Голові разової спеціалізованої вченої ради
Державного університету
«Київського авіаційного інституту»
доктору юридичних наук, професору,
завідувачу кафедри кримінального права і процесу ДУ «КАІ»,
Лиховій Софії Яківні

РЕЦЕНЗІЯ
доктора юридичних наук, доцента Філінович Валерії Вікторівни,
на дисертацію Криволапа Євгенія Володимировича
на тему:
«Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України»,
подану на здобуття ступеня доктора філософії в галузі знань 08 «Право»
за спеціальністю 081 «Право»

Актуальність дисертаційної роботи. Беззаперечним є той факт, що у сучасних реаліях широкого впровадження нових інформаційно-комунікаційних технологій, з одного боку, і тенденцій їх використання для завдання шкоди особам, підприємствам, суспільству, державі, з іншого боку, перед державою постає завдання надійного захисту кібернетичної безпеки суб'єктів. Зокрема, із загостренням воєнної ситуації наростають і ризики у кіберпросторі. Таким чином, поняття інформаційної безпеки нерозривно пов'язане з поняттям кібербезпеки. З точки зору національної (інформаційної) безпеки держави слід підкреслити, що кібервійна стає все більш важливою складовою гібридної війни. Саме тому можна стверджувати, що тема дисертації «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України» є на часі. Дослідження дисертанта слугує важливим внеском до наукового доробку з питань публічного управління сферою забезпечення кібернетичної безпеки України. Отже, можна погодитися із автором дисертаційного дослідження, що питання забезпечення кібернетичної безпеки як чинника 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 полягає у тому, що вперше за напрямком досліджень теоретичних і методологічних основ наук адміністративного та інформаційного права та на засадах міждисциплінарного підходу у галузі інформаційної та кібер-безпеки отримані нові науково обґрунтовані результати у галузі адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України. Як результат проведеного дослідження його наукову новизну відображають основні положення за ступенями:

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 положення Закону Європейського Союзу про кіберстійкість (Cyber Resilience Act, CRA), спрямованого 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 «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, 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;

– структуру 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 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 (зареєстрованих) ЗМІ.

Практична значущість роботи полягає в тому, що висунуті та теоретично обґрунтовані положення, пропозиції і висновки дослідження сприятимуть можливості їх використання: 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 національний 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).

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 науково-теоретичного пошуку. Усі наукові положення, висновки та рекомендації достатньою мірою обґрунтовані, підкріплені теоретичними положеннями, нормативно-правовою базою, статистичними та науково-технічними даними, достатнім обсягом дослідженого матеріалу. Автором правильно обрані методи наукового пізнання, які відповідають поставленим у роботі меті та завданням дослідження. Автором запропоновано і реалізовано міждисциплінарний підхід у сфері інформаційної та

кібернетичної безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права, інформаційного права, пра́ва кібербезпеки, теорії психології впливів, деліктології. Автором правильно вказується на використання у роботі таких методичних підходів: системний метод (застосовано для упорядкування емпіричної інформації та проведення класифікації досліджуваних правових явищ); документальний аналіз (застосовано для дослідження документальних джерел правових явищ); метод абстрагування (дозволив виявляти у досліджуваних явищах найбільш характерні властивості); компаративний метод (метод порівняння – порівняння законодавства України та ЄС); метод об'єктивної істини (перехресна перевірка даних, використаних при дослідженні, з інших джерел). Всі ці методи були використані комплексно.

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 усталеним вимогам до таких праць і не викликає заперечень. Виклад змісту дисертації логічний та послідовний. У вступі переконливо 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.

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. Міждисциплінарний підхід як він запропонований і використовується у даній дисертаційній роботі, полягає у поєднанні засобів, методів і правил адміністративного права, інформаційного права, права кібербезпеки, теорії психології впливів, деліктології. Системно розглянуті обставини, які призводять до потреб у такому регулюванні, а саме – технологічні аспекти виникнення кіберзагроз і проблеми протидії цим загрозам. Особлива увага приділяється питанням правового забезпечення протидії вразливостям та їх нейтралізації. Розглянуті правові засади забезпечення належного рівня кібербезпеки Інтернет-речей (IoT) як чинників вразливостей, правильно наголошується, що в умовах повсюдного поширенні «розумних» пристроїв останні стають слабким ланцюгом у системі забезпечення кібербезпеки. Проаналізовані особливості концептів «інформаційна безпека», «безпека інформації», «кібербезпека», «когнітивна безпека» в контексті безпекових стратегій України 2020-2021 років. Звідти робиться висновок, що в сучасному інформаційному просторі актуальною стає не тільки захист інформації, але й захист від інформації. На цій основі

запропоновані також 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. В історико-правовому контексті 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)), Конвенція Ради Європи «Про кіберзлочинність» з Додатковим протоколом до цієї Конвенції, Рекомендації Комітету міністрів Ради Європи щодо запровадження обмежень на показ контенту у телевізійній мережі в контексті забезпечення когнітивної безпеки громадян і суспільства. Правильно встановлюється, що розвиток сучасного національного права в Україні здійснюється в парадигмі європейського законодавства. Обґрунтовується, що ключовим правовим актом України у сфері забезпечення кібербезпеки є Закон від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Встановлено, що цей Закон в основних своїх концептуальних рисах, відповідає європейському регулюванню у цій сфері; у той же час запропоновані окремі зміни і доповнення. Запропонована логіка побудови структури досліджених підзаконних нормативно-правових актів України у сфері кіберзахисту, яка формалізована схематично. Розглянуті окремі проблеми публічного адміністрування у сфері протидії кіберконфліктам та запропоновані шляхи їх вирішення, заслуговує на підтримку прагнення автора сформувати напрями захисту прав інтелектуальної власності від Інтернет-піратства.

Третій розділ роботи присвячений питанням забезпечення вимог інформаційної безпеки у системі кіберзахисту і захисту інформаційних прав громадян. Докладно досліджується роль і значення досягнення надійного рівня кібербезпеки в системі забезпечення національної безпеки України, забезпечення інформаційної безпеки засобами кіберзахисту, захисту прав громадян у сфері кібербезпеки. Заслуговують на підтримку запропонована авторська структура інформаційних прав громадян, а також авторські визначення окремих компонентів прав, зокрема: «захист прав інтелектуальної власності в мережі Інтернет»; «право на захист від кримінальних посягань у кіберпросторі». Наголошено, що з точки зору конституційного принципу гарантій свободи думки і слова, права на вільне вираження своїх поглядів і переконань, обіг інформації в інформаційно-комунікаційних системах, зокрема, в Інтернеті, підкоряється принципу, відповідно до якого такі свободи не можуть бути безмежними. Проблема встановлення меж свободи самовираження, з одного боку, і допустимості її обмежень, з іншого боку особливо гостро виникає внаслідок практичних потреб обмеження ворожих інформаційно-психологічних впливів, що є особливо гострим саме в інформаційно-комунікаційних системах у зв’язку із особливостями їх можливостей з точки зору доступу до аудиторії (адресатів ворожих думок) – широта охоплення аудиторії, швидкість поширення

інформації, відносно низька трудомісткість і вартість її виготовлення. Зазначене надає підстави для обмежень державою поширення телевізійного контенту і Інтернет-мереж. Вперше системно досліджені дії російських/проросійських пропагандистів щодо маскування фейкової інформації під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН.

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. Вищевказане дозволяє стверджувати, що представлена на рецензування дисертація є самостійним, завершеним науковим дослідженням, результати якого у достатній мірі опубліковані та мають значення для розвитку вітчизняної науки і практики. Відносно наукових статей, опублікованих у співавторстві, визначений творчий доробок кожного із співавторів.

Дані про відсутність текстових запозичень та порушення академічної доброчесності. Під час детального розгляду дисертаційної роботи порушень академічної доброчесності не виявлено. Усі запозичення та посилання оформлені відповідно до чинних вимог академічного 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) Дисертант приділяє певну увагу питання захисту прав інтелектуальної власності у кіберпросторі. При цьому питання щодо небезпеки порушення прав розглядаються у підрозділі 2.3, а питання захисту таких прав – у підрозділі 3.3. Розпорошеність такого розгляду по декількох розділах знижує рівень концентрації читача на цьому питанні.

2) У підрозділі 3.3 Дисертант сформулював рекомендації щодо технічних способів захисту прав інтелектуальної власності в мережі Інтернет: використання цифрових водяних знаків (watermark); DRM (Digital Rights Management) – технології контролю копіювання контенту; системи моніторингу порушень (наприклад, Content ID у YouTube). Було б доцільно надати порівняльний аналіз цих методів, переваги та недоліки.

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 самостійним наукові дослідженням, що вирішує важливу науково-практичну проблему розвитку основ адміністративного і інформаційного права, розроблення теоретичних і практичних основ адміністративно-правового регулювання діяльності із забезпечення кібернетичної безпеки України. Робота оформлена відповідно до чинних вимог, написана науковим стилем і літературною українською мовою. Стиль викладу матеріалу науковий, логічний, виважений та зрозумілий. Дисертація читається легко, викликає зацікавленість досліджуваною проблематикою. За актуальністю, змістом та повнотою викладу її результатів у публікаціях здобувача, обсягом і якістю оформлення 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 31.05.2019 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».

Рецензент:
доктор юридичних наук, доцент,
доцент кафедри цивільного права і процесу
Державного некомерційного підприємства
«Державний університет «Київський авіаційний
інститут» Валерія ФІЛІНОВИЧ

Філінович В.
Особистий підпис
ЗАСВІДЧУЮ
ВЧЕНИЙ СЕКРЕТАР
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Інна НАБОК