ЗАТВЕРДЖУЮ
В.о. президента Науково-дослідного інституту публічного права
д.ю.н, професор
С.О. Короєд
«8» грудня 2025 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід», поданої на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право», затвердженої Вченою радою Науково-дослідного інституту публічного права від 21 листопада 2022 року (протокол № 15)

ВИТЯГ

із протоколу спільного засідання відділів актуальних питань філософії права та юридичної лінгвістики, науково-правових експертиз та законопроектних робіт, проблем публічного права, організаційного забезпечення наукових проектів і міжнародної діяльності Науково-дослідного інституту публічного права від «8» грудня 2025 року.

Присутні 11 осіб:

Овчарук Сергій Станіславович – доктор юридичних наук, доцент, завідувач відділу проблем публічного права Науково-дослідного інституту публічного права – *головуючий на засіданні*;

Короєд Сергій Олександрович – доктор юридичних наук, професор, в.о. президента Науково-дослідного інституту публічного права;

Боровик Андрій Володимирович – доктор юридичних наук, доцент, віце-президент з наукової роботи Науково-дослідного інституту публічного права;

Сорока Лариса Володимирівна – доктор юридичних наук, професор, завідувач відділу аспірантури Науково-дослідного інституту публічного права – *науковий керівник;*

Куркова Ксенія Миколаївна – доктор юридичних наук, професор, завідувач відділу науково-правових експертиз та законопроектних робіт Науково-дослідного інституту публічного права;

Ріпенко Артем Ігорович – доктор юридичних наук, завідувач відділу актуальних питань філософії права та юридичної лінгвістики Науково-дослідного інституту публічного права;

Луценко-Миськів Леся Ігорівна – доктор юридичних наук, професор, головний науковий співробітник Науково-дослідного інституту публічного права;

Козін Сергій Миколайович – доктор юридичних наук, старший дослідник, провідний науковий співробітник відділу науково-правових експертиз та законопроектних робіт Науково-дослідного інституту публічного права;

Курило Інна Володимирівна – доктор юридичних наук, професор, головний науковий співробітник Науково-дослідного інституту публічного права;

Шкарупа Костянтин Вікторович – доктор юридичних наук, старший дослідник, провідний науковий співробітник Науково-дослідного інституту публічного права;

Даниленко Анна Олександрівна – доктор філософії за спеціальністю 081 Право, старший науковий співробітник Науково-дослідного інституту публічного права.

Запрошені:

Колесник Олександр Олександрович – *здобувач ступеня доктора філософії.*

Порядок денний:

Публічна презентація здобувачем Колесником Олександром Олександровичем наукових результатів дисертації на тему на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» на здобуття ступеня доктора філософії за спеціальністю 081 Право та її обговорення з метою надання висновку про наукову новизну, теоретичне та практичне значення результатів.

Науковий керівник – **Сорока Лариса Володимирівна** – доктор юридичних наук, професор, завідувач відділу аспірантури Науково-дослідного інституту публічного права.

Головуючий по цьому питанню – **Овчарук Сергій Станіславович** – доктор юридичних наук, доцент, головний науковий співробітник відділу Науково-дослідного інституту публічного права.

Слухали:

Здобувача наукового ступеня доктора філософії Колесника О.О. про результати дисертаційного дослідження. У своїй доповіді він обґрунтував актуальність обраної теми дисертаційної роботи, визначив мету, завдання, предмет, об’єкт та методи дослідження, розкрив структуру роботи та основні її положення, показав їх новизну, теоретичне та практичне значення. Здобувач наголосив на таких аспектах свого дослідження.

Повномасштабна збройна агресія Російської Федерації проти України та перехід гібридного протиборства у затяжну фазу істотно трансформували

архітектоніку національної безпеки, актуалізувавши проблему забезпечення кібербезпеки держави. У сучасних умовах кіберпростір набув статусу самостійного виміру стратегічного протиборства, у межах якого кібератаки за масштабом, інтенсивністю та наслідками співвідносяться з традиційними формами воєнних дій. Відтак кібербезпека набула значення ключового системоутворювального компонента національної безпеки, що забезпечує стабільне функціонування державних інститутів, безперервність роботи критичної інфраструктури, захист інформаційних ресурсів і підтримання суспільної довіри до публічної влади.

Разом із тим, за зовнішньою адаптивністю національної системи кібербезпеки простежуються глибинні інституційні та нормативно-правові вразливості, що знижують рівень її цілісності та ефективності. Вони проявляються у фрагментарності правового регулювання, розпорошеності повноважень між суб'єктами сектору безпеки й оборони, відсутності єдиного координуючого центру, а також у дефінітивній невизначеності ключових понять – «кібербезпека», «кіберзахист», «кіберстійкість». Наявність таких диспропорцій унеможливлює формування узгодженої системи державного управління у сфері кібербезпеки, знижує рівень правової визначеності та перешкоджає створенню сталої моделі колективної кіберстійкості, побудованої на принципах підзвітності, спільної відповідальності та технологічної прозорості.

Особливої уваги потребує нормативне закріплення механізмів державно-приватної взаємодії, які у провідних державах світу становлять основу ефективного кіберзахисту. Недостатня правова деталізація таких механізмів в Україні ускладнює координацію дій між державними та недержавними суб'єктами, створює прогалини у розмежуванні повноважень і відповідальності, а також гальмує процес інституціоналізації партнерських форматів типу ISAC/CSIRT. Це, у свою чергу, негативно позначається на своєчасності виявлення та атрибуції кібератак, обмежує можливості доказування у справах, пов'язаних із кіберзлочинами, і створює ризики порушення принципу належної обачності (due diligence) у транскордонних інцидентах.

