

РЕЦЕНЗІЯ

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. Конституція України визначає забезпечення інформаційної безпеки України однією з найважливіших функцій держави. При цьому сучасний розвиток інформаційно-комунікаційних технологій обумовлює перенесення обігу інформації у віртуальний (кібернетичний) простір. Зазначене створює як позитивні наслідки стрімкого розвитку людства, так і негативні наслідки щодо широкого поширення через віртуальні мережі негативних ворожих інформаційних та інформаційно-психологічних впливів, а також атак на апаратні і програмні засоби і дані. Таким чином, поняття інформаційної безпеки стає нерозривно пов'язаним з поняттям кібербезпеки. Саме тому тема наукового дослідження, яка обрана у дисертації **Криволапа Євгенія Володимировича** «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України» є актуальною. Дослідження дисертанта слугує важливим внеском у науку публічного управління сферою забезпечення інформаційної безпеки України. Отже, правомірним є висновок автора, що питання забезпечення кібернетичної безпеки в контексті забезпечення інформаційної безпеки України є актуальними.

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).

Наукова новизна дисертаційного дослідження. Рецензент погоджується з твердженням дисертанта, що в роботі вперше за напрямком досліджень теоретичних і методологічних основ наук адміністративного та інформаційного права та на засадах міждисциплінарного підходу у галузі інформаційної та кібернетичної безпеки отримані нові науково обґрунтовані результати у галузі адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України. Рецензент погоджується із сформульованими дисертантом аспектами наукової новизни, відповідно до яких:

вперше:

– системно обґрунтовано 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;

– розкрито реалізацію 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;

– введено 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; здійснено дослідження його ключових положень та визначено їх значення для формування національної правової доктрини у сфері кібербезпеки;

– 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;

– запропоновано поширити 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;

– запропоновано включити законодавче 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»;

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, кіберінцидентам, 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 копій, 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 заборonoю 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 гібридних 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 (zareestrovanih) ЗМІ.

Практична значущість роботи полягає в тому, що в роботі удосконалено науково-теоретичні підходи до методів і засобів публічного управління у сфері забезпечення кібербезпеки, систематизовано національне і міжнародне законодавство з цієї проблематики, здійснено порівняння з актами ЄС і Ради Європи, що особливо важливо в контексті прагнення України до вступу в ЄС, вибудовано та систематизовано структуру підзаконних нормативно-правових актів України у сфері кіберзахисту. Сформульовані висновки і пропозиції можуть бути ефективно впроваджені: Секретаріатом Касаційного цивільного суду у складі Верховного Суду дозволить організувати та планувати роботу з протидії правопорушенням у кібермережі (довідка про впровадження від 05.12.2025); ДНП «Державний університет «Київський авіаційний інститут» у науково-дослідній сфері основні положення та висновки дисертації можуть бути основою для подальшої розробки адміністративно-правових питань комплексного забезпечення інформаційної і кібер- безпеки (акт про впровадження від 01.12.2025); Комітетом Верховної Ради України з питань правоохоронної діяльності при формуванні та обґрунтуванні пропозицій щодо вдосконалення нормативно-правових актів у сфері забезпечення інформаційної та кібербезпеки (довідка про впровадження №04-27/12-2022/214837 від 13.12.2022); Київським національним університетом будівництва і архітектури у навчальному процесі матеріали дисертації використовуватимуться під час проведення занять із дисципліни «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» (акт про впровадження від 24.11.2025); Українською асоціацією інвестиційного бізнесу для забезпечення підвищення рівня захисту інформаційних баз даних (довідка про впровадження 01.12.2025).

Ступінь обґрунтованості наукових положень, висновків і рекомендацій. Аналіз тексту дисертації та змісту публікацій **Криволапа Євгенія Володимировича** дають підстави зробити висновок про наукову обґрунтованість та достовірність результатів, отриманих у результаті виконаного дослідження. Обґрунтованість наукових положень, висновків і рекомендацій, сформульованих у дисертації, не викликає заперечень.

