

ВІДГУК

опонента, доктора юридичних наук, професора, заслуженого юриста України КАРЧЕВСЬКОГО Миколи Віталійовича 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

1. Актуальність теми дисертації. Обрана тема дисертаційного дослідження зумовлена безпрецедентними викликами, які постали перед Україною у сфері кібербезпеки в умовах гібридної агресії. Кібератаки стали системним інструментом дестабілізації державних інституцій, критичної інфраструктури та суспільних комунікацій. Традиційна парадигма «кібербезпеки», орієнтована на створення бар'єрів і запобігання проникненню, виявилася недостатньою перед багатовекторними загрозами. Саме тому концепція кіберстійкості, яка передбачає здатність системи передбачати, витримувати, відновлюватися та адаптуватися, набуває ключового значення. Наукове осмислення організаційно-правових та кримінологічних засад кіберстійкості є необхідним для формування дієвої державної політики, що відповідає стандартам ЄС та НАТО. Важливим чинником є також трансформація кіберзлочинності, яка дедалі більше використовує соціальну інженерію та інструменти анонімізації. Це потребує інтеграції кримінологічних методів у систему кіберзахисту. Таким чином, дослідження має стратегічну актуальність як для забезпечення національної безпеки, так і для розвитку правової науки, оскільки воно формує нову парадигму протидії загрозам у цифровому середовищі.

Водночас, актуальність дослідження С.В. Демедюка зумовлена фундаментальним зміщенням парадигми від статичної «кібербезпеки» до динамічної «кіберстійкості» в умовах гібридної агресії. Враховуючи безпрецедентну інтенсивність атак на критичну інфраструктуру України, робота пропонує критично важливі механізми забезпечення життєздатності

соціотехнічних систем навіть у стані часткового ураження. Це відповідає не лише національним інтересам, а й глобальним трендам, зафіксованим у EU Cyber Resilience Act та стандартах NIST.

У цьому контексті особливого значення набуває необхідність гармонізації українського законодавства з європейськими стандартами, що вже закріплюють вимоги до кіберстійкості цифрових сервісів протягом усього життєвого циклу. Це означає, що Україна має не лише реагувати на кібератаки, а й створювати нормативні механізми, які забезпечать життєздатність систем навіть у стані часткового ураження. Важливим є також формування культури кіберстійкості серед громадян, адже людський фактор залишається одним із найвразливіших елементів цифрової екосистеми.

З огляду на вищезазначене, обрана тема наукового дослідження є актуальною та відповідає не лише науковим викликам, а й має прикладне значення для державної політики та практики правоохоронних органів.

Дисертація виконана у межах п. 4 розділу 1 та 47 розділу 3 Стратегії національної безпеки України (Указ Президента України від 14.09.2020 р. № 392/2020); п.п. 4 та 5 Стратегії кібербезпеки України (Указ Президента України від 26.08.2021 р. № 447/2021); п. 1.2 розділу II Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки (Указ Президента України від 11.05.2023 р. № 273/2023); п. 16 Плану заходів на 2025 рік реалізації Стратегії кібербезпеки України (Розпорядження КМУ від 07.03.2025 р. № 204-р); п.п. 3, 7, 11, 13 Тематики наукових досліджень та науково-технічних (експериментальних) розробок на 2025–2029 роки (наказ МВС від 21.05.2024 р. № 326); а також відповідно до тем науково-дослідних робіт Одеського державного університету внутрішніх справ «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (номер державної реєстрації 0123U103538).

