

## РЕЦЕНЗІЯ

**доктора юридичних наук, професора Боровика Андрія Володимировича 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.** Тема дисертаційної роботи Колесника Олександра Олександровича є актуальною та відповідає сучасним науковим і практичним потребам держави у сфері національної безпеки. В умовах триваючої гібридної агресії проти України питання правового забезпечення кібербезпеки набувають стратегічного значення, оскільки кіберпростір став одним із ключових середовищ ведення сучасних конфліктів. Зазначені обставини обумовлюють необхідність комплексних наукових досліджень, здатних запропонувати системний погляд на правові, інституційні й організаційні засади кіберзахисту.

Дисертантом обґрунтовано, що національна система кібербезпеки потребує подальшого нормативного та інституційного вдосконалення, зокрема в частині узгодження компетенцій суб'єктів сектору безпеки, удосконалення механізмів державно-приватної взаємодії, а також адаптації європейських стандартів та практик. Належно висвітлено взаємозв'язок тематики роботи з потребами євроінтеграційного курсу України та імплементації *acquis* ЄС у сфері кіберзахисту.

Таким чином, актуальність теми не викликає сумнівів і цілком відповідає сучасному стану розвитку правової науки та потребам державної політики безпеки.

### **Оцінка наукового рівня дисертації і наукових публікацій здобувача.**

Дисертаційне дослідження вирізняється логічною структурованістю, послідовністю викладення матеріалу та узгодженістю між поставленою метою, завданнями, методологічною базою та отриманими результатами. Автор демонструє здатність працювати з великим обсягом різномірних джерел, насамперед законодавчих і підзаконних актів України, міжнародно-правових

документів, аналітичних матеріалів міжнародних організацій, а також значного масиву наукової літератури, що забезпечує належний рівень обґрунтованості висновків.

Позитивною рисою роботи є поєднання теоретико-правового аналізу з дослідженням практичного виміру кіберзагроз, зокрема їх проявів у період гібридної агресії проти України. Дисертантом запропоновано низку концептуальних положень, що характеризуються ознаками наукової новизни: уточнено дефініційний апарат, сформовано ієрархію референтних об'єктів кіберзахисту, розроблено типологію кіберагресії, запропоновано алгоритмізовані підходи до аналізу кібератак, а також обґрунтовано напрямні адаптації євроатлантичних моделей до українського правового поля з урахуванням національних інституційних і управлінських особливостей.

Разом із тим, дослідження зберігає баланс між теоретичною компонентною і практичною значущістю: результати можуть бути використані у нормотворчій діяльності, підготовці стратегічних документів, удосконаленні інституційних механізмів кіберзахисту та розвитку державно-приватного партнерства.

Наукові публікації здобувача відповідають встановленим вимогам до дисертаційних робіт на здобуття ступеня доктора філософії та належним чином відображають основні положення проведеного дослідження. Результати дисертаційної роботи опубліковано у восьми наукових працях, серед яких — чотири статті у фахових виданнях, включених до Переліку МОН України, а також чотири тези доповідей, представлених на всеукраїнських науково-практичних конференціях. Тематика цих публікацій повністю відповідає змісту дисертації, засвідчує системність наукової роботи здобувача та достатню апробацію отриманих результатів.

**Новизна представлених теоретичних та/або експериментальних результатів проведених здобувачем досліджень, повнота викладу в опублікованих працях.** Наукова новизна дисертаційного дослідження Колесника Олександра Олександровича полягає у формуванні комплексного теоретико-правового підходу до кібербезпеки як складової системи національної та

міжнародної безпеки. У роботі запропоновано низку положень, що мають ознаки наукової новизни: сформульовано інтегральне визначення поняття «кібербезпека», розроблено ієрархічну модель референтних об'єктів кіберзахисту, представлено аналітичну типологію кіберагресії та верифікаційний каркас аналізу кібератак, а також обґрунтовано системну модель адаптації євроатлантичних підходів до національного правового поля. Удосконалено теоретико-методичні підходи до аналізу кіберстійкості, нормативно-правового регулювання кібероперацій та порівняльно-правового дослідження державно-приватної взаємодії. Подальшого розвитку набули питання побудови правової архітектури кібербезпеки України, періодизації кіберагресії РФ, ідентифікації вразливостей критичної інфраструктури та переходу до проактивних моделей кіберзахисту. Представлені результати є концептуально узгодженими, належно обґрунтованими та мають прикладне значення для вдосконалення правового забезпечення кібербезпеки.

