ЗАТВЕРДЖУЮ
Ректор Одеського державного університету внутрішніх справ
полковник поліції

В'ячеслав ДАВИДЕНКО

«06» березня 2026 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів докторської дисертації Сергія Васильовича ДЕМЕДЮКА на тему «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» поданої на здобуття наукового ступеня доктора юридичних наук за науковими спеціальностями: 12.00.07- адміністративне право та процес; фінансове право; інформаційне право; 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право.

ДЕМЕДЮК Сергій Васильович виконав дисертаційну роботу у Одеському державному університеті внутрішніх справу самостійно. Тема дисертації затверджена Вченою радою Одеського державного університету внутрішніх справ 27 січні 2026 року (протокол № 2). Рецензенти, призначені Вченою радою Одеського державного університету внутрішніх справ 24 лютого 2026 року (протокол № 3), - доктор юридичних наук, професор Андрій БАБЕНКО, доктор юридичних наук, професор Аліна ДЕНИСОВА, доктор юридичних наук, професор Дар'я БАЛОБАНОВА, - констатують, що 03 березня 2026 року кафедрою кримінально-правових дисциплін, кафедрою адміністративно-правових дисциплін Інституту права та безпеки та кафедрою кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Одеського державного університету внутрішніх справ було проведено фаховий семінар для апробації докторської дисертації Сергія ДЕМЕДЮКА «Організаційно-правові та кримінологічні засади кіберстійкості в Україні», поданої на здобуття наукового ступеня доктора юридичних наук за науковими спеціальностями: 12.00.07- адміністративне право та процес; фінансове право; інформаційне право; 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право. У семінарі брали участь зазначені рецензенти (протокол засідання кафедри у формі фахового семінару від 03 березня 2026 року № 6). Результати семінару взято до уваги під час підготовки висновку.

Провівши попередню експертизу докторської дисертації Сергія ДЕМЕДЮКА «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» та наукових публікацій, у яких висвітлено основні

наукові положення докторської дисертації, а також за результатами фахового семінару рецензенти встановили:

1. Подана для попередньої експертизи докторська дисертація є кваліфікаційною науковою працею, виконаною здобувачем самостійно. Робота містить науково обґрунтовані, достовірні висновки і результати, отримані автором особисто.

2. Докторська дисертація містить наукові положення, які характеризуються новизною, мають теоретичну і практичну цінність та свідчать про вагомий особистий внесок здобувача у науку щодо вирішення важливої теоретико-прикладної проблеми, що має соціально-правове значення та є надзвичайно важливою та актуальною в умовах воєнного стану, зміст якої полягає у визначенні пріоритетних напрямів стратегічного планування у сфері протидії злочинності; розробка рекомендацій шодо впровадження моделі «стійкість через право»; визначенні ключових спроможностей системи кіберстійкості; здійснено комплексне теоретико-правове та кримінологічне дослідження кіберстійкості як новітньої парадигми забезпечення національної безпеки України в умовах цифрової трансформації та гібридної агресії; доведнено, що традиційна модель кібербезпеки, орієнтована на запобігання інцидентам і захист периметра, є обмежено ефективною в умовах зростання складності, масштабності та багатовекторності кіберзагроз, що зумовлює необхідність переходу до концепції кіберстійкості як здатності соціотехнічних систем передбачати, протидіяти, витримувати, відновлюватися та адаптуватися до деструктивних впливів.

Робота виконана у галузі права і відповідає паспорту наукових спеціальностей: 12.00.07- адміністративне право та процес; фінансове право; інформаційне право; 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право. Дисертація характеризується єдністю змісту та відповідає принципам академічної доброчесності.