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

Аналіз змісту дисертації та реферату, висновків і рекомендацій свідчить, що наукові положення дисертації відзначаються високим рівнем обґрунтованості, що підтверджується використанням комплексної методології та широкої джерельної бази. Автор застосував компаративний аналіз для зіставлення українських нормативних актів із європейськими стандартами (NIS2, Cyber Resilience Act, моделі НАТО CIMIC), що дозволило сформулювати практичні рекомендації щодо гармонізації законодавства. Висновки дисертації логічно випливають із проведеного аналізу: обґрунтовано необхідність переходу від парадигми «кібербезпеки» до парадигми «кіберстійкості», яка забезпечує здатність системи адаптуватися до багатовекторних загроз. Рекомендації щодо формування інституційної моделі кіберстійкості базуються на функціонально-структурному аналізі суб'єктів національної системи кібербезпеки та визначенні їхніх ролей у забезпеченні стійкості. Водночас, достовірність висновків підтверджується залученням емпіричних даних, OSINT-аналітики та кримінологічних досліджень сучасних кіберзагроз. Практична цінність рекомендацій полягає у можливості їх застосування для розробки державної політики, удосконалення нормативної бази та формування механізмів цивільно-військового співробітництва.

Зазначене дозволяє констатувати, що основні наукові положення дисертації базуються на використанні цілісної системи методів, зокрема генетико-морфологічного аналізу еволюції стійкості та ризик-орієнтованого підходу. Обґрунтованість висновків підтверджується застосуванням методу моделювання для побудови концепції «координаційного хабу» на базі НКЦК та мережевої екосистеми Cyber-CIMIC. Практичні рекомендації, викладені в дисертації, є достатньою мірою обґрунтованими, логічними і послідовними. Достовірність висновків і рекомендацій, сформульованих в дисертації, забезпечена використанням наукової методології та застосуванням сучасних методів проведення досліджень.

3. Новизна і загальнонаціональне значення здобутих результатів.

Наукова новизна полягає у першому комплексному дослідженні

кіберстійкості як «вищого рівня» кібербезпеки. Ознайомлення зі змістом дисертації, наукових публікацій та реферату дисертації дає підставу визначити основні наукові положення й висновки, що характеризуються науковою новизною і відображають особистий внесок автора, ступінь їх обґрунтованості та достовірності:

- комплексно переосмислено категорію «кіберстійкість» як інтегрованої правової та кримінологічної конструкції, що поєднує організаційно-правові та кримінологічні засади. Вперше сформульовано дефініцію національної кіберстійкості як емерджентної властивості соціо-кібернетичної системи;

- автор уперше здійснив системне розмежування понять «кібербезпека» та «кіберстійкість», довівши, що остання є якісно новою парадигмою, яка враховує неминучість компрометації цифрових систем і потребу їх адаптації.

- важливим новим положенням є розробка інституційної моделі кіберстійкості, що передбачає взаємодію державних органів, приватного сектору та громадянського суспільства: Обґрунтовано модель «спільної відповідальності», де стійкість держави є похідною від здатності суб'єктів КІ до самовідновлення;

- новим є й концепт «Cyber-CIMIC» – цивільно-військового співробітництва у сфері кіберзахисту, що дозволяє інтегрувати ресурси державних органів, приватного сектору та громадянського суспільства. Дисертація також містить авторське визначення поняття «інституціоналізація кіберстійкості» як процесу закріплення відповідних норм у правовій системі та практиці державного управління та пропонує концепцію «Cyber-CIMIC» як основу цивільно-військового співробітництва у сфері кіберзахисту.

Загальнонаціональне значення результатів полягає у можливості їх використання для розробки нової доктрини кібербезпеки України, гармонізації законодавства з європейськими стандартами, а також формування практичних механізмів забезпечення життєздатності критичної інфраструктури та державної політики й розробки стратегічних документів у сфері кібербезпеки.

Практичні рекомендації дисертації спрямовані на підвищення

життєздатності критичної інфраструктури та забезпечення безперервності функціонування державних інституцій, що має ключове значення для національної безпеки України.