У дисертації міститься також низка додаткових положень і практичних рекомендацій, що підтверджують цілісність, завершеність і наукову значущість проведеного дослідження.

**Наукова обґрунтованість отриманих результатів, наукових положень, висновків і рекомендацій, сформульованих у дисертації.** Наукові результати, отримані Колесником Олександром Олександровичем, характеризуються високим рівнем обґрунтованості, логічною послідовністю та методологічною виваженістю. Дисертаційне дослідження базується на системному аналізі широкого кола джерел: міжнародно-правових актів ООН, ОБСЄ, Ради Європи та Європейського Союзу, законодавства України у сфері національної та інформаційної безпеки, стратегічних документів з кіберзахисту, а також значного масиву наукових праць вітчизняних та зарубіжних авторів. Використання такої багатовимірної джерельної бази забезпечило глибину та достовірність отриманих висновків і дало можливість ґрунтовно дослідити правові, інституційні й організаційні аспекти функціонування національної системи кібербезпеки.

У роботі простежується чітка логіка переходу від загальнотеоретичного аналізу феномену кібербезпеки до прикладних рекомендацій щодо вдосконалення нормативної, інституційної та управлінської складових національного механізму кіберзахисту. Висновки кожного розділу безпосередньо корелюють із поставленими завданнями, що свідчить про належну методологічну узгодженість та завершеність дослідження.

Дисертант послідовно розкрив закономірності розвитку національної системи кібербезпеки, обґрунтував її структурні й функціональні характеристики, визначив ключові вразливості та проблеми інституційного середовища, а також охарактеризував специфіку кіберагресії в умовах гібридної війни проти України. Аргументація спирається на аналіз реальних кіберінцидентів, офіційних даних, стратегічних документів та міжнародних підходів, що забезпечує належний рівень об'єктивності та достовірності висновків.

Важливою складовою наукової обґрунтованості є ретельний аналіз євроатлантичних нормативних моделей, що дав можливість сформулювати виважені рекомендації щодо їх адаптації до національного правопорядку. Запропоновані у роботі пропозиції щодо вдосконалення законодавства, інституційної архітектури та механізмів державно-приватної взаємодії ґрунтуються на зіставленні міжнародних стандартів із поточним станом української системи кібербезпеки.

У дисертації збережено внутрішню наукову логіку: від аналізу дефініцій та концепцій – до кваліфікації кібероперацій у міжнародно-правовому вимірі та формулювання конкретних, практично спрямованих рекомендацій. Сформульовані висновки вирізняються теоретичною узгодженістю та мають прикладну цінність для нормотворчої діяльності, стратегічного планування та розвитку державної політики у сфері кібербезпеки й кіберстійкості держави.

У цілому наукові положення та рекомендації, сформульовані у дисертації, є належним чином аргументованими, послідовними та такими, що відповідають сучасним науковим підходам і практичним потребам удосконалення національної системи кіберзахисту.

**Рівень виконання поставленого наукового завдання, оволодіння здобувачем методологією наукової діяльності.** Дисертаційна робота Колесника Олександра Олександровича засвідчує достатньо високий рівень сформованості науково-дослідницьких компетентностей та глибоке оволодіння методологією сучасних правових досліджень. Автор продемонстрував уміння коректно добирати й послідовно застосовувати методи, релевантні меті, завданням, об'єкту та предмету дисертації, що забезпечило комплексність і внутрішню логічну цілісність проведеного дослідження.

У роботі використано широкий спектр загальнонаукових та спеціально-юридичних методів, які застосовано взаємопов'язано та послідовно. Діалектичний підхід дозволив розкрити кібербезпеку як динамічне соціотехнічне явище та виявити закономірності її розвитку в умовах гібридної агресії. Методи аналізу та синтезу забезпечили структурне опрацювання нормативних, інституційних, технологічних і організаційних елементів системи кіберзахисту та інтеграцію їх у цілісну модель кіберстійкості. Формально-юридичний метод став основою для ґрунтовного аналізу законодавства України у сфері кібербезпеки та оцінки його відповідності міжнародно-правовим стандартам. Системно-структурний метод сприяв визначенню інституційної архітектури національної системи кіберзахисту, встановленню взаємозв'язків між її суб'єктами та оцінці їх функціональної взаємодії. Важливу роль відіграв порівняльно-правовий метод, що дав можливість комплексно проаналізувати євроатлантичну нормативну екосистему, виокремити її ключові характеристики та окреслити напрями адаптації цих підходів до українського контексту. Функціональний метод забезпечив дослідження практичних аспектів реалізації державної політики у сфері кібербезпеки, механізмів реагування на кіберінциденти та взаємодії суб'єктів безпекового сектору. Логіко-семантичний метод дозволив уточнити зміст базових дефініцій, забезпечивши термінологічну чіткість та узгодженість дослідження. Застосування історико-правового методу дало можливість простежити етапи становлення національної системи кібербезпеки та виявити чинники, що впливали на її розвиток. Метод правового прогнозування став підґрунтям для формування

обґрунтованих пропозицій щодо вдосконалення нормативно-правового регулювання та інституційних механізмів кіберзахисту.

Послідовне та коректне застосування методологічного інструментарію свідчить про належний рівень наукової підготовки здобувача та його здатність здійснювати самостійне комплексне дослідження високого наукового рівня. Таким чином, виконання наукового завдання відзначається методологічною виваженістю, внутрішньою узгодженістю та повним оволодінням здобувачем інструментами наукової діяльності, що відповідає вимогам до дисертаційних робіт на здобуття ступеня доктора філософії.

**Теоретичне і практичне значення результатів дослідження.** Результати дисертаційного дослідження Колесника Олександра Олександровича мають вагоме теоретичне й практичне значення з огляду на стратегічну важливість кібербезпеки для сучасної системи національної безпеки України. У теоретичному вимірі робота формує цілісне концептуальне бачення кібербезпеки як комплексного правового та інституційного феномену, що визначає здатність держави забезпечувати стійкість своїх інститутів, критичної інфраструктури та публічних сервісів в умовах гібридних загроз. Запропоновані в дисертації визначення, моделі та типології — інтегральне розуміння кібербезпеки, ієрархія референтних об'єктів кіберзахисту, класифікація кіберагресії, підходи до кваліфікації кібероперацій — розширюють теоретичні засади національної доктрини безпеки та поглиблюють методологічну основу дослідження правових і управлінських аспектів цифрових загроз.

Практичне значення роботи безпосередньо корелює з актуальними завданнями державної політики у сфері національної безпеки. Сформульовані дисертантом пропозиції щодо вдосконалення законодавства, оптимізації інституційної архітектури кіберзахисту, підвищення кіберстійкості критичної інфраструктури, упорядкування механізмів державно-приватної взаємодії, а також адаптації євроатлантичних стандартів можуть бути використані органами державної влади під час розроблення стратегічних документів і нормативних актів. Значущим є й практичний потенціал моделі переходу до проактивної

системи кіберзахисту, яка ґрунтується на стандартизованому обміні даними, своєчасному інцидент-менеджменті та узгодженій взаємодії між суб'єктами сектору безпеки й оборони.

Отже, результати дослідження поглиблюють наукове розуміння кібербезпеки як складової національної безпеки та публічного управління і водночас мають прикладне значення для вдосконалення підходів до формування й реалізації державної політики у сфері протидії сучасним кіберзагрозам.

