

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U003650

Особливі позначки: відкрита

Дата реєстрації: 16-07-2026

Статус: Захищена

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Шаронов Андрій Павлович

2. Andrii Sharonov

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0002-1761-9646

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 081

Назва наукової спеціальності: Право

Галузь / галузі знань: право

Освітньо-наукова програма зі спеціальності: 081 Право

Дата захисту: 08-09-2026

Спеціальність за освітою: правознавство

Місце роботи здобувача: Департамент Кіберполіції Національної поліції України

Код за ЄДРПОУ: 40116400

Місцезнаходження: вул. Бориспільська, Київ, 02093, Україна

Форма власності: Державна

Сфера управління: Міністерство внутрішніх справ України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 16249

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: 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:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 10.71, 10.19, 20.56

Тема дисертації:

1. Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект
2. Counteraction to Cyber Threats by the National Police of Ukraine: Organizational and Legal Aspect

Реферат/анотація:

1. Дисертаційне дослідження присвячене комплексному обґрунтуванню та вдосконаленню організаційно-правового механізму протидії кіберзагрозам у діяльності Національної поліції України в умовах цифрової трансформації, воєнного стану та євроінтеграційного курсу держави. Актуальність теми зумовлена тим, що кіберпростір став самостійним середовищем реалізації прав і свобод людини, надання публічних послуг і здійснення управління, водночас перетворившись на простір концентрації загроз, які вирізняються інноваційністю, латентністю, транснаціональністю та здатністю завдавати масштабної шкоди державним інтересам, критичній інфраструктурі та правам громадян. За таких умов проблематика протидії кіберзагрозам виходить за межі суто технічного реагування та набуває ознак самостійної організаційно-правової проблеми, що потребує системного наукового осмислення в контексті діяльності правоохоронних органів. У дослідженні здійснено систематизацію теоретичних підходів до розуміння кіберзагроз як правової категорії та проведено оцінку їх прикладного значення для реалізації задач Національною поліцією України щодо забезпечення публічної безпеки і порядку та протидії кіберзлочинності. Розкрито зміст і ознаки

кіберзагроз, їх місце у сучасному правовому полі, а також обґрунтовано необхідність розмежування суміжних категорій «загроза», «ризик» і «небезпека» у кіберпросторі з метою підвищення визначеності управлінських та процесуальних рішень. Окрему увагу приділено тому, що кіберзагрози у сучасних умовах слід розглядати не лише як передумову вчинення кримінальних правопорушень, а і як чинник дестабілізації публічного управління, підриву довіри до цифрових сервісів та зниження спроможності державних інституцій ефективно виконувати свої функції. У роботі проаналізовано нормативно-правові засади діяльності Національної поліції України у сфері протидії кіберзагрозам, а також встановлено, що багаторівневість і фрагментарність регулювання ускладнюють чітке визначення компетенцій, процедур і меж повноважень, створюють колізії у взаємодії з іншими суб'єктами кібербезпеки та породжують ризики втрати доказової інформації. Доведено, що сучасний стан правового регулювання потребує не лише усунення термінологічної та процедурної неузгодженості, а й формування цілісної моделі функціонального розподілу повноважень між підрозділами Національної поліції України та іншими учасниками національної системи кібербезпеки. На основі аналізу національного законодавства, стратегічних документів у сфері національної безпеки і кібербезпеки, міжнародних стандартів реагування на інциденти та практик міжвідомчої взаємодії сформульовано висновки щодо необхідності посилення координаційної спроможності, стандартизації первинного реагування та вдосконалення процедур обміну інформацією з урахуванням принципів законності, пропорційності та поваги до прав людини. Аргументується висновок щодо доцільності інституційного поєднання двох взаємопов'язаних контурів управління кіберінцидентом: технічного (локалізація, ізоляція, відновлення, забезпечення безперервності) та процесуального (належність, допустимість і достовірність цифрових доказів), що забезпечує баланс між оперативністю реагування та вимогами кримінального процесу. Обґрунтовано, що саме інтеграція цих контурів у межах єдиного організаційно-правового механізму здатна забезпечити результативність реагування на кіберінциденти без втрати доказового потенціалу цифрових даних. У роботі звертається увага, що у період воєнного стану кіберзагрози набувають ознак елементу гібридної війни, а тому підвищуються вимоги до швидкості реагування, режимності доступу до даних, безпеки комунікацій, стійкості організації служби та узгодженості дій із суб'єктами сектору безпеки і оборони; водночас інтенсифікація реагування не повинна зумовлювати звуження процесуальних гарантій, відступ від принципів законності та пропорційності чи зниження стандартів захисту прав і свобод людини. Підкреслено, що технологічний характер кіберінцидентів вимагає узгодження адміністративно-організаційних заходів реагування з кримінально-процесуальними вимогами щодо фіксації, збереження та подальшого використання цифрових даних як доказів. У цьому аспекті встановлено, що воєнний стан істотно трансформує пріоритети поліцейської діяльності у кіберпросторі, посилюючи значення кіберстійкості, безперервності функціонування інформаційних систем і спеціалізованої міжвідомчої взаємодії. Метою дослідження є розроблення науково обґрунтованих теоретичних положень і практичних рекомендацій щодо вдосконалення організаційно-правового механізму протидії кіберзагрозам у діяльності Національної поліції України. Об'єктом дослідження є суспільні відносини, що виникають у сфері протидії кіберзагрозам у діяльності правоохоронних органів; предметом – організаційно-правовий механізм протидії кіберзагрозам у діяльності Національної поліції України.

2. The dissertation research is devoted to the comprehensive substantiation and improvement of the organizational and legal mechanism for countering cyber threats in the activities of the National Police of Ukraine in the conditions of digital transformation, martial law and the European integration course of the state. The relevance of the topic is due to the fact that cyberspace has become an independent environment for the implementation of human rights and freedoms, the provision of public services and the implementation of governance, while at the same time turning into a space of concentration of threats that are distinguished by innovation, latency, transnationality and the ability to cause large-scale damage to state interests, critical infrastructure and citizens' rights. Under such conditions, the issue of countering cyber threats goes beyond a purely technical response and acquires the characteristics of an independent organizational and legal problem, which requires systematic scientific understanding in the context of the activities of law enforcement agencies. The study systematizes theoretical approaches to understanding cyber threats as a legal category and assesses

their applied significance for the implementation of tasks by the National Police of Ukraine to ensure public security and order and combat cybercrime. The content and characteristics of cyber threats, their place in the modern legal field are revealed, and the need to distinguish between the related categories of «threat», «risk» and «danger» in cyberspace is substantiated in order to increase the certainty of managerial and procedural decisions. Special attention is paid to the fact that cyber threats in modern conditions should be considered not only as a prerequisite for committing criminal offenses, but also as a factor in destabilizing public administration, undermining trust in digital services, and reducing the ability of state institutions to effectively perform their functions. The paper analyzes the regulatory and legal framework of the National Police of Ukraine in the field of countering cyber threats, and also establishes that the multilevel and fragmented nature of regulation complicates the clear definition of competencies, procedures and boundaries of authority, creates conflicts in interaction with other cybersecurity entities and generates risks of loss of evidentiary information. It has been proven that the current state of legal regulation requires not only the elimination of terminological and procedural inconsistencies, but also the formation of a holistic model of the functional distribution of powers between the units of the National Police of Ukraine and other participants in the national cybersecurity system. Based on the analysis of national legislation, strategic documents in the field of national security and cybersecurity, international standards of incident response and practices of interagency interaction, conclusions are formulated on the need to strengthen coordination capacity, standardize initial response and improve information exchange procedures, taking into account the principles of legality, proportionality and respect for human rights. The conclusion is argued on the feasibility of institutionally combining two interconnected cyber incident management circuits: technical (localization, isolation, recovery, ensuring continuity) and procedural (appropriateness, admissibility and reliability of digital evidence), which ensures a balance between the efficiency of response and the requirements of the criminal process. It is substantiated that it is the integration of these contours within a single organizational and legal mechanism that can ensure the effectiveness of responding to cyber incidents without losing the evidentiary potential of digital data. The paper draws attention to the fact that during martial law, cyber threats acquire the characteristics of an element of hybrid warfare, and therefore the requirements for the speed of response, data access regime, communication security, stability of the service organization and coordination of actions with security and defense sector entities increase; at the same time, the intensification of the response should not lead to a narrowing of procedural guarantees, a departure from the principles of legality and proportionality, or a reduction in the standards of protection of human rights and freedoms. It is emphasized that the technological nature of cyber incidents requires coordination of administrative and organizational response measures with criminal procedural requirements for the recording, preservation and further use of digital data as evidence. In this aspect, it has been established that martial law significantly transforms the priorities of police activities in cyberspace, enhancing the importance of cyber resilience,

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:

- Шаронов А.П. Трудові функції оперуповноваженого в парадигмі ІЛР: нормативно-практичні описи та кіберкомпонент. Юридичний бюлетень. № 37. 2025. С. 97-106.
- Шаронов А.П. Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. Морська безпека та оборона. № 2 (6). 2025. С. 106-115.