Не менш важливим викликом залишається необхідність забезпечення належного балансу між безпековими інтересами держави та дотриманням прав і свобод людини у цифровому середовищі. Цей баланс визначає легітимність державної кіберполітики та її відповідність міжнародно-правовим стандартам, що формують основу поліцентричного режиму глобальної кібербезпеки, у межах якого Україна виступає не лише об'єктом, а й активним суб'єктом нормотворення, партнерства та колективного реагування.

Геополітичний курс України на інтеграцію до Європейського Союзу та Північноатлантичного альянсу зумовлює необхідність глибокої гармонізації національної системи кібербезпеки з acquis ЄС і нормативно-організаційними стандартами євроатлантичної спільноти. У цьому контексті особливої

актуальності набуває узгодження правової, інституційної та технічної бази з положеннями директив і регламентів NIS2, DORA, CRA, а також впровадження принципів ризик-орієнтованого управління, інцидент-репортингу, сертифікації та спільних процедур реагування. Водночас відсутність єдиного координаційного центру та чітко визначених механізмів державно-приватного партнерства обмежує ефективність реагування на кіберзагрози, знижує потенціал превенції та ускладнює формування довгострокової, інституційно узгодженої системи кіберстійкості.

Зазначені обставини обумовлюють потребу у комплексному науковому осмисленні кібербезпеки як системоутворювального елемента національної безпеки України, що інтегрує правові, інституційні, технологічні та управлінські виміри. Особливої наукової ваги набуває розроблення концептуально-правових засад функціонування національної системи кіберзахисту, ідентифікація її інституційних вразливостей, адаптація євроатлантичних моделей до українського контексту, а також формування правових механізмів державно-приватної взаємодії у сфері кібербезпеки.

Таким чином, обрана тема дисертаційного дослідження має подвійний вимір значущості: теоретичний – як внесок у розвиток національної доктрини кіберправа та формування методологічної бази публічно-правового регулювання цифрової безпеки; та практичний – як інструмент удосконалення державної політики у сфері кіберзахисту, підвищення кіберстійкості критичної інфраструктури й забезпечення реалізації національних інтересів України в умовах гібридної війни та глобальної цифрової взаємозалежності.

Мета роботи полягає у всебічному теоретико-правовому аналізі системи кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки, визначенні закономірностей її розвитку в умовах гібридної агресії проти України, виявленні ключових інституційно-правових вразливостей і напрямів підвищення кіберстійкості держави, а також у розробленні науково обґрунтованих пропозицій щодо вдосконалення національної моделі правового регулювання та інституційного забезпечення кіберзахисту з урахуванням євроатлантичних підходів.

Для досягнення поставленої мети в дисертації потрібно виконати такі *завдання*:

– розкрити теоретико-правові засади сутності кібербезпеки, з’ясувати її міждисциплінарну природу та співвідношення з суміжними категоріями – інформаційна безпека, кіберзахист, кіберстійкість;

– дослідити міжнародно-правові основи забезпечення кіберзахисту, виявити роль і вплив універсальних та регіональних актів (ООН, ОБСЄ, Ради Європи, ЄС) у формуванні глобальної системи норм та принципів;

– розкрити структуру національної системи кібербезпеки України, її законодавчі засади, інституційну архітектуру, повноваження суб’єктів і механізми взаємодії державного та приватного секторів;

– розкрити еволюцію форм та правову природу кібероперацій як інструмента сучасних воєн і конфліктів, зокрема в контексті російської гібридної агресії.

– провести аналіз основних кібератак проти України у 2014–2024 роках, визначити їхні цілі, масштаби, наслідки та отримані уроки для формування оновленої державної політики безпеки;

– визначити основні інституційно-правові вразливості критичної інфраструктури в умовах воєнного стану у правовому, інституційному та процедурному вимірах, запропонувати напрями їх мінімізації;

– визначити сучасні проблеми протидії кіберзлочинності та кіберагресії, зокрема ефективність нормативно-правових і оперативно-технічних механізмів реагування;

– здійснити порівняльно-правовий аналіз стратегій кіберзахисту США, НАТО та ЄС, визначити їх нормативні, організаційні та технологічні моделі;

– дослідити механізми інтеграції України у міжнародно-правову систему кібербезпеки, зокрема у форматах ЄС, НАТО та Ради Європи, та визначити шляхи гармонізації законодавства України;

– обґрунтувати можливості застосування євроатлантичних практик державно-приватного партнерства як інструменту підвищення кіберстійкості України, сформулювати пропозиції щодо удосконалення правових засад і процедур такої взаємодії.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших комплексних досліджень, присвячених системному теоретико-правовому аналізу феномену кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки України. У роботі розкрито міждисциплінарну природу кібербезпеки, обґрунтовано її концептуальні засади, механізми правового регулювання та напрями гармонізації з євроатлантичними стандартами. За результатами дослідження сформульовано низку нових наукових положень, висновків і пропозицій, запропонованих особисто здобувачем. Основні з них такі:

вперше:

– сформульовано авторське інтегральне визначення поняття «кібербезпека» як стану й безперервного процесу забезпечення стійкого, правомірного та етично врегульованого функціонування цифрового середовища. Його досягнення забезпечується узгодженою взаємодією технологічних засобів, управлінських процедур, правових механізмів і поведінкових норм, спрямованих на захист даних, цифрових сервісів, інфраструктур, соціальних відносин та публічних функцій держави з гарантією їх відновлюваності у разі порушень. Запропоноване визначення інтегрує технічний, управлінський, правовий та етичний виміри у єдину комплексну модель кіберстійкості, що виходить за межі вузько технократичного трактування безпеки;

– розроблено інтегровану методологічну модель кібербезпеки, яка поєднує ієрархічну структуру референтних об’єктів захисту (дані – сервіси –

інфраструктури – соціальні відносини – публічні функції держави) та аналітичну типологію кіберагресії за моделлю «цілі – інструменти – очікувані ефекти». У сукупності ці складники формують єдину систему оцінювання взаємозв'язку між об'єктами кіберзахисту, характером кібервпливів та відповідними правовими режимами реагування, забезпечуючи методологічну цілісність аналізу кібероперацій;

– запропоновано системну модель адаптації євроатлантичних підходів до української правової системи у сфері кібербезпеки, вибудувану за чотирма взаємопов'язаними напрямами – кодифікаційним, гармонізаційним, інституційним і концептуально-принциповим. Модель визначає послідовність правових, організаційних та методологічних кроків для імплементації європейських стандартів управління кіберризиками та забезпечує узгодженість національної системи кібербезпеки з євроатлантичними принципами спільної відповідальності, прозорості та стійкості.