Аналіз дисертаційної роботи дозволяє стверджувати, що наукові положення, висновки і рекомендації, сформульовані в ній, достатньо

переконливі, а їх достовірність забезпечена: правильно обраними і комплексно використаними методами наукового пізнання, які відповідають поставленим у роботі меті та завданням дослідження; професійним вирішенням автором визначених наукових завдань, що сприяло реалізації поставленої мети дослідження; використанням широкої джерельної бази за темою дисертації (366 найменувань); широкою апробацією одержаних результатів на наукових і науково-практичних заходах різних рівнів, зокрема і закордонних. Автором запропоновано і реалізовано міждисциплінарний підхід у сфері інформаційної та кібернетичної безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права, інформаційного права, права кібербезпеки, теорії психології впливів, деліктології. Єдність методології дослідження дозволила автору підготувати цілісне, завершене наукове дослідження.

Характеристика основних положень роботи. Дисертація складається з анотацій (українською та англійською мовами), які повно відображають зміст дисертації, списку публікацій здобувача, змісту, переліку умовних позначень, вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел та додатків. Структура дисертації **Криволапа Євгенія Володимировича** відповідає ustalеним вимогам до таких праць і не викликає заперечень. Виклад змісту дисертації логічний та послідовний. У вступі належним чином обґрунтовано актуальність обраної теми, визначено мету, завдання, об'єкт та предмет дослідження, описані використані для цього методи дослідження, 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.

У першому розділі досліджені теоретико-правові засади забезпечення кібернетичної безпеки країни в адміністративно-правовому вимірі. Розглянуті засади правового забезпечення інформаційної та кібернетичної безпеки як предмета адміністративного права. Розгляд здійснений на засадах міждисциплінарного підходу, який, за висновками автора, полягає у поєднанні засобів, методів і правил адміністративного права, інформаційного права, права кібербезпеки, теорії психології впливів, деліктології. При цьому автор враховує, що принципи діяльності публічної адміністрації мусять переломлюватися крізь призму специфіки тої чи іншої сфери управлінської діяльності. Тому логічним є дослідження автором матеріально-технічної бази, на яку спрямоване досліджуване правове регулювання – закономірності виникнення кіберзагроз, які визначають правові засади протидії таким загрозам. Особлива увага приділяється питанням правового забезпечення протидії вразливостям та їх нейтралізації. Запропонована періодизація запровадження в Україні 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, досліджена загальна логіка пошуку і виявлення вразливостей у системах на засадах системи Bug Bounty. Проаналізовані особливості концептів «інформаційна безпека», «безпека інформації», «кібербезпека», «когнітивна безпека» в контексті безпекових стратегій України 2020-2021 років. За

наслідками цього аналізу запропоновані окремі термінологічні зміни та доповнення в законодавстві.

У другому розділі розглянуті питання адміністративно-правового регулювання заходів забезпечення кібербезпеки. Досліджені особливості побудови системи нормативно правових актів у цій сфері в Європейському Союзі, Раді Європи, а також національного законодавства. Досліджена система актів європейського рівня (Директиви Європейського парламенту і Ради ЄС, Регламенти Європейського парламенту і Ради ЄС, Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)), історія їх змін та удосконалення; проаналізована Конвенція Ради Європи «Про кіберзлочинність» з Додатковим протоколом до цієї Конвенції як правова база протидії кіберзлочинності; узагальнені вимоги, сформульовані в Рекомендаціях Комітету міністрів Ради Європи щодо запровадження обмежень на показ контенту у телевізійній мережі як засоби забезпечення когнітивної безпеки громадян і суспільства. Досліджуються питання відповідності тенденцій розвитку сучасного національного законодавства в Україні європейським правилам і нормам. Запропоновані окремі зміни і доповнення до українського законодавства у цій сфері. Запропонована логіка побудови структури досліджених підзаконних нормативно-правових актів України у сфері кіберзахисту, яка формалізована схематично. Заслужують на увагу узагальнення автора у сфері кіберконфліктів, зокрема, кібербулінг, кіберсталкінг, що реально спрямовано на захист прав осіб у кіберсфері.