- Шаронов А.П. Міжнародні правові стандарти протидії кіберзагрозам: імплементація та розвиток цифрової стійкості в правовій системі України. Актуальні проблеми вітчизняної юриспруденції. № 6. 2025. С. 119-128.
- Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. Юридичний бюлетень. № 39. 2025. С. 147-155.
- Шаронов А.П., Самойлов С.В., Крайнічук (Шелепало) Г.В. Організаційно-правовий аспект використання відбитку браузеру для заходів кіберзахисту. Наше право. 2026. № 1. С. 42-52.
- Шаронов А.П., Виходець Ю.О., Плахотнюк О.В. Криптоактиви як інструмент обходу санкцій у системі кіберзагроз: блокчейн-аналітика, регуляторно-правові рамки та українська практика. Юридичний бюлетень. 2026. № 41. С. 120-136.
- Шаронов А.П. Дефініційний аналіз суміжних понять «інформаційна безпека» та «кібербезпека». Роль та місце правоохоронних органів у розбудові демократичної правової держави: матеріали XVI Міжнародної науково практичної Інтернет конференції, м. Одеса, 29 березня 2024 року. Одеса : ОДУВС, 2024. С. 556-559.
- Шаронов А.П. Правова природа інтероперабельності як категорії адміністративного права. Стан та перспективи розвитку адміністративного права України: матеріали XI Міжнародної науково-практичної онлайн- конференції, м. Одеса, 24 жовтня 2024 року, Одеса : ОДУВС, 2024. С. 215-216.
- Шаронов А.П. Деякі особливості взаємодії Національної поліції з іншими суб'єктами кібербезпеки в Україні. Стан та перспективи розвитку адміністративного права України: матеріали XII Міжнародної науково практичної онлайн-конференції, м. Одеса, 24 жовтня 2025 року. Одеса : ОДУВС, 2025. С. 307-311.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U103538, 0123U103748

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Швець Дмитро Володимирович

2. Dmytro V. Shvets

Кваліфікація: Доктор юридичних наук, професор, 19.00.06

Ідентифікатор ORCID ID: 0000-0002-1999-9956

Додаткова інформація: <https://scholar.google.com.ua/citations?user=2V6hDowAAAAJ&hl=uk>

Повне найменування юридичної особи: Львівський державний університет внутрішніх справ

Код за ЄДРПОУ: 08571995

Місцезнаходження: вул. Городоцька, Львів, 79007, Україна

Форма власності: Державна

Сфера управління: Міністерство внутрішніх справ України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Рижков Едуард Володимирович
2. Eduard Ryzhkov

Кваліфікація: к. ю. н., професор, 21.07.04

Ідентифікатор ORCID ID: 0000-0002-6661-4617

Додаткова інформація:

Повне найменування юридичної особи: Дніпровський державний університет внутрішніх справ

Код за ЄДРПОУ: 08571446

Місцезнаходження: пр. Гагаріна, Дніпро, Дніпровський р-н., 49005, Україна

Форма власності: Державна

Сфера управління: Міністерство внутрішніх справ України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Ковальова Ольга Вікторівна
2. Olha V. Kovalova

Кваліфікація: д. ю. н., доц., 12.00.09

Ідентифікатор ORCID ID: 0000-0003-4555-0172

Додаткова інформація:

Повне найменування юридичної особи: Донецький державний університет внутрішніх справ

Код за ЄДРПОУ: 08571423

Місцезнаходження: вул. Велика Перспективна, Кропивницький, Кропивницький р-н., 25000, Україна

Форма власності: Державна

Сфера управління: Міністерство внутрішніх справ України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Форос Ганна Володимирівна
2. Hanna V. Foros

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

Ідентифікатор ORCID ID: 0000-0002-9504-3681

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. Домброван Наталія Василівна

2. Nataliia Dombrovan

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

Ідентифікатор ORCID ID: 0000-0001-5997-2080

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:

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Пядишев Володимир Георгійович

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Пядишев Володимир Георгійович

**Відповідальний за підготовку
облікових документів**

Медведенко Надія Василівна

Реєстратор

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна