ВІДГУК
офіційного опонента
доктора юридичних наук, професора
Новицької Наталії Борисівни
на дисертацію **Криволапа Євгенія Володимировича**
на тему:
«АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ У СФЕРІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ»,
представлену на здобуття ступеня доктора філософії
зі спеціальності 081 «Право»

Актуальність дисертаційної роботи. Актуальність теми адміністративно-правового забезпечення кібербезпеки України зумовлена насамперед умовами повномасштабної збройної агресії, де кіберпростір став повноцінним доменом ведення бойових дій. Постійні атаки на об'єкти критичної інформаційної інфраструктури, державні реєстри та системи управління вимагають не лише технічного захисту, а й чіткої нормативної бази, яка б регулювала взаємодію суб'єктів кібербезпеки. Адміністративне право у цьому контексті виступає фундаментом для визначення повноважень державних органів, встановлення протоколів швидкого реагування на інциденти та запровадження дієвих механізмів контролю, що безпосередньо впливає на національну стійкість держави.

Крім того, євроінтеграційні прагнення України вимагають інтенсивної адаптації національного законодавства до стандартів ЄС. Сучасний етап характеризується динамічною трансформацією цифрових послуг та масовою диджиталізацією державного сектору, що створює нові виклики для захисту персональних даних та правопорядку в мережі. Оптимізація адміністративно-правових інструментів є необхідною для створення прозорої системи відповідальності та залучення приватного сектору до спільної оборони кіберпростору, оскільки застарілі підходи вже не здатні ефективно протидіяти гібридним загрозам цифровій суверенності країни.

Варто відзначити, що наявні нормативно-правові інструменти часто відстають від темпів розвитку цифрових технологій, що створює прогалини у координації між суб'єктами кібербезпеки. Обмеженість узгоджених процедур,

стандартизованих підходів та належного контролю знижує загальну стійкість національного кіберпростору. Тому вдосконалення адміністративно-правового управління у сфері кіберзахисту є необхідною умовою підвищення ефективності державної політики безпеки та протидії сучасним кіберзагрозам.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження здійснене відповідно до тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року, затверджених постановою КМУ від 07.09.2011 № 942 (із змінами, внесеними постановою КМУ від 09.05.2023 № 463); Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затверджених постановою КМУ від 30.04.2024 № 476; Указу Президента України «Про цілі сталого розвитку України на період до 2030 року» від 30.09.2019 № 722/2019, а також у межах плану наукових досліджень Факультету права та міжнародних відносин Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» (при виконанні робіт – Національний авіаційний університет), зокрема, кафедри конституційного та адміністративного права, теми: «Забезпечення конституційних прав громадян в контексті конвенційних зобов'язань України» (державний реєстраційний номер 0119U103091); «Людиноцентричність публічного права України» (державний реєстраційний номер 0124U003363) та держбюджетної науково-дослідної роботи № 312-ДБ20 «Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України: теорія і практика» (державний реєстраційний номер 0120U102136).

Ступінь обґрунтованості наукових положень, висновків і рекомендацій. Наукові положення, висновки та рекомендації, які містяться в дисертаційні роботі **Криволапа Євгенія Володимировича**, характеризуються належним рівнем обґрунтованості, що ґрунтується на системному аналізі нормативно-правової бази, сучасних підходів до

державного управління кібербезпекою та актуальних наукових досліджень у цій сфері. Рекомендації автора є логічно вивіреними та узгодженими з отриманими результатами, а також відповідають реальним потребам удосконалення адміністративно-правових механізмів забезпечення кіберзахисту. Обґрунтованість запропонованих положень підтверджується коректним використанням методів наукового аналізу, порівняння, узагальнення та моделювання, що дозволяє вважати висновки логічними та переконливими. Методологічний підхід автора повністю відповідає сучасним вимогам і забезпечує належний рівень обґрунтованості отриманих результатів.

Запропоновані автором висновки та практичні рекомендації мають системний і комплексний характер, що підсилює їхню наукову та прикладну цінність у сфері державного управління кібербезпекою.

Загалом ступінь обґрунтованості наукових положень можна оцінити як достатньо високий, оскільки вони базуються на актуальних емпіричних даних, аналітичних матеріалах та ретельному вивченні проблематики кіберзахисту на національному рівні.

