ЗАТВЕРДЖУЮ

Т.в.о. ректора

Дніпровського державного

університету внутрішніх справ

кандидат технічних наук, доцент

Ігор МАГДАЛІНА

19.05. 2026 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика», поданої на здобуття ступеня доктора філософії в галузі знань 08 Право за спеціальністю 081 Право

ВИТЯГ

з протоколу спільного засідання кафедри теорії держави та права, кафедри теорії та історії держави та права, конституційного права та прав людини, кафедри адміністративного права і процесу Дніпровського державного університету внутрішніх справ від 19 травня 2026 року щодо публічної презентації Антоном РЯПОЛОВИМ наукових результатів дисертації на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика»

Головуючий: доктор юридичних наук, професор Валентина БОНЯК

Секретар: Юлія ЛЕБЕДЄВА

Присутні: доктор юридичних наук, професор Олександр ЮНІН, доктор юридичних наук, професор Лариса НАЛИВАЙКО, доктор юридичних наук, старший дослідник Максим ПОЧТОВИЙ, доктор юридичних наук, професор Людмила ДОБРОБОГ, доктор юридичних наук, професор Дмитро СЕЛІХОВ, доктор юридичних наук, професор Роман МИРОНЮК, доктор юридичних наук, професор Борис ЛОГВИНЕНКО, доктор юридичних наук, професор Роман ОПАЦЬКИЙ, кандидат юридичних наук, доцент Ольга КУЛІНІЧ, кандидат юридичних наук, доцент Андрій САМОТУГА, доктор філософії в галузі права Каріна ПІСОЦЬКА.

З 12 присутніх – 9 докторів юридичних наук та 3 кандидати юридичних наук (докторів філософії) – 7 фахівців за профілем поданої на розгляд дисертації.

ПОРЯДОК ДЕННИЙ:

Обговорення дисертаційної роботи Антона РЯПОЛОВА «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика», поданої на здобуття ступеня доктора філософії за спеціальністю 081 «Право» щодо її рекомендації для попереднього розгляду та захисту в разовій спеціалізованій вченій раді.

СЛУХАЛИ:

Доповідь здобувача Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика», поданої на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

У своїй доповіді дисертант визначив мету, задачі, предмет, об'єкт і методи дослідження, розкрив структуру роботи та основні її положення, показав їхню новизну, теоретичне та практичне значення, а також обґрунтував актуальність обраної теми дисертаційної роботи, яка зумовлена необхідністю розв'язання наукового завдання щодо комплексного теоретико-правового аналізу інформаційної безпеки України в умовах воєнного стану, розкриття її сутності, структури та місця у системі національної безпеки, оцінки ефективності нормативно-правового та інституційного забезпечення, а також розроблення науково обґрунтованих пропозицій щодо його удосконалення з урахуванням сучасних викликів, зокрема у сфері кібербезпеки та забезпечення інформаційного суверенітету.

Здобувач зазначив, що у сучасних воєнних конфліктах інформаційна сфера дедалі частіше перетворюється на самостійне поле протистояння. Стрімкий розвиток інформаційних технологій, глобалізації комунікаційних мереж та зростання кіберзагроз забезпечення захисту державної, суспільної та приватної інформації стає критично важливим для стабільного функціонування держави. В умовах воєнного стану питання інформаційної безпеки України виходить на перший план, адже саме вона забезпечує захист суспільства та держави від деструктивного впливу пропаганди, кіберзагроз, маніпуляцій та інформаційних атак.

Інформаційна безпека є одним із основних елементів національної безпеки сучасної держави. Гібридна агресія проти України поєднує в собі традиційні збройні методи із масованими кібератаками, дезінформаційними кампаніями, маніпулюванням суспільною свідомістю та цілеспрямованим руйнуванням інформаційної інфраструктури держави. За таких умов інформаційна безпека перетворюється з одного з елементів національної безпеки на її стратегічну основу, від якої залежить здатність держави зберігати суверенітет, мобілізовувати суспільство та ефективно протистояти агресору.

Проведене дослідження викликано необхідністю комплексного наукового аналізу правових механізмів та нормативно-правового забезпечення інформаційної безпеки України в умовах воєнного стану. Актуальність теми визначається низкою чинників, а саме: зростанням кіберзагроз та кібератак, спрямованих на державні інформаційні системи, критичну інфраструктуру та стратегічні об'єкти, що створює безпосередню загрозу національній безпеці;

необхідністю вдосконалення нормативно-правової бази, що регулює інформаційну безпеку в умовах воєнного стану, з урахуванням сучасних технологічних та військово-політичних викликів; важливістю удосконалення інституційних механізмів, що забезпечують функціонування системи інформаційної безпеки, підвищенням ефективності координації між державними органами, правоохоронними структурами та сектором критичної інфраструктури; недостатньою науково-правовою розробленістю окремих аспектів інформаційної безпеки, особливо щодо інтеграції кібербезпеки, законодавчого регулювання та адаптації зарубіжного досвіду до умов воєнного стану.

Зазначене зумовило мету дисертаційного дослідження, що полягає у комплексному теоретико-правовому аналізі інформаційної безпеки України в умовах воєнного стану, розкритті її сутності, структури та місця у системі національної безпеки, оцінці ефективності нормативно-правового та інституційного забезпечення, а також розробленні науково обґрунтованих пропозицій щодо їх удосконалення з урахуванням сучасних викликів, зокрема у сфері кібербезпеки та забезпечення інформаційного суверенітету.

Для вирішення поставлених завдань і досягнення мети було використано комплекс загальнофілософських підходів, загальнонаукових, спеціальних та власних методів правознавства.

Нормативно-правовим підґрунтям дослідження є міжнародні договори у сфері інформаційної безпеки, згоду на обов'язковість яких надано Верховною Радою України, Конституція України, а також система національних нормативно-правових актів, що регулюють відносини у сфері інформаційної, кібернетичної безпеки та забезпечення інформаційного суверенітету в умовах воєнного стану. *Інформаційну та емпіричну основу* дисертації становлять аналітичні звіти національних та міжнародних організацій, інформаційно-довідкові видання, статистичні дані та ін.

До основних положень, що характеризують вирішення поставленої мети слід віднести:

- розкрити методологічні засади дослідження інформаційної безпеки України;
- проаналізувати стан наукової розробленості проблеми інформаційної безпеки України у вітчизняній та зарубіжній науці;
- уточнити понятійно-категоріальний апарат, визначити сутність, ознаки, структуру інформаційної безпеки України та її місце у системі національної безпеки;
- дослідити зарубіжний досвід забезпечення інформаційної безпеки в умовах воєнного конфлікту та можливості його адаптації в Україні;
- проаналізувати нормативно-правове забезпечення інформаційної безпеки України в умовах воєнного стану, виявити основні проблеми та окреслити перспективи його вдосконалення;
- охарактеризувати інституційне забезпечення інформаційної безпеки України та визначити напрями його удосконалення;
- дослідити кібербезпеку та визначити її роль у забезпеченні національної безпеки в умовах воєнного стану;

- проаналізувати проблеми забезпечення інформаційного суверенітету України в умовах воєнного стану, визначити основні тенденції та перспективи його розвитку.

За темою дисертації опубліковано три статті у фахових виданнях України категорії «Б» з юридичних наук; десять тез доповідей на науково-практичних конференціях.

По завершенню доповіді Антона РЯПОЛОВА присутніми були поставлені такі **запитання:**

Доктор юридичних наук, професор Роман МИРОНЮК: Антоне Павловичу, Ви аналізуєте зарубіжний досвід забезпечення інформаційної безпеки. Обґрунтуйте зміст принципу «пропорційності», який ви пропонуєте використовувати при адаптації цього досвіду, та поясніть, як він допомагає збалансувати заходи національної безпеки з європейськими стандартами прав людини.

Відповідь: Дякую за запитання. Принцип пропорційності в адаптації зарубіжного досвіду передбачає, що будь-які обмежувальні заходи в інформаційній сфері мають бути не лише законними та переслідувати легітимну мета (захист нацбезпеки), а й бути мінімально необхідними та адекватними існуючій загрозі. Впровадження цього принципу дозволяє уникнути надмірного втручання у права людини, зокрема на свободу вираження поглядів, забезпечуючи гармонізацію українського законодавства з правом ЄС навіть в екстремальних умовах воєнного стану. Це створює підґрунтя для формування стійкої демократичної моделі безпеки, яка не втрачає своєї легітимності в очах міжнародної спільноти.

Доктор юридичних наук, професор Борис ЛОГВИНЕНКО: у дисертації інформаційна сфера розглядається як «самостійний стратегічний домен конфлікту». Розкрийте теоретико-правові наслідки такого визнання та поясніть, як це змінює підходи до кваліфікації сучасних кібероперацій та інформаційних атак.