удосконалено:

– теоретико-методичний апарат осмислення феномену кібербезпеки шляхом систематизації типології наукових підходів – технократичних, організаційно-управлінських, правових, соціогуманітарних та освітньо-термінологічних – і обґрунтування необхідності їх інтеграції у межах системного підходу. Такий підхід дозволив розглядати кібербезпеку не як сукупність ізольованих напрямів, а як цілісний процес управління ризиками, довірою та стійкістю у цифровому просторі, що забезпечує комплексність і міждисциплінарність її наукового пізнання;

– концептуалізацію парадигми кіберстійкості як динамічного циклу передбачення, реагування, відновлення та навчання системи, у якому визначено ключову роль людського фактора й етики інформації як внутрішнього регулятора цифрової поведінки. Етика інформації трактується як фундаментальний елемент культури довіри, прозорості та підзвітності у цифровому середовищі, що забезпечує узгодженість між технологічними, правовими та соціальними аспектами функціонування системи кібербезпеки;

– підхід до правової кваліфікації кібероперацій у контексті міжнародного гуманітарного та звичаєвого права. На основі аналізу реальних кейсів кіберагресії проти України обґрунтовано застосовність принципів суверенітету, невтручання, належної обачності (due diligence) до цифрового середовища, що дозволило конкретизувати межі відповідальності держав за шкідливу діяльність у кіберпросторі. Уточнено критерії порогу «застосування сили», розмежування між воєнними та невоєнними кібердіями, а також визначено роль публічної атрибуції як ефективного інструмента формування практики державної відповідальності у сфері міжнародного кіберправа;

– методологію аналізу національної кіберстійкості шляхом розроблення аналітичної матриці «вразливість – прояви – напрями вдосконалення», яка відображає взаємозалежність інституційних, технічних і

соціально-комунікаційних чинників безпеки. Така матриця поглиблює ризик-орієнтований підхід до управління кіберзагрозами, забезпечує системну ідентифікацію критичних вразливостей і дозволяє пріоритизувати напрями реформ, підвищуючи ефективність аудитів та стратегічного планування у сфері кіберстійкості;

– методологію порівняльно-правового аналізу євроатлантичних моделей державно-приватного партнерства у сфері кібербезпеки, у межах якої систематизовано ключові принципи (довіра, прозорість, розподіл відповідальності, обмін у реальному часі) та інституційні механізми (CSIRTs Network, ISACs, публічно-приватні платформи). Удосконалено підхід до визначення ролі держави як фасилітатора партнерства, що забезпечує баланс між регуляцією, саморегулюванням і технологічною автономією приватного сектору.

отримали подальший розвиток:

– наукове розуміння феномену кіберагресії як складової гібридної війни, у межах якої кібероперації розглядаються не як ізольовані технічні дії, а як інтегрований компонент воєнних, інформаційно-психологічних та логістичних кампаній. На основі проведеної періодизації кіберагресії РФ проти України (2014–2024 рр.) обґрунтовано її системний, багаторівневий і скоординований характер, що свідчить про трансформацію кіберпростору у повноцінну сферу стратегічного протиборства та формує методологічну основу для подальшого удосконалення міжнародно-правових і національних механізмів реагування;

– комплексне розуміння про чинники уразливості національної критичної інфраструктури, систематизовані у трьох взаємопов'язаних вимірах –інституційному, технічному та соціально-комунікаційному. На цій основі сформульовано концептуальні орієнтири переходу від реактивної до проактивної моделі кіберзахисту, заснованої на стандартизованому обміні інформацією, взаємній довірі між секторами та інтегрованих механізмах моніторингу, превенції й реагування на кіберзагрози;

– концептуальні засади еволюції української моделі кібербезпеки у напрямі європейського типу врядування, у межах яких деталізовано потребу завершення розмежування повноважень між органами влади, інституціоналізації державно-приватного партнерства, розвитку кадрового потенціалу та забезпечення інтеграції у європейські механізми кризового реагування та кіберстійкості.

Після закінченні доповіді здобувачу присутніми були поставлені такі **питання:**

Запитання Шкарупи К.В.: На сучасному етапі особливої уваги потребує нормативне закріплення механізмів державно-приватної взаємодії, які у провідних державах світу становлять основу ефективного кіберзахисту. А як в Україні вирішується питання нормативне закріплення механізмів державно-приватної взаємодії?

Колесник О.О.: Дякую за запитання. Недостатня правова деталізація таких механізмів в Україні ускладнює координацію дій між державними та недержавними суб'єктами, створює прогалини у розмежуванні повноважень і відповідальності, а також гальмує процес інституціоналізації партнерських форматів типу ISAC/CSIRT. Це, у свою чергу, негативно позначається на своєчасності виявлення та атрибуції кібератак, обмежує можливості доказування у справах, пов'язаних із кіберзлочинами, і створює ризики порушення принципу належної обачності (due diligence) у транскордонних інцидентах.

