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

ВІДГУК

опонента на дисертацію

ДЕМЕДЮКА Сергія Васильовича

«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 дисертації. Обрана тема дисертації є надзвичайно актуальною у зв'язку з тим, що кіберпростір перетворився на ключовий театр сучасних конфліктів. Україна, як держава, що перебуває у стані гібридної війни, зазнає постійних атак на енергетичні системи, транспортні комунікації та цифрові сервіси. Це доводить, що кіберстійкість є не лише технічним, а й правовим та кримінологічним феноменом. Вона потребує комплексного регулювання, яке включає визначення ролі державних органів, формування нормативних стандартів та розробку механізмів цивільно-військового співробітництва.

Важливим є також врахування міжнародного досвіду (директиви NIS2, стандарти NIST, моделі НАТО тощо), що акцентує увагу на ризик-орієнтованому управлінні та інтеграції цивільних і військових спроможностей. Кримінологічний аспект актуальності полягає у тому, що кіберзлочинність швидко адаптується до нових технологій, використовуючи соціальні мережі, хмарні сервіси та фінансові інструменти. Це створює потребу у нових методах аналітичної розвідки та прогнозування. З огляду на зазначене, тема дисертації є надзвичайно своєчасною в контексті

євроінтеграційних процесів та потреби гармонізації українського законодавства, зокрема з Директивою NIS2 Європейського Союзу. Автор слушно зауважує, що існуюче регулювання часто орієнтоване на реакцію, тоді як сучасні виклики вимагають проактивного вибудовування стійких архітектур та легітимізації цивільно-військового співробітництва в цифровому просторі.

На сьогодні актуальність теми підсилюється тим, що кіберзлочинність в Україні дедалі більше інтегрується у фінансову сферу, використовуючи інструменти анонімізації та криптовалютні транзакції. Це створює нові ризики для економічної безпеки та потребує розробки спеціальних кримінологічних стратегій протидії. Крім того, міжнародний досвід свідчить, що кіберстійкість неможлива без міжсекторальної співпраці, де приватні компанії, державні органи та військові структури діють узгоджено. Для України це питання набуває особливої ваги, адже саме цивільні компанії часто першими стикаються з атаками на критичну інфраструктуру.

З огляду на зазначене, дослідження має не лише теоретичну, а й практичну актуальність у контексті побудови інтегрованої моделі національної кібербезпеки.

Водночас, дослідження С.В. Демедюка є своєчасним і необхідним для формування національної доктрини кіберстійкості, яка забезпечить життєздатність держави в умовах постійних цифрових загроз.

Обґрунтованість наукових положень, висновків і рекомендацій, сформульованих у докторській дисертації Демедюка С.В., забезпечується широтою і різноманітністю опрацьованої джерельної бази, веденням коректної полеміки, використанням низки різноманітних методів пізнання, вдало підібраних з урахуванням предмета дисертаційного дослідження, продуманою логікою викладення матеріалу, яка дозволила автору виконати поставлені перед собою завдання.

Схвальної оцінки заслуговує обґрунтованість наукових положень дисертації, що забезпечена системним підходом до аналізу кіберстійкості як

багаторівневої соціотехнічної системи. Автор не обмежився теоретичними узагальненнями, а здійснив функціональний аналіз життєвого циклу стійкості (передбачення, витримування, відновлення, адаптація), що дозволило сформулювати практичні рекомендації для державних органів та операторів критичної інфраструктури. Висновки дисертації підтверджуються порівняльним аналізом чинної нормативної бази України та міжнародних актів, що регулюють сферу кібербезпеки.

Особливу вагу має кримінологічний блок дослідження, де автор доводить інтеграцію злочинних практик у цифрові екосистеми та пропонує нові методи їх виявлення через OSINT та Intelligence-Led Policing. Рекомендації щодо формування культури кіберстійкості серед громадян та залучення цивільних експертів до системи оборони держави мають практичне значення для підвищення рівня національної безпеки.

Достовірність висновків підтверджується використанням прогнозних моделей ризику та соціологічного аналізу кіберзагроз, що дозволяє оцінити їхній вплив на суспільство. У своїх міркуваннях дисертант спирається на результати емпіричної бази, що включає опитування 1013 фахівців у сфері кібербезпеки та 764 співробітників кіберполіції. Автор майстерно поєднує статистичні дані ЄРДР із математично підтвердженими експертними оцінками, що дозволило виявити «безпековий розрив» між центральним та регіональним рівнями управління.

Новизна і загальнонаціональне значення здобутих С.В. Демедюком результатів визначається тим, що автор уперше здійснив системний аналіз кримінологічних детермінант кіберзлочинності у контексті формування кіберстійкості. Дисертація пропонує новітні методологічні засади виявлення злочинної діяльності через OSINT та Intelligence-Led Policing, що раніше не застосовувалися у вітчизняній науці як складові кіберстійкості.

Вважаю, що є добре продуманим і належним чином аргументованим, а тому заслуговує на підтримку розроблена автором інтегрована матрична модель діагностики кіберстійкості, яка поєднує цикли управління інцидентами

(планування, поглинання, відновлення, адаптація) з операційними доменами системи (фізичним, інформаційним, когнітивним, соціальним). Це дозволяє оцінювати здатність державних інституцій до відновлення після атак та формувати пріоритети інвестицій у найбільш вразливі сегменти цифрового простору.