Відповідь: Дякую за запитання. Визнання інформаційного простору окремим доменом конфлікту означає, що інформаційні та кібератаки тепер юридично прирівнюються до традиційних видів озброєного впливу. Це дозволяє кваліфікувати масштабні кіберінциденти проти критичної інфраструктури як акти агресії або застосування сили в розумінні Статуту ООН. Такий підхід вимагає модернізації правових режимів реагування, де кіберзахист перестає бути суто технічною допоміжною функцією і стає частиною активної оборонної стратегії держави.

Доктор юридичних наук, професор Роман ОПАЦЬКИЙ: Антоне Павловичу, Ви вказуєте на застарілість конституційного регулювання інформаційних відносин. Поясніть сутність вашої пропозиції щодо розширення кола суб'єктів управління інформаційним простором у Конституції України та чому ігнорування транснаціональних корпорацій сьогодні є правовим ризиком.

Відповідь: Дякую за запитання. Чинна Конституція обмежує коло суб'єктів системою «громадянин-суспільство-держава», що не відповідає реаліям глобалізованого світу. Дисертант пропонує нормативно визнати роль

транснаціональних корпорацій, наддержавних об'єднань та іноземних акторів як повноцінних учасників інформаційних процесів. Ігнорування їхнього впливу створює ризик втрати цифрового суверенітету, оскільки значна частина національного інформаційного простору та даних громадян фактично перебуває під управлінням приватних глобальних платформ, що діють поза межами національної юрисдикції.

Доктор юридичних наук, професор Дмитро СЕЛІХОВ: у дисертації Ви розглядаєте концепцію «суверенітету даних». Розкрийте юридичний механізм реалізації цього суверенітету та поясніть його взаємозв'язок із захистом персональних даних громадян в умовах транскордонного інформаційного обміну.

Відповідь: Дякую за запитання. Суверенітет даних передбачає обов'язкове підпорядкування інформації національному законодавству тієї держави, на території якої ці дані були зібрані або де вони обробляються. Юридично це реалізується через вимоги до локалізації серверів для зберігання критично важливих даних та встановлення жорсткого контролю за їх транскордонною передачею. В умовах війни це є запобіжником від несанкціонованого доступу ворожих спецслужб до реєстрів та приватних даних громадян, що забезпечує не лише приватність особи, а й загальну стійкість державних систем.

Доктор філософії у галузі права Каріна ПІСОЦЬКА: у роботі Ви пропонуєте післявоєнний перегляд правових режимів інформаційної безпеки. Обґрунтуйте необхідність такого «аудиту» обмежень та поясніть, які правові ризики несе збереження надзвичайних заходів після закінчення активних бойових дій.

Відповідь: Дякую за запитання. Необхідність післявоєнного перегляду зумовлена ризиком закріплення «надзвичайних» обмежень як нової норми, що може призвести до ерозії демократичних інститутів. Баланс між безпекою та свободою слова має бути відновлений одразу після зникнення фактичних загроз, для яких ці обмеження впроваджувалися. Правовий ризик полягає в тому, що тривале збереження цензури або надмірного державного контролю над медіа та мережами поза межами воєнного часу гальмуватиме розвиток громадянського суспільства та інтеграцію України до європейського правового простору.

Доктор юридичних наук, професор Валентина БОНЯК: у дисертації Ви акцентуєте увагу на важливості «публічно-приватного партнерства» у сфері кібербезпеки. Розкрийте зміст вашої пропозиції щодо правового врегулювання діяльності «добровольчих кібервійськ» та визначення їхнього статусу в системі сектору безпеки і оборони.

Відповідь: Дякую за запитання. Дисертант пропонує нормативно закріпити статус добровольчих кіберспільнот як специфічного резерву сектору безпеки. Це передбачає розробку правових регламентів їх залучення до захисту критичної інфраструктури, визначення меж їхньої відповідальності та надання їм певних правових гарантій. Такий підхід дозволяє легалізувати потужний інтелектуальний потенціал IT-сектору для потреб оборони, інтегруючи мережеві структури громадянського суспільства у державну систему кіберзахисту без створення громіздких бюрократичних апаратів.

Після цього слово було надано **рецензентам** наукової праці:

Доктор юридичних наук, професор Дмитро СЕЛІХОВ відзначив високий рівень наукового дослідження Антона РЯПОЛОВА за темою «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика».

В умовах повномасштабної збройної агресії російської федерації проти України інформаційна сфера перетворилась на самостійний і стратегічно важливий простір протиборства. Масштабні дезінформаційні кампанії, систематичні кібератаки на об'єкти критичної інфраструктури, цілеспрямовані інформаційно-психологічні операції проти українського суспільства та міжнародних партнерів – усе це засвідчує, що інформаційна безпека перестала бути допоміжним елементом національної безпеки і набула ознак її стратегічної основи. Від ефективності правових та інституційних механізмів забезпечення інформаційної безпеки нині залежить здатність держави зберігати суверенітет, мобілізовувати суспільство та успішно протидіяти агресору.

Актуальність обраної здобувачем теми визначається, насамперед, правовим виміром: введення і тривале застосування режиму воєнного стану спричинило суттєву трансформацію правового регулювання інформаційних відносин, однак чинна нормативно-правова база демонструє значні прогалини і суперечності, що знижують ефективність державної інформаційної політики. Інституційний вимір актуальності полягає у тому, що система органів, відповідальних за забезпечення інформаційної безпеки, формувалася переважно в мирний час і виявилася недостатньо адаптованою до умов повномасштабної агресії. Доктринальний вимір зумовлений тим, що вітчизняна правова наука ще не сформувала усталеного понятійно-категоріального апарату у цій сфері, а теоретичні розробки подекуди відстають від динаміки суспільних відносин і законодавчих змін. Наведені аргументи є достатніми для висновку про те, що проведене дослідження є безперечно актуальним.

Коректно і обґрунтовано визначено об'єкт, предмет, методи, мету та завдання дослідження. Методологія роботи є комплексною і включає діалектичний, системний, структурно-функціональний, порівняльно-правовий, формально-юридичний, герменевтичний та антропологічний підходи, що забезпечує всебічний аналіз досліджуваних явищ. Здобувач переконливо обґрунтовує необхідність поєднання загальнофілософських, загальнонаукових, спеціальних та власних методів правознавства з міждисциплінарними підходами, що відображає багатовимірну природу інформаційної безпеки як соціально-правового явища.

Теоретична, нормативна та емпірична бази дослідження є поглибленими і репрезентативними. Теоретична основа охоплює праці провідних вітчизняних і зарубіжних вчених у сфері права, кібербезпеки, теорії інформаційного суспільства та міжнародної безпеки. Нормативну основу складають Конституція України, ратифіковані міжнародні договори, ключові законодавчі акти у сфері інформаційної та кібербезпеки, а також стратегічні документи. Нормативно-правовим підґрунтям дослідження є міжнародні договори у сфері інформаційної безпеки, згоду на обов'язковість яких надано Верховною Радою України,

Конституція України, а також система національних нормативно-правових актів, що регулюють відносини у сфері інформаційної, кібернетичної безпеки та забезпечення інформаційного суверенітету в умовах воєнного стану. Інформаційну та емпіричну основу дисертації становлять аналітичні звіти національних та міжнародних організацій, інформаційно-довідкові видання, статистичні дані та ін.

Структура дисертації є логічно побудованою і забезпечує послідовне розкриття предмету дослідження. Серед найбільш вагомих здобутків слід відзначити такі.

Здобувач уперше репрезентує методологію дослідження інформаційної безпеки як цілісну концептуальну конструкцію, обґрунтовує її багатовимірну природу та формує сучасне бачення інформаційної безпеки як системоутворюючого елементу національної безпеки в умовах воєнного стану. Це є важливим теоретичним внеском, оскільки визначає логіку подальших наукових досліджень у цій сфері.

Принципово значущим є авторський підхід до кібербезпеки як системоутворюючої складової інформаційної безпеки держави, що поєднує правові, організаційні та політичні інструменти захисту. Здобувач обґрунтовує пріоритетні напрями розвитку національної системи кібербезпеки в умовах воєнного стану, серед яких особливої уваги заслуговує пропозиція щодо нормативного врегулювання правового статусу добровольчих кібервійськ – явища, що не має аналогів у мирний час і потребує виключно воєнно-правового осмислення.

Важливим є також визначення структури інформаційного суверенітету як багатокомпонентного явища, що включає політико-правову, організаційно-інституційну, інформаційно-технічну та культурно-гуманітарну складові.

