Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0526U000083

Особливі позначки: відкрита

Дата реєстрації: 07-04-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Демедюк Сергій Васильович
2. Serhii Demediuk

Кваліфікація: к. ю. н., доц., 12.00.07

Ідентифікатор ORCID ID: 0009-0008-1359-5265

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 12.00.07

Назва наукової спеціальності: Адміністративне право і процес; фінансове право; інформаційне право

Галузь / галузі знань: Не застосовується

Шифр наукової спеціальності: 12.00.08

Назва наукової спеціальності: Кримінальне право та кримінологія; кримінально-виконавче право

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 07-05-2026

Спеціальність за освітою: Правознавство

Місце роботи здобувача: Національна академія Служби безпеки України

Код за ЄДРПОУ: 20001823

Місцезнаходження: вул. М. Максимовича, Київ, 03022, Україна

Форма власності: Державна

Сфера управління: Служба безпеки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 41.884.04

Повне найменування юридичної особи: Одеський державний університет внутрішніх справ

Код за ЄДРПОУ: 08571570

Місцезнаходження: вул. Успенська, Одеса, 65014, Україна

Форма власності: Державна

Сфера управління: Міністерство внутрішніх справ України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Організація відсутня

Код за ЄДРПОУ: 00000000

Місцезнаходження: ------, Київ, 00000, Україна

Форма власності: Змішана

Сфера управління:

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 10.17, 10.81

Тема дисертації:

1. Організаційно-правові та кримінологічні засади кіберстійкості в Україні.

2. Organisational, legal and criminological foundations of cyber resilience in Ukraine.

Реферат:

1. У дисертації здійснено комплексне теоретико-правове та кримінологічне дослідження кіберстійкості як новітньої парадигми забезпечення національної безпеки України в умовах цифрової трансформації та гібридної агресії. Обґрунтовано, що традиційна модель кібербезпеки, орієнтована на запобігання інцидентам, виявляється недостатньо ефективною в умовах зростання складності та багатовекторності кіберзагроз, що зумовлює необхідність переходу до концепції кіберстійкості як здатності системи передбачати, протидіяти, відновлюватися та адаптуватися до деструктивних впливів. У роботі розкрито генезис і еволюцію поняття «стійкість» у міждисциплінарному вимірі, що дозволило сформувати сучасне розуміння кіберстійкості як емерджентної властивості соціотехнічних систем. Запропоновано авторське визначення кіберстійкості та здійснено теоретичне розмежування категорій «кібербезпека» і «кіберстійкість», доведено доцільність зміщення акцентів із захисту периметра на забезпечення безперервності функціонування критичних процесів. Значну увагу приділено аналізу міжнародного досвіду формування кіберстійкості, зокрема підходів Європейського Союзу, США, Великої Британії та НАТО, що дозволило обґрунтувати напрями гармонізації

національного законодавства із євроатлантичними стандартами. Встановлено, що ефективна система кіберстійкості має базуватися на поєднанні регуляторних, стандартизаційних і ринкових механізмів, які формують цілісну інституціональну архітектуру кіберуправління. У дисертації розроблено концептуальну модель інституціоналізації кіберстійкості, що передбачає інтеграцію державного, приватного та громадянського секторів на засадах спільної відповідальності. Обґрунтовано необхідність розвитку цивільно-військового співробітництва у кіберпросторі, зокрема через впровадження моделі «Cyber-CIMIC», створення інституту цивільного кіберрезерву та запровадження спеціальних правових режимів для залучення недержавних суб'єктів до кібероборони. Окремий блок дослідження присвячено методології аналітичної розвідки у сфері кіберстійкості. Доведено, що ефективне стратегічне управління кіберзагрозами можливе лише за умов синергії методів OSINT, стратегічного форсайту та ризик-орієнтованого підходу. Запропоновано модель інтелектуальної стійкості, яка забезпечує трансформацію даних у стратегічні рішення та підвищує адаптивність національної системи кібербезпеки. На основі емпіричного аналізу здійснено ранжування кіберзагроз за рівнем ризику та визначено пріоритетні напрями зміцнення кіберстійкості України, зокрема у сферах критичної інфраструктури. Розроблено комплексну матричну модель діагностики кіберстійкості, що поєднує функціональні етапи управління інцидентами з операційними доменами системи та дозволяє оцінювати її здатність до відновлення і адаптації. У роботі також досліджено сучасний стан кіберзлочинності, визначено її ключові тенденції, інструменти та кримінологічні детермінанти. Обґрунтовано необхідність переходу до предиктивних моделей протидії кіберзлочинності на основі стратегічного аналізу та ризик-менеджменту. Сформовано наукове бачення щодо формування цілісної теоретико-методологічної концепції кіберстійкості як вищого рівня кібербезпеки, розробки інституціональних, організаційно-правових і кримінологічних засад її забезпечення, а також створення інноваційних моделей оцінювання та управління кіберризиками.

