ЗАТВЕРДЖУЮ
Президент державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»

_____ Ксенія СЕМЕНОВА

«11» грудня 2025 року

ВИСНОВОК

Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» (далі – КАІ) про наукову новизну, теоретичне та практичне значення результатів дисертації Криволапа Євгенія Володимировича на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», поданої на здобуття ступеня доктора філософії за спеціальністю 081 «Право»

Витяг
із протоколу № 1 розширеного засідання кафедри теорії держави і права, конституційного та адміністративного права КАІ
від 09 грудня 2025 року

Присутні на засіданні науково-педагогічні працівники кафедри теорії держави і права, конституційного та адміністративного права:

Головуючий на засіданні – Макеєва О.М., зав. кафедри, к.ю.н., доцент
Калюжний Р.А., д.ю.н., професор, професор кафедри,
Кунєв Ю.Д., д.ю.н., професор, професор кафедри,
Легенький М.І., д.ю.н., професор, професор кафедри,
Сопілко І.М., д.ю.н., професор, професор кафедри,
Головко С.Г., к.і.н., доцент, професор кафедри,
Вишновецький В.М., к.ю.н., доцент, доцент кафедри,
Устинова І.П., к.ю.н., доцент, професор кафедри,
Череватюк В.Б., к.і.н., доцент, доцент кафедри,
Чистякова Ю.В., к.ю.н., доцент кафедри

Присутні на засіданні науково-педагогічні працівники ФПМВ КАІ:

Жукорська Я.М., к.ю.н., доцент, декан Факультету права та міжнародних відносин;

Стригуль М.В., к.с.н., доцент, заступник декана Факультету права та міжнародних відносин;

Вишновецька С.В., д.ю.н., професор, завідувач кафедри цивільного права і процесу;

Лихова С.Я., д.ю.н., професор, завідувач кафедри кримінального права і процесу;

Філінович В.В., д.ю.н., доцент, доцент кафедри цивільного права і процесу.

Серед присутніх 7 докторів юридичних наук і 5 кандидатів юридичних наук, 2 кандидата історичних наук, 1 кандидат соціологічних наук

Порядок денний:

Обговорення дисертаційної роботи аспіранта кафедри теорії держави і права, конституційного та адміністративного права КАІ Криволапа Євгенія Володимировича на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», поданої на здобуття ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право».

Науковий керівник – доктор юридичних наук, професор, професор кафедри теорії держави і права, конституційного та адміністративного права КАІ Кунєв Юрій Дем'янович.

Дисертація виконувалась на кафедрі теорії держави і права, конституційного та адміністративного права Факультету права та міжнародних відносин КАІ. Тема дисертації затверджена на засіданні Вченої ради Юридичного факультету НАУ (протокол № 8 від 31 жовтня 2022 року).

Виступили:

Аспірант кафедри теорії держави і права, конституційного та адміністративного права КАІ Криволап Євгеній Володимирович на тему: «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», поданої на здобуття ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право»

Доповідач обґрунтував актуальність обраної теми, визначив мету, завдання, методологію та методику, охарактеризував об'єкт та предмет дисертації, виклав основні наукові положення та висновки, що виносяться на захист, вказав науково-практичну значущість роботи, зазначив про впровадження результатів дослідження.

Автором зазначено, що проведений аналіз існуючого на сьогодні змісту правовідносини щодо публічного управління у сфері кібербезпеки дав змогу дійти наступних висновків:

1. Усвідомлення сучасних викликів у зв'язку із широкомасштабною агресією рф проти України 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 особам, підприємствам, суспільству, державі, з іншого боку, перед державою постає завдання надійного захисту кібернетичної безпеки суб'єктів та їх прав у кіберпросторі. Впровадження міжнародних стандартів може підвищити рівень загальної готовності України до інформаційних загроз. Крім того, міжнародна співпраця є ключем до протидії інформаційним загрозам.

2. В роботі запропонований, обґрунтовується і досліджується міждисциплінарний підхід до вивчення та реалізації ефективних засобів правового забезпечення інформаційної й кібер- безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права (принципи діяльності публічної адміністрації і організації публічного управління в демократичному суспільстві),

інформаційного права (поєднання свободи інформаційної діяльності із захистом національного інформаційного простору України від розповсюдження ворожої інформаційної продукції, створення та використання інформаційних технологій), пра́ва кібербезпеки (врахування конкретних ситуацій прийняття рішень публічною адміністрацією), теорії психології впливів (захист осіб від шкідливих інформаційних впливів, забезпечення когнітивної безпеки), деліктології (вивчення заходів державного примусу адміністративно-правового і кримінально-правового характеру для забезпечення встановлених правил у сфері інформаційної та кібр-безпеки). В умовах, коли мережеві та інформаційні системи та послуги відіграють важливу роль у суспільстві, їхня надійність та безпека суттєві для економічної та соціальної діяльності і, зокрема, для функціонування внутрішнього ринку. Отже, належне правове регулювання суспільних відносин, пов'язаних із запровадженням та використанням інформаційно-комунікаційних систем, є необхідним для їх ефективного використання. Вперше узагальнені встановлені КУпАП делікти у сфері обігу інформації і використання інформаційно-комунікаційних систем.

3. Наголошено, на необхідності системної нейтралізації вразливостей, на що вказується у Стратегії кібербезпеки України, міжнародному стандарті ISO 27005, рекомендаціях Держспецзв'язку, відомчих нормативних документах, наприклад, Нормативному документі НД ТЗІ 1.1-003-99 Служби безпеки України «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу». Разом із тим, у Законі України «Про основні засади забезпечення кібербезпеки України» не надається визначення цього терміну, що обмежує уніфікацію робіт у цій сфері. Пропонується доповнити цей Закон визначенням поняття «вразливості», згідно із міжнародним стандартом інформаційної безпеки ISO 27005.

Пропонується авторське розуміння адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України, яке полягає у використанні засобів і методів адміністративного права (публічне адміністрування, нормативно-правове регулювання, встановлення відповідальності за порушення встановлених нормативних правил), з урахуванням технічних аспектів і технологічних небезпек в кіберпросторі, включаючи протидію вразливостям, кіберінцедентам, кіберконфліктам.

Розглянуті правові засади застосування методу пошуку вразливостей на засадах системи Bug Bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Виконана періодизація офіційного правового запровадження даної системи в Україні, виділено 2 етапи: 1-й етап – запровадження відповідних змін до КК України, 2-й етап – запровадження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого Постановою КМУ від 16.05.2023 № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж». Розглянуті принципи взаємодії між замовником і виконавцем(цями) при пошуку вразливостей, зокрема, висунення публічній пропозиції, підготовка звітів, виплата

винагороди тощо.

Сформульовано положення про те, що загальна логіка пошуку і виявлення вразливостей у системах на засадах системи Bug Bounty ґрунтується на аналізі архітектури систем, конфігурації та програмного забезпечення, а також за допомогою тестування, яке може включати сканування на наявність вразливостей, проникнення та інші методи, у тому числі імітацію дій зловмисників для перевірки стійкості системи, з метою виявлення вразливостей; виявлення слабких місць у програмному забезпеченні та конфігурації. Практичне значення нормативно-правових актів про Bug Bounty полягає у тому, що це правове регулювання служить для розробки та впровадження заходів безпеки, що допомагають запобігти несанкціонованому доступу та іншим видам атак.

4. Розглянуті правові засади забезпечення належного рівня кібербезпеки Інтернет-речей (IoT) як чинників вразливостей – електронно-цифрових пристроїв, приєднаних до інформаційно-комунікаційних систем: «розумні» годинники, «розумні» лічильники, системи «розумний будинок», «розумне авто», розумні роботи, Wi-Fi роутери, ноутбуки, смартфони, датчики та камери, смарт-карти, мобільні пристрої, розумні колонки, маршрутизатори, перемикачі, промислові системи управління, програмне забезпечення, прошивка, операційні системи, мобільні додатки, настільні програми, відеоігри; компоненти (як апаратні, так і програмні); блоки обробки комп’ютера; відеокарти; програмні бібліотеки тощо. Небезпека цих пристроїв, коли вони приєднані до інформаційно-комунікаційних систем, полягає у тому, що вони є потенційною точкою входу для кібератаки. У підключеному середовищі інцидент кібербезпеки в одному продукті може вплинути на всю організацію або весь ланцюг постачання, часто поширюючись через кордони внутрішнього ринку за лічені хвилини. Вперше введено в український правовий науковий оборот Закон про кіберстійкість (The Cyber Resilience Act (CRA)) – це нормативний акт ЄС щодо покращення кібербезпеки та кіберстійкості в ЄС шляхом встановлення спільних стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, таких як обов'язкові звіти про інциденти та автоматичні оновлення безпеки. Досліджені його основні положення, якими запропоновано доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Одночасно запропоновано поширити вимоги цього Закону на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет, навіть якщо вони не містять інформацію, необхідність захисту якої встановлена законом, оскільки ці системи за визначенням взаємодіють із публічними мережами електронних комунікацій, зокрема, Інтернет. Де-факто інтереси інформаційного захисту потребують такого регулювання.