Дисертаційна робота Демедюка С.В. містить нові, раніше не захищені наукові положення, а обґрунтовані результати у сукупності розв'язують актуальне наукове завдання, яке полягає у тому, що сформульовані у дисертації висновки, узагальнення та пропозиції становлять науково-теоретичний і практичний інтерес та можуть бути використанні у:

– *правотворчій діяльності* – для удосконалення законодавства, що регулює відносини у сфері кібербезпеки (довідка №89д9/10-2025/251968 від 03.11.2025 про впровадження у діяльності ВРУ при розробленні законопроекту № 12207 «Проект Закону про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки»);

– *науково-дослідній сфері* – для наукових розробок проблемних аспектів окремих напрямів удосконалення кібербезпеки та формування національної системи кіберстійкості в Україні (акт впровадження в наукову діяльність Одеського державного університету внутрішніх справ від 15.01.2026 року);

– *правозастосовній діяльності* – для впровадження моделі стійкого правопорядку, що забезпечує перехід від констатації вчинених злочинів до проактивного виявлення латентних загроз та ідентифікації складних кримінальних схем, та передбачає вдосконалення координації суб'єктів національної системи кібербезпеки через автоматизований обмін даними про аномальну активність у реальному часі; методологія аналітичної розвідки має базуватися на інтеграції алгоритмів машинного навчання та предиктивного аналізу великих даних для виявлення транскордонних злочинних мереж, задіяних у гібридній війні, що посилює кіберстійкість суспільства шляхом підвищення інституційної спроможності органів правопорядку, впровадження стандартів безпеки на етапі проектування систем та мінімізації економічної привабливості кіберзлочинності;

– освітньому процесі – при викладанні навчальних дисциплін «Кримінально-правова та кримінологічна характеристика кіберзлочинності», «Інформаційна та кібернетична безпека», «Кримінальний аналіз», «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції», «Протидія кіберзлочинності», при підготовці відповідних розділів підручників, навчальних посібників, програм, проведенні занять з професійної підготовки працівників оперативних підрозділів Національної поліції України (акт впровадження в освітній процес Одеського державного університету внутрішніх справ від 15.01.2026 року).

4. Повнота викладення основних результатів дисертації в опублікованих працях, зарахованих за темою дисертації.

Основний зміст дисертації відображено у 33 наукових працях, серед яких 2 одноосібні розділи в колективних монографіях. Особливої уваги заслуговує публікація результатів у провідних міжнародних виданнях, що індексуються Scopus (зокрема 1 стаття рівня Q1 та 2 статті Q3) та Web of Science.

Результати дослідження та основні положення, висновки та рекомендації оприлюднено на Київському міжнародному форумі кіберстійкості (м. Київ, 19-20 лютого 2026 р.) та 15 конференціях та круглих столах, зокрема: «Закарпатські правові читання» (м. Ужгород, 27 квітня 2023 р.), «Безпекотворення: питання теорії, практики та правові аспекти» (м. Київ, 06 квітня 2023 р.), «Актуальність та особливості наукових досліджень в умовах воєнного стану» (м. Київ, 23 травня 2023 р.), «Стан та перспективи розвитку адміністративного права України» (м. Одеса, 20 жовтня 2023 р.), «Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення» (м. Київ, 26 вересня 2023 р.), «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, 17 листопада 2023 р.), «Кібербезпека в Україні: правові та організаційні питання» (м. Одеса, 17 листопада 2023 р.), «Management in Global Information Networks» (м. Велятино, 25 січня 2024 р.), «Актуальні питання забезпечення безпекового середовища в Україні» (м. Київ, 19 квітня 2024 р.), «Актуальність та особливості наукових досліджень в умовах

воєнного стану» (м. Київ, 22 травня 2024 р.), «Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки» (м. Київ, 27 вересня 2024 р.), «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, 01 листопада 2024 р.), «Протидія організованій злочинності і корупції в умовах збройного конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ» (м. Кропивницький, 04 жовтня 2024 р.), «Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів» (м. Одеса, 23 травня 2025 р.), «Роль OSINT-досліджень у підвищенні рівня національної безпеки України» (м. Львів, 07 травня 2025 р.).

