

ВІДГУК

офіційного опонента, кандидата юридичних наук Рички Дениса Олеговича на дисертацію Олійника Артема Андрійовича за темою «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри», подану на здобуття ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право»

1. Актуальність теми дисертаційного дослідження

Дисертаційне дослідження Олійника Артема Андрійовича присвячене актуальним питанням юридичної науки на цей час - кримінологічним засадам забезпечення інформаційної безпеки у міжнародному, національному та зарубіжному вимірах. Обрана тема має не лише теоретико-правове, а й безпосереднє прикладне значення, оскільки інформаційна безпека в умовах цифрової трансформації, воєнного стану, активного застосування штучного інтелекту, поширення кіберзлочинності та інформаційно-психологічних операцій перетворилася на один із ключових елементів національної безпеки України.

Актуальність роботи зумовлюється тим, що сучасна кіберзлочинність давно вийшла за межі класичних посягань на комп'ютерні системи та охоплює широкий спектр суспільно небезпечних проявів: атаки на критичну інфраструктуру, цифрове шахрайство, використання штучного інтелекту для створення синтетичного контенту (так звані дипфейки), маніпулятивний вплив на суспільну свідомість, дезінформаційні кампанії, транскордонне приховування джерел кібератак, використання анонімізаційних технологій, а також посягання на персональні дані та цифрові права людини.

Для України зазначена проблематика має особливе значення, адже в умовах повномасштабної збройної агресії російської федерації кіберпростір став фактично окремим виміром протистояння. Кібератаки на державні реєстри, енергетичні системи, органи публічної влади, об'єкти критичної інфраструктури, а також масові інформаційно-психологічні операції проти населення створюють комплексну загрозу державному суверенітету, правам людини, стабільності демократичних інститутів і довірі до держави.

У цьому контексті дисертація є своєчасною, науково виправданою та суспільно значущою. Її актуальність також підтверджується тим, що автор намагається поєднати кримінологічний, кримінально-правовий, міжнародно-правовий, правозахисний, технологічний і віктимологічний підходи до осмислення інформаційної безпеки як складного багаторівневого об'єкта правової охорони та кримінологічної превенції.

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

Позитивної оцінки заслуговує зв'язок дисертаційного дослідження з актуальними напрямками державної політики та наукових досліджень у сфері національної безпеки, кібербезпеки, захисту прав людини, реформування органів правопорядку та європейської інтеграції України.

Робота корелює з положеннями стратегічних документів України у сфері національної безпеки, кібербезпеки, цифрового розвитку, реформування органів правопорядку, а також із науково-дослідною тематикою кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара “Забезпечення реалізації та захист основних свобод, прав людини, національних інтересів держави в умовах гібридних загроз і безпекових викликів”.

Такий зв’язок свідчить, що дисертація виконана не ізольовано від сучасних потреб науки і практики, а в межах актуального дослідницького напрямку, який має важливе значення для правової системи України в умовах війни та майбутнього повоєнного відновлення.

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій.

Наукові положення, висновки та рекомендації, сформульовані у дисертації, загалом є достатньо обґрунтованими. Автор використав широкий методологічний інструментарій, зокрема діалектичний, системно-структурний, порівняльно-правовий, статистичний, віктимологічний, праксеологічний, аксіологічний методи, а також метод факторного аналізу. Такий підхід дозволив комплексно розглянути інформаційну безпеку не лише як технічну чи адміністративно-правову категорію, а як об’єкт кримінологічного захисту, що охоплює інфраструктурний, правовий і соціально-психологічний рівні.

Сильною стороною дисертації є міждисциплінарний характер дослідження. Автор не обмежується аналізом норм кримінального чи спеціального законодавства, а залучає положення міжнародного права, практику ЄСПЛ, стандарти ЄС, документи НАТО, матеріали міжнародних безпекових інституцій, аналітичні звіти щодо кіберзагроз, положення доктрини інформаційної безпеки, кримінології, віктимології та цифрових прав людини.

Достатньо переконливою є емпірична база дослідження. Автор посилається на статистичні дані Офісу Генерального прокурора, Національної поліції України, Департаменту кіберполіції, аналітичні матеріали міжнародних організацій, судову практику, доктринальні джерела, а також міжнародні стандарти у сфері кібербезпеки та захисту персональних даних. Значний масив використаних джерел - 347 найменувань - свідчить про належне опрацювання автором наукової, нормативної та аналітичної бази.

