ЗАТВЕРЖУЮ
Перший проректор Одеського
державного університету внутрішніх справ
доктор юридичних наук, професор

Максим КОРНІЄНКО
«16» 06 2026 року

ВИСНОВОК

Одеського державного університету внутрішніх справ щодо дисертації ШАРОНОВА Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект», поданої на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право»

ВИТЯГ

з протоколу спільного засідання кафедри кримінального аналізу та інформаційних технологій та науково-дослідної лабораторії з актуальних питань кримінального аналізу Одеського державного університету внутрішніх справ № 6 від 04 червня 2026 року щодо проведення публічної презентації та обговорення наукових результатів дисертації аспіранта Одеського державного університету внутрішніх справ Шаронова Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект».

ГОЛОВУЮЧИЙ: доктор юридичних наук, професор, професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ Пядишев Володимир Георгійович.

ПРИСУТНІ:
Корнієнко М.В. доктор юридичних наук, професор
Пядишев В.Г. доктор юридичних наук, професор
Форос Г.В. кандидат юридичних наук, доцент
Меликов Р.Г. доктор філософії у сфері права
Балтовський О.А. доктор технічних наук, доцент
Калугін В.Ю. кандидат юридичних наук, доцент
Моргунова Т.І. кандидат технічних наук, доцент
Грезіна О.М. доктор філософії у сфері права
Сіфоров О.І. кандидат технічних наук, доцент
Лісніченко Д.В. кандидат юридичних наук, доцент
Теслюк І.О. кандидат юридичних наук, доцент

Всього присутньо: 11 осіб, з яких 3 доктора наук, 2 доктора філософії та 6 кандидатів наук – фахівців за профілем поданої на розгляд дисертації.

ПОРЯДОК ДЕННИЙ:

Обговорення наукового дослідження аспіранта Одеського державного університету внутрішніх справ Шаронова Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект», поданої на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право» з метою надання висновку про наукову новизну, теоретичне та практичне значення результатів дисертації.

Робота виконана в Одеському державному університеті внутрішніх справ.

Науковий керівник: доктор юридичних наук, професор Швець Д.В. ректор Львівського державного університету внутрішніх справ.

Шаронов Андрій Павлович в 2022 році отримав освітній ступінь магістра в Одеському державному університеті внутрішніх справ за спеціальністю 124 Системний аналіз.

На сьогодні працює першим заступником начальника Департаменту кіберполіції Національної поліції України.

З 23 вересня 2024 року Шаронов Андрій Павлович наказом ректора зарахований до докторантури та аспірантури Одеського державного університету внутрішніх справ. Тему дисертації затверджено Вченою радою Одеського державного університету внутрішніх справ від 23.09.2024 року протокол № 2.

Освітньо-наукову програму підготовки здобувачів третього (освітньо-наукового) рівня вищої освіти спеціальності 081 «Право» виконано у повному обсязі.

Здобувач має 9 наукових публікацій за темою дисертації, 6-ть з яких опубліковано в наукових фахових виданнях України та 3-ри тези доповідей на науково-практичних конференціях.

СЛУХАЛИ:

Доповідь аспіранта Шаронова Андрія Павловича, про результати виконаного наукового дослідження на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект». Здобувач ознайомив присутніх зі структурою дисертації, обґрунтував актуальність обраної теми дослідження. Тему дисертації було обрано з урахуванням пріоритетного напрямку розвитку Національної поліції України та власного досвіду роботи на керівних посадах Департаменту кіберполіції НПУ.

У дисертації здійснено аналіз стану наукового дослідження протидії кіберзагрозам Національною поліцією України. Мета роботи полягає в розроблені науково обґрунтованих теоретичних положень і практичних рекомендацій щодо вдосконалення організаційно-правового механізму протидії кіберзагрозам у діяльності Національної поліції України.

Предметом дослідження є організаційно-правовий механізм протидії кіберзагрозам у діяльності Національної поліції України.

Хронологічні межі дисертаційного дослідження окреслені зазначеними завданнями.

За результатами дослідження автором:

Концептуалізовано кіберзагрози як самостійний різновид загроз національній безпеці та встановлено, що, характеризуючись нематеріальністю слідів, транскордонністю, масштабованістю й асиметричністю впливу, вони в умовах загальної цифровізації держави та гібридних/воєнних викликів набувають підвищеної суспільної небезпечності, що зумовлює їх прямий вплив на реалізацію прав і свобод людини, функціонування критичних сервісів і стійкість держави.

Уточнено категоріально-понятійний апарат і методологічні засади ризик-орієнтованого підходу та доведено, що принципове розмежування понять «загроза» як динамічної ймовірнісної категорії і «небезпека» як стану наявної вразливості/дефіциту захищеності є необхідною передумовою формування правових і управлінських механізмів оцінювання, пріоритизації та ескалації кіберінцидентів.

Сформульовано комплексне техніко-юридичне визначення поняття «кіберзагроза» і сформовано науково придатну для практики Національної поліції України модель їх класифікації, доведено, що кіберзагрози, з одного боку, проявляються як технологічні вектори (шкідливе ПЗ, експлуатація вразливостей, DDoS, компрометація ланцюгів постачання, атаки на хмарні сервіси, соціальна інженерія тощо), а з іншого – детермінують застосування матеріально-правових і процесуальних норм (управління ризиками, інцидент-репортинг, режими доступу, аудит, збереження цифрових доказів), у зв'язку з чим ефективна класифікація має бути багатовимірною (суб'єкт, вектор доступу, тип впливу, об'єкт посягання, масштаби та наслідки) та придатною до використання в управлінських і процесуальних рішеннях.

Запропоновано систему критеріїв оцінювання небезпечності кіберзагроз і прозорої ескалації інцидентів та встановлено, що для управлінських і процесуальних рішень визначальними є: імовірність реалізації, організованість, вплив на конфіденційність–цілісність–доступність і довіру до даних, часові параметри детектування/реагування, потенціал поширення та правові наслідки, тоді як регулярне оновлення цих критеріїв з урахуванням практик ENISA і національних попереджень CERT-UA підвищує актуальність оцінювання в мінливому середовищі загроз.

Уточнено методологічні основи ризик-орієнтованого підходу та визначено, що принципове розмежування категорій «загроза» як ймовірнісної, прогнозної й динамічної та «небезпека» як стану наявної вразливості/дефіциту захищеності є необхідною передумовою правомірної пріоритизації реагування, обґрунтованого вибору інструментів втручання й побудови прозорих механізмів ескалації.

Доведено доцільність використання превентивних онлайн-ресурсів як емпіричного джерела та обґрунтовано, що консультаційно-попереджувальні платформи (зокрема chatovi.online) можуть застосовуватися для ідентифікації й уточнення масових соціально-інженерних загроз із високою латентністю, що посилює превентивний компонент діяльності Національної поліції України та підвищує якість кримінально-аналітичної пріоритизації.

Обґрунтовано, що одним із ключових напрямів удосконалення законодавства України має стати нормативне закріплення базових категорій, без яких подальша гармонізація національного права з підходами OECD є неповною. Передусім це стосується дефініцій «критична функція», «цифрова екосистема», «ризик цифрової безпеки/стійкості», «управління ризиками цифрової безпеки», «культура цифрової безпеки/стійкості», «власник ризику цифрової безпеки», а також пов'язаних понять, що описують сучасну багаторівневу цифрову взаємозалежність. Уведення таких категорій до

законодавства має не лише термінологічне значення, а й створює правову основу для ризик-орієнтованого управління, персоналізації відповідальності, формування системи підзвітності та побудови сучасної моделі цифрової стійкості держави.

Виявлено ключові проблеми імплементації міжнародних стандартів у національне правове поле та, констатовано загальну позитивну динаміку розвитку регулювання, а також встановлено його фрагментарність і термінологічну неузгодженість, крім того неповне відображення ризик-орієнтованих підходів щодо ланцюгів постачання, ролі приватного сектору, відповідальності керівництва й культури цифрової стійкості, що додатково обґрунтовує потребу системної гармонізації з європейськими підходами.

Визначено функціональне місце поліції в національній системі кібербезпеки та її адміністративно-правовий інструментарій, яке полягає у виконанні нею функції правоохоронного компонента державного механізму протидії кіберзагрозам, спрямованого на охорону прав і свобод людини. Також, доведено, що ефективність правоохоронного реагування зумовлюється чітким розмежуванням компетенцій між суб'єктами сектору безпеки, наявністю формалізованих процедур взаємодії (обмін інформацією, спільні аналітичні продукти, координація під час інцидентів) та неухильним дотриманням стандартів законності, пропорційності й прав людини як меж втручання у цифровій сфері.

Обґрунтовано пріоритет процесуальної придатності цифрових даних як передумови результативності кіберрозслідувань та встановлено, що її забезпечення визначається перевірюваністю й відтворюваністю, безперервністю ланцюга збереження, правомірністю здобуття та належним документуванням, тоді як стандартизація первинного реагування є критичною для недопущення втрати даних і мінімізації ризику визнання доказів недопустимими.

Запропоновано перспективний механізм процесуалізації даних, сформованих системами штучного інтелекту, та обґрунтовано, що практично реалістичним є їх залучення через судову експертизу із нормативним виокремленням алгоритмічної (цифрової) експертизи, за умови верифікації точності/похибки й відтворюваності результатів та належного опису застосованих методик, що забезпечує перевірюваність і допустимість відповідних даних.

Проведене дослідження дає підстави стверджувати, що інституційна спроможність кіберпідрозділів Національної поліції України має розглядатися не лише як сукупність організаційних ресурсів і технічних засобів, а як цілісна система нормативно визначених процедур, професійних компетентностей, стандартів поводження з цифровими доказами та моделей міжвідомчої взаємодії. Саме така системна конструкція забезпечить спроможність поліції ефективно реагувати на кіберінциденти, належно документувати цифрові сліди та перетворювати інформаційні дані на процесуально допустимі докази. Отже, інституційна спроможність кіберпідрозділів є не допоміжною організаційною характеристикою, а одним із ключових елементів організаційно-правового механізму протидії кіберзагрозам.

Обґрунтовано, що регламентація процедур та стандартизація діяльності кіберпідрозділів НПУ повинні охоплювати щонайменше три взаємопов'язані блоки: первинне реагування і фіксацію події; роботу з цифровими доказами; координацію та взаємодію як усередині системи НПУ, так і на міжвідомчому рівні. Такий поділ має не лише методичне, а й правове значення, оскільки дозволяє забезпечити послідовність дій, збереження цілісності інформації, прозорість процедур та належну доказову перспективу кримінального провадження. Встановлено, що саме процедурна впорядкованість на початкових етапах реагування значною мірою визначає якість подальшого слідчого, оперативного та аналітичного забезпечення.

Встановлено, що кадрова складова інституційної спроможності кіберпідрозділів охоплює не лише питання укомплектування посад, а насамперед спеціалізацію, компетентнісну модель та безперервний професійний розвиток особового складу. Умови стрімкої еволюції кіберзагроз, поширення шкідливого програмного забезпечення, використання криптоактивів, соціальної інженерії та хмарної інфраструктури зумовлюють потребу переходу від моделі разової підготовки до моделі безперервного професійного розвитку, у тому числі із залученням міжнародних експертів. Така модель має інтегрувати як технічні компетентності – мережевий аналіз, цифрову криміналістику, роботу з логами, аналіз шкідливого коду, реверс-інжиніринг, – так і правові та процесуальні компетентності, пов'язані з дотриманням прав людини, межами втручання, режимом доступу до даних та правилами процесуалізації цифрової інформації.

Встановлено, що перспективна модель професійного стандарту «Оперуповноважений (поліція)» має бути істотно розширена за рахунок включення компетентностей, пов'язаних із ILP, електронними доказами, OSINT, цифровою криміналістикою, криптоактивами, застосуванням моделей штучного інтелекту в аналітичній підтримці розслідувань, а також NIS2-сумісною взаємодією у сфері кібербезпеки. Така деталізація дасть змогу привести професійні вимоги до посади у відповідність із сучасними організаційно-правовими викликами та міжнародними тенденціями розвитку поліцейської діяльності в цифровому середовищі.

Доведено, що особливого значення набуває інституціоналізація трудових функцій, пов'язаних з моніторингом відкритих джерел, документуванням результатів OSINT, відстеженням руху віртуальних активів, кластеризацією транзакцій, взаємодією з постачальниками послуг віртуальних активів, виявленням криптоанонімізаторів та використанням моделей штучного інтелекту для виявлення аномалій. Це свідчить про якісне розширення предмета правоохоронної діяльності, у межах якого цифрова аналітика, інтеграція та відтворюваність аналітичних процедур перетворюються на складові належного доказового забезпечення.

Результати дослідження дозволяють дійти висновку, що проєкт «BRAMA» є показовим прикладом практичної реалізації координаційної функції держави у сфері кібербезпеки, оскільки підтверджує ефективність міжінституційної взаємодії органів публічної влади, правоохоронних органів, приватного сектору та інститутів громадянського суспільства. Водночас його функціонування свідчить про доцільність подальшого нормативного оформлення, організаційного зміцнення та інтеграції подібних механізмів до цілісної загальнодержавної системи запобігання і протидії кіберзагрозам.

Сформульовано авторське визначення інтероперабельності у кібербезпеці та обґрунтовано її системоутворювальну роль, визначивши інтероперабельність як інтеграційну властивість і спроможність технічних, організаційних, процедурних і нормативно-правових компонентів різних суб'єктів забезпечувати узгоджену, безпечну та безперебійну взаємодію на основі гармонізованих стандартів, форматів даних і регламентів обміну, що формує «простір довіри» для координації дій і підтримання єдиного рівня кіберстійкості з урахуванням стандартотворчих практик ISO та підходів NATO.

Поглиблено організаційні підходи до реагування у воєнний час та обґрунтовано ILP-орієнтовану модель управління, встановивши центральну дилему «швидкість/безперервність реагування – процесуальна якість/відтворюваність доказів» і довівши доцільність інституційно закріпленої моделі, що поєднує міжвідомчу координацію, внутрішні стандартизовані процедури реагування (мінімальні форензичні

вимоги, тригери ескалації) та аналітично кероване управління ресурсами (ILP-цикл) із посиленням ролеорієнтованих компетентностей персоналу.

Встановлено, що використання криптоактивів для обходу міжнародних санкцій набуло системного та технологічно адаптивного характеру, інтегрувавшись у структуру сучасних фінансових і кіберзагроз. Це зумовлює необхідність комплексної протидії, що має ґрунтуватися на поєднанні санкційного комплаєнсу, блокчейн-аналітики, цифрової криміналістики, міжвідомчої координації та вдосконалення спеціалізованого правового регулювання.

Запропонована удосконалена п’ятиетапна модель Аналітичного Життєвого Циклу Крипто-Санкцій, яка відображає регуляторні рубежі 2026 року та забезпечує системне поєднання аналітичних, правозастосовних і комплаєнс-механізмів у сфері протидії обходу санкцій із використанням криптоактивів.

Дисертант детально доповів, яким чином ним вирішувалися завдання, що ставилися перед дослідженням, висвітлив наукову та практичну значущість одержаних результатів.

По закінченні доповіді дисертанта, присутніми було поставлено ряд запитань.

Калугін В.Ю. кандидат юридичних наук, доцент: Андрій Павлович, у мене до Вас одне запитання: в чому, на Вашу думку полягає наукова новизна авторського підходу до визначення правової природи кіберзагроз?

Шаронов А.П. дякую за запитання. Щодо питання, то наукова новизна запропонованого підходу полягає у тому, що кіберзагрози обґрунтовано розглядаються не лише як технічні або криміногенні явища, а як самостійний різновид загроз національній безпеці, що мають комплексну техніко-правову природу. У дисертації доведено, що кіберзагроза виникає на стику декількох вимирів: технологічної, організаційної, правової та соціальної. Саме тому її не можна пояснювати виключно через категорії інформаційної безпеки або лише через технічні параметри уразливості систем. Обґрунтовано, що правова природа кіберзагроз має подвійний вимір. З одного боку, йдеться про реальні або потенційні деструктивні впливи на інформаційно-комунікаційні системи, цифрові сервіси, критичну інфраструктуру та пов’язані з ними суспільні відносини. З іншого боку, такі впливи набувають юридичного значення через нормативне закріплення обов’язків суб’єктів щодо управління ризиками, реагування на інциденти, збереження цифрових доказів, захисту персональних даних і забезпечення кіберстійкості. Таким чином, у роботі фактично доведено, що кіберзагроза є не просто технічною подією в мережі, а юридичним фактом, здатним породжувати правові наслідки, включаючи обов’язок реагування, процесуальне документування та застосування заходів юридичної відповідальності. Крім того, у нашій дисертації запропоновано розмежування суміжних категорій «небезпека», «загроза», «ризик» і «кіберзагроза», що має не лише теоретичне, а й прикладне значення для побудови ризик-орієнтованої моделі діяльності Національної поліції України. Саме це створює методологічну основу для класифікації кіберзагроз, оцінювання їх небезпеки та формування пріоритетів реагування.

Пядишев В.Г. доктор юридичних наук, професор: шановний здобувач, яке на Вашу думку, практичне значення має запропонована у дисертації класифікація кіберзагроз для діяльності Національної поліції України?

Шаронов А.П. Практичне значення запропонованої класифікації полягає в тому, що вона орієнтована не лише на доктринальне впорядкування знань про кіберзагрози, а насамперед на створення придатного для правозастосування інструменту, який може використовуватися підрозділами Національної поліції України у процесі виявлення, аналізу, документування та нейтралізації кіберзагроз. У дисертації доведено, що для НПУ найбільш доцільною є багатовимірна класифікація кіберзагроз, яка враховує природу та мотивацію правопорушника, спосіб проникнення, тип технічного впливу, об'єкт посягання та масштаб наслідків. Такий підхід дозволяє перейти від загального опису загроз до їх функціонального аналізу в інтересах кримінального аналізу, оперативно-розшукової діяльності та досудового розслідування. На практиці це означає можливість формувати ризик-орієнтовані моделі реагування, визначати пріоритетність загроз, ефективніше розподіляти сили та засоби, а також вибудовувати міжвідомчу взаємодію з іншими суб'єктами сектору безпеки і оборони. Окреме значення має те, що така класифікація узгоджується з міжнародними підходами, зокрема з практиками ENISA, правом ЄС та вимогами NIS2 щодо управління ризиками й інцидент-менеджменту. Це підсилює інтероперабельність національної системи кібербезпеки та дозволяє НПУ використовувати уніфіковані критерії оцінки загроз у співпраці з міжнародними партнерами. Отже, запропонована класифікація має безпосереднє прикладне значення як для стратегічного планування у сфері кібербезпеки, так і для щоденної практики кіберполіції, слідчих та аналітиків правоохоронних органів.

Балтовський О.А. доктор технічних наук, доцент: скажіть будь ласко який основний науковий висновок дисертації щодо імплементації міжнародних стандартів у діяльність Національної поліції України?

Шаронов А.П. Дякую за запитання. Це питання набирає особливою важливості саме зараз для нашої держави, так як ми зараз в процесі євроінтеграції. Щодо основного наукового висновку, то він полягає в тому, що імплементація міжнародних стандартів у діяльність Національної поліції України повинна здійснюватися не лише на рівні загальнодержавної політики кібербезпеки, а й на рівні функціональної адаптації правоохоронної практики. У дисертації доведено, що для НПУ міжнародні стандарти мають значення як джерело методології класифікації кіберзагроз, оцінювання їх небезпечності, стандартизації реагування на інциденти та організації обігу цифрових доказів. Зокрема, Будапештська конвенція формує для правоохоронних органів основу кримінально-правової кваліфікації кіберзлочинів і міжнародного співробітництва щодо електронних доказів; NIS2 задає рамки ризик-орієнтованого управління, інцидент-репортингу та координації між державою і приватним сектором; GDPR і Конвенція 108+ визначають межі допустимого поводження з персональними даними у правоохоронній та безпековій діяльності. Саме тому в роботі зроблено висновок, що для НПУ імплементація міжнародних стандартів має бути виражена у впровадженні уніфікованих підходів до класифікації кіберзагроз, формалізації критеріїв їх оцінювання, розвитку міжвідомчої та міжнародної взаємодії, а також

посиленні аналітичної та доказової спроможності підрозділів. Іншими словами, міжнародні стандарти повинні бути перетворені на внутрішні організаційно-правові механізми щоденної діяльності поліції.

Форос Г.В. кандидат юридичних наук, доцент: шановний Андрій Павлович, як Ви бачите чи не створює запозичення європейських стандартів ризик механічного перенесення моделей, не адаптованих для України, а тим більше до умов воєнного стану в Україні?

Шаронов А.П. Дякую за запитання. Такий ризик, безумовно, існує, і саме тому в дисертації наголошено не на механічному запозиченні, а на адаптивній імплементації міжнародних стандартів. Сутність наукової позиції полягає в тому, що європейські та міжнародні акти повинні використовуватися як нормативно-методологічний орієнтир, але не як шаблон для буквального копіювання. Український контекст визначається воєнним станом, високою інтенсивністю державних і квазідержавних кібератак, гібридною війною, значною вразливістю критичної інфраструктури та особливою роллю сектору безпеки і оборони.

Отже, імплементація повинна будуватися на принципі функціональної сумісності, а не текстуальної ідентичності. Саме в цьому полягає одна з центральних ідей дисертації: міжнародні стандарти мають адаптуватися з урахуванням українського безпекового режиму, пріоритетів воєнного часу, потреб НПУ, системи критичної інфраструктури та можливостей національних інституцій.

Грезіна О.М. доктор філософії у сфері права: Чому в дисертації обґрунтовується необхідність включення ILP-компетентностей, цифрових доказів і криптоактивів до професійного стандарту оперуповноваженого поліції?

Шаронов А.П. Дякую за поставлене запитання. Сучасна цифрова форма злочинної діяльності докорінно трансформувала зміст правоохоронної роботи. У дисертації доведено, що оперуповноважений у системі НПУ вже не може ефективно діяти, спираючись лише на традиційний інструментарій оперативно-розшукової діяльності. Цифрове середовище вимагає від нього здатності працювати з OSINT, аналізувати віртуальні активи, збирати електронні докази, проводити аналітичну розвідку та ризик-аналіз, а також із новітніми інструментами виявлення аномальної активності, включаючи моделі штучного інтелекту. Саме тому в роботі обґрунтовано, що перехід до інтелектуально-керованої моделі поліцейської діяльності робить ILP-компетентності системоутворювальними. Без них правоохоронна діяльність залишається реактивною.

Після відповідей на запитання слово було надано **науковому керівнику**, доктору юридичних наук, професору Швецю Д.В., який дав загальну оцінку науковому дослідженню, а також охарактеризував Шаронова А.П., як людину відповідальну, грамотну та досвідчену, з творчим науковим мисленням, цілеспрямовану, відповідальну та ініціативну. Здобувач дуже успішно зумів використати свій творчий потенціал і досить ґрунтовно та досконало виконав наукове дослідження.

Завдання, які поставив перед собою Андрій Павлович, він їх поступово розкрив в дисертації, надав слушні висновки.

Шаронов Андрій Павлович цілком сформувався як науковець, його дисертаційне на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект», представлена на публічній презентації є завершеною працею, яка має суттєве значення для вітчизняної юридичної науки, а його автор готов до атестації здобувача ступеня доктора філософії.

Науковий керівник подякував всім присутнім за підтримку наукового дослідження та здобувача.

Під час наукової дискусії учасниками публічної презентації надано свої думки і міркування, щодо представленого на розгляд дослідження.

Корнієнко М.В. доктор юридичних наук, професор: шановні колеги, дозвольте висловити свою позицію щодо дисертаційного дослідження Андрія Шаронова на тему «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект». Передусім хочу відзначити, що автором обрано надзвичайно актуальну для сучасної правоохоронної системи України тему. В умовах воєнного стану, цифровізації державного управління, активного використання електронних сервісів та зростання кількості кіберінцидентів саме Національна поліція України виступає одним із ключових суб'єктів практичної протидії кіберзагрозам. Здобувачем опрацьовано значний масив нормативних, аналітичних та наукових джерел, що дозволило комплексно розкрити організаційно-правову природу протидії кіберзагрозам у діяльності Національної поліції України. Робота є завершеною, цілісною та самостійною науковою працею, що містить елементи наукової новизни, має практичне значення та може бути використана як у науковій, так і в освітній та правоохоронній діяльності. Особливо позитивно оцінюю спробу автора поєднати адміністративно-правовий, організаційний та функціональний підходи до аналізу протидії кіберзагрозам. Вважаю, що здобувач сформувався як дослідник, здатний самостійно ставити й розв'язувати наукові завдання. Дисертаційну роботу підтримую.

Форос Г.В. кандидат юридичних наук, доцент: дозвольте висловити свою думку щодо дисертаційної роботи Шаронова А.П. Тема дослідження є безумовно актуальною, оскільки протидія кіберзагрозам сьогодні вийшла за межі суто технічної проблематики й набула значення одного з ключових напрямів забезпечення національної безпеки, публічного порядку, захисту прав людини та стабільності цифрової держави. У роботі достатньо переконливо розкрито роль Національної поліції України у протидії кіберзагрозам, визначено організаційні та правові засади такої діяльності, охарактеризовано окремі напрями міжвідомчої взаємодії, інформаційно-аналітичного забезпечення та превентивної роботи. Разом із тим, на мій погляд, у дисертації можна було б глибше розкрити європейський вимір цієї проблематики, зокрема співвідношення української моделі протидії кіберзагрозам із підходами Європейського Союзу у сфері кібербезпеки, кіберстійкості, поліцейського співробітництва та захисту критичної інфраструктури. Більш розгорнуте порівняння із практиками ЄС посилило б міжнародний і порівняльно-правовий аспект роботи. Водночас хочу підкреслити, що автор добре орієнтується в обраній темі, володіє належним науковим апаратом і зміг показати практичну значущість дослідження. Робота має логічну структуру, відповідає заявленій меті та містить обґрунтовані висновки. Особливо важливим є

те, що дослідження спрямоване не лише на опис чинного стану, а й на пошук шляхів удосконалення організаційно-правового механізму протидії кіберзагрозам Національною поліцією України. Підтримую здобувача та його наукову працю.

Пядишев В.Г. доктор юридичних наук, професор: сьогодні ми розглядаємо дисертаційну роботу, присвячену надзвичайно важливій проблемі – протидії кіберзагрозам Національною поліцією України в організаційно-правовому аспекті. На моє переконання, обрана тема є своєчасною, оскільки кіберзагрози сьогодні безпосередньо впливають на безпеку громадян, функціонування державних інституцій, захист персональних даних, електронних сервісів та критичної інформаційної інфраструктури. У цілому дисертація є завершеним науковим дослідженням, яке має практичну цінність і відповідає вимогам, що висуваються до такого виду наукових робіт. Вважаю, що Шаронов А.П. успішно виконав поставлені наукові завдання, а робота може бути підтримана.

Грезіна О.М. доктор філософії у сфері права: дозвольте мені також висловити своє бачення щодо представленої дисертаційної роботи. Приєднуючись до вже висловлених позитивних оцінок, хочу зазначити, що тема «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» є особливо значущою саме для сучасного етапу розвитку української правової системи. Умови цифровізації, воєнні виклики та зростання ролі інформаційних технологій у повсякденному житті об’єктивно вимагають від правоохоронної системи нових підходів до виявлення, попередження та нейтралізації кіберзагроз. Позитивним у роботі є те, що автор не обмежився загальним описом кіберзагроз, а намагався показати саме організаційно-правову модель діяльності Національної поліції України. У роботі розглянуто питання компетенції, взаємодії, інформаційного забезпечення, правових меж діяльності поліції, а також значення дотримання прав і свобод людини під час реагування на кіберзагрози.

Водночас вважаю, що окремі положення щодо захисту прав людини в умовах застосування цифрових інструментів могли б бути розкриті ширше. Йдеться про баланс між ефективністю правоохоронної діяльності, доступом до цифрової інформації, обробкою персональних даних і гарантіями приватності. Проте загалом робота справляє позитивне враження, є логічно побудованою, актуальною та практично орієнтованою. Підтримую здобувача і його дисертаційне дослідження.

Лісніченко Д.В. доктор філософії у сфері права: шановні колеги, дозвольте і мені висловити свої думки щодо роботи А.П. Шаронова. Насамперед хочу зазначити, що дисертація присвячена темі, яка має не лише теоретичне, а й безпосереднє практичне значення для діяльності Національної поліції України. Кіберзагрози сьогодні змінюють саму логіку правоохоронної діяльності, оскільки значна частина протиправних дій переміщується у цифрове середовище або супроводжується використанням цифрових технологій. Позитивно оцінюю те, що автор розглядає протидію кіберзагрозам не фрагментарно, а через систему організаційно-правових елементів: нормативне забезпечення, повноваження суб’єктів, міжвідомчу взаємодію, інформаційно-аналітичне забезпечення, кадрову підготовку, технічну спроможність та превентивну діяльність. Такий підхід

дозволяє краще зрозуміти не лише зміст діяльності Національної поліції України, а й проблеми її практичної реалізації. Разом із тим, на мою думку, у подальших дослідженнях автору варто було б більше уваги приділити питанню взаємодії Національної поліції з приватним сектором, провайдерами електронних комунікацій, банківськими установами, адміністраторами цифрових платформ та міжнародними партнерами. Саме ця взаємодія сьогодні часто визначає ефективність реагування на кіберзагрози. Проте це не применшує значення проведеного дослідження. Робота виконана на належному науковому рівні, має внутрішню логіку, завершений характер і практичну спрямованість. Вважаю, що здобувач заслуговує на підтримку, а його дисертаційна робота відповідає встановленим вимогам.

ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації ШАРОНОВА Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект», поданої на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право»

Обґрунтування вибору теми дослідження. Інформаційно-аналітична діяльність займає одне з провідних позицій у діяльності НПУ та є надзвичайно дієвим інструментом для забезпечення діяльності управлінців та керівників. Ефективність розслідування кримінальних проваджень значною мірою забезпечується шляхом проведення комплексу заходів інформаційно-аналітичної діяльності та якісної ідентифікації, аналізу та оцінювання загроз і ризиків. З огляду на те, що інформаційно-аналітична діяльність є технологічною та організаційною сферою, яка потребує відповідного сучасного нормативно-правового забезпечення, враховуючи євроінтеграційні процеси в нашій державі, існує необхідність імплементації європейського досвіду в діяльність НПУ.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до основних положень Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 № 392/2020; Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схваленого Указом Президента України від 11.05.2023 № 273/2023; Плану реалізації Стратегії кібербезпеки України, введеним в дію Указом Президента України від 01.02.2022 року № 37/2022; Плану заходів із реалізації Стратегії розвитку Національної поліції України на 2026-2030 роки, затвердженого Наказом Національної поліції України від 21.01.2026 року № 38; Пріоритетних напрямів та завдань (проєктів) цифрової трансформації на 2024-2026 роки, схваленої розпорядженням КМУ від 02.08.2024 № 735-з, Річних планів науково-дослідної діяльності Одеського державного університету внутрішніх справ на період 2023-2028 років «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» № 0123U103538 та кафедри кримінального аналізу та інформаційних технологій Одеського державного

університету внутрішніх справ на період 2023-2028 років «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період № 0123U103748.

Тема дисертації затверджена на засіданні Вченої ради Одеського державного університету внутрішніх справ (Протокол № 2 від 23 вересня 2024 року).

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

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

- розкрити правову природу кіберзагроз та їх місце у сучасному правовому полі;
- здійснити класифікацію кіберзагроз і визначити критерії оцінки їх небезпеки у контексті діяльності Національної поліції України;
- проаналізувати міжнародно-правові стандарти боротьби з кіберзагрозами та стан їх імплементації в законодавство України;
- дослідити нормативно-правові засади діяльності Національної поліції у сфері протидії кіберзагрозам;
- оцінити інституційну спроможність та організаційну структуру підрозділів кіберполіції;
- визначити проблеми та виклики організації діяльності Національної поліції у сфері кібербезпеки в умовах воєнного стану;
- обґрунтувати напрями вдосконалення правових та організаційних механізмів протидії кіберзагрозам.

Об'єктом дослідження є суспільні відносини, що виникають у сфері протидії кіберзагрозам у діяльності правоохоронних органів.

Предметом дослідження є організаційно-правовий механізм протидії кіберзагрозам у діяльності Національної поліції України.

Методи дослідження. Методологічну основу дослідження становить сукупність загальнонаукових і спеціально-юридичних методів пізнання. Зокрема, діалектичний метод – для комплексного сприйняття і системного опрацювання теоретичних та нормативних положень, що стосуються ґенези та кваліфікації кіберзагроз у сучасному правовому полі (підрозділи 1.1, 1.2); метод спостереження – для виявлення й узагальнення закономірностей практики виявлення кіберзагроз (підрозділи 1.2, 3.3); історико-правовий метод – для розкриття наукових поглядів на розвиток та правове регулювання інституту кіберзагроз у різні періоди й у різних правових системах (підрозділи 1.1, 1.2, 1.3, 3.1); компаративний метод – для порівняльного аналізу міжнародного досвіду та визначення можливостей його імплементації у національну практику (підрозділи 1.2, 1.3, 3.1, 3.2); логіко-юридичний метод – для тлумачення понять, категорій та правових норм, пов'язаних із організаційно-правовими засадами протидії кіберзагрозам НПУ України (підрозділи 1.1, 2.1, 2.2, 3.1, 3.2, 3.3); метод системного аналізу – застосовано для дослідження протидії кіберзагрозам Національною поліцією України як цілісного організаційно-правового механізму, що складається з взаємопов'язаних елементів і функціонує в умовах динамічного зовнішнього середовища (кіберпростір, воєнний стан, міжнародні зобов'язання, технічні стандарти реагування) (підрозділи 1.2, 2.2, 2.3, 3.1, 3.2); догматичний

метод застосовано для дослідження позитивного права у сфері протидії кіберзагрозам – через аналіз змісту правових норм, їх структури, юридичних конструкцій, системних зв'язків, а також правил тлумачення і застосування (підрозділи 1.1, 1.2, 1.3, 2.1, 3.2).

Емпіричну базу дослідження становлять: матеріали правозастосовної та організаційної практики Національної поліції України (узагальнення роботи підрозділів кіберполіції, типові сценарії реагування на інциденти, внутрішні регламенти – у межах доступності); статистичні та аналітичні дані щодо динаміки кіберзлочинності й кіберінцидентів; звіти, методичні матеріали та рекомендації профільних суб'єктів кібербезпеки; результати наукового узагальнення типових проблем взаємодії між правоохоронними та іншими суб'єктами кібербезпеки.

Наукова новизна одержаних результатів полягає в комплексному обґрунтуванні організаційно-правового механізму протидії кіберзагрозам Національною поліцією України як системи норм, інституцій і процедур, що має забезпечувати одночасно: оперативність реагування; процесуальну якість доказування; міжвідомчу та міжнародну взаємодію; дотримання прав і свобод людини; адаптацію до умов воєнного стану. У результаті проведеного дослідження сформульовано низку нових концептуальних положень, висновків та рекомендацій, запропонованих особисто здобувачем, які мають важливе теоретичне та практичне значення. Основні з такі:

вперше:

- обґрунтовано комплексне трактування кіберзагроз як самостійного підкласу загроз національній безпеці з подвійною (техніко-юридичною) природою, що поєднує технологічні вектори з юридично значущими наслідками для правового режиму реагування, доказування та комплаєнсу в діяльності НПУ;
- сформульовано авторське визначення «інтероперабельності у кібербезпеці» як системної спроможності технічних, організаційних, процедурних і нормативних компонентів різних суб'єктів забезпечувати узгоджену, безпечну та безперебійну взаємодію на основі гармонізованих стандартів, форматів даних і регламентів обміну інформацією (для створення простору довіри та підтримання кіберстійкості на національному і транскордонному рівнях);
- розроблено концептуальну модель механізму протидії кіберзагрозам у діяльності НПУ як єдиного циклу взаємопов'язаних дій (превенція/моніторинг → виявлення/первинне реагування → оцінювання та пріоритизація → координація → фіксація та збереження цифрових даних → розслідування/процесуальне оформлення → аналіз досвіду та вдосконалення практик), де ключовою умовою результативності визначено стандартизованість первинного реагування та контроль ланцюга збереження;
- доведено доцільність використання превентивних інформаційно-консультаційних онлайн-ресурсів (зокрема chatovi.online) як емпіричного джерела для ідентифікації та уточнення масових соціально-інженерних кіберзагроз із високою латентністю, що має практичне значення для профілактичних і комунікаційних заходів НПУ.

удосконалено підходи:

- до класифікації кіберзагроз для потреб НПУ шляхом операціоналізації багатовимірної моделі (суб'єкт – вектор доступу – тип технічного впливу – об'єкт посягання) із прямою прив'язкою до управлінських рішень (координація, ресурсне

планування, пріоритети реагування) та процесуальних вимог (допустимість/доказовість);

- до системи критеріїв оцінювання небезпечності кіберзагроз у поліцейській діяльності через поєднання юридичних та операційних параметрів (імовірність реалізації; організованість/складність; вплив на конфіденційність–цілісність–доступність; швидкість детектування/реагування; потенціал поширення; правові наслідки; репутаційний ефект), що підвищує порівнюваність рішень і прозорість ескалації інцидентів у НПУ;
- до визначення місця НПУ в національній системі кібербезпеки як правоохоронного компонента координаційної моделі, що вимагає процедурно формалізованої взаємодії з іншими суб'єктами кібербезпеки при дотриманні принципів законності, пропорційності та поваги до прав людини;
- до забезпечення процесуальної придатності цифрових даних у протидії кіберзагрозам шляхом акцентування на правомірності способу здобуття й збереження даних, їх відтворюваності та перевірюваності, що обумовлює потребу у стандартизації процедур фіксації, документування та збереження;
- до концептуального вирішення питання допустимості даних, сформованих системами штучного інтелекту, через процесуалізацію таких даних у форматі судової експертизи з виокремленням алгоритмічної (цифрової) експертизи, вимогами до верифікації точності/похибки, умов відтворюваності та документування методик.

дістали подальший розвиток:

- наукові уявлення про співвідношення категорій «загроза», «небезпека» і «ризик» у кіберпросторі через їх прикладне значення для ризик-орієнтованого управління та побудови моделей реагування у публічному управлінні кібербезпекою;
- підходи до гармонізації національного правового регулювання з міжнародними стандартами та практиками (кримінально-правовий, управлінський/ризиковий і правозахисний виміри) через обґрунтування необхідності усунення фрагментарності та термінологічної неузгодженості, а також посилення регулювання щодо ролі приватного сектору, ланцюгів постачання і культури цифрової стійкості;
- організаційно-правові підходи до діяльності кіберполіції у воєнний час через обґрунтування переходу від «ситуативного менеджменту інцидентів» до інституційно закріпленої моделі, що інтегрує: міжвідомчу координацію; внутрішні стандартизовані процедури та мінімальні форензичні вимоги; аналітичне управління ресурсами на основі ILP;
- підходи до інституціалізації «подвійного контуру» управління інцидентом (технічний – безперервність/відновлення; процесуальний – допустимість/доказовість) з розмежуванням ролей і сценаріями залучення слідчих та оперативних працівників НПУ;
- положення щодо нормативного та компетентнісного забезпечення трудових функцій (у парадигмі ILP) шляхом деталізації компетентностей у частині електронних доказів, взаємодії з об'єктами критичної інфраструктури, роботи з криптоактивами, штучним інтелектом, а також NIS2-сумісної взаємодії та ризик-орієнтованих показників результативності;

- підходи до оцінки координаційних ініціатив у кібербезпеці (зокрема проєкт «BRAMA») як практики міжсекторної взаємодії, що має потенціал для нормативного закріплення та інтеграції у загальнодержавну систему протидії кіберзагрозам.

Практичне значення одержаних результатів полягає в тому, що положення, висновки, пропозиції та рекомендації, сформульовані у процесі наукового дослідження, мають прикладний характер і можуть бути використані в низці сфер діяльності державних інституцій. Зокрема:

правотворчості – результати дослідження містять обґрунтовані пропозиції щодо вдосконалення чинного законодавства у сфері протидії кіберзагрозам, зокрема щодо уточнення понятійно-категоріального апарату (кіберзагроза/кіберінцидент/цифровий слід), розмежування компетенцій Національної поліції України та інших суб'єктів кібербезпеки, а також нормативного закріплення процедур координації, обміну інформацією і реагування на інциденти з дотриманням принципів законності, пропорційності та гарантій прав людини. Реалізація зазначених пропозицій сприятиме підвищенню узгодженості нормативної бази, правової визначеності повноважень і якості правозастосування у секторі безпеки і оборони України;

правозастосовній діяльності – сформульовані у роботі рекомендації можуть бути використані в організації діяльності підрозділів Національної поліції України (насамперед кіберполіції, слідчих та оперативних підрозділів) під час виявлення, припинення та документування кіберінцидентів і кіберзлочинів, удосконалення алгоритмів взаємодії з іншими суб'єктами кібербезпеки, а також стандартизації процесів фіксації цифрових слідів і забезпечення належності, допустимості та достовірності електронних доказів у кримінальному провадженні. Це підвищить оперативність реагування, знизить ризики втрати доказової інформації та посилить керованість міжвідомчих процедур; (акт впровадження Департаменту кіберполіції Національної поліції України від 12.05.2026 року);

науково-дослідній роботі – теоретичні узагальнення, методологічні підходи та запропонована модель організаційно-правового механізму протидії кіберзагрозам можуть бути використані як концептуальна основа для подальших досліджень у галузі адміністративно-правового забезпечення діяльності правоохоронних органів у кіберпросторі, зокрема для розроблення критеріїв оцінки небезпеки кіберзагроз, моделей інституційної спроможності кіберпідрозділів, а також для порівняльно-правових досліджень гармонізації національного законодавства з міжнародними стандартами кібербезпеки (акт впровадження Одеського державного університету внутрішніх справ від 01.06.2026 року);

освітньому процесі – результати дисертації можуть бути використані при підготовці навчально-методичних матеріалів, спецкурсів і тренінгових модулів для здобувачів юридичної освіти та працівників НПУ (зокрема щодо правових основ реагування на кіберінциденти, процедур взаємодії, прав людини в цифровому середовищі, роботи з електронними доказами), а також у системі службової підготовки й безперервного професійного розвитку працівників кіберполіції (акт впровадження Одеського державного університету внутрішніх справ від 01.06.2026 року).

Апробація результатів дисертації. Основні результати дослідження, у тому числі загальні підсумки опрацювання проблематики, її окремі положення, отримані узагальнення та сформульовані висновки, було представлено дисертантом у вигляді доповідей і повідомлень на науково-практичних і науково-теоретичних конференціях: XVI Міжнародній науково-практичній конференції «Роль та місце правоохоронних органів у розбудові демократичної правової держави» (м. Одеса, 29 березня 2024 року); XI Міжнародній науково-практичній онлайн-конференції (м. Одеса, 24 жовтня 2024 року); XII Міжнародній науково-практичній онлайн-конференції (м. Одеса, 24 жовтня 2025 року).

Публікації. Основні положення дисертації опубліковано в 9 працях, серед яких 6 – в наукових фахових виданнях України, визнаних фаховими з юридичних наук, праць апробаційного характеру – 3.

Структура та обсяг дисертації. Дисертація складається із вступу, трьох розділів, що об'єднують 9 підрозділів, висновків, списку використаних джерел (222 найменувань – на 24 сторінці) та 14 додатків – на 24 сторінках. Повний обсяг дисертації становить 233 сторінок, із них основний обсяг тексту – 159 сторінка.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації, які засвідчують апробацію матеріалів дисертації, в яких опубліковані основні наукові результати дисертації:

1. Шаронов А.П. Трудові функції оперуповноваженого в парадигмі ILP: нормативно-практичні ориси та кіберкомпонент. *Юридичний бюлетень.* № 37. 2025. С. 97-106. DOI: https://doi.org/10.32850/LB2414-4207.2025.37.13

2. Шаронов А.П. Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. *Морська безпека та оборона.* № 2 (6). 2025. С. 106-115. DOI: https://doi.org/10.32782/msd/2025.2/13

3. Шаронов А.П. Міжнародні правові стандарти протидії кіберзагрозам: імплементація та розвиток цифрової стійкості в правовій системі України. *Актуальні проблеми вітчизняної юриспруденції.* № 6. 2025. С. 119-128. DOI: https://doi.org/10.32782/2408-9257-2025-6-18

4. Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. *Юридичний бюлетень.* № 39. 2025. С. 147-155. DOI: https://doi.org/10.32850/LB2414-4207.2025.39.17

5. Шаронов А.П., Самойлов С.В., Крайнічук (Шелепало) Г.В. Організаційно-правовий аспект використання відбитку браузера для заходів кіберзахисту. *Наше право*. № 1. 2026. С. 42-52. DOI: https://doi.org/10.71404/NP.2026.1.6

6. Шаронов А.П., Виходець Ю.О., Плахотнюк О.В. Криптоактиви як інструмент обходу санкцій у системі кіберзагроз: блокчейн-аналітика, регуляторно-правові рамки та українська практика. *Юридичний бюлетень.* № 41. 2026. С. 120-136. DOI: https://doi.org/10.32850/LB2414-4207.2026.41.15

Публікації, які засвідчують апробацію матеріалів дисертації:

1. Шаронов А.П. Дефініційний аналіз суміжних понять «інформаційна безпека» та «кібербезпека». *Роль та місце правоохоронних органів у розбудові демократичної правової держави*: матеріали XVI Міжнародної науково-практичної Інтернет конференції, м. Одеса, 29 березня 2024 року. Одеса : ОДУВС, 2024. С. 556-559.
2. Шаронов А.П. Правова природа інтероперабельності як категорії адміністративного права. *Стан та перспективи розвитку адміністративного права України:* матеріали XI Міжнародної науково-практичної онлайн-конференції, м. Одеса, 24 жовтня 2024 року, Одеса : ОДУВС, 2024. С. 215-216.
3. Шаронов А.П. Деякі особливості взаємодії Національної поліції з іншими суб'єктами кібербезпеки в Україні. *Стан та перспективи розвитку адміністративного права України:* матеріали XII Міжнародної науково-практичної онлайн-конференції, м. Одеса, 24 жовтня 2025 року. Одеса : ОДУВС, 2025. С. 307-311.

УХВАЛИЛИ:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації ШАРОНОВА Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект», поданої на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право» з метою надання висновку про наукову новизну, теоретичне та практичне значення результатів дисертації.
2. Констатувати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація ШАРОНОВА Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» відповідає спеціальності 081 «Право» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах) затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року № 261, 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 дисертацію ШАРОНОВА Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» до вченої ради для захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 081 «Право».

Головуючий на засіданні
доктор юридичних наук, професор **Володимир ПЯДИШЕВ**