Автор уперше здійснив кримінологічний аналіз сучасних кіберзагроз, інтегрувавши методи OSINT та Intelligence-Led Policing у систему кіберстійкості. Новим є також підхід до прогнозування кіберризиків через використання стратегічного форсайту та соціологічного аналізу. Загальнонаціональне значення результатів полягає у тому, що вони створюють основу для побудови комплексної системи кіберстійкості, яка відповідає міжнародним стандартам (NIS2, NIST, MITRE) і водночас враховує специфіку українських реалій. Практичне застосування висновків дисертації можливе у правотворчій діяльності, правоохоронній практиці та стратегічному плануванні, що забезпечує підвищення рівня кіберзахисту держави.

У дисертаційній роботі схвальної оцінки заслуговує розроблена С.В. Демедюком унікальна для вітчизняної науки концептуальна модель «Cyber-CIMIC», яка легітимізує участь IT-волонтерів у кібероборонні через механізми «цивільного кіберрезерву» та «регуляторних пісочниць». Це має світове значення, оскільки трансформує Україну з реципієнта допомоги у донора унікального практичного досвіду для країн НАТО та ЄС.

Дисертація Демедюка Сергія Васильовича є самостійним оригінальним дослідженням, що відповідає принципам академічної доброчесності. Порушень, плагіату, фабрикацій чи фальсифікацій не виявлено. Використання праць інших авторів супроводжується належними посиланнями.

У роботі чітко простежується безпосередній **зв'язок з науковими програмами, планами та темами.** Зокрема, дисертаційне дослідження узгоджується з низкою положень Стратегії національної безпеки України; Стратегії кібербезпеки України; Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони

України на 2023-2027 роки; Плану заходів на 2025 рік реалізації Стратегії кібербезпеки України; Тематики наукових досліджень та науково-технічних (експериментальних) розробок на 2025–2029 роки.

Тему і структуру дисертації затверджено рішенням Вченої ради Одеського державного університету внутрішніх справ (протокол № 2 від 27.01.2026 року).

Висновки та пропозиції, які містяться в дисертації, по-перше, можуть бути впроваджені у законотворчу діяльність у галузі, яка регулює відносини у сфері кібербезпеки (довідка №89д9/10-2025/251968 від 03.11.2025 про впровадження у діяльності ВРУ при розроблені законопроекту № 12207 «Проект Закону про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки»), загалом відзначаються конкретністю, оригінальністю, аргументованістю та логічно підсумовують проведене дослідження; і, по-друге, вже використовуються у правозастосуванні, освітньому процесі та науково-дослідній діяльності, що підтверджується відповідними актами впровадження.

Наукові положення, висновки і рекомендації, сформульовані у дисертації, повно відображено у 18 наукових статтях у фахових виданнях та активно апробовано на 13 науково-практичних заходах, включаючи Київський міжнародний форум кіберстійкості 2026. Матеріали публікацій повністю охоплюють всі завдання дослідження від теоретичного аналізу генезису стійкості до стратегій протидії онлайн-шахрайству.

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

1. Автор акцентує на кримінологічних детермінантах кіберзлочинності, проте дискусійним є питання: чи достатньо враховано соціально-економічні чинники, які формують мотивацію до вчинення кіберзлочинів?

2. Автор пропонує розмежування понять «кібербезпека» та «кіберстійкість», проте дискусійним залишається питання: чи не є

кіберстійкість лише еволюційним етапом розвитку кібербезпеки, а не окремою парадигмою?

3. В дисертації акцентується на використанні OSINT для виявлення кіберзлочинності, але дискусійним є питання: чи достатньо розроблено механізми правового регулювання використання відкритих джерел, щоб уникнути порушення прав людини?

4. Використання стратегічного форсайту для прогнозування кіберзагроз є перспективним, проте дискусійним є питання: чи можливо забезпечити достовірність таких прогнозів в умовах високої невизначеності?

5. Аналіз соціальної інженерії та людського фактора є важливим, але чи достатньо уваги приділено психологічним аспектам кіберзлочинності, зокрема впливу травматичного досвіду війни?

6. Інтегрована матрична модель діагностики є новаторською, але дискусійним залишається питання: чи можливо її застосувати у реальних умовах обмежених ресурсів та кадрового дефіциту?

7. Автор пропонує превентивні інвестиції у найбільш вразливі сегменти цифрового простору, проте чи не створює це ризику недофінансування інших важливих сфер, які також потребують захисту?

Зроблені зауваження і побажання стосуються дискусійних питань, не вливають на належний науковий рівень дисертації, не піддають сумніву основні наукові результати, отримані здобувачем, і не лише підтверджують складність і злободенність досліджуваної С.В. Демедюком проблематики.

З огляду на викладене, вважаю, що дисертація Демедюка Сергія Васильовича «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» є науковою кваліфікаційною працею, що відповідає вимогам, які висуваються до докторських дисертацій та встановлені Порядком присудження та позбавлення наукового ступеня доктора наук, затвердженим постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197 зі змінами.

Автор дисертації – Демедюк Сергій Васильович – на основі публічного захисту 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.

ОФІЦІЙНИЙ ОПОНЕНТ

професор кафедри права
Навчально-наукового юридичного інституту
Державного університету економіки і технологій,
доктор юридичних наук, професор **Микола ВЕСЕЛОВ**

Підпис М. Веселова засвідчую.
Учений секретар Я. Багачова