Науковий підхід до адаптації зарубіжного досвіду також є удосконаленим: застосування принципу пропорційності як базового критерію відбору правових механізмів дозволяє чітко розмежовувати заходи легітимного захисту національної безпеки і практики, несумісні з європейськими стандартами прав людини. Порівняльний аналіз досвіду Німеччини, Франції, Естонії, Ізраїлю та США є ґрунтовним і практично орієнтованим.

Практичне значення одержаних результатів є безперечним. Конкретні пропозиції щодо доповнення Закону України «Про правовий режим воєнного стану» у частині статей 8 і 15, рекомендації щодо розробки Інформаційного кодексу України, а також обґрунтування спеціального режиму цифрових доказів в умовах воєнного стану мають пряме прикладне значення для законотворчої діяльності та правозастосовної практики. Це підтверджується актом впровадження результатів дослідження у діяльність Дніпропетровського окружного адміністративного суду.

Достовірність наукових положень, висновків і рекомендацій дисертації підтверджується їх апробацією на 10 наукових конференціях (4 міжнародних і 6 всеукраїнських), а також висвітленням у 3 наукових статтях у фахових виданнях України категорії «Б».

Загальна позитивна оцінка дисертаційної роботи не виключає можливості висловити окремі зауваження, які мають дискусійний і рекомендаційний характер та не ставлять під сумнів наукові результати здобувача.

1. Автор декларує «інтегративну методологію», що поєднує діалектичний, системний, синергетичний, герменевтичний, антропологічний та кібернетичний підходи (с. 28 дис.). Однак у тексті відсутнє пояснення, яким чином ці підходи утворюють єдину методологічну конструкцію, а не просто перелік. Обґрунтуйте внутрішню логіку їх поєднання та ієрархію застосування.

2. У підрозділі 1.2 виокремлено чотири підходи до розуміння інформаційної безпеки – правовий, безпековий, соціально-комунікаційний і технологічний. Однак у висновку стверджується, що «концептуальна різноманітність не є недоліком» (с. 59 дис.). Чи не є це захисною риторикою, що замінює наукове завдання синтезу? Де у роботі пропонується власна інтегративна концепція, а не лише констатація множинності підходів?

3. Здобувач пропонує визначення інформаційної безпеки як «перманентного процесу і результату забезпечення стану захищеності» (с. 88 дис.). Водночас категорії «процес» і «результат» відображають різні способи опису явища: процес акцентує динаміку та безперервність, тоді як результат – певний досягнутий стан. Чи не є поєднання цих двох категорій в одному визначенні внутрішньо суперечливим? І чи можна вважати таку конструкцію справжнім синтезом статичного і динамічного підходів, а не їх формальним поєднанням?

4. У підрозділі 1.4 здійснюється порівняльний аналіз досвіду США, Великої Британії, Ізраїлю, Франції, Німеччини та держав Балтії. Водночас зазначені держави суттєво відрізняються за конституційною моделлю, безпековим контекстом, історичним досвідом і структурою правової системи. У зв'язку з цим виникає питання щодо tertium comparationis – спільного методологічного критерію, який робить такі системи порівнюваними між собою. Який саме критерій покладено в основу порівняльного аналізу і яким чином він дозволяє формулювати рекомендації, релевантні для України?

5. Автор пропонує як кодифікаційне рішення Інформаційний кодекс України (підрозділ 2.1), а також окрему рекомендацію щодо прийняття спеціального закону або внесення змін до закону про національну безпеку щодо режимів кібербезпеки у воєнний час (підрозділ 2.3). У зв'язку з цим виникає питання про системну узгодженість цих пропозицій: чи не дублює спеціальне законодавче регулювання функції майбутньої кодифікації? Якщо ні – то яким чином запропонований спеціальний закон має бути інтегрований у структуру Інформаційного кодексу України в перспективі?

Проте висловлені зауваження та пропозиції мають дискусійний і рекомендаційний характер та не ставлять під сумнів отримані здобувачем наукові результати.

Дисертаційна робота Ряполова Антона Павловича є завершеним науковим дослідженням, що має наукову новизну та практичну значущість і розвиває окремі положення доктрини інформаційної безпеки, кібербезпеки та інформаційного суверенітету держави в умовах воєнного стану та

євроінтеграційних процесів. За своїм змістом, рівнем обґрунтованості наукових положень, висновків і рекомендацій, а також повнотою викладу дисертаційна робота та опубліковані за її результатами праці відповідають встановленим вимогам до дисертацій на здобуття наукового ступеня доктора філософії.

Дисертаційна робота Ряполова Антона Павловича «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» виконана на належному науковому та методологічному рівнях і відповідає вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами від 03 квітня 2019 року № 283), а також пунктам 6, 7, 8 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.

Кандидат юридичних наук, доцент Андрій САМОТУГА відзначив належний фаховий рівень дисертаційного дослідження Антона РЯПОЛОВА «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика», виконаного на актуальну тему.

Андрій САМОТУГА зазначив, що дисертант обрав актуальну тему для дослідження. Ґрунтовне вивчення і критичний аналіз тексту поданої на захист дисертації і наукових праць здобувача, опублікованих за обраною темою надали підстави зробити такий висновок.

Сучасний етап розвитку інформаційного права характеризується суттєвим ускладненням структури інформаційних відносин, що зумовлено одночасним впливом правових, технологічних та інституційних трансформацій. У цих умовах інформаційна безпека дедалі більше набуває ознак комплексної правової категорії, яка виходить за межі традиційного розуміння захисту інформації та охоплює широкий спектр регулятивних механізмів публічного права.

Дисертаційне дослідження Ряполова Антона Павловича на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» є актуальним і має істотне значення для розвитку доктрини інформаційного права, удосконалення правового регулювання у сфері інформаційної безпеки та формування системного підходу до її забезпечення в сучасних умовах. Особливої актуальності дослідження набуває у зв'язку зі зміною характеру державного регулювання інформаційної сфери, що потребує переосмислення співвідношення між безпековими функціями держави, гарантіями прав і свобод людини та вимогами ефективного функціонування інформаційного простору. У цьому контексті зростає значення формування цілісного теоретико-правового підходу до розуміння інформаційної безпеки як елемента системи публічно-правового регулювання.

Важливим чинником актуалізації теми є також динамічний розвиток цифрового середовища та пов'язаних із ним ризиків для стабільності правових режимів у сфері обробки, поширення та захисту інформації. Це зумовлює потребу у вдосконаленні нормативно-правових та інституційних механізмів, які

забезпечують узгоджене функціонування державної політики у сфері інформаційної безпеки. Додаткову актуальність теми зумовлює недостатній рівень її комплексного теоретико-правового осмислення у вітчизняній юридичній науці. Попри наявність значної кількості досліджень окремих аспектів інформаційної та кібернетичної безпеки, спостерігається дефіцит цілісних наукових робіт, у яких інформаційна безпека розглядалася б як системна правова конструкція в структурі національного публічного права. У зв'язку з цим дисертація має належний рівень наукової новизни та заповнює існуючу доктринальну прогалину.

Наукова новизна одержаних результатів. Наукова новизна одержаних результатів полягає в тому, що дисертація є однією із перших у вітчизняній науці, в якій здійснено комплексне теоретико-правове обґрунтування змісту, структури та механізмів забезпечення інформаційної безпеки України в умовах воєнного стану та євроінтеграції, систематизовано існуючі проблеми, розроблено науково обґрунтовані рекомендації щодо їх подолання, а також сформульовано практичні рекомендації, спрямовані на підвищення рівня кіберзахищеності та забезпечення інформаційного суверенітету держави.

Особливої уваги заслуговують положення щодо: концептуалізації методології дослідження інформаційної безпеки як цілісної наукової конструкції; визначення кібербезпеки як системоутворюючої складової інформаційної безпеки держави; удосконалення підходів до інституційного забезпечення інформаційної безпеки; формування напрямів забезпечення інформаційного суверенітету в умовах воєнного стану; обґрунтування необхідності модернізації інформаційного законодавства України; розвитку стратегічних комунікацій як окремої функції сектору безпеки і оборони.

Перший розділ дисертації присвячений теоретико-методологічним засадам дослідження інформаційної безпеки України. Автором здійснено ґрунтовний аналіз сучасних наукових підходів до розуміння інформаційної безпеки, проаналізовано стан наукової розробленості проблематики у вітчизняній та зарубіжній науці, досліджено еволюцію наукових концепцій у цій сфері. Позитивної оцінки заслуговує здійснена автором спроба сформувати цілісне концептуальне бачення інформаційної безпеки як багаторівневої соціально-правової системи, що функціонує в умовах сучасних безпекових викликів.