Не менш важливим викликом залишається необхідність забезпечення належного балансу між безпековими інтересами держави та дотриманням прав і свобод людини у цифровому середовищі. Цей баланс визначає легітимність державної кіберполітики та її відповідність міжнародно-правовим стандартам, що формують основу поліцентричного режиму глобальної кібербезпеки, у межах якого Україна виступає не лише об'єктом, а й активним суб'єктом нормотворення, партнерства та колективного реагування.

Запитання Луценко-Миськів Л.І.: Що ви розумієте під поняття «кібербезпека»?

Колесник О.О.: Дякую за запитання. Нами запропоновано авторське визначення поняття «кібербезпека», відповідно до якого кібербезпека – це стан і безперервний процес забезпечення стійкого, правомірного та етично врегульованого функціонування цифрового середовища, що досягається через узгоджену взаємодію технологічних засобів, управлінських процедур, правових механізмів і поведінкових норм, спрямованих на захист даних, інфраструктур, соціальних відносин і публічних функцій держави від деструктивних впливів і забезпечення їх відновлюваності у разі порушень. Це визначення інтегрує технічні, правові, управлінські й етичні компоненти в єдину системно-комплексну модель кіберстійкості.

Запитання Козіна С.М.: Які комунікаційно-психологічні ефекти від кібератак?

Колесник О.О.: Дякую за запитання. Комунікаційно-психологічні ефекти охоплюють девальвацію суспільної довіри до офіційних джерел інформації, дезорієнтацію населення та формування атмосфери невизначеності. Такі наслідки часто є цілеспрямованими: кібератаки супроводжуються інформаційно-психологічними кампаніями, спрямованими на послаблення морального стану населення та дискредитацію інституцій влади.

Запитання Боровика А.В.: Що означає правові «сірі зони» у контексті кіберагресії?

Колесник О.О.: Дякую за запитання. Аналіз характеру сучасних кібероперацій засвідчує, що їх правова природа досі перебуває у полі невизначеності. На відміну від традиційних форм збройної агресії, дії у кіберпросторі рідко мають однозначно ідентифікованого суб'єкта, чітко встановлений причинно-наслідковий зв'язок або безпосередні матеріальні наслідки. Саме ці чинники створюють «сірі зони» у міжнародному праві, де

важко визначити, чи певний кіберінцидент становить втручання у внутрішні справи держави, порушення її суверенітету, чи акт застосування сили. Як зазначає М. Шмітт, у кіберпросторі традиційні пороги суверенітету й невтручання «розмиваються», а більшість дій відбувається нижче рівня, який запускає класичні механізми колективної безпеки.

Цю тезу підтверджує і практика кібератак проти України. Значна частина з них мала комбінований характер – одночасно технічний, інформаційно-психологічний та політичний. Вони не супроводжувалися прямими руйнівними наслідками, однак порушували стабільність державного управління, функціонування критичної інфраструктури та довіру громадян до офіційних джерел інформації. Відповідно, виникає питання кваліфікації таких дій: чи можуть вони розглядатися як застосування сили у розумінні статті 2(4) Статуту ООН, чи лише як недружній акт або реторсія у межах права держави на відповідь.

Запитання Овчарука С.С.: Що на Вашу думку становить базову складову кіберстійкості?

Колесник О.О.: Дякую за запитання. У науковій та аналітичній літературі підкреслюється, що системні програми підвищення обізнаності, освіти та підготовки кадрів у сфері кібербезпеки становлять базову складову кіберстійкості як на рівні окремих організацій, так і на рівні держави загалом. Ефективна кібербезпека неможлива без формування сталої культури інформаційної безпеки серед користувачів, що передбачає регулярне навчання, оцінювання рівня обізнаності та впровадження поведінкових стандартів кібергігієни. Аналогічний підхід простежується у стратегіях кібербезпеки держав ЄС, зокрема Німеччини, де розвиток професійних компетентностей і цифрової грамотності суспільства визначено одним із ключових напрямів забезпечення національної кіберстійкості, а в українських дослідженнях кібергігієна розглядається як необхідна умова підвищення стійкості до сучасних загроз.

У подальшому обговоренні дисертаційного дослідження взяли участь присутні члени спільного засідання.

Науковий керівник – **Сорока Лариса Володимирівна** – доктор юридичних наук, професор, завідувач відділу аспірантури Науково-дослідного інституту публічного права зазначила, що підготовлена Колесником Олександром Олександровичем дисертація на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід», подана на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право», є результатом кропіткої науково-теоретичної та практичної діяльності здобувача. Під час роботи над дисертацією Олександр Олександрович проявив себе як наполегливий дослідник, який вміло використовує методи наукового-пізнання, поєднує теоретичні пошуки з практичними навичками.

Структура та зміст роботи неодноразово узгоджувалися з науковим керівником. Олександр Олександрович показав себе сформованим науковцем, виявив стійкі вміння глибокого аналізу законодавства, дослідження спеціальної літератури, формування та аргументації власних висновків. Тому після кожного розділу дослідження та у кінці роботи здобувачем належним чином оформлювалися аргументовані висновки та узагальнення. Протягом періоду написання дисертаційного дослідження була здійснена серйозна наукова робота та опрацьована значна кількість наукових праць. Дисертація базується на основі чинних, на момент її обговорення, положень законодавчих та підзаконних актів, що дозволяє безпосередньо застосовувати її матеріали як теоретико-методологічну основу а для подальших досліджень питань правового регулювання цифрової безпеки, міжнародного кіберправа та публічного управління у сфері кіберзахисту, для підвищення ефективності управління кіберризиками, розвитку публічно-приватного партнерства, створення механізмів обміну інформацією між державними та приватними структурами, а також оптимізації процедур реагування на кіберінциденти.