Наукова новизна отриманих результатів пояснюється тим, що дисертація є першим комплексним дослідженням, у якому системно висвітлюється концепт кіберстійкості як вищий рівень кібербезпеки України та сформульовано низку нових положень, зокрема:

вперше:

- сформульовано дефініцію національної кіберстійкості як динамічної емерджентної властивості соціо-кібернетичної системи, що інтегрує не лише технічні параметри захисту, а й когнітивні та організаційні аспекти адаптації до умов високої невизначеності;

- запропоновано концептуальну модель «спільної відповідальності» в межах національної екосистеми кіберстійкості, де держава виступає фасилітатором та ризик-менеджером, надаючи бізнесу інструменти самооцінки та розвідувальні дані в обмін на прозору звітність, а стійкість держави розглядається як похідна від здатності окремих суб'єктів критичної інфраструктури до самовідновлення;

- обґрунтовано трикомпонентну інституціональну модель кіберстійкості (маркетинг – стандартизація – регулювання) як цілісну систему формування та реалізації політики кіберстійкості, що дозволяє інтегрувати економічні, організаційні та правові механізми в єдину архітектуру кіберменеджменту;

- сформульовано концептуальну модель «Cyber-CIMIC» як специфічну форму цивільно-військового співробітництва в цифровому просторі, що, на відміну від класичної моделі CIMIC НАТО (орієнтованої на підтримку військових операцій у фізичних доменах), розглядається як безперервний процес соціотехнічної взаємодії державних, військових та приватних акторів для забезпечення національної кіберстійкості;

- обґрунтовано необхідність запровадження інституту «цивільного кіберрезерву» та правового режиму «регуляторних пісочниць» у сфері кібероборони, що дозволяє легітимізувати участь недержавних суб'єктів у відсічі збройній агресії в кіберпросторі без обов'язкової комбатантизації за класичними ознаками;

- сформульовано концептуальну модель «Стійкість через право», яка базується на переході від декларативного характеру норм кібербезпеки до жорсткої юридичної фіксації необхідних функціональних спроможностей суб'єктів (передбачення, витримування, відновлення, адаптація);

- обґрунтовано концептуальну модель «інтелектуальної стійкості», яка розглядає аналітичну розвідку як цілісний процес трансформації первинних даних у стратегічні рішення через синергію OSINT як джерела актуальної фактологічної бази, форсайту як інструменту предиктивного моделювання альтернативних сценаріїв і «слабких сигналів» та ризик-орієнтованого підходу як механізму пріоритезації ресурсів, що у сукупності забезпечує перехід від реактивного захисту до проактивного управління життєздатністю критичної інфраструктури в умовах гібридної агресії;

- сформовано ієрархічну модель кіберзагроз для України, яка інтегрує технічні вразливості з деструктивними наслідками гібридної агресії та кібертероризму в єдиному розрахунковому полі ризиків;

- експериментально встановлено та математично підтверджено залежність між профілем професійного досвіду експерта (стаж <3, 3–10, >10 років) та суб'єктивною оцінкою рівня ризику специфічних кіберзагроз;

- розроблено та апробовано комплексну діагностичну матрицю кіберстійкості національної інфраструктури, яка дозволяє вимірювати нелінійні зв'язки між технічною стабільністю фізичного домену та ефективністю ухвалення рішень у когнітивній і соціальній сферах;

- обґрунтовано та емпірично підтверджено існування «безпекового розриву» між центральним та регіональним рівнями управління кібербезпекою України, що потребує переходу від уніфікованого до диференційованого правового регулювання;

- здійснено комплексне зіставлення експертних оцінок на основі ризик-орієнтованого підходу з статистичними даними ЄРДР, що дозволило виявити

розбіжності у обліку кіберзлочинів (зокрема за ст. 362 ККУ) та обґрунтувати необхідність вдосконалення системи кодування злочинів у цифровій сфері;

- обґрунтовано та реалізовано стратегічний аналіз кіберзлочинності в Україні, що базується на інтеграції ризик-орієнтованого підходу та методології Europol IOCTA, що передбачає не лише аналіз статистичних даних ЄРДР, а й обов'язкове залучення експертної думки;

- ідентифіковано та класифіковано специфічний інструментарій кіберзлочинців за рівнем поширеності в українському сегменті, зокрема встановлено домінування операційної системи Kali Linux та використання методів Брутфорс і DoS-атак як ключових засобів вчинення кіберзлочинів;

- на основі емпіричних даних обґрунтовано вплив анонімізації на ефективність правоохоронної діяльності через оцінку популярності VPN-сервісів та мережі Tor, а також прогнозування майбутніх ризиків їх використання як засобів приховування злочинної діяльності в умовах цифровізації.

