РЕЦЕНЗІЯ

на дисертаційну роботу Ряполова Антона Павловича «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика», подану на здобуття наукового ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право»

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.

Попри значну кількість наукових праць, присвячених окремим аспектам інформаційної безпеки – кібербезпеці, захисту персональних даних, медіарегулюванню, – комплексне теоретико-правове дослідження, яке б системно охоплювало нормативно-правове забезпечення, інституційний механізм, кібербезпеку та інформаційний суверенітет саме в умовах воєнного стану, у вітчизняній правовій науці фактично відсутнє. Дисертація Ряполова Антона Павловича заповнює цю прогалину і є однією із перших комплексних теоретико-правових робіт у зазначеній сфері.

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. Перший розділ формує теоретико-методологічну основу: підрозділ 1.1 присвячено методології дослідження, 1.2 – аналізу стану наукової розробленості проблематики, 1.3 – понятійно-категоріальному апарату, 1.4 – зарубіжному досвіду. Другий розділ охоплює нормативно-правове забезпечення (2.1), інституційне забезпечення (2.2), кібербезпеку (2.3) та інформаційний суверенітет (2.4). Така структура забезпечує комплексний і системний підхід до вирішення поставлених завдань.

Наукова новизна одержаних результатів є переконливою: у роботі 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.

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 (с. 26-28 дис.). 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 (с. 180 дис.). 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 (с. 31 дис.). Ця чотириелементна конструкція є авторською систематизацією, яка відсутня у запропонованому вигляді в інших дослідженнях.

Заслуговує на увагу концептуалізація стратегічних комунікацій як окремої функції сектору безпеки і оборони, а не лише складової інформаційної політики (с. 47, 51, 104 дис.). Здобувач аргументує необхідність її інституційного закріплення з чітким розмежуванням повноважень між суб'єктами публічної влади – що є практично значущою пропозицією в умовах тривалого інформаційного протиборства.

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 (с. 111-112 дис.). 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.

Рецензент:

доктор юридичних наук, професор,
професор кафедри теорії держави та права
Навчально-наукового інституту права
та інноваційної освіти
Дніпровського державного універеитету
внутрішніх справ **Дмитро СЕЛІХОВ**