Індивідуальний план наукової роботи та навчальний план виконано Колесником О.О. у повному обсязі.

У межах роботи над дисертацією здобувачем підготовлено три одноосібних статті та одна у співавторстві у наукових виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, чотири – тези доповідей і повідомлень на міжнародних науково-практичних конференціях.

Загалом дисертація відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її автор – Колесник О.О. заслуговує на присудження ступеня доктора філософії за спеціальністю 081 «Право».

Вважаю, що дисертаційну роботу можна представити до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

Далі надано слово *рецензентам роботи.*

Курило Інна Володимирівна – доктор юридичних наук, професор, головний науковий співробітник Науково-дослідного інституту публічного права, *як рецензент роботи* відзначила, що актуальність дисертаційної роботи Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» не викликає сумнівів, зокрема з огляду на стратегічний курс України на інтеграцію до Європейського Союзу та НАТО, розбудову цифрової держави й підвищення кіберстійкості критичної інфраструктури.

Зміст дисертації свідчить про продуманий підхід дисертанта до розкриття теми дослідження, висвітлює логічний ланцюг дослідження теоретичних і практичних питань правових аспектів кібербезпеки як системоутворювального елемента національної безпеки України в умовах гібридної війни та з урахуванням міжнародного досвіду провідних держав і міжнародних організацій. Фундаментальність та комплексність роботи проявляється у всебічному та поступовому вивченні дисертантом предмету дослідження. У дисертації чітко сформульовані мета та завдання дослідження, їх постановка та послідовність дозволяють розкрити основний зміст теми.

Належний рівень вірогідності наукової обґрунтованості результатів виконаного дослідження забезпечено використанням значного обсягу узагальнених теоретичних матеріалів та відповідних наукових методів. Новизна підходів до вирішення ряду проблем, аргументованість в основних висновках відрізняють дослідження дисертанта.

На окрему увагу заслуговують висновки дисертанта щодо кодифікаційного, інституційного, концептуально-принципового напрямів адаптації євроатлантичних підходів державно-приватного партнерства у сфері кібербезпеки до українського контексту.

Загалом дисертаційну роботу Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» слід визнати самостійною, завершеною науковою працею, яку виконано за актуальною та практично значущою темою. Робота містить науково обґрунтовані результати, які в комплексі вирішують теоретичні, правові і практичні проблеми кібербезпеки як системоутворювального елемента національної безпеки України, що інтегрує правові, інституційні, технологічні та управлінські виміри..

Дисертація відповідає спеціальності 081 «Право», Вимогам до оформлення дисертації, затвердженим наказом Міністерства освіти і науки України від 12 січня 2017 року № 40, Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44, та може бути подана до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

Луценко-Миськів Леся Ігорівна – доктор юридичних наук, професор, головний науковий співробітник Науково-дослідного інституту публічного права, *як рецензент роботи* відзначила, що дисертант виконав усі поставлені завдання дослідження, запропонував низку теоретично обґрунтованих положень, а також пропозицій та рекомендацій, спрямованих на вдосконалення правових, інституційних та організаційних механізмів формування, функціонування й розвитку системи кібербезпеки України як складової національної безпеки.

Практичне значення отриманих результатів полягає в тому, що сформульовані та обґрунтовані в дисертаційному дослідженні висновки, наукові положення й конкретні пропозиції мають прикладне значення для вдосконалення системи правового, організаційного та інституційного забезпечення кібербезпеки України, а також для гармонізації національної політики з євроатлантичними стандартами.

Заслуговують на позитивну оцінку виявлені дисертантом основні вразливості критичної інформаційної інфраструктури, державних органів і суспільства в умовах воєнного стану, а також запропоновані напрями їх мінімізації.

Зміст роботи, перелік наукових публікацій доводить наукову зрілість, володіння здобувачем методикою дослідницької роботи, умінням узагальнювати досягнуте в науці і на основі досягнутого самостійно формулювати гіпотези, положення, висновки, які мають концептуальний характер та є основою для подальших наукових пошуків у цьому напрямку.

Дисертація Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» є самостійною, завершеною науковою працею, яку виконано за актуальною та практично значущою темою.

Дисертація відповідає спеціальності 081 «Право», Вимогам до оформлення дисертації, затвердженим наказом Міністерства освіти і науки України від 12 січня 2017 року № 40, Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 та може бути подана до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

В *обговоренні* дисертаційного дослідження взяли участь:

Короєд Сергій Олександрович – доктор юридичних наук, професор, в.о. президента Науково-дослідного інституту публічного права зазначив, що дисертація Колесника Олександра Олександровича є цікавою, новою, актуальною та практично важливою. При оформленні дисертаційного дослідження автором дотримані вимоги щодо структури роботи, формування списку використаних джерел.

Належний рівень вірогідності наукової обґрунтованості результатів виконаного дослідження забезпечено використанням значного обсягу узагальнених теоретичних матеріалів, а також комплексу загальнонаукових і спеціально-юридичних методів, кожен із яких мав визначальне значення для досягнення поставленої мети, розв’язання дослідницьких завдань і формування науково обґрунтованих висновків.

Основні положення, висновки та рекомендації дисертації містять елементи наукової новизни, є повністю обґрунтовані та аргументовані і отримали необхідну апробацію на науково-практичних конференціях. У публікаціях здобувача знайшли відображення всі положення дисертаційного дослідження.

Мета роботи, яка полягала у всебічному теоретико-правовому аналізі системи кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки, визначенні закономірностей її розвитку в умовах гібридної агресії проти України, виявленні ключових інституційно-правових вразливостей і напрямів підвищення кіберстійкості держави, а також у розробленні науково обґрунтованих пропозицій щодо вдосконалення національної моделі правового регулювання та інституційного забезпечення кіберзахисту з урахуванням євроатлантичних підходів, була досягнута.