Важливим науковим здобутком дисертації є запропоноване автором уточнення понятійно-категоріального апарату у сфері інформаційної безпеки. Зокрема, заслуговують на увагу сформульовані підходи до розуміння інформаційної безпеки, інформаційного суверенітету, цифрового суверенітету та кібербезпеки, а також визначення їх місця у системі національної безпеки держави.

Другий розділ дисертації присвячено аналізу нормативно-правового та інституційного забезпечення інформаційної безпеки України в умовах воєнного стану. Автором досліджено сучасний стан правового регулювання інформаційної безпеки, визначено основні проблеми функціонування чинного законодавства, виявлено прогалини та колізії правового регулювання у цій сфері.

На особливу увагу заслуговує проведений у роботі аналіз інституційного механізму забезпечення інформаційної безпеки. Автором обґрунтовано, що однією з ключових проблем сучасної системи забезпечення інформаційної безпеки України є фрагментарність системи суб'єктів, недостатній рівень координації між ними та відсутність єдиного координаційного механізму у сфері інформаційної безпеки. У дисертації запропоновано напрями удосконалення інституційної спроможності держави, розвитку міжвідомчої взаємодії та посилення ролі стратегічних комунікацій у системі національної безпеки.

Значну увагу в роботі приділено дослідженню кібербезпеки як системоутворюючої складової інформаційної безпеки держави. Автором аргументовано необхідність удосконалення нормативно-правового регулювання кібербезпеки в умовах воєнного стану, розвитку механізмів реагування на кіберінциденти, формування системи міжнародного співробітництва у сфері кіберзахисту та забезпечення технологічного суверенітету держави.

Позитивної оцінки заслуговують положення дисертації щодо забезпечення інформаційного суверенітету України. Автором розкрито зміст інформаційного суверенітету як багатокомпонентного явища, що включає політико-правову, організаційно-інституційну, інформаційно-технічну та культурно-гуманітарну складові. Важливим є також акцент на необхідності підвищення рівня медіаграмотності населення, розвитку національної консолідації та посилення інформаційної стійкості суспільства.

Дотримання вимог академічної доброчесності. Аналіз змісту дисертації «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» дає підстави стверджувати, що під час його виконання здобувачем повною мірою дотримано вимог академічної доброчесності.

Бібліографічний апарат оформлено відповідно до встановлених вимог, що узгоджується з принципами наукової етики та чинними стандартами оформлення наукових робіт. У роботі належним чином здійснено посилання на використані наукові джерела вітчизняних і зарубіжних авторів, нормативно-правові акти, міжнародні документи у сфері інформаційної та кібербезпеки, статистичні матеріали, аналітичні звіти та результати правозастосовної практики. Цитування наукових позицій інших дослідників оформлено коректно із обов'язковим зазначенням першоджерел, що забезпечує належний рівень прозорості та верифікованості використаного наукового матеріалу.

Структура дисертації, логіка викладення матеріалу, послідовність аргументації та характер сформульованих висновків свідчать про самостійний характер виконаного дослідження, а також про системний підхід автора до опрацювання складної та багатовимірної проблематики інформаційної безпеки в умовах воєнного стану. У процесі аналізу тексту дисертації не виявлено ознак академічного плагіату, неправомірного запозичення, фрагментарного копіювання або некоректного використання чужих наукових результатів без належного посилання.

Отже, дисертаційне дослідження виконано з дотриманням основних принципів академічної доброчесності, зокрема чесності, відповідальності,

прозорості, наукової коректності та поваги до інтелектуальної власності інших дослідників.

Зміст та оформлення дисертації. Дисертація складається з анотації, переліку умовних позначень, вступу, двох розділів, що містять вісім підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації, її структурна побудова та співвідношення основного й допоміжного матеріалу відповідають встановленим вимогам до дисертаційних робіт на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

Побудова дисертації є логічною, послідовною та внутрішньо узгодженою. Така структура дозволила повно і системно розкрити теоретико-правові аспекти інформаційної безпеки України, забезпечивши послідовний перехід від аналізу методологічних і концептуальних засад дослідження до характеристики нормативно-правового та інституційного забезпечення інформаційної безпеки в умовах воєнного стану.

Зміст дисертації характеризується концептуальною цілісністю та належним рівнем опрацювання складної й багатовимірної проблематики інформаційної безпеки в умовах воєнного стану. Робота охоплює широкий спектр теоретико-правових, нормативних, інституційних і доктринальних аспектів, що дало змогу здійснити всебічний аналіз досліджуваного явища як складової національної безпеки держави.

Структура роботи забезпечує внутрішню узгодженість викладу: від розкриття теоретико-методологічних засад дослідження, аналізу наукових підходів та формування понятійно-категоріального апарату – до характеристики нормативно-правового та інституційного забезпечення інформаційної безпеки України в умовах воєнного стану та формулювання пропозицій щодо вдосконалення відповідних механізмів. Це забезпечує тісний взаємозв'язок між теоретичними положеннями та практичними рекомендаціями.

Позитивної оцінки заслуговує міждисциплінарний підхід до дослідження інформаційної безпеки, зокрема врахування її взаємозв'язку з кібербезпекою, інформаційним суверенітетом, стратегічними комунікаціями та правовим режимом воєнного стану. Автор демонструє здатність інтегрувати різні наукові підходи та галузеві напрями юридичної науки для формування цілісного бачення досліджуваної проблематики.

Варто відзначити належний рівень аналізу детермінантів загроз інформаційній безпеці, включно з внутрішніми та зовнішніми факторами, що є особливо актуальним в умовах гібридної війни та масштабних інформаційно-психологічних операцій. Окремої уваги заслуговує прагнення здобувача пов'язати результати дослідження з потребами вдосконалення державної політики у сфері національної та інформаційної безпеки, що підвищує практичну цінність роботи.

Здобувач демонструє належний рівень володіння юридичною термінологією, вміння працювати з широкою джерельною базою, аналізувати нормативно-правові акти, наукові позиції та матеріали правозастосовної практики, що свідчить про сформовану наукову культуру дослідження та здатність до самостійного наукового пошуку.

У цілому зміст дисертації повністю відповідає заявленій темі, меті та завданням дослідження, характеризується логічністю викладення матеріалу, аргументованістю наукових положень і практичною спрямованістю сформульованих висновків. Робота є завершеним науковим дослідженням, що має вагоме теоретичне та прикладне значення для розвитку науки конституційного та інформаційного права, а також удосконалення механізмів забезпечення інформаційної безпеки України.

Практичне значення результатів дослідження полягає у можливості їх використання у правотворчій діяльності, діяльності органів державної влади та сектору безпеки і оборони, у науково-дослідній сфері, а також в освітньому процесі під час викладання юридичних дисциплін. Сформульовані у роботі висновки та пропозиції можуть бути використані під час удосконалення державної політики у сфері інформаційної та кібербезпеки, розроблення нормативно-правових актів та підвищення ефективності функціонування механізмів протидії інформаційним загрозам.

Основні результати дисертації пройшли належну апробацію на міжнародних та всеукраїнських науково-практичних конференціях, а також відображені у наукових публікаціях автора, що свідчить про достатній рівень наукової обґрунтованості та достовірності отриманих результатів.

Зауваження щодо змісту та оформлення дисертації. Водночас слід зазначити, що дисертаційні дослідження, присвячені проблематиці інформаційної безпеки в умовах воєнного стану, з огляду на складність, багатовимірність та динамічність відповідних суспільних відносин, об'єктивно не можуть бути повністю позбавлені окремих дискусійних положень. Особливо це стосується наукових робіт, що поєднують теоретико-правові, безпекові, інформаційно-технологічні та інституційні аспекти дослідження. Разом із тим такі положення не знижують загальної позитивної оцінки дисертації, а, навпаки, свідчать про актуальність, наукову складність і перспективність обраної тематики, створюючи підґрунтя для подальших наукових дискусій та розвитку відповідного напряму юридичної науки. У зв'язку із цим доцільно звернути увагу на окремі аспекти дослідження, які можуть бути предметом подальшого наукового осмислення та вдосконалення, серед яких варто виокремити такі:

1. Підрозділ 1.2 містить широкий огляд зарубіжної літератури у сфері інформаційної та кібербезпеки, зокрема праць Joseph Nye (Джозеф Най), Manuel Castells (Мануель Кастельс), Thomas Rid (Томас Рід), Peter Singer (Пітер Сінгер), Claire Wardle (Клер Вордл), Richard Clarke (Річард Кларк) та інших. Водночас у тексті майже не відображені наявні між ними теоретичні та концептуальні розбіжності. Наприклад, Thomas Rid (Томас Рід) заперечує можливість «кібервійни» у класичному розумінні, тоді як Richard Clarke (Річард Кларк) і Robert Knake (Роберт Кнейк) розглядають кіберпростір як повноцінний домен ведення воєнних дій. Яким чином автор методологічно узгоджує ці різні теоретичні позиції у межах власного дослідження і чи не потребував огляд літератури більш виразного відображення наявних наукових полемік та концептуальних суперечностей?

