практики кібератак проти України у 2014–2024 роках. Залучення широкої джерельної бази — від стратегічних документів і законів до спеціальних досліджень, аналітичних доповідей та емпіричного матеріалу щодо гібридної агресії РФ — забезпечило глибину, репрезентативність і достовірність зроблених у роботі висновків.

Обґрунтованість положень дисертації підтверджується чіткою кореляцією між метою, завданнями, структурою, змістом розділів і сформульованими висновками. Дисертант послідовно переходить від методологічного аналізу поняття «кібербезпека» та окреслення його міждисциплінарної природи — до дослідження національної системи кіберзахисту, її інституційної архітектури, вразливостей критичної інфраструктури та механізмів протидії кіберагресії, а далі — до комплексного порівняльно-правового аналізу євроатлантичних моделей та формулювання пропозицій з їх адаптації до українського контексту. Така логіка викладу забезпечує наступність наукового пошуку та демонструє внутрішню узгодженість усіх елементів дослідження.

Висновки й рекомендації здобувача побудовані на системному використанні сучасного інструментарію правової науки: діалектичного, формально-юридичного, порівняльно-правового, історико-правового, функціонального, логіко-семантичного та методів правового прогнозування. Це дозволило не лише уточнити понятійно-категоріальний апарат кіберправа, а й запропонувати комплексні підходи до оцінки національної кіберстійкості, типологізації кіберагресії, аналізу кібероперацій та моделювання державно-приватної взаємодії.

Сформульовані Колесником О.О. наукові положення відзначаються високим рівнем новизни та переконливістю. Авторське інтегральне визначення кібербезпеки, ієрархічна модель референтних об’єктів кіберзахисту, аналітична типологія кіберагресії та системна модель адаптації євроатлантичних підходів до української правової системи мають концептуальний характер і ґрунтуються на всебічному аналізі чинної нормативної бази, міжнародних стандартів та практики їх впровадження. Кожне з поданих рішень логічно випливає з проведеного аналізу й узгоджується з поставленими у вступі метою і завданнями.

Обґрунтованість висновків дисертації додатково підтверджується їх практичною спрямованістю та відповідністю актуальним потребам державної політики у сфері кібербезпеки. Запропоновані рекомендації можуть бути

використані при вдосконаленні законодавства України про кібербезпеку й критичну інфраструктуру, доопрацюванні законопроєкту щодо державно-приватної взаємодії у сфері кіберзахисту, розробленні підзаконних актів, а також у діяльності органів публічної влади, наукових установ і закладів вищої освіти. Це свідчить про високий рівень наукової обґрунтованості та практичної значущості результатів, отриманих у дисертації.

Рівень виконання поставленого наукового завдання, оволодіння здобувачем методології наукової діяльності. Дисертація Колесника Олександра Олександровича засвідчує належний рівень оволодіння здобувачем методологічним апаратом сучасних правових досліджень. Обрані методи відповідають природі досліджуваного явища та логіці наукового аналізу, застосовані послідовно й обґрунтовано, що забезпечило цілісність і наукову переконливість отриманих результатів.

Діалектичний метод використано для розкриття внутрішньої динаміки та суперечностей розвитку кібербезпеки в умовах гібридної агресії, що дало змогу належним чином окреслити її концептуальні межі. Методи аналізу та синтезу застосовані для структурування основних компонентів системи кібербезпеки та формування узагальненої моделі національної кіберстійкості. Формально-юридичний метод забезпечив ґрунтовний аналіз законодавства України у сфері кіберзахисту й оцінку його відповідності міжнародним стандартам.

Системно-структурний підхід дав змогу визначити інституційну архітектуру системи кібербезпеки та взаємозв’язки між її елементами. Порівняльно-правовий метод використано для дослідження євроатлантичних підходів до кіберзахисту й визначення можливостей їх адаптації до національного правопорядку. Функціональний метод застосовано для аналізу механізмів реалізації державної політики та процедур реагування на кіберінциденти. Логіко-семантичний і історико-правовий методи забезпечили уточнення понятійно-категоріального апарату й простеження еволюційних етапів формування національної системи кібербезпеки.

Метод правового прогнозування дав можливість розробити комплекс практичних рекомендацій щодо вдосконалення правового регулювання, розвитку державно-приватної взаємодії та зміцнення кіберстійкості критичної інфраструктури. Допоміжні методи систематизації, індукції, дедукції та теоретичного узагальнення сприяли досягненню внутрішньої узгодженості дослідження.

Узагальнюючи, слід зазначити, що здобувач упевнено володіє методологією наукової роботи, коректно поєднує різні методи пізнання та застосовує їх відповідно до завдань і структури дослідження. Виконані ним наукові завдання є методологічно обґрунтованими, а рівень їх реалізації відповідає вимогам, які висуваються до дисертаційних робіт на здобуття ступеня доктора філософії за спеціальністю 081 – Право.

Теоретичне і практичне значення результатів дослідження. Дисертаційне дослідження Колесника О.О. має вагоме теоретичне значення, оскільки розширює доктрину кіберправа та права національної безпеки, вводить нові категорії та концепти, удосконалює методологію аналізу кіберзагроз і уточнює понятійний апарат сфери кібербезпеки. Запропоновані автором моделі та підходи створюють системну основу для подальших наукових досліджень і розвитку міждисциплінарного дискурсу.

Практичне значення роботи полягає у формуванні цілісного теоретико-методичного фундаменту для модернізації державної політики у сфері кібербезпеки, розвитку інституційних механізмів та удосконалення правового регулювання. Отримані результати можуть слугувати орієнтиром для подальших наукових розробок і експертних оцінок у галузі кіберзахисту.

Оцінка змісту дисертації, її завершеності в цілому. Тема дисертаційного дослідження є концептуально важливою для сучасної юридичної науки та практики забезпечення національної безпеки, відповідає нагальним потребам суспільного розвитку в умовах гібридної агресії проти України та цифрової трансформації публічного управління. Дисертація виконана українською мовою, її зміст відзначається логічною структурованістю з чітким розподілом на вступ, основну частину

(теоретичний, аналітичний та прикладний аспекти) і висновки, що загалом відповідає вимогам МОН України та Порядку присудження ступеня доктора філософії.

Дисертаційна робота містить анотацію, список публікацій, зміст, вступ, три розділи, що включають десять підрозділів, висновки, список використаних джерел і додатки.

Дисертантом висвітлено всі ключові аспекти заявленої тематики, виклад має комплексний характер із належним урахуванням практичних вимірів функціонування національної системи кібербезпеки. Усі завдання, сформульовані у вступі, виконано; обсяг, глибина опрацювання матеріалу та рівень теоретико-прикладних узагальнень відповідають вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії.

Після кожного розділу та дисертації загалом сформульовано висновки, у яких послідовно та вичерпно відображено зміст розглянутих питань. Висновки корелюють із отриманими результатами, характеризуються належним рівнем аргументованості, внутрішньою логічною узгодженістю та достатньою мірою достовірності.

Джерельна база є репрезентативною, включає нормативно-правові акти України та міжнародні документи, наукові праці вітчизняних і зарубіжних дослідників, аналітичні матеріали, що забезпечує належний рівень наукової обґрунтованості одержаних результатів.

Рекомендації щодо подальшого використання результатів дисертації на практиці. Отримані результати дисертаційного дослідження Колесника Олександра Олександровича можуть бути використані для подальшого вдосконалення державної політики у сфері кібербезпеки, підвищення інституційної спроможності сектору безпеки й оборони та розвитку державно-приватної взаємодії.

У нормотворчій діяльності напрацювання автора доцільно застосовувати під час оновлення законодавства, що регулює систему кіберзахисту України. Зокрема, вони можуть бути корисними при доопрацюванні законопроєктів і змін до базових актів у сфері кібербезпеки та критичної інфраструктури,

уточненні координаційних повноважень між суб'єктами національної системи кібербезпеки, а також при розробленні нормативних механізмів державно-приватного партнерства. Ці рекомендації сприятимуть гармонізації українського законодавства з вимогами Європейського Союзу та стандартами євроатлантичної спільноти.

У практичній діяльності органів публічної влади результати дослідження можуть бути використані для підвищення ефективності управління кіберризиками, вдосконалення міжвідомчої взаємодії, оптимізації реагування на кіберінциденти та створення сталих каналів обміну інформацією між державними органами й приватним сектором. Напрацьовані підходи можуть допомогти у формуванні проактивної моделі забезпечення кіберстійкості в умовах гібридних загроз і воєнного стану.

У міжнародному контексті рекомендації автора можуть бути використані для посилення участі України у співробітництві з ЄС, НАТО та Радою Європи, зокрема у сфері інцидент-репортингу, обміну інформацією, розвитку процедур реагування та вдосконалення механізмів публічного адміністрування у сфері кібербезпеки з урахуванням міжнародних стандартів.

У науково-дослідній сфері результати дисертації можуть слугувати базою для подальших міждисциплінарних досліджень у галузях міжнародного кіберправа, інформаційної безпеки, публічного управління та права національної безпеки. Наукові положення, сформульовані у роботі, можуть бути використані для підготовки монографій, дисертацій, статей і аналітичних матеріалів, присвячених питанням кіберзагроз, кіберагресії та національної стійкості.

В освітньому процесі результати дослідження можуть бути інтегровані у навчальні програми з кібербезпеки, інформаційного та міжнародного права, публічного управління, а також використані при розробленні методичних матеріалів і практичних кейсів для підготовки та підвищення кваліфікації державних службовців і фахівців у сфері цифрової безпеки.

У цілому, отримані результати створюють прикладне підґрунтя для модернізації правових, організаційних та інституційних механізмів

кіберзахисту України, що відповідає потребам держави в умовах гібридної війни та стратегічного курсу на євроатлантичну інтеграцію.

Зауваження щодо оформлення та змісту дисертації, запитання до здобувача. Загалом позитивно оцінюючи представлену наукову працю, доцільно звернути увагу на окремі питання, які потребують додаткових пояснень або уточнень з боку здобувача під час захисту, оскільки вони мають дискусійний характер і можуть сприяти поглибленню фахової розмови:

1) у підрозділі 1.1 автор обґрунтовано акцентує увагу на людському та етичному вимірах кібербезпеки. Водночас доцільним виглядає уточнення, яким саме чином ці чинники інтегруються в запропоноване автором бачення національної моделі кіберзахисту та з яких підстав їх включення розглядається як методологічно необхідне;

2) у Розділі 1 автор значну увагу приділяє проблемі термінологічної неузгодженості у сфері кібербезпеки. Було б корисно уточнити, які саме сегменти державної політики, на думку автора, зазнають найбільшого впливу від відсутності уніфікованих дефініцій та як це позначається на практичному функціонуванні системи кіберзахисту;

3) у підрозділі 3.1 дисертації автор використовує термін «державно-приватне партнерство» для позначення взаємодії держави та приватного сектору у сфері кібербезпеки. Водночас у національному законодавстві України закріплено поняття «публічно-приватне партнерство». У зв’язку з цим доцільно було б уточнити, з яких підстав автор надає перевагу саме категорії «державно-приватне партнерство»;

4) Таблиця 2.1 – матриця відповідності типів кібератак та інцидентів (2014–2024 рр.) у Розділі 2 демонструє значну технічну деталізацію окремих інцидентів, включаючи опис інструментів, векторів та конкретних шкідливих програм. Водночас юридичні та організаційні наслідки відповідних атак у таблиці відображено меншою мірою. Через це технічна складова переважає над аналітичними висновками щодо впливу кожного інциденту на розвиток національної системи кіберзахисту та еволюцію правових механізмів

реагування. Доцільним було б дещо збалансувати подачу та підсилити зв’язок між технічними характеристиками й правовим виміром.

Слід відзначити, що вказані зауваження і побажання є рекомендаційними і в цілому не позначаються на позитивній оцінці дисертації, оскільки спрямовані на поглиблення наукової дискусії під час прилюдного захисту.

Відсутність порушень академічної доброчесності. Під час аналізу дисертаційного дослідження та наукових публікацій автора фактів порушення академічної доброчесності не виявлено. Дисертація Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» є оригінальною, самостійно виконаною науковою працею, що вирізняється високим рівнем авторського опрацювання, коректним використанням джерельної бази та належним дотриманням етичних стандартів наукової діяльності.

Висновок про відповідність дисертації поставленим вимогам. Дисертація Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід», подана на здобуття ступеня доктора філософії за спеціальністю 081 «Право», є комплексним, цілісним і завершеним науковим дослідженням, у якому на високому теоретико-методологічному рівні розкрито сутність, структуру та механізми функціонування національної системи кібербезпеки України в умовах гібридної агресії. У роботі здійснено всебічний теоретико-правовий аналіз кібербезпеки як системоутворювального елемента сучасної архітектури національної та міжнародної безпеки, обґрунтовано концептуальні засади правового регулювання та інституційного забезпечення кіберзахисту, а також сформульовано науково обґрунтовані пропозиції щодо адаптації євроатлантичних стандартів, удосконалення державно-приватної взаємодії й підвищення кіберстійкості критичної інфраструктури України.

Зміст дисертації свідчить про досягнення поставленої мети й успішне розв'язання визначених у вступі завдань дослідження. Структура роботи відповідає логіці наукового пошуку: від теоретико-методологічного осмислення феномену кібербезпеки та її місця в системі національної і міжнародної безпеки – до аналізу національної моделі кіберзахисту в умовах гібридної війни та вироблення практично орієнтованих рекомендацій щодо гармонізації з acquis ЄС і стандартами євроатлантичної спільноти. Отримані автором результати відзначаються науковою новизною, що проявляється, зокрема, в інтегральному визначенні поняття «кібербезпека», ієрархічній моделі референтних об'єктів кіберзахисту, аналітичній типології кіберагресії, верифікаційному каркасі аналізу кібератак, а також у системній моделі адаптації євроатлантичних підходів до української правової системи. Практичне значення роботи підтверджується можливістю використання її висновків і рекомендацій у нормотворчій діяльності, публічному управлінні, наукових дослідженнях та освітньому процесі.

Дисертація за своїм змістом і структурою відповідає спеціальності 081 «Право» та всім вимогам, установленим у Порядку підготовки здобувачів вищої освіти (наукових установах), затвердженому постановою Кабінету Міністрів України від 23 серпня 2016 року № 261 (із змінами і доповненнями від 3 квітня 2019 року № 283), наказу МОН України від 12 січня 2017 року № 40 «Про затвердження Вимог до оформлення дисертації» (зі змінами від 12 липня 2019 року) та Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженому постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

Отже, дисертаційне дослідження Колесника Олександра Олександровича за змістом, науковим рівнем, структурою, повнотою обґрунтування висновків і практичних рекомендацій повністю відповідає встановленим вимогам, а його автор заслуговує на присудження наукового

ступеня доктора філософії у галузі знань 08 «Право», спеціальність 081 «Право».

Офіційний опонент –
професор кафедри публічного управління,
адміністрування та права
Національного університету «Полтавська політехніка
імені Юрія Кондратюка»,
доктор юридичних наук, професор **Віталій ОКСІНЬ**