Загалом дисертація Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» є завершеним дослідженням, яке виконано за актуальною та практично значущою темою.

Аналіз результатів проведеного дисертаційного дослідження дає змогу стверджувати, що на захист винесено результати наукового пошуку, що мають концептуально новий підхід до питань, які були визначені в роботі і така робота може бути рекомендована спеціалізованій вченій раді до захисту.

Овчарук Сергій Станіславович – доктор юридичних наук, доцент, завідувач відділу проблем публічного права Науково-дослідного інституту публічного права зазначив, що актуальність дисертації, яка розглядається, очевидна. Тематика дисертаційного дослідження органічно вписується у стратегічні пріоритети державної політики України, спрямовані на зміцнення національної безпеки, розвиток цифрової інфраструктури, підвищення кіберстійкості та виконання євроінтеграційних зобов’язань у сфері кібербезпеки.

Слушними є висновки автора щодо сучасних проблем протидії кіберзлочинності та кіберагресії, а також оцінки ефективності нормативно-правових і оперативно-технічних механізмів реагування.

Дисертаційне дослідження вирізняє новизна підходів до вирішення ряду проблем, а також аргументованість висновків, рекомендацій і пропозицій.

Уважне ознайомлення зі змістом дисертації, методологічною базою дослідження, його висновками, дозволяє стверджувати, що автор наукового дослідження Колесник О.О. з поставленим завданням успішно впорався. Належний рівень вірогідності наукової обґрунтованості результатів виконаного дослідження забезпечено використанням значного обсягу узагальнених теоретичних матеріалів та відповідних наукових методів.

Дисертаційну роботу Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» слід визнати завершеним дисертаційним дослідженням, що виконано за актуальною та практично

значущою темою. Робота містить науково обґрунтовані результати, які в комплексі вирішують теоретичні, правові і практичні проблеми кібербезпеки як системоутворювального елемента національної безпеки України в умовах гібридної війни та з урахуванням міжнародного досвіду провідних держав і міжнародних організацій.

Загалом дисертація Колесника О.О. може бути рекомендована для захисту в спеціалізованій вченій раді.

Колесник О.О. висловив виступаючим та всім присутнім подяку за позитивну оцінку його дисертаційного дослідження, за висловлені побажання та професійні поради, що сприяли вдосконаленню змісту та форми дисертаційної роботи та корекції подальших науково-дослідних планів.

Присутні на засіданні одноголосно запропонували визнати дисертацію Колесника Олександра Олександровича завершеною теоретично та практично-значимою науковою роботою, що містить висновки, які сприяють вирішенню нагальної наукової проблеми та є суттєвим внеском у розвиток юридичної науки, і яка може бути рекомендована до захисту у спеціалізованій вченій раді. Запропоновано схвалити такий висновок:

ВИСНОВОК
щодо дисертації Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» на здобуття ступеня доктора філософії зі спеціальності 081 «Право»

Актуальність теми дисертаційного дослідження обумовлена тим, що повномасштабна збройна агресія Російської Федерації проти України та перехід гібридного протиборства у затяжну фазу істотно трансформували архітектоніку національної безпеки, актуалізувавши проблему забезпечення кібербезпеки держави. У сучасних умовах кіберпростір набув статусу самостійного виміру стратегічного протиборства, у межах якого кібератаки за масштабом, інтенсивністю та наслідками співвідносяться з традиційними формами воєнних дій. Відтак кібербезпека набула значення ключового системоутворювального компонента національної безпеки, що забезпечує стабільне функціонування державних інститутів, безперервність роботи критичної інфраструктури, захист інформаційних ресурсів і підтримання суспільної довіри до публічної влади.

Разом із тим, за зовнішньою адаптивністю національної системи кібербезпеки простежуються глибинні інституційні та нормативно-правові вразливості, що знижують рівень її цілісності та ефективності. Вони проявляються у фрагментарності правового регулювання, розпорошеності повноважень між суб’єктами сектору безпеки й оборони, відсутності єдиного координуючого центру, а також у дефінітивній невизначеності ключових понять – «кібербезпека», «кіберзахист», «кіберстійкість». Наявність таких диспропорцій унеможливлює формування узгодженої системи державного

управління у сфері кібербезпеки, знижує рівень правової визначеності та перешкоджає створенню сталої моделі колективної кіберстійкості, побудованої на принципах підзвітності, спільної відповідальності та технологічної прозорості.

Особливої уваги потребує нормативне закріплення механізмів державно-приватної взаємодії, які у провідних державах світу становлять основу ефективного кіберзахисту. Недостатня правова деталізація таких механізмів в Україні ускладнює координацію дій між державними та недержавними суб'єктами, створює прогалини у розмежуванні повноважень і відповідальності, а також гальмує процес інституціоналізації партнерських форматів типу ISAC/CSIRT. Це, у свою чергу, негативно позначається на своєчасності виявлення та атрибуції кібератак, обмежує можливості доказування у справах, пов'язаних із кіберзлочинами, і створює ризики порушення принципу належної обачності (due diligence) у транскордонних інцидентах.

Не менш важливим викликом залишається необхідність забезпечення належного балансу між безпековими інтересами держави та дотриманням прав і свобод людини у цифровому середовищі. Цей баланс визначає легітимність державної кіберполітики та її відповідність міжнародно-правовим стандартам, що формують основу поліцентричного режиму глобальної кібербезпеки, у межах якого Україна виступає не лише об'єктом, а й активним суб'єктом нормотворення, партнерства та колективного реагування.