Метою дисертаційної роботи визначено розкриття сутності і змісту адміністративно-правових засад спрямування методів і засобів забезпечення кібернетичної безпеки на вирішення завдань забезпечення інформаційної та кібер- безпеки, поставлених у Стратегії від 15.10.2021 р. інформаційної безпеки та Стратегії від 14.05.2021 р. кібербезпеки України, затверджених Указами Президента України від 28.12.2021 р. № 685/2021 та від 26.08.2021 р. № 447/2021 відповідно.

Наукові завдання дослідження логічно та структурно узгоджені між собою, а їх кількість є достатньою для розкриття тематики та досягнення поставленої мети. Ознайомлення з дисертацією дозволяє стверджувати, що визначена мета досягнута, а поставлені завдання виконані в повному обсязі.

Особливої уваги заслуговують мова, стиль і логічність викладення матеріалу. Текст написано грамотно, а спосіб подання теоретичних положень, висновків і рекомендацій забезпечує їхню зрозумілість та доступність.

Наукова новизна дисертаційного дослідження. Наукові положення, висновки й рекомендації, запропоновані автором, є переконливими та добре обґрунтованими. Найбільш значущими серед них є:

- системне обґрунтування проблеми адміністративно-правового забезпечення діяльності у сфері кібербезпеки України на засадах міждисциплінарного підходу, що інтегрує засоби, методи та принципи адміністративного права, інформаційного права, права кібербезпеки, теорії психологічних впливів та деліктології;

– розкриття реалізації владних повноважень публічної адміністрації у сфері кібербезпеки крізь призму адміністративно - правових зобов'язань, що охоплюють здійснення публічного управління, надання адміністративних послуг, визначення відповідності публічної адміністрації у разі неправомірних дій чи порушення діяльності за її діяльністю, а також відповідальності суб'єктів суспільства;

- введення в український правовий науковий обіг Закон Європейського Союзу про кіберстійкість (Cyber Resilience Act, CRA), спрямований на підвищення рівня кібербезпеки та кіберстійкості шляхом встановлення єдиних стандартів захисту продуктів із цифровими елементами; здійснення дослідження його ключових положень та визначення їх значення для формування національної правової доктрини у сфері кібербезпеки;

– пропозиції щодо: поширення вимоги Закону України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет як потенційні точки входу для кібератаки та включення законодавчого регулювання сутності і змісту Стратегії зовнішньополітичної діяльності України, Стратегії інформаційної безпеки, Стратегії забезпечення державної безпеки, Стратегії енергетичної безпеки в Закон України «Про національну безпеку України».

В дисертаційному дослідженні *удосконалено:*

- підходи до вивчення кіберконфліктів, розуміння сутності поняття «кіберконфлікт», взаємозв'язку між поняттями «кіберконфлікт», з одного боку, та кіберінцидент і кіберзлочин, з іншого боку;

– розуміння адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України, яке полягає у поєднанні засобів і методів адміністративного права з урахуванням технічних аспектів і технологічних небезпек в кіберпросторі, включаючи протидію вразливостям, кіберінцедентам, кіберконфліктам;

– рекомендації для підвищення ступеня інформаційної безпеки: використання надійних паролів, регулярне оновлення програмного забезпечення, використання антивірусного програмного забезпечення та брандмауера, уникнення відкриття підозрілих електронних листів, завантаження неперевіреного вмісту та переходів за сумнівними посиланнями, активація двофакторної аутентифікації, створення резервних копії, використання тільки ліцензійних та офіційних програм;

– розуміння рекомендацій Комітету Міністрів РЄ № R (89) 7 від 27.04.1989 р. «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», № R (97) 19 від 30.10.1997 р. «Про показ насильства електронними ЗМІ», № R (97) 20 від 30.10.1997 р. «Про розпалювання ненависті» як документів щодо впровадження заходів забезпечення когнітивної безпеки від інформаційно-психологічного впливу електронних засобів комунікації;

– структура інформаційних прав громадян: свобода слова; право на доступ до інформації, у тому числі право на звернення; захист персональних даних; захист інформаційної безпеки; захист прав інтелектуальної власності; право на захист від кримінальних посягань у кіберпросторі. Розкриті особливості забезпечення кожного із видів прав;

– обґрунтування заходів керівництва України щодо обмежень в інформаційно-комунікаційному середовищі країни: заборона російських соціальних мереж і сайтів; запровадження санкцій проти засобів масової

інформації із забороною їх трансляції в умовах агресивної інформаційної війни рф проти України;

дістали подальшого розвитку:

– розуміння сучасних викликів у зв'язку із широкомасштабною агресією рф проти України, яке (розуміння) полягає у тому, що у сучасних реаліях широкого впровадження нових інформаційно-комунікаційних технологій, з одного боку, і тенденцій їх використання у гібрідних війнах для завдання шкоди суб'єктам інформаційних відносин, з іншого боку, перед державою постає завдання надійного захисту кібернетичної безпеки суб'єктів та їх прав у кіберпросторі;

– періодизація запровадження системи пошуку вразливостей Bug Bounty, яка полягає у контрольованих кібератаках певних інформаційно-комунікаційних систем з метою перевірки їх стійкості до таких атак і пошуку вразливостей;

– розуміння, що українська система безпекових стратегій побудована за моделлю НАТО та ЄС, відповідно до якої (моделі) НАТО розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен;

– узагальнення встановлених Кодексом України про адміністративні правопорушення деліктів у сфері обігу інформації і використання інформаційно-комунікаційних систем;

– уявлення про дії російських/проросійських пропагандистів щодо маскування фейкової інформації під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН. Проаналізовані приклади фактичних фейкових повідомлень (сайтів);

– обґрунтування правового регулювання інтернет-ресурсів як ЗМІ; запропоноване поняття «презумпція достовірності інформації», під якою розуміється відсутність необхідності додатково перевіряти достовірність інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ.

Отримані результати вирізняються значною теоретичною цінністю та практичною значущістю; їх новизна полягає як у вперше запропонованих положеннях, так і в подальшому розвитку та вдосконаленні наявних підходів. Наукові висновки мають суттєве значення для подальшого розвитку науки адміністративного та інформаційного права.

Практична значущість роботи полягає в тому, що висунуті та теоретично обґрунтовані положення, пропозиції і висновки дослідження сприятимуть подальшому їх впровадженню у: науково-дослідній сфері ДНП «Державний університет «Київський авіаційний інститут» – як підґрунтя для подальшої розробки проблем адміністративно-правових питань комплексного забезпечення інформаційної і кібернетичної безпеки (підтверджено актом про впровадження від 01.12.2025); законотворчій діяльності Комітету Верховної Ради України з питань правоохоронної діяльності – в результаті дослідження сформульована низка пропозицій щодо удосконалення нормативно-правових актів у сфері забезпечення інформаційної і кібернетичної безпеки (підтверджено довідкою про впровадження №04-27/12-2022/214837 від 13.12.2022); правозастосовній діяльності Секретаріату Касаційного цивільного суду у складі Верхового Суду – використання одержаних результатів дозволить покращити практичну роботу забезпечення інформаційної і кібернетичної безпеки (підтверджено довідкою про впровадження від 05.12.2025), для забезпечення підвищення рівня захисту інформаційних баз даних Українською асоціацією інвестиційного бізнесу (підтверджено довідкою про впровадження від 01.12.2025); освітньому процесі Київського національного університету будівництва і архітектури – матеріали дисертації використовуватимуться під час проведення занять із дисциплін «Цифрові трансформації у суспільстві та електронне урядування», «Захист персональних даних», «Адміністративне право і процес», «Конституційне право України», «Верховенство права через призму конституційного та адміністративного права та процесу» (підтверджено актом про впровадження від 24.11.2025).

Характеристика основних положень роботи. Дисертація складається з анотацій (українською та англійською мовами), які повно відображають зміст дисертації, списку публікацій здобувача (з виділенням творчого внеску співавторів наукових статей, опублікованих у співавторстві), змісту, переліку умовних позначень, вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел та додатків. Структура дисертації **Криволапа Євгенія Володимировича** відповідає усталеним вимогам до таких праць і не викликає заперечень. Виклад змісту дисертації логічний та послідовний.

У вступі обґрунтовано актуальність обраної теми, визначено мету, завдання, об'єкт та предмет дослідження, описані використані для цього методи дослідження і коротко обґрунтовано такий вибір, розкрито наукову новизну та практичну значущість отриманих результатів, подано відомості щодо апробації отриманих результатів та їх впровадження у науково-дослідну сферу, правотворчість, правозастосовну діяльність, в навчальний процес. Відносно наукових статей, опублікованих у співавторстві, визначений творчий внесок кожного із співавторів.

Основний зміст дисертації викладений у трьох логічно пов'язаних розділах, кожен із яких послідовно розкриває окремі аспекти проблематики.

У першому розділі представлено теоретико-правовий аналіз кібернетичної безпеки як предмета адміністративного права. Автор приділяє увагу міждисциплінарному характеру правового забезпечення кібербезпеки, демонструє взаємозв'язок правових, технологічних і організаційних чинників. Значний акцент зроблено на дослідженні природи сучасних кіберзагроз, їх технологічного підґрунтя та наслідків для функціонування державних і приватних інституцій. Особливістю розділу є глибокий аналіз концептуальних засад інформаційної, кібернетичної та когнітивної безпеки з урахуванням стратегічних документів України 2020–2021 років, що дозволяє окреслити еволюцію державної політики у цій сфері та виявити її сильні й слабкі сторони.

У другому розділі дисертант зосереджується на адміністративно-правовому регулюванні заходів забезпечення кібербезпеки. Проаналізовано нормативні акти європейського рівня, зокрема директиви та регламенти у сфері кіберзахисту, стандарти NIS та інші документи, які формують сучасну політику цифрової безпеки ЄС. Паралельно досліджено національне правове поле та встановлено рівень імплементації європейських вимог, виокремлено існуючі колізії та прогалини. Важливою складовою розділу є розгляд питань публічного адміністрування у сфері протидії кіберконфліктам, визначення ролі органів державної влади, їх компетенцій та механізмів взаємодії у кризових ситуаціях.

Третій розділ присвячений аналізу забезпечення вимог інформаційної безпеки в системі кіберзахисту та захисту інформаційних прав громадян. Автор комплексно досліджує роль кібербезпеки у структурі національної безпеки, визначає ключові цілі та функціональні елементи системи кіберзахисту держави. Автор доводить, що комплексне стратегічне планування в Україні побудоване за моделлю НАТО та ЄС – НАТО розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен. Значну увагу приділено питанням захисту персональних даних, приватності, цифрових прав та гарантій громадян у контексті сучасних викликів. Розкрито структуру інформаційних прав, проблеми їх належного забезпечення та адміністративно-правові механізми відновлення порушених прав у сфері кібербезпеки. Проведений аналіз дозволяє чітко окреслити взаємозв'язок між ефективністю державної політики у сфері кіберзахисту та станом забезпечення прав людини в цифровому середовищі.

Узагальнюючи здобуті результати, слід відзначити, що дисертація має завершений науково-прикладний характер, відзначається логічною структурою, ґрунтовністю теоретичного підґрунтя та комплексним підходом до розв'язання поставлених завдань. Робота поєднує в собі аналіз правових норм, технологічних аспектів кіберзагроз, адміністративно-правових

механізмів управління та інституційного забезпечення кібербезпеки. Запропоновані висновки та рекомендації мають значну наукову й практичну цінність для вдосконалення державної політики, формування сучасної нормативно-правової бази та підвищення ефективності діяльності суб'єктів публічної влади в умовах розвитку кіберпростору. Наведені обґрунтування щодо правомірності обмежень Україною поширення телевізійного контенту і Інтернет-мереж в контексті Конвенції Ради Європи про захист прав людини і основоположних свобод 1950 року (стаття 10).

Кожен розділ роботи забезпечений висновками, що повністю відповідають змісту і науковим результатам розділу.

Наукові результати роботи узагальнені у висновках по роботі в цілому.

Список використаних літературних джерел нараховує 366 джерел, з яких 314 найменувань – кирилицею і 52 – латиницею.

Повнота викладення матеріалів дисертації у роботах, які опубліковані автором. Основні наукові положення дисертації, висновки та рекомендації **Криволап Євгеній Володимирович** достатньо повно представив у 19,5 наукових друкованих працях, зокрема: у 6,5 наукових статтях, опублікованих у наукових фахових виданнях України категорії Б з юридичних наук (з присвоєнням DOI), перелік яких затверджено МОН України, а також у 13 тезах доповідей, опублікованих за результатами участі в науково-практичних конференціях, у тому числі міжнародних, всеукраїнських і зарубіжних. Відносно наукових статей, опублікованих у співавторстві, визначений творчий доробок кожного із співавторів.

Кількість і якість цих публікацій підтверджують належний рівень опрацювання теми дисертаційного дослідження.

Отримані результати були оприлюднені до моменту захисту, а зміст публікацій повністю відображає основні положення дисертації та засвідчує самостійний характер проведеного наукового дослідження.

Дані про відсутність текстових запозичень та порушення академічної доброчесності. У дисертаційній роботі не виявлено фактів

академічного плагіату, фальсифікації чи фабрикації, що підтверджує дотримання автором принципів академічної доброчесності. Усі запозичення та посилання оформлені відповідно до чинних вимог академічного цитування.

Дискусійні положення та зауваження до змісту та оформлення дисертації. У цілому високо оцінюючи результати виконаного **Криволапом Євгенієм Володимировичем** дослідження, необхідно звернути увагу на окремі спірні аспекти роботи, що вимагають уточнення у ході наукової дискусії:

1. Одним із положень наукової новизни автор зазначає що в роботі вперше «уточнено та розширено понятійно-категорійні характеристики категорій «безпека інформації», «інформаційна безпека» та «кібербезпека» в контексті акцентованої уваги на феномені «когнітивної безпеки», що дозволило сформулювати положення, згідно з якими в сучасному інформаційному просторі актуалізується не лише завдання захисту інформації, а й необхідність захисту від деструктивного інформаційного впливу» Варто відзначити що, у поданому положенні спостерігається певна дескриптивність (описовість) та недостатня конкретизація авторського внеску, оскільки твердження про актуальність захисту від деструктивного інформаційного впливу в сучасному просторі є загальновизнаним науковим фактом, а не особистим здобутком дослідника. Для посилення наукової новизни слід чітко розмежувати, як саме когнітивний аспект трансформує кожну з трьох зазначених категорій («безпека інформації», «інформаційна безпека», «кібербезпека»), адже без уточнення специфічних відмінностей між ними в контексті когнітивістики перелік термінів виглядає надлишковим, а сама новизна звужується до констатації розширення термінологічного апарату без розкриття сутності його якісних змін.

2. Незважаючи на розгляд автором методів соціальної інженерії у межах кількох підрозділів, цей аналіз має фрагментарний та переважно ілюстративний характер, що позбавляє роботу необхідної системності в контексті дослідження психологічних механізмів маніпуляції. Дисертантом

детально описано інструментарій добровільної передачі конфіденційної інформації під впливом зовнішніх чинників, проте поза увагою залишилося теоретичне узагальнення цих процесів, що призвело до відсутності відповідних висновків щодо місця соціальної інженерії в ієрархії загроз когнітивній безпеці. Така незавершеність аналізу нівелює можливість практичного застосування результатів дослідження для розробки комплексних стратегій протидії деструктивному впливу на людину як критичну ланку інформаційної системи.

3. У роботі поза увагою дослідника залишилися специфічні особливості правового регулювання наукового відкриття як особливого об'єкта інтелектуальної власності в умовах функціонування кіберсередовища, що знижує комплексність аналізу правової охорони результатів інтелектуальної діяльності. Враховуючи транскордонний характер глобальних мереж та вразливість пріоритету наукового результату до несанкціонованого копіювання чи плагіату, відсутність розмежування режимів охорони наукових відкриттів у цифровому просторі позбавляє роботу необхідної глибини в частині правового забезпечення когнітивної та інформаційної безпеки суб'єктів наукової діяльності. Це обмежує можливість формулювання авторських пропозицій щодо вдосконалення законодавства в частині фіксації та захисту прав на нематеріальні активи, які стають об'єктами деструктивного впливу або кібершпигунства.

Втім, зазначені зауваження не знижують загальний високий рівень проведеного дослідження та можуть бути обговорені у процесі дискусії під час захисту.

Загальний висновок: Дисертаційна робота **Криволапа Євгенія Володимировича** на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», що подана до захисту на здобуття ступеня доктора філософії в галузі знань 08 «Право» спеціальності 081 «Право», є завершеним, логічно структурованим та комплексним дослідженням у сфері державного управління кібербезпекою. Автор

продемонстрував високий рівень наукової підготовки, провів ґрунтовний теоретико-правовий аналіз і запропонував практично значущі рекомендації, які можуть бути використані для вдосконалення нормативно-правової бази та механізмів кіберзахисту. Положення роботи відзначаються оригінальністю та науковою новизною, а висновки обґрунтовані й узгоджені з результатами дослідження. Обсяг наукових публікацій з теми дослідження і апробації на конференціях різного рівня відповідає вимогам МОН. Загалом робота відповідає вимогам до дисертацій на здобуття ступеня доктора філософії, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 081 «Право».

Офіційний опонент,
доктор юридичних наук, професор,
професор кафедри цивільного права
та процесу
Державного податкового університету **Наталія НОВИЦЬКА**