2. Серед методів дослідження автором заявлено антропологічний підхід, що спрямований на розгляд права крізь призму прав і свобод людини (вступ, підрозділ 1.1). Водночас у підрозділах 2.1–2.4 права людини переважно виступають як нормативні межі реалізації безпекових заходів держави, а не як самостійна основа формування змісту інформаційної безпеки. У зв'язку з цим виникає питання: чи реалізовано антропологічний підхід у роботі як самостійну аналітичну рамку, чи він фактично виконує допоміжну функцію обмеження державного втручання? Інакше кажучи, де саме у дисертації інтереси людини як суб'єкта інформаційних відносин виступають не лише як обмеження державної політики, а як один із системоутворюючих елементів концепції інформаційної безпеки?

3. Автор зазначає, що правове регулювання процесів в інформаційному просторі здебільшого здійснюється «post factum», тобто реагує на загрози вже після їх виникнення (с. 118 дисертації). Водночас у роботі пропонуються нові нормативно-правові механізми забезпечення інформаційної безпеки. У зв'язку з цим виникає питання: яким чином автор узгоджує реактивний характер правового регулювання у цифровому середовищі з ідеєю підвищення ефективності нормативного забезпечення інформаційної безпеки? Чи можливе, на думку автора, формування проактивної моделі правового регулювання у сфері, де технологічні та інформаційні загрози змінюються швидше, ніж законодавство?

4. На с. 203 дисертації зазначено, що «Україна має досить слабку інформаційну політику». Водночас у підрозділі 2.4 аналізуються діяльність Центру протидії дезінформації, розвиток стратегічних комунікацій та програми медіаграмотності. У зв'язку з цим виникає питання: за якими саме критеріями автор оцінює інформаційну політику як «слабку» і яка методологія такої оцінки застосовується у роботі? Чи йдеться про відсутність окремих інституційних механізмів, чи про недостатню системність та ефективність їх функціонування?

5. У розвиток зазначеного питання щодо критеріїв оцінки ефективності інформаційної політики держави у підрозділі 2.4 також зазначається, що надмірний державний контроль за медіапростором в умовах воєнного стану може підривати демократичні принципи та знижувати рівень суспільної довіри. Водночас автор наголошує на недостатній ефективності протидії інформаційній агресії рф. У зв'язку з цим постає питання про критерії допустимого державного втручання у медіасферу: яким чином у роботі розмежовуються «ефективний» та «надмірний» контроль і за якими правовими або інституційними ознаками визначається межа між необхідними безпековими заходами та непропорційним обмеженням демократичних свобод?

Загальні підсумки. Дисертаційне дослідження Ряполова Антона Павловича на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика», подане на здобуття наукового ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право», є завершеною науковою працею, у якій комплексно та всебічно вирішено поставлені дослідницькі завдання, що мають істотне значення для розвитку теоретико-

правових засад інформаційної безпеки та вдосконалення механізмів її забезпечення в умовах воєнного стану.

Отримані результати мають вагоме теоретичне та прикладне значення і можуть бути використані у правотворчій діяльності, практиці органів державної влади та сектору безпеки і оборони, а також у науково-дослідній та освітній діяльності при викладанні навчальних дисциплін юридичного профілю.

Дисертаційне дослідження виконано з дотриманням вимог академічної доброчесності та відповідає встановленим нормативним критеріям щодо структури, змісту та оформлення наукових робіт такого рівня. Наявні дискусійні положення не знижують загальної наукової цінності роботи, а, навпаки, підкреслюють складність та актуальність досліджуваної проблематики, а також окреслюють перспективи для подальших наукових розвідок у цій сфері.

З огляду на викладене, дисертація Ряполова Антона Павловича відповідає спеціальності 081 «Право» та вимогам 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 р. № 44 (із змінами), а також вимогам до оформлення дисертації, затвердженим наказом МОН України від 12 січня 2017 р. № 40, а її автор заслуговує на присудження наукового ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право».

В обговоренні дисертаційного дослідження взяли участь:

Доктор юридичних наук, професор Роман МИРОНЮК наголосив, що автором дисертаційного дослідження коректно, ґрунтовно та на належному науково-методологічному рівні сформульовано актуальність обраної теми, яка є особливо значущою в умовах сучасних безпекових викликів, зумовлених воєнним станом та посиленням інформаційних загроз. Відзначено, що дослідження має чітко окреслену наукову проблематику, логічно вибудувану структуру та внутрішню цілісність. Також підкреслено, що здобувачем обґрунтовано та виважено обрано методологічний інструментарій дослідження, який є адекватним поставленій меті, об'єкту та предмету роботи, що забезпечило належний рівень наукової достовірності отриманих результатів. Окремо відзначено послідовність викладу матеріалу, системність підходу до аналізу проблематики та достатній рівень теоретичного узагальнення.

Загалом дисертація Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» відповідає встановленим вимогам до такого виду наукових робіт і може бути рекомендована до розгляду в разовій спеціалізованій вченій раді для захисту.

Доктор юридичних наук, професор Борис ЛОГВИНЕНКО підкреслив, що тема дослідження є складною, багатогранною та водночас надзвичайно актуальною. Автором опрацьовано значний масив нормативних і наукових джерел, що дозволило забезпечити належний рівень наукової обґрунтованості результатів. Водночас проблематика інформаційної безпеки в умовах воєнного стану потребує подальшого поглибленого дослідження, з огляду на її динамічний характер та суспільну значущість.

У цілому дисертаційна робота Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» є завершеним, самостійним науковим дослідженням, що відповідає вимогам, які висуваються до дисертацій на здобуття ступеня доктора філософії за спеціальністю 081 «Право», та може бути рекомендована до захисту у разовій спеціалізованій вченій раді.

Доктор юридичних наук, професор Роман ОПАЦЬКИЙ відзначив актуальність обраної теми дисертаційного дослідження, її своєчасність в умовах сучасних викликів, а також належний науковий рівень виконання роботи. Було підкреслено, що дисертація присвячена важливій та суспільно значущій проблематиці забезпечення інформаційної безпеки в умовах воєнного стану й містить ґрунтовний теоретико-правовий аналіз досліджуваних питань.

Водночас доповідач звернув увагу на доцільність більш детальної конкретизації окремих статистичних даних, результатів досліджень та посилення аргументації окремих положень дисертаційної роботи. Проте висловлені зауваження мають переважно рекомендаційний і дискусійний характер та не впливають на загальну позитивну оцінку дисертаційного дослідження. Було також відзначено, що автором коректно визначено мету, об'єкт, предмет і завдання дослідження, забезпечено належний рівень наукової аргументації та логічну послідовність викладу матеріалу.

З урахуванням викладеного Роман ОПАЦЬКИЙ зазначив, що дисертаційне дослідження Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» відповідає спеціальності 081 «Право» та вимогам пунктів 6, 7, 8 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, і може бути рекомендоване до захисту в разовій спеціалізованій вченій раді за спеціальністю 081 «Право».

Доктор юридичних наук, професор Валентина БОНЯК зазначила, що дисертаційна робота Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» присвячена комплексному дослідженню актуальних теоретико-правових проблем забезпечення інформаційної безпеки в умовах воєнного стану, зокрема захисту честі, гідності, здоров'я та життя людини в умовах збройної агресії та інформаційних загроз. У сучасних умовах розвитку держави та суспільства обрана тема дослідження є надзвичайно актуальною, суспільно значущою та такою, що має вагоме наукове й практичне значення. Було наголошено, що дисертація вирізняється високим рівнем наукової обґрунтованості, логічністю та послідовністю викладу матеріалу, ґрунтовністю проведеного аналізу, належним рівнем теоретичних узагальнень і коректним використанням сучасного наукового інструментарію. Робота написана на високому науковому та мовностилістичному рівні, а сформульовані автором висновки й пропозиції характеризуються аргументованістю, самостійністю та практичною цінністю.

Валентина БОНЯК підкреслила, що результати дисертаційного дослідження можуть бути використані у науково-дослідній діяльності, нормотворчому процесі, правозастосовній практиці, а також в освітньому процесі під час викладання правничих дисциплін.