удосконалено:

- теоретичне розмежування категорій «кібербезпека» та «кіберстійкість» у контексті державного управління, що полягає у трактуванні кіберстійкості не як технічного стану, а як динамічної інституційної спроможності системи до адаптації та самовідновлення, що потребує інтеграції в загальну стратегію корпоративного та державного управління;

- підхід до формування національної екосистеми кіберстійкості шляхом синтезу трьох складників: нормативної обов'язковості (досвід ЄС), технологічної адаптивності (досвід США) та соціотехнічної синергії (досвід Великобританії), що дозволяє перейти від фрагментарного захисту до створення «колективного імунітету» держави;

- механізм інтеграції метрик кіберстійкості, на основі ризик-орієнтованого підходу, у загальну систему управління державними ризиками, що забезпечує перехід від кількісного підрахунку інцидентів до оцінки реальної готовності інфраструктури до відновлення;

- підхід до інституційного забезпечення кіберстійкості на національному рівні шляхом визначення функціональної моделі розподілу повноважень між суб'єктами кібербезпеки, що забезпечує комплексність, уникнення дублювання функцій та підвищення ефективності управління кіберризиками

- функціональну схему розподілу повноважень суб'єктів національної системи кібербезпеки, де, на основі аналізу чинного законодавства, чітко розмежовано вектори впливу: регуляторний (Держспецзв'язку), стандартизуючий (НКЦК як методологічний хаб) та стимулюючий (Мінцифра), що усуває дублювання функцій та підвищує керованість системи;

- понятійно-категоріальний апарат щодо змісту терміна «цивільно-військове співробітництво у сфері кібербезпеки», який на відміну від існуючих підходів, трактується не як ситуативна взаємодія, а як сталий

правовий та організаційний механізм інтеграції ресурсів волонтерських ІТ-спільнот та приватного сектору до загальнодержавної системи кібероборони;

- організаційно-функціональну структуру взаємодії суб'єктів кібербезпеки, де роль Національного координаційного центру кібербезпеки (НКЦК) трансформована із суто дорадчого органу в стратегічний «комунікаційний хаб», що забезпечує вертикальну та горизонтальну сумісність військових і цивільних стандартів обміну інформацією;

- методологію стратегічного аналізу кіберзагроз через інтеграцію інструментарію OSINT у структуру ризик-менеджменту, що перетворює відкриті дані на верифіковані індикатори для розрахунку ймовірності та впливу загроз;

- класифікацію кіберзагроз у контексті ІПСО та гібридної війни, де кібератака розглядається не лише як технічний акт, а як інструмент маніпуляції суспільною довірою та дискредитації військово-політичного керівництва;

- модель міждоменної комунікації в кіберсистемах, де когнітивний домен визначено як ключовий чинник «живучості» системи через його здатність перерозподіляти інформаційні потоки у разі руйнування фізичних вузлів;

- типологію on-line шахрайства через диференціацію загроз із використанням платіжних карток (фішинг, вішинг) та без них (торгівля віртуальними товарами, криптовалютні махінації), що дозволяє правоохоронним органам точніше фокусувати оперативні ресурси;

- типологію засобів анонімізації злочинців, де в системному аналізі розмежовано використання комерційних VPN, власноналаштованих серверів та децентралізованих мереж;

- типологію фінансової активності кіберзлочинців через розмежування платіжних інструментів за рівнем ризику: від традиційних банківських переказів до використання криптовалют (Bitcoin, USDT) та систем електронних грошей (EasyPay, PayPal), що сприяє розробці ефективніших механізмів фінансового моніторингу;

- систему джерел кримінологічної інформації про on-line шахрайства, де окрім матеріалів кримінальних проваджень, враховано значну питому вагу довідково-аналітичних матеріалів (близько 30%), що дозволяє нівелювати вплив високої латентності цього виду злочинів.

дістали подальшого розвитку:

- міждисциплінарна теорія стійкості через адаптацію екологічних та інженерних принципів стійкості до специфіки функціонування сучасних кіберфізичних систем та ІТ-мереж;

- теоретичні підходи до розуміння кіберстійкості як складної адаптивної системи, в якій ключову роль відіграє не сукупність заходів, а їх узгодженість, пріоритезація та здатність до динамічної трансформації в умовах невизначеності;

- концепція міжнародної суб'єктності України в глобальному кіберпросторі на основі подальшого розвитку та трансформації України з

реципієнта міжнародної технічної допомоги у ключового донора унікального практичного досвіду для країн НАТО та ЄС, що легітимізує національні безпекові протоколи як основу для майбутніх міжнародних стандартів колективної стійкості;

- підходи до гармонізації національного законодавства із євроатлантичними вимогами, зокрема в частині адаптації стандартів ISO/IEC 27000 та положень Директиви NIS2, що забезпечує інституційну сумісність України з міжнародними мережами реагування на інциденти;

- наукові підходи до формування мережевої моделі кібероборони, що базується на принципах функціональної комплементарності та розподіленої відповідальності, що дозволяє ефективно масштабувати спроможності держави за рахунок гнучкого залучення цивільного інтелектуального капіталу в умовах гібридної війни;

- методика багаторівневої фільтрації експертних даних у сфері кібербезпеки на основі «тесту на логічну узгодженість», що дозволило статистично значущо підвищити надійність прогнозних моделей розвитку кіберзагроз;

- використання методів інтелектуального аналізу даних для моніторингу регіональних та галузевих особливостей поширення кіберризиків в Україні;

- кримінологічна теорія мотивації кіберзлочинців, доповнена факторами «гібридної війни» та «колабораційної співпраці», що виходить за межі класичного корисливого мотиву;

- кримінологічна характеристика способів комунікації в кіберпросторі, яку доповнено порівняльним аналізом використання месенджерів (Telegram – 66%, WhatsApp – 56,3%, Viber – 52,3%) як основних каналів взаємодії між злочинцями та жертвами, а також прогнозуванням ризиків їх використання у післявоєнний період;

- розуміння впливу технологічних чинників на ландшафт кіберзлочинності, зокрема щодо експлуатації вразливостей Інтернету речей (IoT) для створення ботнетів та проведення DDoS-атак, що розглядається як критична загроза для стабільності цифрової інфраструктури в умовах масової цифровізації;

- теоретичні засади протидії соціальній інженерії, які розширено через аналіз динаміки поширення методів фішингу, вішингу та смішингу, а також обґрунтування того, що людський фактор залишається найбільш критичною ланкою в системі забезпечення кіберстійкості держави.

3. Обґрунтованість та достовірність наукових положень, висновків і рекомендацій, запропонованих автором у дисертації, характеризуються: системним підходом до розгляду проблематики кримінологічних та правових засад кіберстійкості як вищої форми кібербезпеки в Україні, що забезпечено вдало розробленою структурою роботи, яка корелюється з поставленими на вирішення завданнями. Зокрема, дисертація складається зі списку умовних позначень, анотації, вступу, чотирьох розділів, які об'єднують тринадцять підрозділів, висновків, списку використаних джерел (424 найменування на 49

сторінках), 4 додатків на 42 сторінках. Повний обсяг дисертації складає 525 сторінок, з яких основний текст – 412 сторінок.

З метою досягнення об'єктивного наукового результату та формування відповідних положень та висновків, що характеризують наукову новизну роботи, використано сукупність сучасних загальнонаукових та спеціально-наукових методів наукового пізнання. Зокрема: *генетико-морфологічний аналіз* використаний у підрозділі 1.1 для дослідження історичного походження терміна «стійкість»; *компаративний аналіз* застосований для розмежування понять «кібербезпека» та «кіберстійкість» та порівняння класичної парадигми «кібербезпеки» з новітньою концепцією «кіберстійкості» (2.1); зіставлення євроатлантичних стандартів (Директива NIS2, моделі CIMIC НАТО) із поточною нормативною базою та практичним досвідом України (2.2, 2.3); аналізу міжнародних інструментів співпраці (4.3) та розробки пропозицій щодо гармонізації українського законодавства; *системний підхід* застосований для дослідження національної системи кібербезпеки як складного соціотехнічного комплексу (2.1-2.3); *функціонально-структурний аналіз* використаний у підрозділі 1.2 для декомпозиції життєвого циклу стійкості на окремі фази (передбачення, витримування, відновлення, адаптація); для розмежування повноважень суб'єктів кібербезпеки України відповідно до їхніх ролей у забезпеченні стійкості (2.2) та визначення специфічних функцій «цивільних асистентів» та «кіберрезерву» у системі оборони держави; *контент-аналіз нормативно-правової бази* використаний у підрозділі 1.3 для вивчення стратегій кібербезпеки України та провідних держав світу, а також критичного аналізу Закону «Про основні засади забезпечення кібербезпеки України» та Директиви NIS2 (2.3); *метод термінологічного аналізу та дефініції* використаний для уточнення понятійно-категоріального апарату, виявлення «термінологічного розриву» у чинному законодавстві та формулювання авторського визначення понять «інституціоналізація кіберстійкості» (2.1) та «Cyber-CIMIC» (2.3); *метод моделювання* застосовано для розробки теоретичної моделі багаторівневої взаємодії суб'єктів, побудови моделі «координаційного хабу» на базі НКЦК та моделі цивільно-військового співробітництва, що охоплює стратегічний, тактичний та операційний рівні (2.2, 2.3); *метод екстраполяції та прогнозування* застосовано для визначення перспектив розвитку національної системи кіберстійкості (2.2, 2.3, 3.1); *оціологічний аналіз* використаний для переосмислення природи кіберзагроз не лише як технічних проблем, а як соціальних ризиків, що дозволило обґрунтувати необхідність залучення громадян як активних суб'єктів кіберстійкості (розділ 3); *ризик-орієнтований метод* застосований як наскрізний інструмент для обґрунтування пріоритетності інвестицій у кіберстійкість та протидії кіберзлочинності (розділи 3, 4); *метод стратегічного управління* застосований для визначення пріоритетів державної політики у сфері кібербезпеки, що дозволило сформувати ієрархію цілей: від захисту індивідуального користувача до гарантування безпеки критичної інфраструктури держави (розділи 3, 4).

4. Теоретичне та практичне значення результатів дисертації полягає в тому, що обґрунтовані в дисертації положення впроваджені й можуть бути використані за такими напрямами:

– *науково-дослідна робота* – 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); *правотворча діяльність* – для удосконалення законодавства, що 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»); *правозастосовна діяльність* – 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; *освітній процес* – 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).

5. Апробація та повнота опублікування результатів дослідження: наукові результати докторської дисертації висвітлено у 33 наукових працях, з яких: 2 – одноосібні розділи колективних монографій, 18 – наукові статті в фахових виданнях (з яких 5 – у періодичних виданнях іноземних держав (фахові видання, включені до наукометричних баз Scopus, зокрема 2 – Q3 і 1 – Q1) та Web of Science), 13 – тези доповідей.

Вказане підтверджує повноту попереднього оприлюднення основних результатів дисертації публікаціях та дотримання вимог п. 8 Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого Постановою Кабінету Міністрів України від 17 листопада 2021 року №1197.

У наукових працях, опублікованих у співавторстві, використані лише ті

ідеї та положення, які с результатом особистого дослідження дисертанта, що зазначено у переліку наукових праць. Матеріали та висновки кандидатської дисертації в докторському дослідженні не використовувалися

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Монографії

1. Демедюк С.В. Розділ 26. Кібервійна та форсайт кіберстійкості. Реалізація філософії ILP в системі кримінального аналізу Національної поліції України: монографія / О.Є. Користін, Б.А. Денисенко, С.В. Демедюк та ін. ; за заг. ред. д-ра юрид. наук, проф. О.Є. Користіна. Київ: ВАЙТЕ, 2024. С. 343-357. DOI: https://doi.org/10.36486/978-966-2310-66-5-26

2. Демедюк С.В. Розділ 1. Стратегічний ландшафт застосування OSINT в секторі національної безпеки. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. С. 21-36.

Статті у наукових періодичних виданнях інших держав, у тому числі проіндексованих у базах даних Web of Science Core Collection, Scopus

1. Demedyuk S.V., Demedyuk T.S. Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. 2018. Vol. 68 № 6. P. 278-290. DOI: 10.33407/itlt.v68i6.2582 (WoS)

2. Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. *International Journal of Computer Network and Information Security*. 2024. Vol. 16. №. 1. P. 24-34. DOI: https://doi.org/10.5815/ijcnis.2024.01.02 (Scopus Q3)

3. Korystin O., Demediuk S., Sviridyuk N., Mitina O., Aleksander M., Yuriy Kardashevskyy. Risk Forecasting of Information-content-security. *Cyber Hygiene & Conflict Management in Global Information Networks*: Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks. 2025. Vol. 3925. P. 273–280. (Scopus Q4)

4. Korystin O., Demediuk S., Likhovitskyy Y., Kardashevskyy Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns. *International Journal of Information Technology and Computer Science.* 2025. Vol. 17. No. 2. P. 24-35. DOI: https://doi.org/10.5815/ijitcs.2025.02.03 (Scopus Q3)

5. Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability.* (2025). Vol. 17. Is. 19. P. 8757. https://doi.org/10.3390/su17198757 (Scopus Q1)

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

6. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона.* 2023. № 1(59). С.77-85. DOI: https: //doi.org/10.36486/np.2023.1(59).8

7. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона.* 2023. № 2(60). С.78-85. DOI: https: //doi.org/10.36486/np.2023.2(60).8

8. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис.* 2023. № 3. С.53-59. DOI https://doi.org/10.32850/sulj.2023.3.10

9. Демедюк С.В. Захист критично важливих послуг у цифрову епоху. *Наука і правоохорона.* 2023. № 3(61). С.26-34 DOI (Issue): https://doi.org/10.36486/np.2023.3(61).3

10. Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет».* 2023. №06. С. 708-713. DOI: https://doi.org/10.24144/2788-6018.2023.06.122

11. Демедюк С.В. Інституціоналізація кіберстійкості. *Наука і правоохорона.* 2023. № 4(62). С.31-41. DOI: https://doi.org/10.36486/np.2023.4(62).4

12. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. *Наука і правоохорона.* 2024. № 1(63). С.133-141. DOI: https://doi.org/10.36486/np.2024.1(63).13

13. Демедюк С.В. OSINT в контексті кібербезпеки. *Юридичний бюлетень.* 2024. № 34. С.200-207. DOI:10.32850/LB2414-4207.2024.34.26

14. Демедюк С.В. OSINT в контексті виявлення та запобігання кіберзлочинам. *Південноукраїнський правничий часопис.* 2024. № 4. С. 38-41. DOI: https://doi.org/10.32850/sulj.2024.4.7

15. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона.* 2024. Том 3-4. № 65-66. С. 142-154. DOI: https://doi.org/10.36486/np.2024.3(65).12

