

*До разової спеціалізованої вченої ради
Одеського державного університету внутрішніх справ
щодо захисту дисертації Шаронова А.П.
(65014, м. Одеса, вул. Успенська, 1)*

РЕЦЕНЗІЯ

**кандидата юридичних наук, доцента Форос Г.В. на дисертацію
Шаронова Андрія Павловича на тему «Протидія кіберзагрозам
Національною поліцією України: організаційно-правовий аспект», подану
на здобуття наукового ступеня доктора філософії
за спеціальністю 081 «Право»**

Актуальність теми дисертаційного дослідження.

Сучасний етап розвитку української держави характеризується системною цифровою трансформацією публічного управління, економіки, правоохоронної діяльності та суспільних комунікацій. Переміщення значної частини суспільних відносин у цифрове середовище закономірно супроводжується виникненням якісно нових загроз, для яких характерні транснаціональність, технологічна складність, латентність, динамічність, асиметричність та потенційна здатність завдавати значної шкоди правам і свободам людини, державним інтересам, інформаційним ресурсам, критичній інфраструктурі та належному функціонуванню державних інституцій. У цьому контексті кіберзагрози перестають бути виключно технологічною проблемою та набувають комплексного правового, правоохоронного й безпекового значення.

Слушною є позиція здобувача щодо необхідності розглядати кіберпростір не лише як технологічне середовище, а як особливу сферу реалізації суспільних відносин, у межах якої здійснюються публічне управління, надання електронних послуг, комунікація, економічна діяльність та реалізація основоположних прав людини. Відповідно, кіберзагрози безпосередньо впливають на стан публічної та інформаційної безпеки,

стійкість цифрової інфраструктури, рівень довіри громадян до цифрових сервісів і спроможність держави належним чином виконувати свої функції.

Особливого значення досліджувана проблематика набуває для діяльності Національної поліції України, яка виступає одним із ключових правоохоронних суб'єктів у сфері виявлення, припинення, документування та розслідування кримінальних правопорушень, учинених у кіберпросторі або з використанням інформаційно-комунікаційних технологій. Водночас ефективність такої діяльності значною мірою залежить не лише від технічного оснащення відповідних підрозділів, а й від чіткості правового регулювання їх компетенції, належної організації міжвідомчої взаємодії, нормативної визначеності процедур реагування на кіберінциденти, забезпечення процесуальної придатності цифрових даних та дотримання прав людини.

Актуальність дисертаційного дослідження істотно посилюється умовами правового режиму воєнного стану, за яких кіберзагрози дедалі частіше виступають складовою гібридного впливу на державу. Кібератаки на інформаційні системи органів державної влади, державні реєстри, об'єкти критичної інфраструктури, системи зв'язку та фінансові сервіси обумовлюють необхідність оперативного, скоординованого та водночас юридично коректного реагування. При цьому цілком обґрунтованою є позиція автора щодо неприпустимості протиставлення оперативності правоохоронного реагування вимогам законності, пропорційності та гарантіям прав і свобод людини.

Важливою детермінантою актуальності теми є також євроінтеграційний курс України, що потребує розвитку ризик-орієнтованих механізмів забезпечення кібербезпеки, удосконалення інституційної взаємодії, стандартизації процедур реагування на кіберінциденти, забезпечення захисту персональних даних та безперервності критичних функцій.

Заслуговує підтримки аргументація здобувача щодо існування низки системних проблем у цій сфері, насамперед фрагментарності нормативного регулювання, недостатньої визначеності компетенції окремих суб'єктів,

необхідності вдосконалення процедур взаємодії Національної поліції України з іншими суб'єктами кібербезпеки, а також наявності проблемних питань щодо отримання, фіксації, збереження та подальшого процесуального використання цифрових даних.

Отже, обрана тема дисертаційного дослідження характеризується належним ступенем наукової актуальності, має виразне теоретичне та практичне значення й відповідає сучасним потребам удосконалення правового забезпечення діяльності Національної поліції України в умовах цифрової трансформації, воєнного стану та подальшої інтеграції України до європейського безпекового і правового простору.

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

Дисертаційне дослідження має належний зв'язок із пріоритетними напрямами державної політики у сфері національної безпеки, реформування органів правопорядку, кібербезпеки та цифрової трансформації.