Обґрунтованість висновків посилюється тим, що дисертаційне дослідження має чітку внутрішню логіку: від теоретико-методологічного осмислення інформаційної безпеки як об’єкта кримінологічної превенції - до аналізу національного виміру запобігання загрозам інформаційній безпеці України та подальшого звернення до зарубіжного досвіду й напрямів удосконалення національної системи кримінологічного реагування.

4. Наукова новизна одержаних результатів

Наукова новизна дисертації полягає у спробі комплексного кримінологічного осмислення інформаційної безпеки у трьох взаємопов’язаних вимірах: міжнародному, національному та зарубіжному. Робота є цікавою саме тому, що автор прагне подолати вузькотехнологічне розуміння кібербезпеки і

пропонує ширшу модель інформаційної безпеки, в якій технічний захист, правовий режим даних, когнітивна стійкість особи та суспільства розглядаються як взаємозалежні елементи єдиної системи.

До вагомих положень наукової новизни слід віднести такі:

- По-перше, автором обґрунтовано комплексну трирівневу модель інформаційної безпеки як об'єкта кримінологічного захисту. Зазначена модель базується на розширенні класичної Тріади CIA - конфіденційність, цілісність, доступність - елементами автентичності та неспростовності, що має особливе значення для кримінального процесуального доказування у справах про кіберзлочини.
- По-друге, заслуговує на підтримку авторське розмежування інформаційної безпеки, кібербезпеки та цифрової безпеки. Такий підхід є корисним для подальшого розвитку понятійно-категоріального апарату юридичної науки, оскільки в науковому й нормативному дискурсі ці поняття нерідко використовуються як близькі або навіть взаємозамінні, що знижує точність правового регулювання.
- По-третє, цікавим є обґрунтування дворівневої природи кіберстійкості: кіберстійкості держави та кіберстійкості особи. Така постановка питання є перспективною, адже дозволяє поєднати макрорівень — інституційну спроможність держави підтримувати критичні функції, адаптуватися до гібридних загроз і відновлювати цифрову інфраструктуру — з мікрорівнем, на якому ключового значення набувають правова обізнаність, кібергігієна, когнітивні навички та здатність людини протистояти маніпулятивним інформаційним впливам.
- По-четверте, науково продуктивною є концепція “когнітивного імунітету” суспільства як кримінологічної та віктимологічної категорії. Запропонований підхід відповідає сучасним викликам, оскільки інформаційні атаки, соціальна інженерія, дезінформація та маніпулятивний контент дедалі частіше спрямовуються не стільки на технічні системи, скільки на поведінку, сприйняття, волю та рішення людини.
- По-п'яте, на увагу заслуговує пропозиція щодо створення національного Інституту безпеки штучного інтелекту за аналогією з іноземними моделями. Ця ідея має практичний потенціал, особливо в умовах стрімкого поширення генеративного ШІ та його використання як у легітимній діяльності, так і для створення нових криміногенних ризиків.
- По-шосте, автор вдосконалює віктимологічний підхід до запобігання кіберзлочинності через поняття “техногенної віктимності” організацій. Таке положення є важливим, оскільки сучасні кіберінциденти нерідко зумовлені не лише активністю правопорушника, а й організаційною недбалістю, помилками конфігурації, слабкою договірною підзвітністю, недостатньою кібергігієною персоналу та неефективним управлінням цифровими ризиками.

5. Теоретичне та практичне значення результатів дисертації

Теоретичне значення дисертації полягає в тому, що її положення можуть бути використані для подальшого розвитку кримінології, кримінального права, кримінального процесу, міжнародного права, інформаційного права, права національної безпеки та теорії цифрових прав людини.

Особливо важливим є запропонований автором перехід від реактивного технічного захисту до проактивної моделі кримінологічної превенції, яка охоплює державу, суспільство, організації та окрему особу. Такий підхід може бути корисним для подальших наукових досліджень у сфері протидії кіберзлочинності, дезінформації, інформаційній агресії, злочинному використанню штучного інтелекту, а також у сфері формування національної кіберстійкості.

Практичне значення роботи проявляється у можливості використання її положень:

- у правотворчій діяльності - під час удосконалення законодавства про кібербезпеку, інформаційну безпеку, захист персональних даних, протидію дезінформації, регулювання штучного інтелекту та цифрових доказів;
- у правозастосовній діяльності - для підвищення ефективності роботи правоохоронних органів під час виявлення, розслідування та запобігання кіберзлочинам транскордонного характеру;
- у діяльності органів сектору безпеки і оборони - для розроблення превентивних моделей реагування на гібридні загрози, інформаційно-психологічні операції та атаки на критичну інфраструктуру;
- в освітньому процесі - під час викладання кримінології, кримінального права, інформаційного права, кібербезпеки, дисциплін, пов'язаних із цифровою державою, правами людини в цифровому середовищі та протидією злочинності в умовах глобалізації.