16. Демедюк С.В. Зміст та особливості експертної вибірки в оцінюванні кіберризиків. *Морська безпека та оборона.* 2025. №1. С.17-24. DOI: https://doi.org/10.32782/msd/2025.1/03

17. Демедюк С.В. Сучасні тенденції on-line шахрайства в Україні. *Право і суспільство.* 2025. №4. Т. 2. С. 186-194. DOI: https://doi.org/10.32842/2078-3736/2025.4.2.28

18. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. *Правові новели.* 2025. № 26. 157-166. DOI: https://doi.org/10.32782/ln.2025.26.18

Наукові праці, які засвідчують апробацію матеріалів дисертації

1. Демедюк С.В. Стійкість системи кібербезпеки та її правове забезпечення в Україні. *Закарпатські правові читання*: збірник тез за матеріалами XV міжнародної науково-практичної конференції (Ужгород, 27 квітня 2023 р.). Ужгород: УжНУ, 2023. С. 5-7.

2. Демедюк С.В. Захист критично важливої інформаційної інфраструктури в системі кібербезпеки. *Стратегії безпеки підприємництва в*

умовах воєнного стану: Збірник тез за матеріалами XIV міжнародної науково-практичної конференції «Безпекотворення: питання теорії, практики та правові аспекти» (Київ, 06 квітня 2023 р.) / за ред. Тимошенко О.І., Київ: Видавництво Європейського університету», 2023. С. 26-27.

3. Демедюк С.В. Розбудова кіберстійкості на національному рівні. *Актуальність та особливості наукових досліджень в умовах воєнного стану*: збірник матеріалів III Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки – 2023 в Україні (Київ, 23 травня 2023 р.). Київ: ДНДІ МВС України, 2023. С. 133-134.

4. Демедюк С.В. Актуалізація сучасних методологій аналізу кіберзлочинності. *Стан та перспективи розвитку адміністративного права України*: матеріали X міжнародної науково-практичної інтернет-конференції (Одеса, 20 жовтня 2023 р.). Одеса: ОДУВС. С. 63-66.

5. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення*: матеріали науково-практичного круглого столу (Київ, 26 вересня 2023 р.) / [Редкол.: Вербенський М. Г., Опришко І. В., Кулик О. Г. та ін.]. Київ : ДНДІ МВС України, 2023. С. 168-170.

6. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції. (Київ, 17 листопада 2023 р.). Київ: НАВС. С.40-44.

7. Демедюк С.В. Захист критично важливих кібер-активів. *Кібербезпека в Україні: правові та організаційні питання*: збірник матеріалів міжнародної науково-практичної конференції (Одеса, 17 листопада 2023 р.). Одеса: ОДУВС. С.55-57.

8. Демедюк С.В. Показники кіберстійкості. *Актуальні питання забезпечення безпекового середовища в Україні*: збірник тез наукових доповідей Всеукраїнської науково-практичної конференції (Київ, 19 квітня 2024 р.). Київ: ДНДІ МВС України, 2024. С.38-41.

9. Демедюк С.В. Щодо питань розвитку кіберстійкості. *Актуальність та особливості наукових досліджень в умовах воєнного стану*: збірник матеріалів IV Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки-2024 в Україні (Київ, 22 травня 2024 р.). Київ: ДНДІ МВС України, 2024. С.19-21.

10. Демедюк С.В. Використання злочинцями комп'ютерних систем та мереж. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки*: збірник матеріалів всеукраїнської науково-практичної конференції (Київ, 27 вересня 2024 р.). Київ: ДНДІ. С. 203-207.

11. Демедюк С.В. Особливості онлайн шахрайства в Україні. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (Київ, 01 листопада 2024 р.). Київ: НАВС, 2024. С. 35-38.

12. Демедюк С.В. Поширення та характерні складові кіберзалежних злочинів. *Протидія організованій злочинності і корупції в умовах збройного*

конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ: збірник матеріалів Міжнародної науково-практичної конференції (Кропивницький, 04 жовтня 2024 року). Кропивницький: ДонДУВС, 2024. С. 268-273.