Роботу виконано з урахуванням положень Стратегії національної безпеки України, Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, Плану реалізації Стратегії кібербезпеки України, Плану заходів із реалізації Стратегії розвитку Національної поліції України на 2026-2030 роки, а також пріоритетних напрямів цифрової трансформації. Дослідження узгоджується з тематикою науково-дослідної діяльності Одеського державного університету внутрішніх справ та кафедри кримінального аналізу та інформаційних технологій. Тема дисертації затверджена Вченою радою Одеського державного університету внутрішніх справ.

Зазначене свідчить про системний зв'язок дисертації як із загальнодержавними пріоритетами розвитку сектору безпеки і оборони, так і з відповідними напрямами наукового забезпечення правоохоронної діяльності.

Крім того, дослідження проводилось згідно наукових досліджень Одеського державного університету внутрішніх справ за період 2023-2028 р.р. при виконанні теми «Пріоритетні напрямки розвитку реформування

правоохоронних органів в умовах розгортання демократичних процесів у державі» (державний реєстраційний номер 0123U103538) та «Використання кримінального аналізу в правоохоронній діяльності» (номер державної реєстрації 0124U001432, 2024-2029 р.р.).

Метою дисертаційного дослідження визначено розроблення науково обґрунтованих теоретичних положень і практичних рекомендацій щодо вдосконалення організаційно-правового механізму протидії кіберзагрозам у діяльності Національної поліції України.

Для досягнення зазначеної мети автором поставлено взаємопов'язаний комплекс *наукових завдань*, спрямованих на розкриття правової природи кіберзагроз, їх класифікацію та визначення критеріїв небезпечності; дослідження міжнародно-правових стандартів протидії кіберзагрозам та рівня їх імплементації; аналіз нормативно-правових засад діяльності Національної поліції України; оцінювання інституційної спроможності підрозділів кіберполіції; визначення особливостей організації діяльності в умовах воєнного стану та розроблення напрямів удосконалення правового й організаційного механізмів протидії кіберзагрозам.

Об'єктом дослідження визначено суспільні відносини, що виникають у сфері протидії кіберзагрозам у діяльності правоохоронних органів, а предметом — організаційно-правовий механізм протидії кіберзагрозам у діяльності Національної поліції України.

Мета, завдання, об'єкт і предмет дослідження є взаємоузгодженими та створюють належну концептуальну основу для комплексного розкриття обраної наукової проблематики.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Належний рівень обґрунтованості результатів дисертаційного дослідження забезпечується комплексним характером використаного методологічного інструментарію. Методологічну основу становить сукупність загальнонаукових та спеціально-юридичних методів, серед яких діалектичний,

історико-правовий, компаративний, логіко-юридичний, системний, догматичний методи, а також метод спостереження.

Позитивною рисою методології є предметна прив'язка окремих методів до конкретних напрямів дослідження. Застосований інструментарій дає можливість поєднати доктринальний аналіз правової природи кіберзагроз із дослідженням нормативної основи правоохоронної діяльності, організаційних механізмів реагування та міжнародного досвіду.

Комплексний характер роботи додатково підтверджується заявленою емпіричною базою, яка охоплює матеріали правозастосовної й організаційної практики Національної поліції України, типові сценарії реагування на кіберінциденти, статистичні та аналітичні відомості щодо кіберзлочинності й кіберінцидентів, матеріали профільних суб'єктів кібербезпеки та результати узагальнення практики міжвідомчої взаємодії.

Нормативно-правову основу дослідження становлять Конституція України, законодавство, що визначає правовий статус та компетенцію Національної поліції України, нормативні акти у сфері кібербезпеки, захисту інформації, персональних даних і критичної інфраструктури, а також міжнародно-правові акти та стандарти.

Наукова новизна отриманих результатів.

Наукова новизна дисертації полягає передусім у комплексному теоретичному обґрунтуванні організаційно-правового механізму протидії кіберзагрозам Національною поліцією України як взаємопов'язаної системи правових норм, інституцій, організаційних зв'язків та процедур, функціонування якої має забезпечувати оперативність реагування, належну процесуальну якість роботи з цифровими даними, міжвідомчу та міжнародну взаємодію, дотримання прав людини та адаптивність правоохоронної системи до умов воєнного стану.

На особливу увагу заслуговує запропоноване автором комплексне трактування кіберзагроз як самостійного підкласу загроз національній безпеці з подвійною техніко-юридичною природою. Такий підхід є методологічно

перспективним, оскільки дозволяє подолати суто технократичне розуміння кіберзагрози та безпосередньо пов'язати її технологічні характеристики з юридичними наслідками для вибору правового режиму реагування, здійснення доказування та визначення компетенції відповідних суб'єктів.

Науково значущим є сформульоване авторське визначення «інтероперабельності у кібербезпеці», під якою запропоновано розуміти системну спроможність технічних, організаційних, процедурних та нормативних компонентів різних суб'єктів забезпечувати узгоджену, безпечну й безперебійну взаємодію на основі гармонізованих стандартів, форматів даних і регламентів інформаційного обміну. Запропонований підхід дозволяє перевести категорію інтероперабельності з переважно технологічної площини у площину організаційно-правового забезпечення кібербезпеки.

Суттєвий науковий інтерес становить концептуальна модель механізму протидії кіберзагрозам у діяльності Національної поліції України, побудована як єдиний цикл: превенція та моніторинг → виявлення і первинне реагування → оцінювання та пріоритизація → координація → фіксація і збереження цифрових даних → розслідування та процесуальне оформлення → аналіз досвіду й удосконалення практик. Її цінність полягає у поєднанні організаційно-управлінської, технічної та кримінально-процесуальної складових реагування.

Оригінальним є також положення щодо можливості використання превентивних інформаційно-консультаційних онлайн-ресурсів як додаткового емпіричного джерела для виявлення та уточнення масових соціально-інженерних кіберзагроз із високим рівнем латентності.

Заслужують позитивної оцінки вдосконалені автором підходи до класифікації кіберзагроз для потреб Національної поліції України через багатовимірну модель «суб'єкт – вектор доступу – тип технічного впливу – об'єкт посягання» та її безпосередню прив'язку до управлінських і процесуальних рішень.

Науково обґрунтованим видається поєднання юридичних та операційних критеріїв оцінювання небезпечності кіберзагроз, зокрема імовірності реалізації, рівня складності, впливу на конфіденційність, цілісність та доступність інформації, швидкості детектування і реагування, потенціалу поширення, юридичних та репутаційних наслідків.

Важливе практико-прикладне значення має розвиток положень щодо процесуальної придатності цифрових даних, де акцент зроблено на законності способу їх отримання, належному документуванні, збереженні, відтворюваності та перевірюваності.

Окремої позитивної оцінки заслуговує спроба автора концептуалізувати проблему використання результатів систем штучного інтелекту у кримінальному провадженні та пов'язати їх процесуальне використання з необхідністю верифікації алгоритмічних результатів, установлення показників точності й похибки, документування методики та забезпечення відтворюваності.

Подальшого розвитку в дисертації набули положення щодо співвідношення категорій «загроза», «небезпека» та «ризик» у кіберпросторі; гармонізації національного правового регулювання з міжнародними стандартами; діяльності кіберполіції в умовах воєнного стану; запровадження «подвійного контуру» управління кіберінцидентом; розвитку професійних компетентностей працівників правоохоронних органів у парадигмі Intelligence-Led Policing та інституціоналізації міжсекторної взаємодії.

Таким чином, сформульовані у дисертації положення наукової новизни мають системний характер, взаємопов'язані із завданнями дослідження та спрямовані не лише на розвиток теоретичних положень юридичної науки, але й на вирішення конкретних проблем організації правоохоронної діяльності у кіберпросторі.

Повнота оприлюднення основних положень дисертації в публікаціях та особистий внесок автора в отримання наукових результатів.

Основні результати дисертаційного дослідження опубліковано у 9 наукових працях, серед яких 6 статей у наукових фахових виданнях України з юридичних наук та 3 праці апробаційного характеру. Результати дослідження також доповідалися на міжнародних науково-практичних та науково-теоретичних конференціях.

Зазначене дозволяє констатувати належний рівень апробації основних результатів дисертаційної роботи.

Наукове та практичне значення отриманих результатів.

Практичне значення дисертаційного дослідження має комплексний характер та полягає у можливості використання сформульованих положень і рекомендацій у правотворчій, правозастосовній, науково-дослідній та освітній діяльності.