Позитивної оцінки заслуговує також пропозиція автора щодо запровадження міждисциплінарного спецкурсу "Правові засади кіберстійкості та цифрова держава". Такий спецкурс може мати практичне значення для підготовки нової генерації правників, управлінців, політологів, соціологів, журналістів та фахівців, здатних працювати в умовах гібридних загроз і цифрової трансформації.

6. Оцінка змісту та структури дисертації

Структура дисертації загалом відповідає її меті та завданням. Робота складається з анотації, вступу, трьох розділів, дев'яти підрозділів, висновків, списку використаних джерел і додатків.

У першому розділі розкрито теоретико-методологічні основи кримінологічного забезпечення інформаційної безпеки. Автор досліджує інформаційну безпеку як об'єкт кримінологічного захисту, аналізує генезис наукової думки, етапи становлення правових засад забезпечення інформаційної безпеки, а також принципи і механізми міжнародно-правового забезпечення інформаційної безпеки. Цей розділ має важливе концептуальне значення, оскільки саме в ньому закладається авторське бачення інформаційної безпеки як багаторівневого об'єкта кримінологічної превенції.

У другому розділі досліджено національний вимір кримінологічного запобігання загрозам інформаційній безпеці України. Автор аналізує особливості забезпечення інформаційної безпеки в умовах воєнного стану, законодавчі та інституційні засади інформаційної безпеки України, а також

кримінологічну превенцію у сфері інформаційної безпеки в контексті балансу між державним суверенітетом і захистом прав людини. Сильним аспектом цього розділу є спроба поєднати безпекову проблематику із правозахисною оптикою, що є особливо важливим в умовах воєнного стану.

У третьому розділі розглянуто зарубіжний досвід і напрями вдосконалення національної системи кримінологічного реагування. Автор звертається до порівняльно-правового аналізу зарубіжних стратегій забезпечення інформаційної безпеки, міжнародного співробітництва у протидії транснаціональним кіберзагрозам, а також формулює пропозиції щодо розвитку національної кіберстійкості України. Цей розділ має прикладне значення, оскільки спрямований на пошук моделей, які можуть бути адаптовані до українських реалій.

Загальні висновки дисертації відповідають поставленим завданням і відображають основні результати проведеного дослідження. Вони є логічним підсумком викладеного матеріалу та підтверджують, що мета дослідження в цілому досягнута.

7. Повнота викладення наукових результатів у публікаціях.

Основні положення дисертаційного дослідження висвітлено у 10 наукових працях здобувача, з яких 5 є статтями у наукових фахових виданнях України, а 5 - тезами доповідей у матеріалах науково-практичних конференцій, форумів і круглих столів.

Тематика опублікованих праць відповідає темі дисертації та відображає основні напрями проведеного дослідження: сутність інформаційної безпеки як правового явища, превентивна роль інформаційної безпеки і кримінально-правової політики, запобігання правопорушенням у сфері інформаційної безпеки, кіберстійкість і права людини, міжнародне запобігання злочинності у сфері цифрових технологій, забезпечення правопорядку на звільнених територіях у контексті протидії гібридним загрозам.

У дисертації також зазначено особистий внесок здобувача у спільну публікацію, що відповідає усталеним вимогам академічної доброчесності та дозволяє ідентифікувати власний науковий доробок автора.

8. Дотримання академічної доброчесності.

За результатами аналізу змісту дисертації можна зробити висновок, що автор загалом дотримується вимог академічної доброчесності: використані ідеї, положення, статистичні дані, нормативні акти та наукові джерела супроводжуються посиланнями; у роботі наведено значний список використаних джерел; зазначено публікації здобувача та особистий внесок у спільній праці.

Водночас остаточно оцінка дотримання академічної доброчесності, зокрема в частині технічної перевірки на академічний плагіат, фабрикацію чи фальсифікацію, має здійснюватися закладом вищої освіти відповідно до встановлених процедур. У межах наукового аналізу тексту дисертації підстав для висновку про недоброчесність здобувача не встановлено.

9. Дискусійні положення та зауваження до дисертації.

Позитивно оцінюючи дисертаційне дослідження загалом, слід висловити окремі зауваження та побажання, які мають переважно дискусійний і рекомендаційний характер та не знижують загальної позитивної оцінки роботи.