Отже, дисертаційна робота Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» є завершеною самостійною науковою працею, що відповідає вимогам, встановленим до дисертацій на здобуття ступеня доктора філософії за спеціальністю 081 «Право», та може бути рекомендована до захисту в разовій спеціалізованій вченій раді.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика», поданої на здобуття ступеня доктора філософії за спеціальністю 081 «Право»

Обґрунтування вибору теми дослідження. У сучасних воєнних конфліктах інформаційна сфера дедалі частіше перетворюється на самостійне поле протистояння. Стрімкий розвиток інформаційних технологій, глобалізації комунікаційних мереж та зростання кіберзагроз забезпечення захисту державної, суспільної та приватної інформації стає критично важливим для стабільного функціонування держави. В умовах воєнного стану питання інформаційної безпеки України виходить на перший план, адже саме вона забезпечує захист суспільства та держави від деструктивного впливу пропаганди, кіберзагроз, маніпуляцій та інформаційних атак.

Інформаційна безпека є одним із основних елементів національної безпеки сучасної держави. Гібридна агресія проти України поєднує в собі традиційні збройні методи із масованими кібератаками, дезінформаційними кампаніями, маніпулюванням суспільною свідомістю та цілеспрямованим руйнуванням інформаційної інфраструктури держави. За таких умов інформаційна безпека перетворюється з одного з елементів національної безпеки на її стратегічну основу, від якої залежить здатність держави зберігати суверенітет, мобілізовувати суспільство та ефективно протистояти агресору.

Проведене дослідження викликано необхідністю комплексного наукового аналізу правових механізмів та нормативно-правового забезпечення інформаційної безпеки в умовах воєнного стану. Актуальність теми визначається низкою чинників, а саме: зростанням кіберзагроз та кібератак, спрямованих на державні інформаційні системи, критичну інфраструктуру та стратегічні об'єкти, що створює безпосередню загрозу національній безпеці; необхідністю вдосконалення нормативно-правової бази, що регулює інформаційну безпеку в умовах воєнного стану, з урахуванням сучасних технологічних та військово-політичних викликів; важливістю удосконалення інституційних механізмів, що забезпечують функціонування системи інформаційної безпеки, підвищенням ефективності координації між державними органами, правоохоронними

структурами та сектором критичної інфраструктури; недостатньою науково-правовою розробленістю окремих аспектів інформаційної безпеки, особливо щодо інтеграції кібербезпеки, законодавчого регулювання та адаптації зарубіжного досвіду до умов воєнного стану.

До того ж актуальність теми обґрунтована взаємозумовленими вимірами: *правовим* – ведення воєнного стану спричинило суттєву трансформацію правового регулювання інформаційних відносин. Водночас чинна нормативно-правова база демонструє значні прогалини й суперечності, які знижують ефективність державної політики у сфері інформаційної безпеки в умовах воєнного стану; *інституційним* – система органів державної влади, відповідальних за забезпечення інформаційної безпеки, формувалася переважно в мирний час і виявилася недостатньо адаптованою до умов повномасштабної агресії; *доктринальним* – незважаючи на зростання практичної значущості питань інформаційної безпеки, вітчизняна правнича наука ще не сформувала усталеного понятійно-категоріального апарату у цій сфері, а теоретико-правові дослідження подекуди відстають від динаміки суспільних відносин та законодавчих змін. Вивчення досвіду інших держав, які стикалися із збройними конфліктами та інформаційною агресією, містить цінні моделі правового та інституційного реагування, адаптація яких до українських реалій є науково та практично виправданою.

Незважаючи на існування низки наукових праць у сфері інформаційної безпеки, сучасні виклики воєнного часу висувають нові завдання щодо захисту державних інформаційних ресурсів, інфраструктури та суспільного інформаційного простору, що потребує детального теоретико-правового дослідження. *Доктринальною основою* дослідження виступили дисертаційні роботи, монографії та інші наукові праці українських і зарубіжних учених у сфері права, національної та інформаційної безпеки, політології, соціології, кібербезпеки та теорії інформаційного суспільства. Серед українських авторів, які досліджували проблематику інформаційної безпеки, кібербезпеки, інформаційного суверенітету та інформаційного протиборства в умовах воєнних конфліктів, слід відзначити таких: А. Авер'янова, В. Аніщук, І. Арістова, О. Баранов, І. Березовська, В. Брижко, Н. Влажик, В. Горбулін, В. Гурковський, В. Демиденко, О. Дзьобань, О. Довгань, О. Додонов, І. Забара, Р. Калюжний, Є. Кобко, В. Конах, О. Косогов, Б. Кормич, І. Котерлін, В. Котляров, В. Кучер, О. Кирилюк, О. Литвиненко, В. Ліпкан, Д. Лобода, Н. Лугіна, Ю. Максименко, А. Марущак, Л. Наливайко, А. Нашинець-Наумова, Н. Ніжник, В. Остроухов, М. Панов, А. Пазюк, О. Передерій, В. Пилипчук, В. Політанський, Г. Почепцов, М. Присяжнюк, А. Самотуга, Д. Селіхов, О. Сивак, С. Стрельцов, О. Тихомиров, П. Ткачук, В. Хорошко, В. Цимбалюк, О. Юдін, О. Юнін, М. Шевчук та ін.

Зарубіжні вчені, які здійснили вагомий внесок у розвиток теорії інформаційного суспільства, кібербезпеки та цифрового суверенітету, включають таких дослідників: А. Росс Андерсон (Ross J. Anderson), Д. Белл (Daniel Bell), Ю. Бенклер (Yochai Benkler), М. Кастельс (Manuel Castells), Л. Лессіг (Lawrence Lessig), Т. Рід (Thomas C. Reed), П. Сінгер (Peter W. Singer),

Е. Тоффлер (Alvin Toffler), М. Хансен (Morten Hansen), К. Шеннон (Claude Shannon), Б. Шнайєр (Bruce Schneier) та ін.

Окрім сучасних викликів для національної безпеки та інформаційного простору, вибір теми дисертації зумовлений практичною необхідністю формування ефективних правових механізмів захисту інформації в умовах воєнного стану. Результати дослідження можуть стати основою для формування ефективних державних політик та правових механізмів захисту інформаційного простору, удосконалення нормативно-правової бази та підвищення готовності держави до протидії сучасним інформаційним загрозам. Зазначене і зумовило вибір теми дослідження, визначення мети та завдань дисертаційної роботи.

Нормативно-правовим підґрунтям дослідження є міжнародні договори у сфері інформаційної безпеки, згоду на обов'язковість яких надано Верховною Радою України, Конституція України, а також система національних нормативно-правових актів, що регулюють відносини у сфері інформаційної, кібернетичної безпеки та забезпечення інформаційного суверенітету в умовах воєнного стану. *Інформаційну та емпіричну основу* дисертації становлять аналітичні звіти національних та міжнародних організацій, інформаційно-довідкові видання, статистичні дані та ін.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дослідження виконано відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392/2020; Стратегії воєнної безпеки України, затвердженої Указом Президента України від 25 березня 2021 р. № 121/2021; Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16 лютого 2022 р. № 56/2022; 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, затвердженого постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476; Тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2025-2029 роки, затвердженої Наказом Міністерства внутрішніх справ України від 21 травня 2024 р. № 326; Стратегії розвитку Національної академії правових наук України на 2021-2025 рр., затвердженої постановою загальних зборів НАПрН України від 26 березня 2021 р. № 12-21 (1.11. Правове забезпечення у сфері національної безпеки та оборони).

Мета і завдання дослідження. *Мета дослідження* полягає у комплексному теоретико-правовому аналізі інформаційної безпеки України в умовах воєнного стану, розкритті її сутності, структури та місця у системі національної безпеки, оцінці ефективності нормативно-правового та інституційного забезпечення, а також розробленні науково обґрунтованих пропозицій щодо їх удосконалення з урахуванням сучасних викликів, зокрема у сфері кібербезпеки та забезпечення інформаційного суверенітету.

Для досягнення зазначеної мети у дисертації поставлено такі *завдання:*

- розкрити методологічні засади дослідження інформаційної безпеки України;

- проаналізувати стан наукової розробленості проблеми інформаційної безпеки України у вітчизняній та зарубіжній науці;
- уточнити понятійно-категоріальний апарат, визначити сутність, ознаки, структуру інформаційної безпеки України та її місце у системі національної безпеки;
- дослідити зарубіжний досвід забезпечення інформаційної безпеки в умовах воєнного конфлікту та можливості його адаптації в Україні;
- проаналізувати нормативно-правове забезпечення інформаційної безпеки України в умовах воєнного стану, виявити основні проблеми та окреслити перспективи його вдосконалення;
- охарактеризувати інституційне забезпечення інформаційної безпеки України та визначити напрями його удосконалення;
- дослідити кібербезпеку та визначити її роль у забезпеченні національної безпеки в умовах воєнного стану;
- проаналізувати проблеми забезпечення інформаційного суверенітету України в умовах воєнного стану, визначити основні тенденції та перспективи його розвитку.