Третій розділ роботи присвячений питанням забезпечення вимог інформаційної безпеки у системі кіберзахисту і захисту інформаційних прав громадян. На підставі аналізу змісту безпекових стратегій України 2020-2021 рр. щодо забезпечення кібербезпеки докладно досліджується роль і значення досягнення надійного рівня кібербезпеки в системі забезпечення складових національної безпеки України. Автором доводиться, що українська система безпекових стратегій побудована за моделлю НАТО та ЄС – НАТО розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен. ЄС у «Стратегії кібербезпеки для цифрового десятиліття» («Cybersecurity Strategy for the Digital Decade») (2020) також наголошує на взаємозалежності інформаційної стійкості, цифрового суверенітету та кіберзахисту. Дисертантом запропонована структура інформаційних прав громадян, які захищаються в системі кіберзахисту, а також досліджена межа здійснення цих прав в умовах гібридної війни – проблема встановлення меж свободи самовираження гостро виникає внаслідок практичних потреб обмеження ворожих інформаційно-психологічних впливів. Зазначене надає підстави для обмежень державою поширення телевізійного контенту і Інтернет-мереж.

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: 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. Ці публікації відображають матеріали практично усіх підрозділів дисертації, на які (публікації) автор робить посилання по ходу викладення матеріалів дисертації. Отже, результати дисертаційного дослідження вичерпно оприлюднені в науковій літературі. Щодо статей, опублікованих спільно співавторами, визначений творчий внесок кожного з них.

Дані про відсутність текстових запозичень та порушення академічної доброчесності. Аналіз тексту дисертаційної роботи дозволив констатувати, що викладення роботи відповідає вимогам до академічної доброчесності. Посилання на використані джерела у тексті дисертації оформлені відповідно до чинних вимог наукового цитування.

Дискусійні положення та зауваження до змісту та оформлення дисертації. З урахуванням змісту дисертації **Криволапа Євгенія Володимировича** «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», доцільно сформулювати такі науково обґрунтовані зауваження, що можуть бути предметом фахової дискусії під час захисту:

1) Недостатньо представлені адміністративні процедури щодо притягнення до адміністративної відповідальності у сфері використання і обігу інформації.

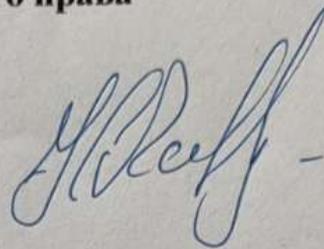
2) Не розглянуто питання криміналізації кібербулінгу.

Наведені зауваження не знижують наукову і практичну значущість виконаного дисертаційного дослідження.

Загальний висновок: Аналіз змісту і структури дисертації дозволяє дійти висновку, що за актуальністю порушеної проблеми, науковою новизною, теоретичною і практичною значущістю результатів, достовірністю і повнотою висвітлення їх у публікаціях дисертація **Криволапа Євгенія Володимировича** на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», представлена до захисту на здобуття ступеня доктора філософії в галузі знань 08 «Право» спеціальності 081 «Право», є самостійним, цілісним, завершеним науковим дослідженням, спрямованим на вирішення проблем публічного адміністрування у сфері забезпечення інформаційної безпеки в системі кіберзахисту, з урахуванням технологічних і технічних особливостей у цій сфері. Робота оформлена відповідно до чинних вимог, написана науковим стилем і літературною українською мовою. Виходячи з викладених у рецензії позитивних висновків, дисертація відповідає спеціальності 081 «Право» та вимогам до оформлення дисертації, затвердженим Наказом Міністерства освіти і науки України від 12.01.2017 р. № 40 (зі змінами, внесеними Наказом Міністерства освіти і науки України від 3 1.05.2019 р. № 759) та «Порядку

присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (Постанова Кабінету Міністрів України від 12.01.2022 р. № 44), а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 081 «Право».

**Професор кафедри теорії та історії держави і права,
конституційного та адміністративного права
Державного університету
«Київський авіаційний інститут,
доктор юридичних наук, професор**



— М. І. Легенький