5. Проаналізовані особливості концептів «інформаційна безпека», «безпека інформації», «кібербезпека», «когнітивна безпека» в контексті безпекових стратегій України 2020-2021 років. Наголошується, що в сучасному інформаційному просторі актуальною стає не тільки захист інформації, але й захист від інформації. Це поділяє поняття «інформаційна безпека» на підмножини «безпека інформації» та «когнітивна безпека», тобто «інформаційно-психологічна безпека особи». Крім того, у якості підмножини «безпека інформації» слід розглядати поняття «кібербезпека» як захищеність життєво важливих інтересів

людини і громадянина, суспільства та держави під час використання кіберпростору. У кібербезпеці захищають кіберресурси, у когнітивній безпеці – розум людини. Ворожі інформаційні впливи можуть нести небезпеки не тільки інформаційним (комп'ютерним) системам, але й безпосередньо особам, оскільки можуть бути задіяні для доставляння небажаної інформації в обхід запобіжників отримання (доставляння) цієї інформації. Інформація формує у свідомості людини систему знань, поглядів, смислів, якими людина керується у своїх вчинках – не тільки лояльних по відношенню до оточення, суспільства, держави, але й ворожих по відношенню до них. Інформаційний вплив може змінювати поведінку людей, нав'язувати їм цілі, які об'єктивно не входять в число їх інтересів. Отже, необхідно враховувати зворотній вплив кібербезпеки на когнітивну безпеку. Кібератаки активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення.

Запропоновано напрями термінологічного узгодження у ч. 2 ст. 8 та абз. 2 ч. 4 ст. 8 ЗУ «Про захист інформації в інформаційно-комунікаційних системах» та у ч. 3 ст. 6 ЗУ «Про основні засади забезпечення кібербезпеки України» («слова «інформаційної безпеки» замінити словами «безпеки інформації»).

6. Визначені особливості правового регулювання заходів забезпечення кібербезпеки правовими актами європейського рівня, розглянуті ключові акти у цій сфері, в їх історичному розвитку, а саме: Директива 2016/1148 від 06.07.2016 (Директива була замінена Директивою 2022/2555 від 14.12.2022 року, яка набрала чинності 16.01.2023 року); Директива 2008/114/ЄС від 08.12.2008 року (Директива була замінена Директивою 2022/2557 від 14.12.2022 року, яка набрала чинності 16.01.2023 року); Директива 95/46/ЄС від 24.10.1995 року (Директива замінена Регламентом 2016/679 від 27.04.2016 року, який набрав чинності 24.05.2016 року; Директива 2018/1972 від 11.12.2018 року; Регламент 2019/881 від 17.04.2019 року (Акт про кібербезпеку); Конвенція від 23.11.2001 року Ради Європи «Про кіберзлочинність»; Додатковий протокол від 28.01.2003 до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи; Рекомендація від 30.10.1997 р. № R (97) 19 Комітету міністрів Ради Європи «Про показ насильства електронними ЗМІ», ухвалена Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.; Рекомендація від 30.10.1997 р. № R (97) 20 Комітету міністрів Ради Європи «Про розпалювання ненависті», ухвалена Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.; Рекомендація від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», ухвалена Комітетом міністрів на 425-му засіданні заступників міністрів від 27.04.1989 р. Сюди ж слід віднести Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)). Наголошено, що перші 4 перелічені (чинні) документи (Директива 2022/2555 від 14.12.2022; Директива 2022/2557 від 14.12.2022; Регламент 2016/679 від 27.04.2016; Регламент 526/2013 від 17.04.2019) підлягають імплементації у законодавство України відповідно до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони,

Розділ ІІІ «Юстиція, свобода та безпека». Прийняття Закону України від 16.12.2020 року № 1089-IX «Про електронні комунікації» є імплементацією Директиви 2018/1972 від 11.12.2018 року про запровадження Європейського кодексу електронних комунікацій. Встановлені факти належної імплементації положень Директиви 2022/2555 в Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України», зокрема, щодо норм про захист критичної інформаційної інфраструктури, щодо створення національної системи реагування на кіберзагрози, щодо розробки національної стратегії кібербезпеки та її змісту.

7. Встановлено, що Конвенція Ради Європи «Про кіберзлочинність» з Додатковим протоколом до неї є універсальним міжнародним документом, що спрямований на боротьбу з Інтернет-злочинністю та комп'ютерною злочинністю (кіберзлочинністю) й встановлює і класифікує злочини у сфері кіберзлочинності. Об'єктом таких кіберзлочинів може стати не тільки і навіть не стільки будь-який користувач Інтернету, але й особа, яка не є користувачем Інтернету. Наприклад об'єктом злочину у вигляді поширення контрафактної продукції через мережу Інтернет може стати суб'єкт авторського права, який не є користувачем Інтернету. Метою Додаткового протоколу до Конвенції Ради Європи «Про кіберзлочинність» є внесення доповнень у відносинах між Державами – сторонами Протоколу до положень Конвенції про кіберзлочинність, які стосуються криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Отже, цей Протокол повинен забезпечити кримінально-правовий захист когнітивної безпеки осіб та суспільства в частині запобігання проявам дій расистського та ксенофобного характеру. Констатовано важливість Конвенції Ради Європи «Про кіберзлочинність» для України в умовах сучасної злочинної кібервійни рф проти України, у тому числі масової антиукраїнської пропаганди та закликів до геноциду українського народу. Важливість цього напряму захисту когнітивної безпеки проілюстровано історією з радіо «Тисячі пагорбів».

8. Подальшими керівними документами щодо впровадженням заходів забезпечення когнітивної безпеки від інформаційно-психологічного впливу електронних засобів комунікації є Рекомендації 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». Базовим принципом підходу до обмежень в даній сфері є правила, встановлені ст. 10 Конвенції Ради Європи про захист прав людини і основоположних свобод 1950 року.

9. Визначені особливості правового регулювання заходів забезпечення кібербезпеки актами національного права. Встановлена система законів і підзаконних нормативно-правових актів у сфері забезпечення кібербезпеки. Наголошено, що правозастосовна і прикладна діяльність у сфері кіберзахисту повинна здійснюватися, зокрема, з максимально можливим застосуванням національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки. Узагальнені наступні принципи правового регулювання у сфері кібербезпеки: верховенство права, захист національних інтересів, прозорість і стабільність кіберпростору, державно-приватну взаємодію, пропорційність заходів

кіберзахисту, пріоритет запобігання загрозам і невідворотність покарання за кіберзлочини. Встановлено, що хоча законодавство з кіберзахисту звернено, перш за все, до суб'єктів національної системи кібербезпеки, це законодавство покликано також до забезпечення безпеки, прав, свобод та інтересів широкого кола користувачів об'єктами кібербезпеки та кіберзахисту, – через належне виконання уповноваженими суб'єктами національної системи кібербезпеки своїх обов'язків та повноважень у сфері кіберзахисту.

Доведено, що в контексті реалізації «відносини адміністративних зобов'язань», які притаманні засобам і способам адміністративного права, у Законі «Про основні засади забезпечення кібербезпеки України» послідовно реалізовані усі: а) відносини публічного управління – управлінські функції і повноваження Президента України, КМУ, міністерств, інших центральних органів виконавчої влади; місцевих державних адміністрацій; органів місцевого самоврядування; б) відносини адміністративних послуг – кібербезпека та адміністративні послуги пов'язані через цифровізацію державних сервісів, де захист даних стає ключовим завданням; в) відносини відповідальності публічної адміністрації за неправомірні дії або бездіяльність – суб'єкти національної системи реагування на кіберінциденти, кіберзагрози, кібератаки … несуть адміністративну, цивільно-правову, кримінальну відповідальність за неправомірне розголошення, неправомірне розкриття, неправомірне використання та інші неправомірні дії з інформацією про кіберінциденти відповідно до закону (ч. 3 ст. 9 Закону № 2163-VIII). Адміністративна відповідальність настає за порушення, передбачені КУпАП (за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем та інше); г) відповідальності суб'єктів суспільства за порушення порядку і правил, встановлених публічною адміністрацією у межах її повноважень – посадові особи власників або розпорядників інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси та/або службова інформація та інформація, що становить державну таємницю, посадові особи операторів критичної інфраструктури, власників або розпорядників об'єктів критичної інформаційної інфраструктури несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов'язку щодо здійснення обов'язкових повідомлень про кіберінциденти, кібератаки (ч. 6 ст. 9-1 Закону № 2163-VIII).

Запропонована логіка побудови структури описаних підзаконних нормативно-правових актів України у сфері кіберзахисту, яка формалізована схематично.

10. Вперше в наукових дослідженнях встановлено, що сукупність нормативних приписів у сфері забезпечення кібербезпеки та протидії кіберзлочинності доповнена також таким специфічним актом, як Типологія легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році, затверджені Наказом від 25.12.2013 № 157 Державної служба фінансового моніторингу України. У Документі розглядаються наступні питання щодо кіберзлочинності: види кіберзлочинів, загрози та ризики кіберзлочинів, шахрайство з використанням інформаційно-комунікаційних систем та

комп'ютерних технологій; кіберзлочинність нефінансового характеру, загальні напрямки протидії кіберзлочинам, виявлення підозрілих фінансових операцій. Наведені в Типології підходи використані в судовій практиці (Постанова від 21.06.2023 року у справі № 922/4091/19 Верховного Суду у складі колегії суддів Касаційного господарського суду).

11. Здійснені системні дослідження з питань кіберконфліктів. Проаналізована сутність поняття «кіберконфлікт». Вперше розглянутий взаємозв'язок між поняттями «кіберконфлікт», з одного боку, та кіберінцидент і кіберзлочин, з іншого боку. Встановлено, що інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора), спрямованих проти систем електронних комунікацій, систем управління технологічними процесами, а негативні прояви «кіберконфліктів» спрямовані проти інтересів осіб. Тобто, без врахування людського фактору як об'єкту негативного впливу розгляд проблематики кіберінцидентів є недостатнім та неповним. Систематизовані види кіберконфліктів, які породжуються різноманітними зловживаннями у кіберпросторі. Доведено, що не усі поширені зловживання прямо криміналізовані (передбачені у КК України як злочини у кібернетичній сфері), що утруднює їх кваліфікацію як злочинів.

12. Вперше системно розглянута сукупність безпекових стратегій, прийнятих в Україні протягом 2020-2021 рр., зокрема Стратегія національної безпеки України від 14.09.2020 р.; Стратегія воєнної безпеки України від 25.03.2021 р.; Стратегія кібербезпеки України від 14.05.2021 р.; Стратегія інформаційної безпеки від 15.10.2021 р. Ключовою в системі наведених безпекових Стратегій є Стратегія національної безпеки України, на підставі якого розроблені галузеві стратегії розвитку. Прийняті Стратегії свідчать про серйозну безпекову роботу української влади напередодні розширення агресивних дій рф проти України, вони є логічно взаємопов'язаними документами, реалізація яких ґрунтується на вимогах Стратегії національної безпеки України, а також на застосуванні механізмів забезпечення інформаційної безпеки і кібербезпеки України. В цьому контексті слід зазначити, 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.

В Стратегії кібербезпеки України важлива роль приділяється кіберзагрозам саме в інформаційній сфері. Визнаєтьcя, що засоби кібербезпеки захищають не тільки апаратні і програмні засоби, але й інформацію, що там обробляється. Кібербезпека – технічна і технологічна основа інформаційної безпеки.

Встановлено, що законодавче регулювання сутності і змісту безпекових Стратегій визначається Законом України «Про національну безпеку України». Разом із тим, також встановлено, що такі безпекові Стратегії, як Стратегія зовнішньополітичної діяльності України, Стратегія інформаційної безпеки, Стратегія забезпечення державної безпеки, Стратегія енергетичної безпеки цим Законом не регулюються і в Законі не згадуються, хоча сам Закон розглядає ці види безпек складовою частиною національної безпеки. Запропоновано імплементувати вказані Стратегії в Закон «Про національну безпеку України».

13. Запропонована авторська структура інформаційних прав громадян. Виходячи з того, що «інформаційні права» не тотожні «праву на інформацію», запропонована і розглянута наступна структура інформаційних прав: свобода слова (право вільно виражати свої думки та погляди); право на доступ до інформації, у тому числі право на звернення (можливість отримувати інформацію, що перебуває у володінні суб'єктів владних повноважень, та інформацію, яка становить суспільний інтерес); захист персональних даних (право контролювати використання та поширення своєї особистої інформації); захист інформаційної безпеки (право на захист від несанкціонованого доступу до особистої інформації та можливість регулювати цей доступ), захист прав інтелектуальної власності (захист авторських прав на контент), право на захист від кримінальних посягань у кіберпросторі (право вимагати від уповноважених органів держави запобігання, виявлення, припинення та розкриття кіберзлочинів). Розкритті особливості і механізми забезпечення вказаних прав осіб у кібермережі.

Запропоновані авторські визначення окремих компонентів прав: «захист прав інтелектуальної власності в мережі Інтернет» – це система правових, технічних і організаційних заходів, спрямованих на попередження, виявлення та припинення порушень авторських і суміжних прав, прав на торговельні марки, патенти, промислові зразки тощо в онлайн-просторі (авторське визначення); «право на захист від кримінальних посягань у кіберпросторі» – це гарантоване державою право кожної особи на безпеку, недоторканність її цифрової інформації, персональних даних, майна й честі від злочинних дій, що здійснюються з використанням інформаційно-комунікаційних технологій.

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. В умовах агресивної інформаційної війни рф проти України керівництво країни було вимушене вдатися до певних обмежень в інформаційно-комунікаційному середовищі: заборона російських соціальних мереж і сайтів (Указ Президента України від 15.05.2017 року № 133/2017 з подальшим продовженням заборони Указом Президента України від 14.05.2020 року № 184/2020; запровадження санкцій проти засобів масової інформації (Указ Президента України від 02.02.2021 року № 43/2021) із забороною їх трансляції. Обґрунтована правомірність цих рішень в контексті частини 2 статті 10 ЄКПЛ, а також частини 3 статті 34 Конституції України.

14. Досліджені дії російських/проросійських пропагандистів щодо маскування фейкової інформації під зовнішнє оформлення відомих та

авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН. Наведені приклади фактичних фейкових повідомлень (сайтів).

15. Запропоноване поняття «презумпція достовірності інформації», під якою розуміється відсутність необхідності додатково перевіряти достовірність інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ. ЄСПЛ не вважає прийняття національних нормативних актів щодо державної реєстрації Інтернет-видань порушенням свободи слова. Навпаки, Європейський Суд з прав людини висновував, що принцип презумпції достовірності інформації, яка розміщена в Інтернеті, може бути застосований тільки щодо інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ. За умови належного правового регулювання (у відповідності із вимогами ЄКПЛ) навпаки, така реєстрація підсилює гарантії діяльності журналістів і розширює коло інформації, до якої можна застосовувати презумпцію достовірності, – при одночасному підвищенні відповідальності таких Інтернет-видань за поширення неналежної інформації.

16. Вперше введений у правовий науковий оборот поняття «мережевий нейтралітет» – це принцип, згідно з яким провайдери телекомунікаційних послуг не віддають переваги одному цільовому призначенню перед іншим, або одним класам додатків перед іншими. Це означає, що провайдер не може дискримінувати користувачів, надаючи одним вигідніші умови доступу до контенту, ніж іншим; не має права втручатися в зміст, походження або призначення даних. Всі дані повинні оброблятися однаково, незалежно від того, хто їх надсилає або хто їх отримує. Провайдер не може, наприклад, навмисно уповільнювати роботу певного сервісу, щоб надати перевагу власному сервісу або сервісу, з яким він має договір. Скасування мережевого нейтралітету може дозволити провайдерам створювати платні «швидкісні коридори» для певних компаній, а також блокувати або обмежувати доступ до конкурентів чи небажаних для них сайтів. ЄС займає жорстку позицію щодо дотримання цього принципу. Відмова від цього принципу може негативно вплинути на конкуренцію, свободу слова та доступ до інформації в мережі.