5. Оцінка змісту дисертації та її оформлення.

Аналіз змісту реферату дисертації та основних положень тексту дисертаційного дослідження С.В. Демедюка засвідчив їх повну ідентичність в частині формулювання мети, об'єкту, предмету, завдань, положень новизни, висновків до розділів, загальних висновків. Загалом зміст реферату дисертації відтворює інформацію про методологію дослідження, способи аргументації положень, основні ідеї тексту дисертації викладені стисло. Дисертація і реферат дисертації оформлені відповідно до вимог.

6. Відсутність порушень академічної доброчесності.

Аналіз дисертації та опублікованих праць С.В. Демедюка не виявив фактів порушення академічної доброчесності, зокрема плагіату чи фальсифікацій. У дослідженні належним чином зазначено джерела при використанні ідей, тверджень і фактів; дотримано вимог законодавства про авторське право; представлено достовірні результати наукової діяльності; методика та джерела супроводжуються відповідними посиланнями.

7. Дискусійні питання та зауваження стосовно положень докторської дисертації.

Позитивно оцінюючи дисертаційну роботу в цілому, обґрунтованість її теоретико-методологічних положень, доречно зробити декілька зауважень і звернути увагу на дискусійні положення дисертаційної роботи, саме:

1. Використання ризик-орієнтованого підходу як наскрізного методу є виправданим, але чи не обмежує це дослідження інші методологічні перспективи, наприклад поведінкові чи когнітивні моделі?

2. Визначення кіберстійкості як здатності системи «передбачати, витримувати, відновлюватися та адаптуватися» є концептуально сильним, проте чи не потребує воно більш чіткого нормативного закріплення для уникнення різночитань у правозастосуванні?

3. Порівняння стандартів ЄС, НАТО та США є цінним, однак дискусійним є питання: чи можлива повна імплементація цих моделей в Україні без урахування її специфічних правових та інституційних особливостей?

4. Автор акцентує на інтеграції OSINT та Intelligence-Led Policing, проте дискусійним є питання: чи не створює це ризик надмірної залежності від технологічних інструментів, які можуть бути вразливими до маніпуляцій?

5. Пропозиція превентивних інвестицій у найбільш вразливі сегменти цифрового простору є логічною, але чи не створює вона ризику нерівномірного розвитку інших сфер, які також потребують захисту?

6. Штучний інтелект є перспективним інструментом кіберстійкості і, водночас, одним з джерел новітніх загроз для кібербезпеки. Однак автор недостатньо досліджує цю проблематику.

Разом з тим, висловлені зауваження та рекомендації носять переважно дискусійний характер і не знижують загального позитивного враження від представленої дисертаційної роботи.

8. Загальний висновок.

Дисертація Демедюка Сергія Васильовича на тему «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» є самостійним, завершеним дослідженням актуального наукового завдання. Дисертація виконана на високому теоретичному рівні, викладена науковою мовою, розділи дисертації пов'язані між собою структурно і змістовно, висновки ґрунтуються на результатах проведеного дослідження, які, в свою чергу, є достатньо аргументованими та доказовими.

Враховуючи актуальність, новизну, важливість одержаних результатів, їх обґрунтованість і достовірність, а також практичну цінність сформульованих положень і висновків, можна стверджувати, що дисертаційна робота повністю відповідає вимогам Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197 (зі змінами), Вимогам до оформлення дисертації, затверджених наказом Міністерства освіти та науки України від 12 січня 2017 р. № 40 (зі змінами) та іншим вимогам Міністерства освіти та науки України, а її автор – Демедюк Сергій Васильович – 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.

професор кафедри права імені академіка УАН
о. Івана Луцького
ЗВО «Університет Короля Данила»,
доктор юридичних наук, професор



Микола КАРЧЕВСЬКИЙ

«14» квітня 2026 р.