**Оцінка змісту дисертації, її завершеності в цілому.** Дисертаційна робота Колесника Олександра Олександровича є цілісним, концептуально завершеним дослідженням, що відповідає сучасним вимогам до дисертацій на здобуття ступеня доктора філософії за спеціальністю 081 «Право» та відображає комплексність проблематики кібербезпеки у системі національної безпеки. Авторіві вдалося не лише всебічно розкрити теоретичні засади кіберзахисту, а й інтегрувати їх у ширший контекст національної безпеки, що додає дослідженню міждисциплінарної узгодженості та практичної релевантності.

Структура дисертації є логічною та збалансованою: у трьох розділах послідовно охоплено теоретичні засади кібербезпеки, інституційно-правову характеристику національної системи кіберзахисту та аналіз міжнародних і євроатлантичних підходів з урахуванням їх адаптації до умов України. Такий підхід забезпечує чіткий перехід від проблематики концептуального рівня до аналізу реального функціонування системи національної безпеки у її кіберкомпоненті, а також до вироблення конкретних рекомендацій з її вдосконалення.

Усі дослідницькі завдання, визначені у вступі, реалізовані у повному обсязі. У кожному розділі наведено проміжні висновки, які логічно пов'язані з підсумковими положеннями дисертації. Робота вирізняється ретельним опрацюванням наукових джерел, нормативно-правових актів та аналітичних матеріалів, що формують надійну базу для аргументації висновків і рекомендацій. Значна увага приділена аналізу кібератак 2014–2024 рр., який посилює прикладну

спрямованість дослідження та демонструє розуміння здобувачем реальних загроз у сфері кібербезпеки України.

Дисертація містить комплексні теоретичні положення та практичні рекомендації, релевантні сучасним викликам національної безпеки, що свідчить про її завершеність, логічну цілісність та відповідність академічним стандартам. Робота може бути використана як науково-методичне підґрунтя для подальших досліджень, для формування державної політики у сфері кіберзахисту, а також при підготовці фахівців з безпекових та правових дисциплін.

**Рекомендації щодо подальшого використання результатів дисертації в практиці.** Результати дисертаційного дослідження Колесника Олександра Олександровича мають значний практичний потенціал та можуть бути використані у діяльності державних органів, суб'єктів сектору безпеки й оборони, об'єктів критичної інфраструктури, а також у науково-освітньому середовищі.

Запропоновані у дисертації положення та рекомендації становлять практичну цінність для вдосконалення нормативно-правового забезпечення кібербезпеки, зокрема під час доопрацювання законопроектів і підзаконних актів у сфері кіберзахисту, захисту критичної інфраструктури, інцидент-менеджменту та державно-приватної взаємодії. Напрацьовані автором підходи можуть бути використані у процесі гармонізації національного законодавства з євроатлантичними стандартами, а також як методична основа для розроблення та уточнення механізмів координації між суб'єктами національної системи кібербезпеки й побудови узгодженої моделі реагування на кіберінциденти.

Положення щодо інституціоналізації державно-приватного партнерства мають прикладне значення для підвищення ефективності протидії гібридним загрозам. Вони можуть бути використані центральними органами виконавчої влади, регуляторними органами, органами місцевого самоврядування та суб'єктами критичної інфраструктури під час розроблення внутрішніх політик кібербезпеки, а також для оптимізації міжінституційної взаємодії та координації дій.

Матеріали дисертації доцільно використовувати у навчальних програмах юридичних спеціальностей, пов'язаних із проблематикою національної безпеки та публічного управління, зокрема під час викладання дисциплін, що охоплюють правове забезпечення безпеки держави, кібербезпеку, організаційно-правові засади діяльності суб'єктів сектору безпеки й оборони, а також окремі міжнародно-правові аспекти протидії гібридним загрозам.

Результати дослідження можуть слугувати методичною та аналітичною основою для підготовки фахівців у галузі національної безпеки, публічного адміністрування та права, які безпосередньо залучені до формування, реалізації й координації державної політики у сфері кіберзахисту, розроблення нормативних і підзаконних актів, а також організації взаємодії між органами державної влади, органами місцевого самоврядування та суб'єктами приватного сектору.

Таким чином, положення, отримані у дисертації, мають виразну практичну релевантність і здатні сприяти вдосконаленню адміністративно-правових та організаційних механізмів забезпечення національної безпеки, підвищенню ефективності публічного управління у сфері кіберзахисту, зміцненню кіберстійкості держави та розвитку інституційної спроможності органів влади реагувати на сучасні цифрові та гібридні загрози.

**Зауваження щодо оформлення та змісту дисертації, запитання до здобувача.** Позитивно оцінюючи результати виконаного Колесником Олександром Олександровичем дослідження та підкреслюючи його наукову й практичну значущість для сфери національної безпеки, варто водночас звернути увагу на окремі аспекти, що можуть викликати дискусію:

1) у підпункті 1.1 подано розгорнутий огляд міжнародної доктрини кібербезпеки, тоді як еволюція українських дефініцій представлена значно стисло. Це ускладнює простеження логіки формування національного понятійного апарату, зокрема впливу ранніх нормативних актів та особливостей розвитку вітчизняної терміносистеми. У результаті українська доктрина виглядає менш цілісно окресленою порівняно з міжнародною;

2) у підрозділі 3.2 автор детально окреслює розвиток міжнародних механізмів координації у сфері кібербезпеки. Водночас питання внутрішніх процедур контролю, аудиту та моніторингу кіберризиків подано значно стисло. Це частково ускладнює оцінку реалістичності інтеграційних пріоритетів, запропонованих автором, оскільки ефективність зовнішньої взаємодії безпосередньо залежить від стійкості внутрішньої інституційної архітектури;

3) підрозділ 3.3 містить ґрунтовний аналіз широкого спектра міжнародних моделей державно-приватного партнерства у сфері кібербезпеки. Водночас, подання окремих нормативних положень видається дещо перенасиченим деталями, що ускладнює швидке порівняння підходів різних юрисдикцій. Доцільним було б додання узагальнювальної таблиці. Такий формат сприяв би більш наочному зіставленню та полегшив би сприйняття матеріалу;

4) у тексті дисертації простежується активне використання окремих термінів та конструкцій англomовного походження (зокрема “collaborative cyber defence”, “shared responsibility” та ін.), що є обґрунтованим з огляду на міжнародний і міждисциплінарний характер проблематики кібербезпеки. Водночас у деяких фрагментах спостерігається певна насиченість тексту такими англomовними термінами, що може ускладнювати стилістичну цілісність викладу.

Зазначені зауваження та рекомендації мають дискусійний характер і не знижують загалом високого теоретико-методологічного рівня та практичної значущості представленого до захисту дисертаційного дослідження.

**Відсутність порушень академічної доброчесності.** Під час аналізу дисертаційного дослідження Колесника Олександра Олександровича та його наукових публікацій не встановлено фактів порушення академічної доброчесності, зокрема плагіату, самоплагіату, фабрикації чи фальсифікації даних. Текст роботи є оригінальним, логічно структурованим і свідчить про самостійність наукового пошуку. Дисертація відповідає вимогам академічної етики, містить коректні посилання на джерела та демонструє доброчесний підхід автора до опрацювання матеріалу.

**Висновок про відповідність дисертації встановленим вимогам.**

Дисертація Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» є завершеною, самостійно виконаною кваліфікованою науковою працею, що має значне теоретичне і практичне значення для розвитку правового забезпечення національної безпеки та кіберзахисту.

Робота відповідає спеціальності 081 «Право», вимогам Порядку присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а також Вимогам до оформлення дисертацій, затвердженим наказом Міністерства освіти і науки України від 12 січня 2017 р. № 40.

З огляду на наукову новизну, обґрунтованість висновків, практичну значущість результатів та відповідність установленим критеріям, автор дисертації – Колесник Олександр Олександрович – заслуговує на присудження ступеня доктора філософії у галузі знань 08 «Право» за спеціальністю 081 «Право».

**Рецензент –**

**віце-президент з наукової роботи**

**Науково-дослідного інституту публічного права**

**доктор юридичних наук, професор**



**Андрій БОРОВИК**