У правотворчій сфері результати дослідження можуть бути використані для вдосконалення нормативного регулювання протидії кіберзагрозам, уточнення понятійно-категоріального апарату, розмежування компетенції Національної поліції України й інших суб'єктів національної системи кібербезпеки, а також нормативної формалізації процедур координації, інформаційного обміну та реагування на кіберінциденти.

У правозастосовній діяльності запропоновані рекомендації орієнтовані на вдосконалення діяльності кіберполіції, слідчих та оперативних підрозділів під час виявлення, припинення і документування кіберправопорушень, взаємодії з іншими суб'єктами кібербезпеки, фіксації цифрових слідів та забезпечення належності, допустимості й достовірності електронних доказів.

У науково-дослідній діяльності положення дисертації можуть бути використані як методологічна основа для подальшого дослідження організаційно-правових механізмів правоохоронної діяльності в кіберпросторі, критеріїв оцінювання кіберзагроз, інституційної спроможності підрозділів кіберполіції та процесів гармонізації українського законодавства з європейськими стандартами кібербезпеки.

В освітньому процесі результати роботи можуть застосовуватися при підготовці навчальних і методичних матеріалів, спецкурсів та тренінгових програм для здобувачів юридичної освіти і працівників Національної поліції України, зокрема з питань правових засад реагування на кіберінциденти, роботи з цифровими доказами, міжвідомчої взаємодії та захисту прав людини у цифровому середовищі.

Практична спрямованість результатів підтверджується наведеними у вступі відомостями про їх упровадження в діяльність Департаменту кіберполіції Національної поліції України та освітню і науково-дослідну діяльність Одеського державного університету внутрішніх справ.

Оцінка змісту, структури дисертації, мови та стилю викладання.

Аналіз структури дисертаційного дослідження вказує на те, що основний зміст роботи логічно пов'язаний з метою, завданнями, об'єктом і предметом дослідження. Дисертація складається з вступу, трьох розділів, що включають в себе 9 підрозділів, висновків, списку використаних джерел (в кількості 222).

У цілому науковий рівень дисертації дозволяє надати позитивну оцінку змісту дисертації, визнати її завершеною працею, у якій автору вдалося досягти мети дослідження.

Дисертація Шаронова А.П. оформлена згідно з нормативними вимогами і стандартами, які передбачені для такого виду досліджень. Робота написана державною мовою з дотриманням наукового стилю. Текст дисертації позбавлений технічних недоліків. Основні положення, висновки і пропозиції, що містяться у науковій праці, в цілому характеризуються послідовністю, аргументованістю та завершеністю.

Дискусійні положення та зауваження до дисертації.

1. Науково цікавою, проте такою, що потребує додаткової процесуально-правової аргументації, є пропозиція щодо використання результатів систем штучного інтелекту через їх процесуалізацію у форматі судової експертизи та виокремлення алгоритмічної (цифрової) експертизи.

2. Запропонована автором категорія «інтероперабельність у кібербезпеці» має високий потенціал для розвитку організаційно-правового механізму протидії кіберзагрозам, однак потребує подальшої юридичної операціоналізації.

3. З огляду на прикладну спрямованість дисертації та значну кількість положень щодо інституційної спроможності, ефективності реагування й практики міжвідомчої взаємодії, наукову переконливість роботи могло б додатково посилити максимально чітке кількісне визначення емпіричного масиву: періоду дослідження, кількості проаналізованих матеріалів, статистичних масивів, категорій кіберінцидентів та інших показників, якщо їх розкриття не обмежене режимом доступу до відповідної інформації.

Однак, указані недоліки, маючи дискусійний (рекомендаційний) характер, не впливають на загальну позитивну оцінку наукової роботи.

Таким чином, дисертація Шаронова Андрія Павловича на тему «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» є самостійним, завершеним дослідженням, що розв'язує важливу наукову проблему вітчизняної правничої науки, відповідає спеціальності 081 – Право, 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, а її автор – Шаронов Андрій Павлович заслуговує на присудження ступеня доктора філософії за спеціальністю 081 – Право.

Завідувач кафедри

кримінального аналізу та інформаційних технологій

Одеського державного університету внутрішніх справ

кандидат юридичних наук, доцент

Ганна ФОРОС