Об'єктом дослідження є суспільні відносини у сфері забезпечення інформаційної безпеки як елементу національної безпеки.

Предметом дослідження є теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану.

Методи дослідження. Для вирішення поставлених завдань і досягнення мети було використано комплекс загальнофілософських підходів, загальнонаукових, спеціальних та власних методів правознавства. *Діалектичний підхід* сприяв дослідженню інформаційної безпеки у динаміці, що дало змогу виявити суперечності її функціонування в умовах воєнного стану та трансформацію інформаційної сфери у самостійний простір протиборства (підрозділи 1.1, 1.3, 2.4). *Герменевтичний підхід* застосовано для тлумачення норм законодавства у сфері інформаційної безпеки та виявлення особливостей їх реалізації в умовах воєнного стану (підрозділи 2.1, 2.4). *Антропологічний підхід* забезпечив аналіз інформаційної безпеки крізь призму захисту прав і свобод людини в інформаційній сфері (підрозділи 1.3, 2.1). *Аксіологічний підхід* сприяв визначенню ціннісних орієнтирів інформаційної безпеки, зокрема балансу між безпекою держави та правами людини (підрозділи 1.3, 2.4). *Синергетичний підхід* дозволив дослідити процеси самоорганізації системи інформаційної безпеки та її здатність до адаптації в умовах криз і воєнних загроз (підрозділи 1.1, 2.2, 2.4). Використання *системного підходу* дозволило розглядати інформаційну безпеку як цілісну багаторівневу систему, а також виявити взаємозв'язок її елементів (підрозділи 1.1, 1.3, 2.1-2.4). Застосування *структурно-функціонального методу* уможливило визначення елементів інформаційної безпеки та їх функціонального призначення у системі національної безпеки (підрозділи 1.3, 2.2, 2.3). За допомогою *інституційного підходу* досліджено діяльність суб'єктів забезпечення інформаційної безпеки, механізми їх взаємодії та напрями інституційного вдосконалення (підрозділ 2.2). *Історико-правовий метод* застосовано для дослідження еволюції наукових

підходів і правового регулювання інформаційної безпеки (підрозділ 1.2, 2.1). Застосування *кібернетичного підходу* дало змогу розглянути інформаційну безпеку як систему управління інформаційними процесами та загрозами, що функціонує на основі принципів зворотного зв'язку та адаптивності (підрозділи 1.1, 2.3). *Формально-юридичний метод* забезпечив аналіз нормативно-правової бази та дозволив виявити її прогалини, колізії та напрями модернізації (підрозділи 2.1, 2.3, 2.4). *Порівняльно-правовий метод* використано для аналізу зарубіжного досвіду забезпечення інформаційної безпеки та можливостей його адаптації в Україні (підрозділ 1.4). *Метод аналізу та синтезу* дозволив узагальнити наукові підходи та сформувати цілісне бачення інформаційної безпеки (підрозділи 1.2, 1.3). *Метод прогнозування та моделювання* використано для визначення перспектив розвитку системи інформаційної безпеки України (підрозділи 2.1-2.4).

Наукова новизна одержаних результатів полягає в тому, що дисертація є однією із перших у вітчизняній науці, в якій здійснено комплексне теоретико-правове обґрунтування змісту, структури та механізмів забезпечення інформаційної безпеки України в умовах воєнного стану та євроінтеграції, систематизовано існуючі проблеми, розроблено науково обґрунтовані рекомендації щодо їх подолання, а також сформульовано практичні рекомендації, спрямовані на підвищення рівня кіберзахищеності та забезпечення інформаційного суверенітету держави. У результаті проведеного дослідження сформульовано та обґрунтовано низку нових наукових положень, висновків і пропозицій, зокрема:

уперше:

- методологію дослідження інформаційної безпеки України репрезентовано як цілісну концептуальну основу, що, на відміну від існуючих підходів, визначає логіку наукового аналізу та формує сучасне бачення інформаційної безпеки як системоутворюючого елемента національної безпеки; обґрунтовано її багатовимірну природу через сукупність взаємопов'язаних методологічних підходів і методів, що забезпечують цілісний аналіз інформаційної безпеки як динамічної соціально-правової системи та інтегрують проблематику кібербезпеки, інформаційного суверенітету і захисту прав людини у єдину наукову конструкцію;
- кібербезпеку розкрито як системоутворюючу складову інформаційної безпеки держави, що поєднує правові, організаційні та політичні інструменти захисту, а також сформульовано пріоритетні напрями розвитку національної системи кібербезпеки в умовах воєнного стану, зокрема: нормативне визначення правових режимів кібербезпеки; кодифікацію категорій кіберзагроз; правове врегулювання діяльності добровольчих кібервійськ; створення єдиного координаційного центру; запровадження уніфікованого протоколу реагування на кіберінциденти; інтеграцію міжнародних стандартів; розвиток технологічного суверенітету та кадрового потенціалу; впровадження спеціального режиму цифрових доказів та міжнародного співробітництва у сфері кібердоказування;
- визначено структуру інформаційного суверенітету як багатокомпонентного явища, що включає політико-правову, організаційно-

інституційну, інформаційно-технічну та культурно-гуманітарну складові, а також обґрунтовано систему напрямів його забезпечення в умовах воєнного стану, зокрема: модернізацію інформаційного законодавства; посилення інституційної спроможності суб'єктів; розвиток державної інформаційної політики; оновлення інформаційно-комунікаційної інфраструктури; підвищення медіаграмотності та національної консолідації; розширення міжнародного співробітництва у сфері протидії інформаційним загрозам;

удосконалено:

- положення щодо стратегічних комунікацій, які концептуалізовано як окрему функцію сектору безпеки і оборони, а не лише складову інформаційної політики; обґрунтовано, що їх ефективність залежить від інституційного закріплення, чіткого розмежування повноважень суб'єктів публічної влади та налагодження міжвідомчої координації; додатково аргументовано необхідність післявоєнного перегляду правових режимів у сфері інформаційної безпеки з метою недопущення збереження надмірних обмежень і забезпечення балансу між безпековими обмеженнями та гарантіями інформаційних прав;
- науковий підхід до адаптації зарубіжного досвіду забезпечення інформаційної безпеки в умовах воєнного конфлікту, який удосконалено шляхом застосування принципу пропорційності як базового критерію відбору правових механізмів, що дозволяє розмежовувати заходи, спрямовані на легітимний захист національної безпеки, та практики, несумісні з європейськими стандартами захисту прав людини. Обґрунтовано доцільність формування системної нормативно-правової моделі, яка інтегрує норми інформаційного, безпекового та адміністративного права (на прикладі Німеччини, Франції, Естонії, Іспанії та інших країн) і забезпечує узгодженість правового регулювання в умовах кризових і воєнних загроз;
- наукове розуміння інституційної складової забезпечення інформаційної безпеки як організованої системи уповноважених суб'єктів, діяльність яких нормативно врегульована та спрямована на формування і реалізацію державної політики у сфері інформаційної безпеки, а також на забезпечення належного рівня захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері; підхід до структурування системи суб'єктів забезпечення інформаційної безпеки України з урахуванням їх функціональної взаємодії, розподілу ролей та умов відсутності єдиного координаційного органу;

дістало подальшого розвитку:

- положення про інформаційну безпеку як складову національної безпеки України, яке, на відміну від наявних підходів, уточнено через визначення її як перманентного процесу і результату забезпечення стану захищеності національних інтересів, а також розширено шляхом виокремлення структурних складових (об'єкти, загрози, система забезпечення) та систематизації внутрішніх і зовнішніх загроз в умовах воєнного стану;
- теоретико-правове осмислення проблематики інформаційної безпеки, яке полягає в обґрунтуванні відсутності цілісної концепції її функціонування як складової національної безпеки, а також в узагальненні еволюції наукових

підходів (від фрагментарного до міждисциплінарного) і розширенні методологічних засад дослідження шляхом інтеграції концепцій кіберстійкості, управління ризиками, протидії дезінформації та інформаційної стійкості суспільства;

- підходи до правового забезпечення інформаційної безпеки, які удосконалено шляхом виокремлення трирівневої структури (національна безпека і оборона; інформаційні відносини; правовий статус суб'єктів), а також набули розвитку через обґрунтування необхідності систематизації, гармонізації інформаційного законодавства та розробки єдиного кодифікованого акта – Інформаційного кодексу України;

- положення щодо виявлення ключових проблем інституційного забезпечення (фрагментарності, недостатньої координації, нечіткості розподілу повноважень, обмеженої спроможності суб'єктів, слабкої інтеграції недержавного сектору та низького рівня медіаграмотності населення) та обґрунтування пріоритетних напрямів їх вирішення.