13. Демедюк С.В. Інтеграція OSINT в систему кібербезпеки держави: стратегічні та прикладні аспекти. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України*: матеріали круглого столу (Львів, 07 травня 2025 р.). Львів: ЛьвДУВС, 2025. С. 58-61.

Особистий внесок здобувача. Дисертація є самостійною, завершеною науковою працею. Сформульовані в ній положення, узагальнення, висновки, рекомендації та пропозиції обґрунтовано на підставі самостійно проведених досліджень. Доведено, що інституціоналізація кіберстійкості є процесом переходу від статичного захисту периметра до динамічної моделі адаптації та відновлення систем. Визначено, що ефективність цього процесу забезпечується синергією трьох підходів: регулятивного (державні норми), стандартизованого (ISO, NIST) та маркетингового (ринкові стимули, кіберстрахування). Встановлено, що ключовим елементом сучасної інституціоналізації є імплементація стандартів Директиви NIS2, яка впроваджує жорстку відповідальність керівництва та обов'язковість звітування про інциденти. Це дозволяє трансформувати кіберстійкість із вузькотехнічного завдання на стратегічний компонент державного управління. Такий підхід створює умови для формування «культури стійкості», де кожен суб'єкт господарювання стає активним учасником системи національної безпеки, що підвищує загальну адаптивність критичної інфраструктури до гібридних загроз.

6. Дотримання принципів академічної доброчесності. Вивчення змісту дисертації та наукових публікацій дає змогу дійти висновку про відсутність академічного плагіату, фабрикації, фальсифікації чи порушення інших видів принципів та правил академічної, доброчесності, які могли б поставити під сумнів самостійний характер рецензованого дослідження. Зазначене підтверджується наявністю відповідних посилань на згадані автором по тексту літературних джерел, зокрема й під час використання ідей, розробок, відомостей тощо.

За результатами фахового семінару щодо апробації дисертації Демедюка Сергія Васильовича «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» було **ухвалено**:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Демедюка Сергія Васильовича «Організаційно-правові та кримінологічні засади кіберстійкості в Україні», поданої на здобуття наукового ступеня доктора юридичних наук за науковими спеціальностями: 12.00.07- адміністративне право та процес; фінансове право; інформаційне право; 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право.

2. Констатувати, що за актуальністю, ступенем новизни, обґрунтованістю та практичною цінністю здобутих результатів дисертація

Демдюка Сергія Васильовича відповідає паспорту наукових спеціальностей 12.00.07- адміністративне право та процес; фінансове право; інформаційне право; 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право, а також Вимогам до оформлення дисертацій, затверджених наказом Міністерства освіти і науки України від 12 січня 2017 року № 40 (із наступними змінами) та Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197

3. Рекомендувати дисертацію Демедюка Сергія Васильовича «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» до подання на розгляд спеціалізованій вченій раді відповідного профілю.

Рецензент –
завідувач кафедри
кримінально-правових дисциплін
інституту права та безпеки
Одеського державного університету
внутрішніх справ
доктор юридичних наук, професор **Андрій БАБЕНКО**

Рецензент –
завідувач кафедри
адміністративно-правових дисциплін
інституту права та безпеки
Одеського державного університету
внутрішніх справ
доктор юридичних наук, професор **Аліна ДЕНИСОВА**

Рецензент –
професор кафедри
кримінально-правових дисциплін
інституту права та безпеки
Одеського державного університету
внутрішніх справ
доктор юридичних наук, професор **Дар'я БАЛОБАНОВА**

Головуючий на засіданні
завідувач кафедри
кримінального права та кримінології
факультету підготовки фахівців для
органів досудового розслідування Національної поліції України
Одеського державного університету
внутрішніх справ
доктор юридичних наук, професор **Віктор КОНОПЕЛЬСЬКИЙ**