2. The dissertation presents a comprehensive theoretical-legal and criminological study of cyber resilience as a modern paradigm for ensuring the national security of Ukraine in the context of digital transformation and hybrid aggression. It substantiates that the traditional cybersecurity model, focused primarily on incident prevention, proves insufficient under conditions of increasing complexity and multi-vector cyber threats, which necessitates a shift toward the concept of cyber resilience as the ability of a system to anticipate, withstand, recover, and adapt to disruptive impacts. The study explores the genesis and evolution of the concept of "resilience" in an interdisciplinary dimension, which made it possible to formulate a modern understanding of cyber resilience as an emergent property of socio-technical systems. An author's definition of cyber resilience is proposed, and a theoretical distinction between the categories of "cybersecurity" and "cyber resilience" is made, demonstrating the expediency of shifting the focus from perimeter protection to ensuring the continuity of critical processes. Considerable attention is paid to the analysis of international experience in developing cyber resilience, particularly the approaches of the European Union, the United States, the United Kingdom, and NATO, which allowed for the substantiation of directions for harmonizing national legislation with Euro-Atlantic standards. It is established that an effective cyber resilience system should be based on a combination of regulatory, standardization, and market mechanisms that together form a coherent institutional architecture of cyber governance. The dissertation develops a conceptual model for the institutionalization of cyber resilience, which предусматриває integration of the public, private, and civil sectors based on the principle of shared responsibility. The necessity of developing civil-military cooperation in cyberspace is substantiated, in particular through the implementation of the "Cyber-CIMIC" model, the creation of a civil cyber reserve institution, and the introduction of special legal regimes for engaging non-state actors in cyber defense. A separate part of the research is devoted to the methodology of analytical intelligence in the field of cyber resilience. It is proven that effective strategic management of cyber threats is possible only through the synergy of OSINT methods, strategic foresight, and a risk-oriented approach. A model of intellectual resilience is proposed, which ensures the transformation of data into strategic decisions and enhances the adaptability of the national cybersecurity system. Based on empirical analysis, cyber threats are ranked according to their level of risk, and priority directions for strengthening cyber resilience in Ukraine are identified, particularly in the field of critical infrastructure. A comprehensive matrix

model for diagnosing cyber resilience is developed, combining functional stages of incident management with operational domains of the system, enabling the assessment of its capacity for recovery and adaptation. The study also examines the current state of cybercrime, identifying its key trends, tools, and criminological determinants. The necessity of transitioning to predictive models of countering cybercrime based on strategic analysis and risk management is substantiated. A scientific vision is formed regarding the development of a holistic theoretical and methodological concept of cyber resilience as a higher level of cybersecurity, the elaboration of institutional, organizational-legal, and criminological foundations for its provision, as well as the creation of innovative models for assessing and managing cyber risks.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

Стратегічний пріоритетний напрям інноваційної діяльності: Не застосовується

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- 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
- 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.
- 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
- 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
- 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
- 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
- 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
- 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
- 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

- 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
- 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
- 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
- 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
- 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
- Демедюк С.В. OSINT в контексті кібербезпеки. Юридичний бюлетень. 2024. № 34. С.200-207. DOI:10.32850/LB2414-4207.2024.34.26
- 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
- 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
- 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
- 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
- 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
- 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.
- 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.
- Демедюк С.В. Розбудова кіберстійкості на національному рівні. Актуальність та особливості наукових досліджень в умовах воєнного стану: збірник матеріалів ІІІ 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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U103538

VI. Відомості про наукового керівника/керівників (консультанта)

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Карчевський Микола Віталійович
2. Mykola Karchevskyi

Кваліфікація: д.ю.н., професор, 12.00.08

Ідентифікатор ORCID ID: 0000-0002-2693-3592

Додаткова інформація: https://scholar.google.com.ua/citations?user=9_SB4QoAAAAJ&hl=uk; Scopus Author ID: 59125674900

Повне найменування юридичної особи: Заклад вищої освіти "Університет короля Данила"

Код за ЄДРПОУ: 24684167

Місцезнаходження: вул. Євгена Коновальця, Івано-Франківськ, 76018, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Собко Ганна Миколаївна
2. Hanna Sobko

Кваліфікація: д. ю. н., професор, 12.00.08

Ідентифікатор ORCID ID: 0000-0002-5938-3400

Додаткова інформація:

Повне найменування юридичної особи: Одеський державний університет внутрішніх справ

Код за ЄДРПОУ: 08571570

Місцезнаходження: вул. Успенська, Одеса, 65014, Україна

Форма власності: Державна

Сфера управління: Міністерство внутрішніх справ України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Веселов Микола Юрійович
2. Mykola Veselov

Кваліфікація: д. ю. н., професор, 12.00.07

Ідентифікатор ORCID ID: 0000-0002-3963-2764

Додаткова інформація:

Повне найменування юридичної особи: Державний університет економіки і технологій

Код за ЄДРПОУ: 43684645

Місцезнаходження: вул. Медична, Кривий Ріг, Криворізький р-н., 50005, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Конопельський Віктор Ярославович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Конопельський Віктор Ярославович
Відповідальний за підготовку облікових документів	Мельнікова Олена
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна