До спеціалізованої вченої ради Д 41.884.04
в Одеському державному
університеті внутрішніх справ

ВІДГУК

опонента на дисертацію **ДЕМЕДЮКА Сергія Васильовича**
на тему «Організаційно-правові та кримінологічні засади кіберстійкості в Україні», подану на здобуття наукового ступеня доктора юридичних наук за спеціальностями 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право; 12.00.08 - кримінальне право та кримінологія; кримінально-виконавче право

Актуальність обраної теми.

Ступінь актуальності теми дисертації Демедюка Сергія Васильовича визначається тим, що кіберстійкість стала ключовим елементом сучасної національної безпеки. В умовах гібридної агресії проти України кібератаки спрямовані не лише на окремі бази даних, а й на цілісні екосистеми державних послуг, енергетичні та транспортні мережі. Це потребує переходу від реактивної моделі кіберзахисту до проактивної моделі кіберстійкості. Важливим є те, що міжнародні стандарти (EU Cyber Resilience Act, NIS2, National Cyber Strategy Великої Британії, американські стандарти NIST та MITRE) вже закріплюють вимоги до стійкості цифрових продуктів протягом усього життєвого циклу. Для України це означає необхідність гармонізації законодавства та створення інституційної моделі кіберстійкості, яка інтегрує державні органи, приватний сектор і громадянське суспільство.

Важливим є також кримінологічний аспект актуальності, який полягає у тому, що кіберзлочинність дедалі більше використовує людський фактор, соціальну інженерію та інноваційні технології для підриву довіри до

цифрових інституцій. Важливо, що на сьогодні стрімка трансформація кіберзлочинності, що паразитує на вразливостях «людського фактора» та Інтернету речей (IoT), робить традиційні методи захисту обмежено ефективними. Робота заповнює суттєву наукову прогалину, пропонуючи інтеграцію OSINT-моніторингу та стратегічного форсайту в систему національної безпеки, що дозволяє перейти до управління потенціалом адаптації цифрового суспільства, що, в свою чергу, є додатковим аспектом актуальності та потребує розробки нових методів OSINT, Intelligence-Led Policing та прогнозних моделей ризику. Створення прогнозних моделей кіберстійкості також дозволять здійснювати превентивні інвестиції у найбільш вразливі ділянки цифрового простору. Це забезпечить перехід від боротьби з наслідками інцидентів до управління потенціалом адаптації та сталого розвитку національної кіберсистеми. Тому дослідження, яке поєднує організаційно-правові та кримінологічні засади, є своєчасним і необхідним для формування комплексної державної політики у сфері кіберстійкості.

Тож важливо, що дослідження С.В. Демедюка є актуальним як у науковому, так і в практичному вимірі, оскільки воно формує основу для побудови стійкої цифрової держави. Актуальність теми дисертації «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» не лише не викликає сумнівів, а й має стратегічне значення як з точки зору науки адміністративного та кримінального права, так і з позицій стратегічного розвитку національної системи кібербезпеки. Водночас, робота є вдалою спробою усунути наявні теоретичні прогалини, сформулювати єдину національну концепцію кіберстійкості, яка забезпечить життєздатність держави в умовах постійних цифрових загроз, та запропонувати науково обґрунтовані шляхи її реалізації в правозастосовній і нормотворчій практиці.

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

У структурі роботи слід відзначити чіткий логічний поділ на підрозділи, які дозволяють поступово розкрити концептуальні підвалини теми. Висновки до кожного з розділів є змістовними, виваженими і відображають основні положення, що розкриваються в тексті. Загальний підсумок дисертації сформульовано чітко, він узагальнює ключові результати наукового пошуку.

Наукові положення дисертації є належним чином обґрунтованими завдяки використанню багатокомпонентної методології, яка поєднує компаративний, системний, функціонально-структурний та ризик-орієнтований аналіз. Автор переконливо доводить, що кіберстійкість є новою парадигмою захисту, яка виходить за межі традиційної моделі кібербезпеки. Системність дослідження виявляється у логічному переході від міждисциплінарної теорії стійкості до конкретних пропозицій щодо внесення змін до Законів України «Про основні засади забезпечення кібербезпеки» та «Про захист прав споживачів». Кожне наукове положення проходить шлях від теоретичного обґрунтування до апробації на міжнародних форумах.

Висновки дисертації підтверджуються аналізом міжнародного досвіду (ЄС, США, Великобританія, НАТО) та його адаптацією до українських реалій. Рекомендації щодо створення «координаційного хабу» на базі НКЦК та розробки багаторівневої моделі цивільно-військового співробітництва мають практичну значущість для державної політики кібербезпеки.

Кримінологічні положення дисертації обґрунтовані через аналіз сучасних кіберзлочинних практик, включно з використанням соціальної інженерії, анонімізації та фінансових інструментів. Достовірність кожного із висновків, сформульованих у дисертації, підтверджується емпіричними даними, статистичними матеріалами та прогнозними моделями, що дозволяють оцінити рівень ризику поширення кіберзагроз. Практичні рекомендації дисертації можуть бути використані у правотворчій

діяльності, удосконаленні законодавства та формуванні стратегічних орієнтирів державної політики у сфері кіберстійкості.

Новизна і загальнонаціональне значення здобутих результатів.

Наукова новизна дисертації здобутих С.В. Демедюком результатів полягає у розробці авторської концепції кіберстійкості як багаторівневої системи, що охоплює стратегічний, тактичний та операційний рівні. Автор уперше запропонував модель «координаційного хабу» на базі Національного координаційного центру кібербезпеки, яка забезпечує інтеграцію діяльності різних суб'єктів у сфері кіберзахисту.

Важливим новим положенням є обґрунтування ролі «цивільних асистентів» та «кіберрезерву» у системі оборони держави, що розширює можливості залучення громадянського суспільства до забезпечення кіберстійкості. Дисертація також пропонує авторське бачення кримінологічного аналізу кіберзлочинності, яке базується на синергії ризик-орієнтованого підходу та стратегічного аналізу. Автор також уперше здійснив кримінологічний аналіз фінансової екосистеми кіберзлочинності, включно з інструментами анонімізації та комунікації зловмисників, що дозволяє формувати нові стратегії протидії.

Загальнонаціональне значення результатів полягає у тому, що вони можуть бути використані для формування нової доктрини кібербезпеки України, яка інтегрує міжнародний досвід та створення практичних механізмів забезпечення життєздатності критичної інфраструктури. Вперше запропоновано комплексну діагностичну матрицю кіберстійкості, що дозволяє вимірювати нелінійні зв'язки між фізичним, інформаційним, когнітивним та соціальним доменами. Розроблена модель «інтелектуальної стійкості» на основі синергії OSINT та форсайту забезпечує проактивне управління життєздатністю інфраструктури в умовах воєнного стану. Це має стратегічне значення для національної безпеки та стійкості суспільства в умовах гібридної війни.

Практичні рекомендації дисертації мають потенціал для впровадження у діяльність державних органів, правоохоронних структур та операторів критичної інфраструктури, що забезпечить підвищення рівня національної кіберстійкості.

Таким чином, отримані здобувачем результати мають високий ступінь теоретичної новизні, істотну правозастосовну вагу та значний потенціал для обґрунтування розвитку держаної політики та правового регулювання у сфері кібербезпеки.

Здобувачем забезпечено високий рівень висвітлення авторських концепцій (зокрема «Cyber-CIMIC» та моделей ризик-менеджменту) у 33 наукових роботах. Використання сучасних методологій аналізу, таких як Europol IOCTA, детально розкрито у публікаціях у співавторстві з провідними фахівцями галузі.

Наявність або відсутність академічного плагіату, фабрикації чи фальсифікації.

Дисертація Демедюка Сергія Васильовича є самостійною науковою працею, що має оригінальний характер і базується на власних дослідженнях автора. Наукові положення та висновки роботи обґрунтовані результатами дослідницької діяльності здобувача. Для підтвердження окремих тез коректно використано наукові джерела з відповідними посиланнями.

У тексті дисертації не виявлено порушень принципів академічної доброчесності, а також відсутні ознаки академічного плагіату, фабрикації чи фальсифікації.

Водночас дисертаційне дослідження Демедюка С.В. не позбавлене **окремих зауважень і дискусійних положень.**

1. Автор пропонує багатокомпонентну методологію, але дискусійним є питання: чи не ускладнює надмірна кількість методів практичне застосування результатів у державній політиці?

2. Визначення «інституціоналізації кіберстійкості» потребує уточнення: чи достатньо правових норм для її закріплення, чи необхідна також соціальна практика та культура безпеки?

3. Запропонована інституційна модель інтеграції державних і приватних суб'єктів виглядає перспективною, але дискусійним є питання: чи готовий український приватний сектор до такої глибокої інтеграції з державними структурами у сфері кіберзахисту?

4. Автор пропонує гармонізацію законодавства з директивою NIS2, проте чи не виникає ризик надмірного формалізму, який може уповільнити оперативність реагування на кібератаки?

5. Порівняння моделей ЄС, НАТО та США є цінним, але дискусійним залишається питання: чи враховано культурні та соціальні відмінності, які можуть впливати на ефективність імплементації цих моделей в Україні?

6. Пропозиція формування культури кіберстійкості серед громадян є слушною, але чи не варто було б ширше розглянути роль освіти, медіа та громадських організацій у цьому процесі?

7. Інтегрована матрична модель діагностики є новаторською, але дискусійним залишається питання: чи враховує вона соціальні ризики, пов'язані з масовою дезінформацією та інформаційними кампаніями?

Усі висловлені зауваження мають дискусійний характер та не знижують загальної позитивної оцінки проведеного дослідження. Робота виконана на вельми актуальну тему, відрізняється новизною, містить раніше не захищені наукові положення, демонструє приріст наукового знання досліджуваної С.В. Демедюком проблематики.

Із викладеного вище випливає висновок, що дисертація Демедюка Сергія Васильовича «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» є завершеною кваліфікаційною працею, виконаною на належному рівні, і такою, що відповідає вимогам Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого постановою Кабінету Міністрів України від 17 листопада

2021 р. № 1197 (зі змінами), які пред'являються до докторських дисертацій, а також наказу МОН України від 12 січня 2017 року № 40 щодо оформлення дисертації, а її автор заслуговує на присудження наукового ступеня доктора юридичних наук за спеціальностями 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право; 12.00.08 - кримінальне право та кримінологія; кримінально-виконавче право.

Опонент
професор кафедри кримінального права
та кримінології факультету підготовки фахівців
для органів досудового розслідування НПУ
Одеського державного університету
внутрішніх справ,
доктор юридичних наук, професор **Ганна СОБКО**

ЗАСВІДЧУЄ:

Перший проректор
Одеського державного університету
внутрішніх справ,
доктор юридичних наук, професор **Максим КОРНІЄНКО**

«17» квітня 2026 р.

ВІДДІЛ ДОКУМЕНТУВАННЯ СЛУЖБОВОЇ ДІЯЛЬНОСТІ

ПІДПИС Ганни Собко
ЗАСВІДЧУЮ:
ВДСД ОДУВС
«17» 04 2026 р.