17. Пропонуються наступні рекомендації для підвищення ступеня інформаційної безпеки: використання надійних паролів, регулярне оновлення програмного забезпечення**:** операційної системи та всі програми; 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, щоб уникнути втрати даних; використання тільки ліцензійних та офіційних програм.

18. За наслідками виконаного дослідження запропоновано внести такі зміни і доповнення до законодавства у сфері інформаційної і кібер- безпеки:

– доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» положеннями нормативного акту ЄС – Закону про кіберстійкість (The Cyber Resilience Act (CRA)), серед яких (положень) – встановлення стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, зокрема обов'язкові звіти про інциденти та автоматичні оновлення безпеки;

– 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 навіть якщо вони не містять інформацію, необхідність захисту якої встановлена законом, оскільки ці системи за визначенням взаємодіють із публічними мережами електронних комунікацій, зокрема, Інтернет, тому, вони є потенційною точкою входу для кібератаки;

– доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» визначенням поняття «вразливості», згідно із міжнародним стандартом інформаційної безпеки ISO 27005;

– доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» визначенням поняття «кіберконфлікт» як зіткнення різноманітних інтересів в кіберпросторі;

– реалізувати у текстах законів напрями термінологічного узгодження у ч. 2 ст. 8 та абз. 2 ч. 4 ст. 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» та у ч. 3 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» («слова «інформаційної безпеки» замінити словами «безпеки інформації»);

– доповнити Закон України від 01.06.2010 р. № 2297-VI «Про захист персональних даних», визначенням «персональні дані» з Регламенту Європейського парламенту і Ради ЄС 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних: це «будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи»;

– доповнити Закон України «Про національну безпеку України» нормами щодо правового регулювання сутності і змісту Стратегії зовнішньополітичної діяльності України, Стратегії інформаційної безпеки, Стратегії забезпечення державної безпеки, Стратегії енергетичної безпеки.

Після закінчення презентації Криволапа Є.В. присутніми фахівцями були поставлені наступні запитання:

Запитання до здобувача:

1. Вишновецька С.В. д.ю.н., професор, завідувач кафедри цивільного права та процесу

Запитання: В чому Ви вбачаєте труднощі захисту авторських прав в мережі Інтернет?

Відповідь: Дякую за запитання.

По-перше, віртуальні активи складніше візуалізувати, ніж матеріальні. Ми

можемо відносно легко встановити, що авторське право на цю книжку в паперовій формі належить певній особі, однак встановити це у віртуальній площині значно складніше.

По-друге, рух активів в мережі носить транскордонний характер, тобто контрафактні активи можуть безконтрольно переміщуватися через кордон – без будь-якого митного контрою. Транскордонний характер кіберпростору ускладнює визначення приналежності до певної юрисдикції та суб'єктів правопорушень, що негативно позначається на забезпеченні дотримання прав інтелектуальної власності.

Зазначене вимагає для ефективного захисту прав інтелектуальної власності використовувати складні кібернетичні системи. Наприклад, система Content ID створює ідентифікаційний файл для захищеного авторським правом аудіо та відеоматеріалу та зберігає його в базі даних. Коли відео завантажується, воно перевіряється в базі даних і позначається як порушення авторських прав, якщо знайдено збіг. Коли це відбувається, власник вмісту має вибір: заблокувати відео, щоб зробити його недоступним для перегляду, відстежувати статистику переглядів відео або додавати рекламу до відео яке порушує авторські права, при цьому кошти автоматично надходять власнику вмісту.

2. Легенький М.І. д.ю.н., професор, професор кафедри

Запитання: Що Ви розумієте під поняттям «вразливість» і яке це має відношення до адміністративного права?

Відповідь: Дякую за запитання.

Строго кажучи, вразливість – це певною мірою нормативне поняття. У пункті 4.2.11 Нормативного документу НД ТЗІ 1.1-003-99 Служби безпеки України вразливість системи – це нездатність системи протистояти реалізації певної загрози або сукупності загроз.

В доктринальному сенсі вразливості слід розглядати як недоліки в комп'ютерній системі, що послаблюють загальну безпеку пристрою/системи. Вразливості можуть бути слабкими місцями як в апаратному забезпеченні, так і в програмному забезпеченні. Вразливості можуть бути використані зловмисником для виконання неавторизованих (несанкціонованих) дій у комп'ютерній системі. Щоб використати вразливість, зловмисник повинен мати принаймні один відповідний інструмент, який може підключитися до слабкої сторони системи.

Адміністративне право має безпосереднє відношення до протидії використання вразливості. Воно встановлює правила, які, по-перше, регулюють порядок виявлення вразливостей, по-друге, регулюють напрями протидії виникненню вразливостей, по-третє, регламентують порядок дій при виявленні вразливостей. Характерними у цьому сенсі є Постановою КМУ від 16.05.2023 № 497 щодо порядку виявлення вразливостей або Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)) – нормативний акт ЄС щодо покращення кібербезпеки та кіберстійкості в ЄС шляхом встановлення спільних стандартів кібербезпеки для продуктів з цифровими елементами в ЄС – для уникнення або зменшення рівня вразливості.

3. Устинова І.П., к.ю.н., доцент, професор кафедри

Запитання: Як Ви вбачаєте взаємозв'язок між адміністративним правом і кібербезпекою?

Відповідь: Дякую за запитання.

Відносини у кіберпросторі диктуються, перш за все, технічними особливостями комп'ютерів, інформаційно-комунікаційних систем, програмно-апаратних комплексів. Однак засоби і методи адміністративного права встановлюють правила використання цих технічних та апаратних засобів у межах їх технічних можливостей.

Наприклад, контроль доступу передбачає адміністративне правило «надання доступу до мережі лише авторизованим користувачам», технічна реалізація – двофакторна аутентифікація. Контроль «передавання конфіденційної інформації» передбачає адміністративне правило «заборона передавання відкритим каналом», технічна реалізація – використання VPN, SSL/TLS, PGP-шифрування. Тощо.

На державному рівні – національний стандарт ДСТУ ISO/IEC 27001:2015 – регламентує створення системи управління інформаційною безпекою (СУІБ). Закон України «Про основні засади забезпечення кібербезпеки України» – визначає вимоги до державних органів та об'єктів критичної інфраструктури, зокрема, порядок створення переліків об'єктів критичної інфраструктури.

4. Лихова С.Я., д.ю.н., професор, завідувач кафедри кримінального права і процесу

Запитання: Що Ви розумієте під когнітивною безпекою і яка роль кібербезпеки в її забезпеченні?

Відповідь: Дякую за запитання.

Когнітивна безпека – це захищеність мозку і психіки людини від ворожого зовнішнього інформаційно-психологічного впливу. Завдання технічних заходів кіберзахисту – перешкодити негативним інформаційним впливам, доступу ворожого контенту, наприклад, шляхом блокування трансляції ворожих каналів чи блокування доступу до ворожих соціальних мереж, перш за все – російських.

5. Макеєва О.М., к.ю.н., доцент, завідувач кафедри

Запитання: У чому Ви вбачаєте відмінність між кіберінцидентом і кіберконфліктом?

Відповідь: Дякую за запитання.

Інцидент кібербезпеки – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора), спрямованих проти систем електронних комунікацій, систем управління технологічними процесами, а негативні прояви «кіберконфліктів» спрямовані проти інтересів осіб і провокуються протилежною стороною. Тобто, без врахування людського фактору як об'єкту негативного впливу розгляд проблематики кіберінцидентів є недостатнім та неповним.

6. Калюжний Р.А., д.ю.н., професор, професор кафедри

Запитання: Як Ви вбачаєте взаємозв'язок між інформаційною безпекою і кібербезпекою?

Відповідь: Дякую за запитання.

Відповідь на це питання надає безпосередньо пункт 52 Стратегії національної безпеки, яка визначає одним з основних завдань розвитку системи *кібербезпеки* – гарантування *кіберстійкості та кібербезпеки національної інформаційної інфраструктури*, …

Тобто, у цьому положенні прослідковується залежність забезпечення національної безпеки від *інформаційної* та *кібер- безпеки*, а також завдання заходів кібербезпеки – технічний і організаційний захист кіберпростору, захист критичної інфраструктури, цифрових систем, державних реєстрів, захист інформаційного середовища від потрапляння ворожого, підривного контенту, який негативно впливає на населення та суспільство.

Зокрема, пропонуються наступні технічні засоби кіберзахисту захисту інформації, тобто 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; створення резервних копії, щоб уникнути втрати даних; використання тільки ліцензійних та офіційних програм тощо.

Після відповідей на запитання виступили:

Науковий керівник – професор кафедри теорії держави і права, конституційного та адміністративного права КАІ, доктор юридичних наук, професор Кунєв Юрій Дем’янович.

Кунєв Ю.Д. Зазначено, що дисертант успішно виконав індивідуальний план наукової роботи та індивідуальний навчальний план. Підготовлена дисертація готова до захисту. У роботі опрацьовано досить багато різноманітного матеріалу, дуже багато наукових праць – вітчизняні та іншомовні видання, великий нормативний матеріал, у тому числі акти Європейського рівня, що дозволило узагальнити досить широкий світовий досвід і зробити компаративні висновки щодо відповідності національного законодавства європейським вимогам.

У процесі виконання роботи дисертант показав необхідну кваліфікацію для самостійного вирішення поставлених наукових задач, постійно працює над підвищенням свого освітнього і професійного рівня. Вміє проводити наукові дослідження, бере участь у науково-дослідних роботах, має наукові публікації та доповіді у наукових конференціях.

Структура дисертації дозволила автору повною мірою охопити предмет дослідження. Справляє позитивне враження джерельна база роботи, що свідчить про системне і повне опрацювання проблеми й високий рівень наукової підготовки автора.

В дисертаційній роботі автором запропонований міждисциплінарний підхід до вивчення та реалізації ефективних засобів правового забезпечення інформаційної й кібербезпеки, який полягає у поєднанні засобів, методів і правил адміністративного права, інформаційного права, пра́ва кібербезпеки, теорії психології впливів, деліктологія. Широка обізнаність здобувача у вказаних сферах дозволила здобувачу отримати нові цінні наукові і практичні висновки та

сформулювати пропозиції щодо удосконалення законодавства. При цьому, з точки зору діяльнісного підходу, перевага здобувача як виконавця даної роботи полягає у глибокому знанні саме обраного предмету правового регулювання – кібербезпеки. Дана робота є особливо актуальною в умовах широкомасштабної агресії російської федерації проти України, важливою складовою якої була та є інформаційна війна. Дисертантом запропоновані нові науково обґрунтовані положення щодо реалізації публічною адміністрацією владних повноважень у сфері кібербезпеки; запропоновано авторське розуміння адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України; виконано порівняння положень національних нормативно-правових актів з європейськими; запропонована авторська структура інформаційних прав громадян тощо. Внесені пропозиції щодо удосконалення національного законодавства (7 пропозицій).

Отже, дисертація може виступати теоретичною основою для проведення науково-прикладних досліджень у сфері визначення публічного-правових підходів до реалізації систем захисту від кіберзагроз і протидії вразливостям. Основні положення та результати дисертаційного дослідження викладено у 19,5 наукових працях, 6,5 наукових статтях, опублікованих у фахових виданнях України з юридичних наук, а також у 13 тезах доповідей, опублікованих за результатами участі в науково-практичних конференціях, у тому числі міжнародних, всеукраїнських і зарубіжних. Зазначені публікації повною мірою висвітлюють основні наукові положення дисертаційного дослідження. Дисертація є самостійно написаною кваліфікаційною науковою працею із науково-обґрунтованими висновками та рекомендаціями, які виставлені автором для публічного захисту. Використання чинних думок та ідей, результатів дослідження інших авторів мають посилання на відповідні джерела. Загальний аналіз роботи свідчить про самостійність і цілісність проведеного дослідження, його актуальність і науковий рівень, теоретичне й практичне значення. Наукові положення, висновки та рекомендації, сформульовані в роботі, достатньо повно викладені в опублікованих здобувачем наукових публікаціях. Виконані у дисертації дослідження тісно пов’язані з факультетськими, зокрема, 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).

Дисертаційна робота є завершеною науковою працею, яка націлена на вирішення актуальної наукової задачі, відповідає спеціальності 081 «Право», а її автор Криволап Євгеній Володимирович заслуговує присудження наукового ступеня доктора філософії, на підставі Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, який затверджено Постановою Кабінету Міністрів України № 44 від 12.01.2022.

Науковий керівник запропонував затвердити позитивний висновок про наукову новизну, теоретичне та практичне значення результатів зазначеної

дисертації та рекомендувати її до захисту на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

Рецензенти дисертаційної роботи, які наголосили на позитивних аспектах дослідження та висловили свої побажання та зауваження:

Легенький М.І., доктор юридичних наук, професор**.** Зазначив, що робота є вкрай необхідним дослідженням. Зокрема, 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, вибудована та систематизована структура підзаконних нормативно-правових актів України у сфері кіберзахисту, 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– розуміння логіки побудови структури підзаконних нормативно-правових актів України у сфері кіберзахисту. Заслуговують на увагу узагальнення автора у сфері кіберконфліктів, зокрема, кібербулінг, кіберсталкінг, що реально спрямовано на захист прав осіб у кіберсфері. Запропоновано зміни до чинної нормативної бази. Відтак, робота відповідає вимогам для спеціальності 081 «Право», у тому числі за рахунок методів, що знайшли абсолютно чітке впровадження і застосування. Дослідження є надзвичайно актуальним, останні події це підтверджують, коли виникає потреба формування і реалізації економічної співпраці з міжнародними фінансовими організапмціями як учасниками фінансовоїх діяльності в Україні так і закордоном.

Публікації автора є дуже ґрунтовно підготовленими, і вони є в належній кількості, зокрема, у виданнях групи Б. Результати дослідження апробовані на наукових конференціях.

Загалом дисертаційна робота є завершеною та такою, що відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженому постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

Філінович В.В., доктор юридичних наук, доцент. Зазначила, що робота є вкрай актуальним дослідженням. Позитивно оцінила дослідження дисертанта у сфері захисту прав інтелектуальної власності в Інтернеті. Автор правильно розставляє акценти щодо особливостей такого захисту саме в Інтернеті. Позитивною є увага автора до технічних засобів захисту прав інтелектуальної власності у кіберсфері – використання цифрових водяних знаків (watermark); DRM (Digital Rights Management) – технології контролю копіювання контенту; системи моніторингу порушень (наприклад, Content ID у YouTube).

Структура відповідає цілям і завданням дослідження, дозволяє послідовно розглянути всі проблеми, визначені автором. Обґрунтованість положень, сформульованих у дисертації, підтверджується критичним аналізом наявних

літературних джерел, вітчизняного та міжнародного законодавства, статистичних матеріалів та міжнародної практики. Отже, робота відповідає встановленим вимогам і може бути рекомендована до захисту на здобуття наукового ступеня доктора філософії в за спеціальністю 081 Право. Підтримую роботу і бажаю успіхів дисертанту.

В **обговоренні** дисертаційного дослідження взяли участь:

Жукорська Я.М. к.ю.н., доцент, декан Факультету права та міжнародних відносин КАІ

Такий науковий доробок для здобувача доктора філософії це серйозно, бо основні положення дисертаційного дослідження відображено у 19,5 наукових працях, 6,5 наукових статтях, опублікованих у фахових виданнях України з юридичних наук, а також у 13 тезах доповідей, опублікованих за результатами участі в науково-практичних конференціях, у тому числі міжнародних, всеукраїнських і зарубіжних. Бажаю вам успіхів!

Лихова С.Я., д.ю.н., професор, завідувач кафедри кримінального права і процесу

Слід звернути увагу, що тема виконана на актуальну тему з відповідною новизною. Мета, предмет і об'єкт дослідження визначені вірно відповідно до теми. В цілому висновки по роботі відповідають поставленим завданням. Доповідь дисертанта та власне дослідження свідчать про його належний рівень як науковця. Відзначаю активність дисертанта, що підтверджується тезами доповідей на конференціях. Відзначаю позитивні напрацювання дисертанта щодо регулювання адміністративно-правової діяльності правоохоронних органів у сфері запобігання кіберзлочинності. Підтримую дисертаційне дослідження та зазначаю, що автор заслуговує на присудження ступеня доктора філософії.

Калюжний Р.А. д.ю.н., професор, професор кафедри.

Наукове дослідження охоплює широкий спектр проблем, враховує значні напрацювання інших дослідників, характеризується комплексністю і глибиною. Автором було переконливо обґрунтовано пропозиції, які викладені у дисертації. Робота є логічною, матеріал є продуманим, поставлені завдання є чіткими та аргументованими, автором опубліковано належну кількість праць.

Отримані дисертантом результати мають наукову новизну, важливе теоретичне та практичне значення, та заслуговує на позитивну оцінку дисертаційної роботи.

Макеєва О.М., к.ю.н., доцент, завідувач кафедри.

Дисертація складається зі вступу, трьох розділів, які містять 9 підрозділів, висновків, списку використаних джерел (366 найменувань) і 3 додатків. Загальний обсяг дисертації становить 343 сторінок, з них основний текст – 229 сторінок. Під час підготовки дисертаційної роботи Євгеній Володимирович проявив себе як творчий дослідник, йому притаманні такі якості як, сміливість у поєднанні висновків та джерел із різних сфер науки, ретельність в опрацюванні наукового і практичного матеріалу, глибоке знання законодавства, допитливість,

наполегливість, здатність до високого рівня теоретичних і практичних узагальнень. На високому рівні володіє сучасними методами наукового пізнання, має належний рівень теоретичної і практичної підготовки.

ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації Криволапа Євгенія Володимировича на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», поданої на здобуття ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право»

1. Обґрунтування вибору теми дослідження. Широкомасштабна агресія російської федерації проти України, важливою складовою якої була та є інформаційна війна, поставила перед науковцями та практиками нові завдання у галузі протидії інформаційним операціям та інформаційним війнам. Само обґрунтування військового вторгнення російської федерації в Україну є (були) пропагандистські штампи, які створили для керівництва російської федерації «віртуальну реальність», у межах якої і приймалося рішення про вторгнення.

У сучасних умовах у здійсненні інформаційних атак і спеціальних інформаційних операцій провідну роль відіграють сучасні електронні засоби масової комунікації (радіомовлення, телебачення, супутниковий зв'язок, Інтернет). Натомість, розвиток інформаційного суспільства не тільки відкриває великі можливості, але водночас породжує серйозні проблеми, зокрема: протидії негативним ворожим інформаційним впливам – як на українську аудиторію, так і за кордонами України. Тобто, інформаційна війна переміщується у кіберпростір. Агресія російської федерації показала вразливість національної і європейської систем кіберзахисту проти кібератак. Тому стає вкрай актуальною необхідність подальшого унормування правового регулювання діяльності з поширення інформації в мережі Інтернет; формування правових умов для забезпечення об’єктивності та достовірності інформації; вдосконалення правових вимог щодо дотримання журналістами, які працюють в мережі Інтернет, професійних етичних стандартів тощо. При цьому усі ці системи захисту повинні укладатися у демократичні обмеження щодо втручання держави у свободу слова, самовираження, свободу пошуку і поширення інформації

У науковій площині питання публічного регулювання у сфері інформаційної і кібер- безпеки розглядалися і досліджувалися, зокрема у працях таких вчених, як Р.А. Калюжний, Ю.Д. Кунєв, С.Я. Лихова, В.В. Філінович, О.О. Тихомиров, Н.Б. Новицька, М.І. Легенький, І.М. Сопілко, А.І. Марущак, В.Ю. Богданович, В.А. Ліпкан, інші автори. Проте, наразі бракує комплексних досліджень щодо публічного регулювання діяльності у сфері кібербезпеки, оскільки наявні праці розкривають окреслені питання лише в окремих сферах. Саме наведене й зумовлює актуальність пропонованого міждисциплінарного дослідження.

2. Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження виконано 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).

Тема дисертації відповідає освітньо-науковій програмі «Право» за спеціальністю 081 «Право» 08 «Право» в КАІ (зокрема, ОК 1.3.1, ОК 1.3.2, ОК, 1.3.3. та ОК 1.3.4).

3. Мета й завдання дослідження. Метою дисертаційного дослідження визначене розкриття сутності і змісту адміністративно-правових засад спрямування методів і засобів забезпечення кібернетичної безпеки на вирішення завдань забезпечення інформаційної та кібер- безпеки.

Сформульована мета дослідження обумовила необхідність вирішення наступних ***завдань***:

– здійснити системний аналіз наукового доробку вітчизняних та зарубіжних учених за темою дисертаційного дослідження;

– визначити засадничі вимоги безпекових Стратегій 2020-2021 років в Україні (Стратегія національної безпеки України від 14.09.2020 р.; Стратегія воєнної безпеки України від 25.03.2021 р.; Стратегія кібербезпеки України від 14.05.2021 р.; Стратегія інформаційної безпеки від 15.10.2021 р.);

– уточнити та розширити понятійно-категорійні концепти «безпека інформації», «інформаційна безпека», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років;

– обґрунтувати наукове визначення категорії «когнітивна безпека» як складової протидії інформаційно-психологічним операціям ворога;

– дослідити особливості правового регулювання заходів забезпечення кібербезпеки правовими актами європейського рівня;

– розкрити особливостей правового регулювання заходів забезпечення кібербезпеки актами національного права;

– обґрунтувати форми та визначити особливості методів забезпечення кібербезпеки як чинників забезпечення інформаційної безпеки;

– узагальнити повноваження суб'єктів кіберзахисту у сфері забезпечення кібербезпеки як чинників забезпечення інформаційної безпеки;

– розкрити систему прав і свобод людини і громадянина, що забезпечуються в межах кібербезпеки, здійснивши їх класифікацію за видами та окресливши організаційно-правові й технологічні механізми гарантування;

– обґрунтувати потенціал та необхідність міждисциплінарного підходу у сфері інформаційної та кібер- безпеки, що базується на інтеграції доктринальних положень адміністративного та інформаційного права, з одного боку, та наукових здобутків та практичного досвіду інформаційних технологій – з іншого.

4. Об’єктом дослідження є теорія й практика організації діяльності у сфері забезпечення інформаційної і кібернетичної безпеки України.

5. Предметом дослідження є адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України.

6. Методи дослідження. Методологічну основу дисертаційного дослідження становить сукупність взаємопов’язаних методів наукового пізнання, що забезпечили системний підхід до вирішення поставлених завдань, єдність юридичної форми і правового змісту отриманих результатів (усі розділи роботи). Застосовується міждисциплінарний підхід у сфері інформаційної та кібер-безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права (принципи діяльності публічної адміністрації і організації публічного управління в демократичному суспільстві), інформаційного права (поєднання свободи інформаційної діяльності із захистом національного інформаційного простору України від розповсюдження ворожої інформаційної продукції, створення та використання інформаційних технологій), пра́ва кібербезпеки (врахування конкретних ситуацій прийняття рішень публічною адміністрацією), теорії психології впливів (захист осіб від шкідливих інформаційних впливів, забезпечення когнітивної безпеки), деліктології (вивчення заходів державного примусу адміністративно-правового і кримінально-правового характеру для забезпечення встановлених правил у сфері інформаційної та кібр- безпеки) (підрозділи 1.1 + 1.2 + 1.3 + 3.1 + 3.2). Важливе місце у роботі займає використання принципу аналізу-синтезу як методу діалектичного мислення (підрозділ 2.3). Системний метод застосовано для упорядкування емпіричної інформації та проведення класифікації досліджуваних правових явищ (підрозділ 2.3). Документальний аналіз дозволив послідовно дослідити документальні джерела правових явищ, які використані у даній роботі, зокрема, міжнародні акти, акти органів української влади, рішення судів тощо (підрозділи 2.1 + 2.2). Метод абстрагування дозволив залишати на певних етапах дослідження поза увагою конкретні численні сторони і ознаки відповідного явища, але виявити у ньому найбільш характерне, тобто розкрити останнє як наукову категорію (підрозділ 3.3). Компаративний метод (метод порівняння) застосовано для порівняння, з одного боку, законодавства України, а з іншого боку, законодавства Європейського Союзу і Ради Європи (підрозділи 2.1 + 2.2). Використання методу об’єктивної істини здійснено шляхом перехресної перевірки даних, використаних при дослідженні, дослідження із декількох джерел, опори на статистичні дані та судову практику (усі розділи роботи).

Науково-теоретичне підґрунтя для виконання дисертації становлять наукові праці фахівців у галузі адміністративного права, інформаційного права, теорії держави і права, інших галузевих юридичних наук, інформаційно-комунікаційних технологій та кібербезпеки, у тому числі робіт зарубіжних дослідників.

Нормативну основу дослідження становлять Конституція України, чинні законодавчі та підзаконні нормативно-правові акти України, а також міжнародно-правові акти та законодавство зарубіжних країн, приписи якого можуть бути імплементовані у законодавство України. Використані також наукові аналітичні

публікації, публікації у засобах масової інформації, інші інформаційні джерела, не заборонені законодавством.

7. Наукова новизна одержаних результатів полягає в 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 новизни:

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 кіберпрострі, 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 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.

8. Теоретичне значення. У дисертації здійснено теоретичне узагальнення і подано нове розв'язання важливих наукових завдань розвитку основ адміністративного і інформаційного права, розроблення теоретичних і практичних основ адміністративно-правового регулювання діяльності із забезпечення кібернетичної безпеки України. Розв'язане наукове завдання щодо розкриття сутності і змісту адміністративно-правових засад спрямування методів і засобів забезпечення кібернетичної безпеки на вирішення проблем забезпечення інформаційної та кібер- безпеки, усвідомлення сучасних викликів у зв'язку із широкомасштабною агресією рф проти України, визначено та окреслено основні шляхи їх розв'язання. Практично застосовані відомі й запропоновані нові підходи до розробки категорій і принципів діяльності публічної адміністрації у цій сфері, а також засобів оптимізації процесної та системної складових такої діяльності та її правової організації.

9. Практичне значення одержаних результатів дослідження полягає у 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);

– Українською асоціацією інвестиційного бізнесу для забезпечення підвищення рівня захисту інформаційних баз даних (довідка про впровадження від 01.12.2025).

10. Особистий внесок здобувача. У межах дисертаційного дослідження здійснено формулювання теоретичних положень, узагальнень і висновків, що мають наукове та прикладне значення. Розроблені практичні рекомендації та пропозиції ґрунтуються на самостійному комплексному аналізі чинного законодавства, спеціальної наукової літератури та адміністративно-правової практики у сфері забезпечення кібербезпеки. Висвітлені положення є результатом системного осмислення правових механізмів забезпечення кібербезпеки, інформаційних права громадян. у дисертації не використовуються наукові ідеї та розробки, що належать співавторам опублікованих робіт. Висновки та положення дисертації обґрунтовані автором особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

11. Апробація результатів дисертації. Результати дослідження, його основні висновки та рекомендації оприлюднені на 13 наукових конференціях, а саме: «Свобода, безпека та незалежність: правовий вимір» (Київ, 2023), «Наукові дослідження та інновації» (Дніпро, 2023), «Глобальні проблеми та рішення» (Дніпро, 2023), «VI Міжнародний молодіжний науковий юридичний форум» (Київ, 2023), «AEPO-2023. Повітряне і космічне право» (Київ, 2023), «Правова парадигма відновлення України: проблеми та перспективи» (Київ, 2024); «Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором» (Київ, 2024), «VII Міжнародний молодіжний науковий юридичний форум» (Київ, 2024), «Актуальні питання забезпечення кібербезпеки» (Київ, 2024), «Правова система України: європейський вектор розвитку в умовах воєнного стану» (Київ, 2025), «Інновації та нові напрямки в наукових дослідженнях» (Манчестер, Велика Британія, 2025), «AEPO-2024. Повітряне і космічне право» (Київ, 2024), «Соціально-економічний розвиток у контексті викликів сьогодення» (Одеса, 2025).

12. Публікації. Основні положення дисертаційного дослідження відображено у 19,5 наукових працях, зокрема у 6,5 наукових статтях, опублікованих у фахових виданнях України з юридичних наук, а також у 13 тезах, опублікованих за результатами участі в науково-практичних конференціях, у тому числі міжнародних, всеукраїнських і зарубіжних.

Список опублікованих праць за темою дисертації

Статті у наукових фахових виданнях України:

1. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник.*

Повітряне і космічне право». 2022. № 3 (64). С. 78-86. DOI: https://doi.org/10.18372/2307-9061.64.16893

Особистий внесок Бєлкіна Л.М. - постановка завдання,

Особистий внесок Юринець Ю.Л. - огляд стану розроблення питання,

Особистий внесок Бєлкіна М.Л. - підбір літератури,

Особистий внесок Криволапа Є.В. - розмежування понять «інформаційна безпека» і «безпека інформації», виділення поняття «когнітивна безпека».

2. Guoqiang Fu, Криволап Є.В. Особливості термінології в англомовній літературі у сфері кібербезпеки. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право*». 2023. № 1 (66). С. 63-71. DOI: https://doi.org/10.18372/2307-9061.66.17419

Особистий внесок Фу Г. - підбір ключової англомовної термінології з питання,

Особистий внесок Криволапа Є.В. - тлумачення деяких англомовних термінів українською мовою.

3. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Питання нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 3 (68). С. 16-23. DOI: https://doi.org/10.18372/2307-9061.68.17969

Особистий внесок Криволапа Є.В. - вперше виконав адміністративно-правовий аналіз процедури Bug Bounty, проаналізував її правовий аспект,

Особистий внесок Юринець Ю.Л. - огляд напрямів застосування процедури,

Особистий внесок Бєлкіна Л.М. - постановка завдання.

4. Криволап Є.В., Юринець Ю.Л. Взаємозв'язок безпекових стратегій України з інформаційною безпекою та кібербзпекою. *Актуальні питання у сучасній науці*. 2023. № 8 (14). С. 477-487. DOI: https://doi.org/10.52058/2786-6300-2023-8(14)-477-487

Особистий внесок Криволапа Є.В. - встановлення логіки взаємозв'язків і взаємовпливів інформаційної безпеки та кібербезпеки з іншими компонентами національної безпеки,

Особистий внесок Юринець Ю.Л. - постановка завдання.

5. Криволап Є.В. Адміністративно-правове регулювання заходів протидії кіберзагрозам актами європейського рівня. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право*». 2024. № 3 (72). С. 84-92. DOI: https://doi.org/10.18372/2307-9061.72.19064

6. Юринець Ю.Л., Криволап Є.В. Соціальні мережі як чинник впливу на формування іміджу закладу вищої освіти. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2025. № 2 (75). С. 201-210. DOI: https://doi.org/10.18372/2307-9061.75.20235

Особистий внесок Юринець Ю.Л. - постановка завдання,

Особистий внесок Криволапа Є.В. - аналіз властивостей соціальних мереж як чинника формування іміджу.

7. Криволап Є.В. Публічно-правове регулювання підвищення рівня кібербезпеки в Європейському Союзі на підставі акту про кіберстійкість (The

Cyber resilience Act). *Наукові інновації та передові технології (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»)*: журнал. 2025. № 3 (43). С. 516-526. DOI: https://doi.org/10.52058/2786-5274-2025-3(43)-516-526

8. Юринець Ю.Л., Криволап Є.В., Сопілко І.М., Бєлкін Л.М., Бєлкін М.Л. Проблеми формування державної політики у сфері кіберконфліктів. *Успіхи і досягнення у науці (Серія «Право», Серія «Освіта», Серія «Управління та адміністрування», Серія «Соціальні та поведінкові науки»)*, 2025. № 6 (16). С. 249-270. DOI: https://doi.org/10.52058/3041-1254-2025-6(16)-249-270.

Особистий внесок Юринець Ю.Л. - постановка завдання,

Особистий внесок Криволапа Є.В. - формування переліку видів кіберконфліктів та аналіз їх властивостей,

Особистий внесок Сопілко І.М. - підбір правових актів,

Особистий внесок Бєлкіна Л.М. - генезис понять «кіберінцедент» та «кіберконфлікт»,

Особистий внесок Бєлкіна М.Л. - підбір літератури.

Наукові праці, які додатково відображають наукові результати дисертації:

9. Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека». «Когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство. *Свобода, безпека та незалежність: правовий вимір*: матеріали XIII Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 24 лютого 2023 р. С. 195-197.

10. Криволап Є.В. Питання застосування механізмів забезпечення інформаційної безпеки і кібербезпеки в реалізації безпекових стратегій України. *Наукові дослідження та інновації*: матеріали 2-ї Міжнар. науково-практичної інтернет-конференції, 3-4 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 216-218.

11. Криволап Є.В. Засади правового регулювання заходів забезпечення кібербезпеки актами європейського рівня. *Глобальні проблеми та рішення*: матеріали 2-го Міжнародного науково-практичного Інтернет-конгресу, 10-11 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 42-45.