Геополітичний курс України на інтеграцію до Європейського Союзу та Північноатлантичного альянсу зумовлює необхідність глибокої гармонізації національної системи кібербезпеки з acquis ЄС і нормативно-організаційними стандартами євроатлантичної спільноти. У цьому контексті особливої актуальності набуває узгодження правової, інституційної та технічної бази з положеннями директив і регламентів NIS2, DORA, CRA, а також впровадження принципів ризик-орієнтованого управління, інцидент-репортингу, сертифікації та спільних процедур реагування. Водночас відсутність єдиного координаційного центру та чітко визначених механізмів державно-приватного партнерства обмежує ефективність реагування на кіберзагрози, знижує потенціал превенції та ускладнює формування довгострокової, інституційно узгодженої системи кіберстійкості.

Зазначені обставини обумовлюють потребу у комплексному науковому осмисленні кібербезпеки як системоутворювального елемента національної безпеки України, що інтегрує правові, інституційні, технологічні та управлінські виміри. Особливої наукової ваги набуває розроблення концептуально-правових засад функціонування національної системи кіберзахисту, ідентифікація її інституційних вразливостей, адаптація євроатлантичних моделей до українського контексту, а також формування правових механізмів державно-приватної взаємодії у сфері кібербезпеки.

Таким чином, обрана тема дисертаційного дослідження має подвійний вимір значущості: теоретичний – як внесок у розвиток національної доктрини кіберправа та формування методологічної бази публічно-правового регулювання цифрової безпеки; та практичний – як інструмент удосконалення державної політики у сфері кіберзахисту, підвищення кіберстійкості критичної інфраструктури й забезпечення реалізації національних інтересів України в умовах гібридної війни та глобальної цифрової взаємозалежності.

Наукове завдання, за розв'язання якого здобувач заслуговує присудження наукового ступеня полягає у всебічному теоретико-правовому аналізі системи кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки, визначенні закономірностей її розвитку в умовах гібридної агресії проти України, виявленні ключових інституційно-правових вразливостей і напрямів підвищення кіберстійкості держави, а також у розробленні науково обґрунтованих пропозицій щодо вдосконалення національної моделі правового регулювання та інституційного забезпечення кіберзахисту з урахуванням євроатлантичних підходів.

На основі проведеного дослідження сформовано ряд нових наукових положень і висновків, які розв'язують важливу наукову проблему; **найсуттєвішими науковими результатами, які одержав здобувач особисто та які характеризуються достовірністю та науковою новизною, є такі:**

– вперше сформульовано авторське інтегральне визначення поняття «кібербезпека» як стану й безперервного процесу забезпечення стійкого, правомірного та етично врегульованого функціонування цифрового середовища. Його досягнення забезпечується узгодженою взаємодією технологічних засобів, управлінських процедур, правових механізмів і поведінкових норм, спрямованих на захист даних, цифрових сервісів, інфраструктур, соціальних відносин та публічних функцій держави з гарантією їх відновлюваності у разі порушень. Запропоноване визначення інтегрує технічний, управлінський, правовий та етичний виміри у єдину комплексну модель кіберстійкості, що виходить за межі вузько технократичного трактування безпеки;

– вперше розроблено інтегровану методологічну модель кібербезпеки, яка поєднує ієрархічну структуру референтних об'єктів захисту (дані – сервіси – інфраструктури – соціальні відносини – публічні функції держави) та аналітичну типологію кіберагресії за моделлю «цілі – інструменти – очікувані ефекти». У сукупності ці складники формують єдину систему оцінювання взаємозв'язку між об'єктами кіберзахисту, характером кібервпливів та відповідними правовими режимами реагування, забезпечуючи методологічну цілісність аналізу кібероперацій;

– вперше запропоновано системну модель адаптації євроатлантичних підходів до української правової системи у сфері кібербезпеки, вибудувану за чотирма взаємопов'язаними напрямами – кодифікаційним, гармонізаційним, інституційним і концептуально-принциповим. Модель визначає

послідовність правових, організаційних та методологічних кроків для імплементації європейських стандартів управління кіберризиками та забезпечує узгодженість національної системи кібербезпеки з євроатлантичними принципами спільної відповідальності, прозорості та стійкості.

Практичне значення отриманих результатів полягає в тому, що сформульовані та обґрунтовані в дисертаційному дослідженні висновки, наукові положення й конкретні пропозиції мають прикладне значення для вдосконалення системи правового, організаційного та інституційного забезпечення кібербезпеки України, а також для гармонізації національної політики з євроатлантичними стандартами. Результати дослідження вже використовуються та можуть бути використані у:

– *науково-дослідній сфері* – як теоретико-методологічна основа для подальших досліджень питань правового регулювання цифрової безпеки, міжнародного кіберправа та публічного управління у сфері кіберзахисту (акт впровадження Науково-дослідного інституту публічного права);

– *правотворчій діяльності* – під час доопрацювання законопроєкту №14150 «Про державно-приватну взаємодію у сфері кібербезпеки», підготовки змін до законів України «Про основні засади забезпечення кібербезпеки України» та «Про критичну інфраструктуру», а також у процесі розроблення підзаконних актів щодо координації дій суб'єктів кіберзахисту;

– *правозастосовній діяльності* – для підвищення ефективності управління кіберризиками, розвитку публічно-приватного партнерства, створення механізмів обміну інформацією між державними та приватними структурами, а також оптимізації процедур реагування на кіберінциденти;

– *освітньому процесі* – під час викладання навчальних дисциплін «Інформаційні технології у науково-правових дослідженнях», «Проблеми публічно-правового регулювання системи правоохоронних органів в Україні» (акт впровадження Науково-дослідного інституту публічного права), а також при підготовці навчально-методичних матеріалів для програм підвищення кваліфікації державних службовців і фахівців з цифрової та національної безпеки.