Практичне значення одержаних результатів Практичне значення одержаних результатів визначається можливістю їх використання у:

– *у науково-дослідній роботі* – для подальшого розвитку теоретико-правових досліджень у сфері інформаційної безпеки, аналізу нормативно-правових механізмів, інституційного забезпечення та вдосконалення державної політики у сфері кібербезпеки;

– *в освітньому процесі* – при викладанні навчальних дисциплін «Теорія держави та права», «Конституційне право», «Інформаційне право», «Міжнародне право», «Міжнародний захист прав людини», а також при підготовці навчально-методичних матеріалів з цих дисциплін;

– *у сфері правотворчості* – у діяльності суб'єктів правотворчої діяльності як теоретичне підґрунтя для формування ефективних державних правових політик у сфері інформаційної безпеки та удосконалення законодавства щодо забезпечення кібербезпеки та захисту інформаційного суверенітету;

– *у практичній сфері* – у діяльності органів державної влади, силових структур та органів місцевого самоврядування під час реалізації заходів щодо забезпечення інформаційної безпеки, кіберзахисту, захисту критичної інфраструктури та інформаційного суверенітету України (акт впровадження у діяльність Дніпропетровського окружного адміністративного суду від 16 квітня 2026 р.).

Апробація результатів дослідження. Основні теоретичні положення, їх новизна та практична значущість дослідження обговорювалися на засіданнях кафедри теорії держави та права Дніпровського державного університету внутрішніх справ та були оприлюднені на таких науково-практичних конференціях: міжнародних: «Modernization of science and its influence on global processes» (Bern, 2023), «Science and Practice: Implementation to Modern Society» (Manchester, 2023), «Міжнародна та національна безпека: теоретичні і прикладні аспекти» (Дніпро, 2025), «Міжнародна та національна безпека: теоретичні і прикладні аспекти» (Дніпро, 2026); всеукраїнських: «Актуальні проблеми державотворення та правозастосування» (Дніпро, 2023), «Права людини і громадянина під час дії

воєнного стану» (Харків, 2023), «Юридична весна: права людини в умовах воєнного стану» (Харків, 2024), «Конституційні права і свободи людини та громадянина в умовах війни та післявоєнний період» (Львів, 2024), «Проблеми юридичної науки очима молодих науковців» (Рівне, 2024), «Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення» (Дніпро, 2025).

Публікації. За темою дисертації опубліковано три статті у фахових виданнях України категорії «Б» з юридичних наук; десять тез доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається із основної частини (вступу, двох розділів, що об'єднують вісім підрозділів, висновків), списку використаних джерел та додатків.

Список публікацій здобувача за темою дисертації

в яких опубліковані основні наукові результати дисертації:

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Ряполов А. П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Т. 3, № 89. С. 87-91. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/336476/325112

2. Ряполов А. П. Гібридна агресія проти України як виклик модернізації правової політики у сфері інформаційної безпеки. *Український політико-правовий дискурс.* 2025. № 10. С. 1-14. URL: https://ppdnz.com.ua/index.php/home/article/view/236/151

3. Ряполов А. П. Захист інформаційного простору України в умовах гібридної війни: межі між свободою слова та інформаційною безпекою. *Національні інтереси України.* 2025. № 5 (10). С. 746-757. URL: https://perspectives.pp.ua/index.php/niu/article/view/23746/23719

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Ряполов А. П. Теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану. *Modernization of science and its influence on global processes:* collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, Bern, April 14, 2023. Bern, Swiss Confederation : European Scientific Platform, 2023. P. 41-43.

2. Ряполов А. П. Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни. *Science and Practice: Implementation to Modern Society:* with the Proceedingsof the 14 th International Scientific and Practical, Manchester, April 26-28, 2023. Manchester : Peal Press Ltd., 2023. P. 303-307.

3. Ряполов А. П. Співвідношення понять «інформаційна безпека» та «безпека інформації» у сучасному науковому просторі. *Актуальні проблеми державотворення та правозастосування :* матер. Всеукр. наук.-практ. конф., м. Дніпро, 7 груд. 2023 р. Дніпро : ДДУВС, 2024. С. 143-146.

4. Ряполов А. П. Організаційно-правові питання взаємодії органів публічної влади у сфері забезпечення інформаційної безпеки України. *Права людини і громадянина під час дії воєнного стану*: зб. наук. ст. за матеріалами

наук.-практ. конф. з нагоди 75-ї річниці Заг. декларації прав людини, м. Харків, 8 груд. 2023 р.: електрон. наук. вид. Харків : Право, 2023. С. 260-264.

5. Ряполов А. П. Інформаційна безпека України в умовах воєнного стану: проблеми та перспективи. *Юридична весна: права людини в умовах воєнного стану:* збірник тез наук.-практ. конф., м. Харків, 15 квітня 2024 р. Харків : Національний юридичний університет імені Ярослава Мудрого, 2024. С. 170-175.

6. Ряполов А. П. Інституційне забезпечення інформаційної безпеки України. *Конституційні права і свободи людини та громадянина в умовах війни та післявоєнний період* : матер. наук. семінару, м. Львів, 21 червня 2024 р. Львів : ЛьвДУВС, 2024. С. 167-170.

7. Ряполов А. П. Суб'єкти забезпечення інформаційної безпеки України. *Проблеми юридичної науки очима молодих науковців*: матеріали XVIII Всеукр. наук.-практ. онлайн-конф., м. Рівне, 17 жовтня 2024 р. Рівне : Національний університет біоресурсів та природокористування України, 2024. С. 64-67.

8. Ряполов А. П. Інформаційна безпека людини та громадянина як складова національної безпеки держави: загрози та виклики. *Міжнародна та національна безпека: теоретичні і прикладні аспекти :* матер. IX Міжнар. наук.-практ. конф., м. Дніпро, 21 березня 2025 р. ; у 2-х ч. Ч. II. Дніпро : ДДУВС, 2025. С. 458-459.

9. Ряполов А. П. Теоретико-правові засади взаємодії інституту військової експертизи з органами державної влади. *Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення*: матер. Всеукр. наук.-практ. конф., м. Дніпро, 25 квітня 2025 р. Дніпро : ДНДІСЕ МЮУ, 2025. С. 151-155.

10. Ряполов А. П. Свобода вибору та межі інформаційної безпеки в умовах воєнного стану: баланс між національною безпекою та свободою вираження поглядів. *Міжнародна та національна безпека: теоретичні і прикладні аспекти:* матер. XMіжнар. наук.-практ. конф., м. Дніпро, 16 березня 2026 р. ; у 2-х ч. Ч. II. Дніпро : ДДУВС, 2026. С. 476-477.

Характеристика особистості здобувача.

З 2022 року аспірант кафедри теорії держави та права (до червня 2024 року – кафедри загальноправових дисциплін) ДДУВС.

У 2022 році (протокол № 3 від 30.11.2022) затверджено тему дисертаційного дослідження «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» (науковий керівник – доктор юридичних наук, професор, заслуженого юриста України, академіка Національної академії наук вищої освіти України Наливайко Лариса Романівна).

Антон РЯПОЛОВ завершив у 2026 році написання дисертаційного дослідження, виконав індивідуальний план аспіранта кафедри теорії держави та права по виконанню освітньо-наукової програми на здобуття ступеня доктора філософії за спеціальністю 081 «Право».

Оцінка мови та стилю дисертації. Дисертація написана грамотно із застосуванням сучасної української мови та наукових термінів. Кожний із розділів, підрозділів та пунктів побудовані в логічній послідовності. Усе

це забезпечує легкість і доступність сприйняття викладених у дисертації положень.

У результаті попередньої експертизи дисертації Антона РЯПОЛОВА і повноти публікацій основних результатів дослідження

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів Ряполова Антона Павловича за темою «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика».

2. Констатувати, що за своїм змістом, глибиною розробок і оформленням дисертація Антона РЯПОЛОВА на тему «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» відповідає спеціальності 081 «Право» та вимогам пп. 6, 7, 8 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.

3. Рекомендувати Антону РЯПОЛОВУ звернутись до Вченої ради Дніпровського державного університету внутрішніх справ із заявою щодо утворення разової спеціалізованої вченої ради.

Головуючий засідання –
завідувач кафедри
теорії та історії держави та права,
конституційного права та прав людини
Дніпровського державного
університету внутрішніх справ,
доктор юридичних наук, професор **Валентина БОНЯК**
19 травня 2026 року