12. Криволап Є.В. Вплив стратегій інформаційної та кібербзпеки на інші безпекові стратегії України. *VI Міжнародний молодіжний науковий юридичний форум*: матеріали форуму, м. Київ, Національний авіаційний університет, 18 травня 2023 р. С. 119-121.

13. Криволап Є.В., Юринець Ю.Л. До питання вразливості інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *АЕРО-2023. Повітряне і космічне право*: матеріали Всеукраїнської конференції здобувачів вищої освіти і молодих учених, м. Київ, Національний авіаційний університет, 23 листопада 2023 р. Тернопіль: Вектор. С. 118-120.

14. Криволап Є.В. Підвищення рівня контролю і протидії вразливостям інформаційно-комунікаційних систем в аспекті відновлення України. *Правова парадигма відновлення України: проблеми та перспективи*: матеріали XIV

Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 23 лютого 2024 р. Тернопіль: Вектор, 2024. с. 220-223.

15. Криволап Є.В., Бєлкін Л.М., Юринець Ю.Л. Правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором*: зб. матеріалів міжвідомчої науково-практичної конференції, 27 березня 2024 р., Київ / [відп. ред. Парфило О.А.] ; Укр. наук.-дослід. ін.-т спец. техніки та судових експертиз Служби безпеки України. Київ : ІСТЕ СБУ, 2024. С. 99-103.

16. Криволап Є.В. Адміністративно-правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *VII Міжнародний молодіжний науковий юридичний форум*: матеріали форуму, м. Київ, Національний авіаційний університет, 16-17 травня 2024 р. С. 145-147.

17. Бєлкін М.Л., Криволап Є.В., Юринець Ю.Л. Адміністративно-правове регулювання нейтралізації вразливостей інформаційно-комунікаційних систем. *Збірник матеріалів «Актуальні питання забезпечення кібербезпеки» IX Міжнародної науково-практичної конференції*, м. Київ, 13 листопада 2024 року. Київ. МАУП. 13 листопада 2024 року. С. 38-42.

18. Криволап Є.В. Правові підходи до підвищення рівня кібербезпеки в Європейському Союзі (the Cyber Resilience Act, CRA). *Правова система України: європейський вектор розвитку в умовах воєнного стану*: матеріали XV Міжнародної науково-практичної конференції, м. Київ, Державний університет «Київський авіаційний інститут», 21 лютого 2025 р. Тернопіль: Вектор, 2025. С. 201-204.

19. Криволап Є., Юринець Ю., Бєлкін Л., Бєлкін М. Поняття «кіберконфлікти» в системі термінології з кібербезпеки. *Innovations and New Directions in Scientific Research*: Proceedings of the 2nd International Scientific Conference, Manchester, United Kingdom, 20 September 2025. Lulu Press, Inc., 2025. P. 191-195.

20. Криволап Є.В. Використання фейкових сайтів в російській пропаганді. *АЕРО-2024. Повітряне і космічне право*: матеріали Всеукраїнської конференції, м. Київ, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», 20 листопада 2024 р. Тернопіль. «Вектор». С. 113-115.

21. Юринець Ю.Л., Криволап Є.В., Бєлкін Л.М. Використання соціальних мереж для формування іміджу закладів вищої освіти. *Соціально-економічний розвиток у контексті викликів сьогодення*: матеріали III Міжнародної науково-практичної конференції / Східноєвропейський центр наукових досліджень (Одеса, 16 серпня 2025 р). Research Europe, 2025. С. 123-127.

13. Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, які містять 9 підрозділів, висновків, списку використаних джерел (366 найменувань) і 3 додатків. Загальний обсяг дисертації становить 343 сторінок, з них основний текст – 229 сторінок.

14. Характеристика особистості здобувача. Під час підготовки дисертаційної роботи Криволап Є.В. проявив себе як творчий дослідник і науковець. Йому притаманні такі якості, як сміливість у поєднанні висновків та джерел з різних сфер науки, ретельність в опрацюванні наукового і практичного матеріалу, глибоке знання законодавства, допитливість, наполегливість, методологічна грамотність, логічність у викладенні думок, здатність до високого рівня теоретичних і практичних узагальнень; як особистості – патріотизм, пріоритет у захисті українських інтересів в обраній сфері дослідження, висока працездатність, доброзичливість, тактовність тощо. На високому рівні володіє сучасними методами наукового пізнання, має належний рівень теоретичної та практичної підготовки.

15. Оцінка мови та стилю дисертації. Дисертація написана грамотно, науковим стилем, а викладені матеріали дослідження, наукові положення, висновки і рекомендації сприймаються легко та доступно. Матеріали дослідження оформлені у відповідності до вимог Міністерства освіти і науки України.

16. Відповідність принципам академічної доброчесності.

На підставі вивчення тексту дисертації здобувача, наукових праць аспіранта та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано у антиплагіатній інтернет системі Strikeplagiarism.com) встановлено, що дисертаційна робота виконана самостійно, текст дисертації не містить плагіату, а дисертація відповідає вимогам академічної доброчесності.

17. Рецензенти рекомендують: відповідно до пп. 15, 16 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***, пропонується такий склад разової ради:***

Голова спеціалізованої вченої ради:

Лихова Софія Яківна, доктор юридичних наук, професор, завідувач кафедри кримінального права і процесу КАІ;

Рецензенти

Легенький Микола Іванович, доктор юридичних наук, професор**,** професор кафедри теорії держави і права, конституційного та адміністративного права КАІ;

Філінович Валерія Вікторівна, доктор юридичних наук, доцент, доцент кафедри цивільного права та процесу КАІ;

Офіційні опоненти:

Новицька Наталія Борисівна, доктор юридичних наук, професор**,** професор кафедри цивільного права та процесу Державного податкового університету Міністерства фінансів України;

Тихомиров Олександр Олександрович, доктор юридичних наук, доцент, доцент кафедри інформаційної безпеки держави Навчально-наукового інституту інформаційної безпеки і стратегічних комунікацій Національної академії Служби безпеки України.

Усі члени разової спеціалізованої вченої ради не мають реальний чи потенційний конфлікт інтересів щодо здобувача Криволапа Євгенія Володимировича (зокрема, є його близькою особою) та/або його наукового керівника.

У результаті попередньої експертизи дисертації Криволапа Євгенія Володимировича і повноти публікації основних результатів дослідження

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Криволапа Євгенія Володимировича на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України».

2. Вважати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Криволапа Євгенія Володимировича відповідає спеціальності 081 «Право» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року. № 261 (зі змінами і доповненнями від 03 квітня 2019 року № 283), вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 року № 44

3. Рекомендувати дисертаційну роботу «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», подану Криволапом Євгенієм Володимировичем на здобуття ступеня доктора філософії за спеціальністю 081 «Право» до захисту у разовій спеціалізованій вченій раді.

4. Рекомендувати Вченій раді КАІ клопотати про призначення:

Головою спеціалізованої вченої ради:

Лихову Софію Яківну, доктора юридичних наук, професора, завідувача кафедри кримінального права і процесу КАІ;

Рецензентами:

Легенького Миколу Івановича, доктора юридичних наук, професора**,** професора кафедри теорії держави і права, конституційного та адміністративного права КАІ;

Філінович Валерію Вікторівну, доктора юридичних наук, доцента, доцента кафедри цивільного права та процесу КАІ;

Офіційними опонентами:

Новицьку Наталію Борисівну, доктора юридичних наук, професора**,** професора кафедри цивільного права та процесу Державного податкового університету Міністерства фінансів України;

Тихомирова Олександра Олександровича, доктора юридичних наук, доцента, доцента кафедри інформаційної безпеки держави Навчально-наукового інституту інформаційної безпеки і стратегічних комунікацій Національної академії Служби безпеки України.

Результати голосування щодо рекомендації до захисту дисертації Криволапа Євгенія Володимировича:

«за» –10
«проти» – немає
«утримались» – немає

Головуючий на засіданні:
завідувач кафедри теорії держави і права, конституційного та адміністративного права КАІ, кандидат юридичних наук, доцент — Олена МАКЄЄВА

Секретар засідання:
доцент кафедри теорії держави і права, конституційного та адміністративного права КАІ, кандидат історичних наук, доцент — Світлана ГОЛОВКО

ПОГОДЖЕНО:
Проректор з наукових досліджень та трансферу технологій КАІ, доктор технічних наук, професор — Сергій ГНАТЮК