Достовірність і обґрунтованість наукових положень, висновків та рекомендацій забезпечується:

– комплексним застосуванням раціональної сукупності дослідницьких методів пізнання соціальних процесів і явищ у сферах дії держави та права для аналізу і характеристики нормативно-правових актів і наукових праць, присвячених теоретичним, нормативним і практичним аспектам правових, інституційних та організаційних механізмів формування, функціонування й розвитку системи кібербезпеки України у взаємозв'язку з міжнародними стандартами та практиками;

– застосуванням методологічних принципів об'єктивності і неупередженості аналізу та критичного осмислення досліджуваного матеріалу;

– аргументованою науковою полемікою з іншими вченими в тексті дисертації;

– використанням положень чинного законодавства України, а також офіційних аналітичних і статистичних матеріалів, довідкових видань та юридичної публіцистики;

– послідовністю та логікою викладення здобувачем матеріалу, його аргументованістю;

– відповідністю висновків роботи і отриманих результатів поставленим завданням та доведенням сформульованих пропозицій до рівня їх можливого використання у практиці;

– рівнем репрезентативності емпіричного матеріалу.

Особистий внесок здобувача. Наукові положення та узагальнення, які не мають посилання на джерела інформації розроблено автором особисто. Усі положення наукової новизни та висновки дисертаційного дослідження сформовані автором самостійно. У співавторстві з Сорокою Л. підготовлено статтю «Міжнародно-правові принципи регулювання кіберпростору: суверенітет, невтручання та Due Diligence», в якій автором здійснено системне порівняння підходів до поняття суверенітету в кіберпросторі, а також сформовано загальні висновки. Усі інші публікації є результатом самостійної роботи автора.

Апробація матеріалів дисертації. Основні положення, результати та висновки дисертаційного дослідження були апробовані на науково-практичних конференціях: «Проблемні питання юридичної науки в контексті реформування правової системи України» (м. Київ, 19–20 жовтня 2022 р.), «Актуальні проблеми імплементації наукових досягнень у практичну діяльність» (м. Київ, 4–5 червня 2024 р.), «Перспективні напрямки розвитку юридичної науки у 21-му сторіччі» (м. Київ, 18–19 лютого 2025 р.), «Актуальні питання науки і практики та шляхи їх вирішення» (м. Київ, 4–5 червня 2025 р.).

Публікації. Основні результати дисертації, висновки та пропозиції знайшли своє відображення у восьми наукових публікаціях, з яких три одноосібних статті та одна у співавторстві (з Сорокою Л.) – у наукових виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, чотири – тези доповідей і повідомлень на міжнародних науково-практичних конференціях.

Наукові праці Колесника О.О., опубліковані за результатами дисертаційного дослідження, відповідають вимогам п.п. 8 і 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

Всі представлені наукові публікації здобувача зараховуються за темою дисертації, а саме:

1. Колесник О.О. Теоретико-правові засади формування та еволюції поняття кібербезпеки. Юридичний науковий електронний журнал. 2024. № 7. С. 636–641. DOI: https://doi.org/10.32782/2524-0374/2024-7/154

2. Колесник О.О. Нормативно-інституційні засади формування національної системи кібербезпеки України. *Право та державне управління*. 2025. № 1. С. 437–445. DOI: https://doi.org/10.32782/pdu.2025.1.61

3. Колесник О.О. Міжнародні стандарти та українська практика кіберзахисту: уроки війни. *Правові новели*. 2025. № 25. С. 375–382. DOI: https://doi.org/10.32782/ln.2025.25.48

4. Сорока Л.В., ***Колесник О.О.*** Міжнародно-правові принципи регулювання кіберпростору: суверенітет, невтручання та Due Diligence. *Держава та регіони*. Серія: Право. 2025. № 1. С. 246–253. DOI: https://doi.org/10.32782/1813-338X-2025.1.35

Оцінка мови і стилю дисертації. Дисертація написана науковим стилем, українською мовою. Наукові положення, висновки та рекомендації викладені стисло, точно, ясно та просто, що забезпечує легкість і доступність їх сприйняття.

Відповідність дисертації встановленим вимогам і визначеній спеціальності. Форма і зміст дисертації та анотації відповідають вимогам, що встановлені Порядком підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженим постановою Кабінету Міністрів України від 23 березня 2016 р. № 261, Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженим постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 та Вимогам до оформлення дисертації, затвердженим наказом Міністерства освіти і науки України від 12 січня 2017 року № 40.

Дисертація є цілісною, завершеною, кваліфікованою працею, в якій містяться висунуті здобувачем науково обґрунтовані теоретичні і практичні результати та наукові положення, що характеризуються єдністю змісту і свідчать про особистий внесок здобувача в юридичну науку.

Анотація дисертації є узагальненим коротким викладом її основного змісту. В анотації стисло представлені основні результати дослідження із зазначенням наукової новизни та практичного значення, що дає повне уявлення про виконану здобувачем роботу. Обсяг дисертації та анотації, а також зміст роботи відповідають встановленим вимогам.

Адміністративно-правові засади участі громадян у процесі прийняття рішень у сфері охорони навколишнього природного середовища є напрямом, який віднесено до спеціальності 081 «Право».

УХВАЛИЛИ:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Колесника Олександра Олександровича на

тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід».

2. Констатувати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів Колесника Олександра Олександровича відповідає спеціальності 081 «Право» та вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 та Вимогам до оформлення дисертації, затвердженим наказом Міністерства освіти і науки України від 12 січня 2017 року № 40.

3. Рекомендувати дисертацію Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» до захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 081 «Право».

Результати голосування присутніх на засіданні докторів та кандидатів наук за профілем поданої на розгляд дисертації: за – 11, проти – 0, таких, що утримались – 0; здобувач Колесник О.О. – не голосував.

Головуючий на засіданні –
доктор юридичних наук, професор,
завідувач відділу
Науково-дослідного інституту
публічного права  **С.С. Овчарук**