1. **Щодо емпіричної складової дослідження.** Автор використовує статистичні дані щодо кіберзлочинності, матеріали правоохоронної та судової практики, аналітичні звіти міжнародних організацій. Разом із тим робота, на мою думку, виграла б від більш розгорнутого представлення емпіричного матеріалу у вигляді окремих таблиць, діаграм або порівняльних блоків із розмежуванням за видами кримінальних правопорушень, періодами порівняння статистичних даних до та після повномасштабного вторгнення, суб'єктами розслідування, рівнем латентності та типовими способами вчинення кіберзлочинів.
2. **Щодо пропозицій про криміналізацію нових цифрових загроз.** Заслугує на підтримку позиція автора щодо необхідності реагування на нові загрози, пов'язані зі штучним інтелектом, дипфейками та синтетичним контентом експлуатації дітей. Водночас у подальших дослідженнях доцільно було б конкретизувати можливу законодавчу модель такої криміналізації: визначити об'єкт кримінально-правової охорони, межі кримінально караної поведінки, суб'єктивну сторону, кваліфікуючі ознаки та співвідношення нових складів із уже наявними нормами Кримінального кодексу України.
3. **Щодо концепції “когнітивного імунітету”.** Концепція когнітивного імунітету суспільства є однією з найбільш цікавих і перспективних у дисертації. Водночас вона потребує подальшого теоретичного уточнення. Зокрема, бажано чіткіше окреслити її межі як саме кримінологічної категорії, відмежувати її від понять інформаційної грамотності, медіаграмотності, кібергігієни, психологічної стійкості та цифрової компетентності. Також важливо визначити, які саме суб'єкти мають формувати когнітивний імунітет і якими правовими засобами це має здійснюватися без ризику надмірного державного патерналізму або невинновданого обмеження свободи слова.
4. **Щодо пропозиції створення національного Інституту безпеки штучного інтелекту.** Ідея створення такої інституції є цікавою та актуальною. Водночас у дисертації доцільно було б більш детально визначити її можливий правовий статус, місце в системі органів публічної влади, співвідношення з повноваженнями Держспецзв'язку, СБУ, Національної поліції, Міністерства цифрової трансформації, РНБО та інших суб'єктів сектору безпеки. Окремого уточнення потребують гарантії недопущення дублювання повноважень і надмірного адміністративного навантаження на інноваційний сектор.
5. **Щодо міжнародно-правового блоку.** У роботі слушно наголошено на значенні Будапештської конвенції, стандартів ЄС, NIS2, GDPR, міжнародної співпраці, цифрових доказів і проблеми атрибуції кібератак. Разом із тим дисертація виграла б від чіткішого розмежування міжнародно-правової, кримінально-правової та міжнародно-гуманітарної кваліфікації кібератак, особливо в частині визначення критеріїв, за яких кібератака може розглядатися як воєнний злочин.
6. **Щодо балансу між свободою і безпекою.** Автор справедливо зазначає, що надмірний контроль у цифровому середовищі може створювати ризики для прав людини, тоді як його відсутність посилює криміногенні загрози.

Водночас бажано було б ширше розкрити критерії пропорційності, необхідності в демократичному суспільстві, судового контролю та ефективних засобів правового захисту з урахуванням практики Європейського суду з прав людини.

7. Загальний висновок.

Дисертація Олійника Артема Андрійовича «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри» є самостійною, завершеною кваліфікаційною науковою працею, в якій отримано нові науково обґрунтовані результати, що в сукупності вирішують актуальне наукове завдання, важливе для кримінології, правової науки, сфери інформаційної безпеки та практики запобігання кіберзлочинності.

Робота характеризується актуальністю, належним рівнем теоретичної обґрунтованості, міждисциплінарністю, практичною спрямованістю, достатньою апробацією результатів і відповідністю темі дослідження. Основні положення дисертації відображені у наукових публікаціях здобувача.

Сформульовані автором висновки та пропозиції мають наукову новизну, теоретичне і практичне значення.

Дисертація за своїм змістом, структурою, науковим рівнем, ступенем обґрунтованості положень, новизною одержаних результатів, повнотою їх оприлюднення та практичним значенням відповідає спеціальності 081 Право та вимогам, визначеним Порядком підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженим постановою Кабінету Міністрів України від 23.08.2016 № 261 (із змінами), наказом МОН від 12.01.2017 № 40 та 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 № 44 від 12.01.2022 р., а її автор – Олійник Артем Андрійович, на підставі прилюдного захисту заслуговує на присудження ступеня доктора філософії у галузі знань 08 Право за спеціальністю 081 «Право».

Офіційний опонент:

кандидат юридичних наук,
доцент кафедри публічного управління
та права ННІ Придніпровська державна
академія будівництва та архітектури
Українського державного університету
науки та технологій



Денис РИЧКА

