ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ШАРОНОВ АНДРІЙ ПАВЛОВИЧ

УДК 351.74:004.056(477)

ДИСЕРТАЦІЯ

ПРОТИДІЯ КІБЕРЗАГРОЗАМ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ УКРАЇНИ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

081 – Право
08 – Право

Подається на здобуття ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. _____**А.П. Шаронов**

Науковий керівник – Швець Д.В. доктор юридичних наук, професор

Одеса – 2026

АНОТАЦІЯ

Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 – Право. – Одеський державний університет внутрішніх справ, Одеса, 2026.

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. Методологічну основу становить сукупність загальнонаукових і спеціально-юридичних методів, застосованих для системного опрацювання теоретичних, нормативних і практичних аспектів досліджуваної проблематики. Емпіричну базу становлять матеріали організаційної та правозастосовної практики, статистичні й аналітичні дані про динаміку кіберінцидентів і кіберзлочинності, звіти та рекомендації профільних суб’єктів кібербезпеки. Нормативну основу роботи формують акти національного законодавства, стратегічні документи у сфері національної безпеки, кібербезпеки та цифрової трансформації, а також міжнародні правові й технічні стандарти, релевантні для організації реагування на кіберінциденти та використання електронних доказів.

Наукова новизна полягає у комплексному обґрунтуванні механізму протидії кіберзагрозам Національною поліцією України як системи норм,

інституцій і процедур, спрямованої на забезпечення оперативності реагування, процесуальної якості доказування, ефективної міжвідомчої/міжнародної взаємодії та дотримання прав і свобод людини. Уточнено підходи до класифікації кіберзагроз і критеріїв оцінювання їх небезпечності для потреб поліцейської діяльності, обґрунтовано необхідність стандартизації первинного реагування та контролю ланцюга збереження цифрових даних, сформульовано пропозиції щодо підвищення процесуальної придатності цифрових доказів та мінімізації ризиків втрати доказової інформації. Наукова новизна також виявляється у розробленні цілісного підходу до інституційного поєднання адміністративно-організаційного, процесуального та координаційного елементів протидії кіберзагрозам, що дозволяє розглядати діяльність Національної поліції України у цій сфері як складову модернізації всієї системи публічної безпеки в умовах цифровізації та європейської правової гармонізації.

Практичне значення одержаних результатів полягає в можливості їх використання у правотворчості (уточнення понятійно-категоріального апарату, розмежування компетенцій, формалізація процедур координації та обміну інформацією), у правозастосуванні (удосконалення алгоритмів реагування, документування та збереження електронних доказів), у науково-дослідній роботі та освітньому процесі (підготовка навчально-методичних матеріалів і тренінгових модулів для здобувачів юридичної освіти та працівників НПУ). Практична цінність результатів полягає також у можливості їх використання для розроблення внутрішніх інструкцій, положень, типових алгоритмів міжвідомчої взаємодії, навчальних курсів для працівників кіберполіції, слідчих та оперативних підрозділів, а також для підвищення рівня організаційної спроможності Національної поліції України в умовах зростання інтенсивності кіберінцидентів.

Результатом дослідження є вирішення наукового завдання щодо теоретико-методологічного та організаційно-правового обґрунтування цілісної моделі протидії кіберзагрозам у діяльності Національної поліції України, яка поєднує ризик-орієнтований підхід до реагування, процедурну визначеність

взаємодії з іншими суб’єктами кібербезпеки та належне забезпечення процесуальної придатності цифрових доказів з урахуванням особливостей функціонування держави в умовах воєнного стану та вимог правової гармонізації з європейськими підходами. Запропоновані положення, висновки та рекомендації формують підґрунтя для подальшого вдосконалення організаційно-правового забезпечення діяльності Національної поліції України у сфері кібербезпеки та можуть бути використані як на рівні нормативного оновлення, так і у практиці щоденного реагування на кіберзагрози та кіберінциденти.

Ключові слова: інформація; національна безпека, інформаційна безпека, кібербезпека; оцінка кібербезпеки; загрози; кіберзагрози; кіберзлочини; кіберінциденти; воєнний стан; стандарти реагування; OSINT; штучний інтелект (ШІ).

ABSTRACT

Sharonov A.P. Counteraction to Cyber Threats by the National Police of Ukraine: Organizational and Legal Aspect. – Qualification scientific work, manuscript.

Dissertation for the degree of Doctor of Philosophy in the field of Law, specialty 081 – Law. – Odesa State University of Internal Affairs, Odesa, 2026.

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 multi-level 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, continuity of information systems, and specialized interagency interaction.

The purpose of the study is to develop scientifically based theoretical provisions and practical recommendations for improving the organizational and legal mechanism for countering cyber threats in the activities of the National Police of Ukraine. The object of the study is social relations arising in the field of countering cyber threats in the activities of law enforcement agencies; the subject is the organizational and legal mechanism for countering cyber threats in the activities of the National Police of Ukraine. The methodological basis is a set of general scientific and special legal methods used for the systematic study of theoretical, regulatory and practical aspects of the researched issues. The empirical basis is materials of organizational and law enforcement practice, statistical and analytical data on the dynamics of cyber incidents and cybercrime, reports and recommendations of specialized cybersecurity entities. The regulatory framework for the work is formed by acts of national legislation, strategic documents in the field of national security, cybersecurity and digital transformation, as well as international legal and technical standards relevant to the organization of response to cyber incidents and the use of electronic evidence.

The scientific novelty lies in the comprehensive substantiation of the mechanism for countering cyber threats by the National Police of Ukraine as a system of norms, institutions and procedures aimed at ensuring the efficiency of response, procedural quality of evidence, effective interdepartmental/international interaction and observance of human rights and freedoms. The approaches to the classification of cyber threats and the criteria for assessing their danger for the needs of police activities are clarified, the need for standardization of the initial response and control of the digital data storage chain is substantiated, proposals are formulated to increase

the procedural suitability of digital evidence and minimize the risks of loss of evidentiary information. Scientific novelty is also manifested in the development of a holistic approach to the institutional combination of administrative, organizational, procedural, and coordination elements of countering cyber threats, which allows us to consider the activities of the National Police of Ukraine in this area as a component of the modernization of the entire public security system in the context of digitalization and European legal harmonization.

The practical significance of the results obtained lies in the possibility of their use in lawmaking (clarification of the conceptual and categorical apparatus, delimitation of competencies, formalization of coordination and information exchange procedures), in law enforcement (improvement of response algorithms, documentation and preservation of electronic evidence), in scientific research and the educational process (preparation of educational and methodological materials and training modules for legal students and employees of the National Police). The practical value of the results also lies in the possibility of using them to develop internal instructions, regulations, standard algorithms for interdepartmental interaction, training courses for cyber police officers, investigative and operational units, as well as to increase the level of organizational capacity of the National Police of Ukraine in the context of increasing intensity of cyber incidents.

The result of the study is the solution of the scientific task of theoretical, methodological and organizational and legal substantiation of a holistic model of countering cyber threats in the activities of the National Police of Ukraine, which combines a risk-oriented approach to response, procedural certainty of interaction with other cybersecurity entities and proper provision of procedural suitability of digital evidence, taking into account the peculiarities of the functioning of the state under martial law and the requirements of legal harmonization with European approaches.

The proposed provisions, conclusions, and recommendations form the basis for further improvement of the organizational and legal support for the activities of the National Police of Ukraine in the field of cybersecurity and can be used both at the

level of regulatory updating and in the practice of daily response to cyber threats and cyber incidents.

Keywords: information; national security, information security, cybersecurity; cybersecurity assessment; threats; cyber threats; cyber crimes; cyber incidents; martial law; response standards; OSINT; artificial intelligence (AI).

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Шаронов А.П. Трудові функції оперуповноваженого в парадигмі ILP: нормативно-практичні ориси та кіберкомпонент. *Юридичний бюлетень.* № 37. 2025. С. 97-106. DOI: https://doi.org/10.32850/LB2414-4207.2025.37.13
2. Шаронов А.П. Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. *Морська безпека та оборона.* № 2 (6). 2025. С. 106-115. DOI: https://doi.org/10.32782/msd/2025.2/13
3. 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. DOI: https://doi.org/10.32782/2408-9257-2025-6-18
4. Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. *Юридичний бюлетень.* № 39. 2025. С. 147-155. DOI: https://doi.org/10.32850/LB2414-4207.2025.39.17
5. Шаронов А.П., Самойлов С.В., Крайнічук (Шелепало) Г.В. Організаційно-правовий аспект використання відбитку браузера для заходів кіберзахисту. *Наше право*. № 1. 2026. С. 42-52. DOI: https://doi.org/10.71404/NP.2026.1.6
6. 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.* № 41. 2026. С. 120-136. DOI: https://doi.org/10.32850/LB2414-4207.2026.41.15

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. 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.

8. 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.

9. 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.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВРУ – Верховна Рада України;

КМУ – Кабінет міністрів України;

РНБО – Рада національної безпеки і оборони України;

МВС – Міністерство внутрішніх справ;

Мінцифра – Міністерство цифрової трансформації України;

Мінфін – Міністерство фінансів України;

Мін'юст – Міністерство юстиції України;

НПУ – Національна поліція України;

ДКП – Департамент кіберполіції НПУ;

НКЦК – Національний координаційний центр кібербезпеки;

CERT-UA (Computer Emergency Response Team of Ukraine) – Урядова команда реагування на комп'ютерні надзвичайні події України;

ЗСУ – Збройні Сили України;

ЄС – Європейський Союз;

ООН – Організація Об'єднаних Націй;

OSCE (Organization for Security and Co-operation in Europe) – Організація з безпеки та співробітництва у Європі (ОБСЄ);

EUAM (European Union Advisory Mission) – Консультативна місія Європейського Союзу (КМЄС);

CEPOL – Агентство Європейського Союзу з підготовки співробітників органів правопорядку;

ENISA (European Union Agency for Network and Information Security) – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки;

IACA (International Association of Crime Analysts) – Міжнародна асоціація кримінальних аналітиків;

RTCC (Real-Time Crime Center) – централізований підрозділ поліції, який використовує сучасні технології та аналіз даних для надання миттєвої підтримки;

Data Act – Акт про дані;

ІАД – інформаційно-аналітична діяльність;

ІАЗ – інформаційно-аналітичне забезпечення;

ІКТ – інформаційно-комунікаційні технології;

ОРД – оперативно-розшукова діяльність;

Big Data – великі данні;

ШІ (AI) – штучний інтелект;

ILP (Intelligence-Led Policing) – правоохоронна діяльність, керована аналітичною розвідкою;

OSINT (Open Source Intelligence) – аналіз інформації із загальнодоступних джерел;

SOCTA (Serious and Organised Crime Threat Assessment) – стратегічна оцінка загроз тяжких злочинів та організованої злочинності за методологією Європейського поліцейського офісу (Європолу);

IOCTA (Internet Organised Crime Threat Assessment) – стратегічна оцінка загроз кіберзлочинності в ЄС;

GDPR (General Data Protection Regulation) – загальний регламент ЄС про захист даних;

ОКІ – об’єкт критичної інфраструктури;

NDR (Network Detection and Response) – мережеве виявлення та реагування;

NIS-2 (Network and Information Security Directive 2) – Директива ЄС щодо безпеки мереж та інформації, що встановлює вимоги до багатофакторної автентифікації, шифрування та звітування про інциденти;

EDR (Endpoint Detection and Response) – підсистема захисту кінцевих точок;

SIEM/SOAR – платформи для збору та аналізу подій безпеки (SIEM) і автоматизованого реагування на інциденти (SOAR).

DSA – Закону ЄС Про цифрові послуги.

ВСТУП

Актуальність теми дослідження. Цифрова трансформація держави, економіки та суспільства об’єктивно змістила значну частину суспільних відносин у кіберпростір, який сьогодні функціонує як самостійне середовище реалізації прав і свобод людини, надання публічних послуг, комунікації та управління. Одночасно кіберпростір став простором концентрації загроз, що відзначаються високою інноваційністю, асиметричністю, латентністю, транснаціональністю та здатністю завдавати масштабної шкоди державним інтересам, критичній інфраструктурі, персональним даним та в цілому правопорядку. Для правової системи це породжує новий напрям ризиків: кіберзагрози проявляються не лише як різновид кримінальних правопорушень, а й як фактор підриву публічної безпеки, інформаційної безпеки, довіри до цифрових сервісів і спроможності державних інституцій.

Особливе місце в цьому контексті посідає Національна поліція України як суб’єкт, на який покладено забезпечення публічної безпеки і порядку та протидію злочинності, зокрема в частині виявлення, припинення й розслідування кримінальних правопорушень, учинених у кіберпросторі або з використанням інформаційно-комунікаційних технологій. Однак поточна інституційна модель протидії кіберзагрозам характеризується низкою суперечностей: по-перше, нормативне поле є багаторівневим і фрагментованим, що ускладнює чітке визначення компетенцій, процедур і меж повноважень; по-друге, зростає залежність ефективності протидії від міжвідомчої координації, але механізми взаємодії не завжди забезпечують необхідну оперативність та процесуальну допустимість; по-третє, технологічний характер кіберінцидентів вимагає поєднання адміністративно-організаційного реагування (ізоляція, локалізація, відновлення) із кримінально-процесуальними гарантіями допустимості й належності доказів, що породжує практичні колізії та ризики втрати доказової інформації.

Додатковим чинником актуалізації зазначеної проблеми є нажаль діючий на сьогодні правовий режим воєнного стану, коли кіберзагрози набувають

ознак елементу гібридної війни: кібератаки можуть бути спрямовані на порушення роботи об’єктів критичної інфраструктури, державних реєстрів, систем зв’язку, фінансових сервісів, а також на інформаційно-психологічний вплив. Це підвищує вимоги до швидкості реагування, стійкості організації служби, режимності доступу до даних, безпеки комунікацій та узгодженості дій із суб’єктами сектору безпеки й оборони. Водночас посилення оперативності не повинно призводити до нехтуванням стандартів прав та свобод людини, процесуальних гарантій, принципів законності та пропорційності, що є ключовими для легітимності правоохоронної діяльності в демократичній державі.

Євроінтеграційний курс України обумовлює потребу в наближенні національних механізмів кібербезпеки до європейських підходів: ризик-орієнтованого управління, інституційної взаємодії, стандартів реагування на інциденти, захисту персональних даних і забезпечення безперервності критичних послуг. За цих умов наукове обґрунтування організаційно-правового механізму протидії кіберзагрозам Національною поліцією України набуває не лише прикладної, а й стратегічного значення – як складова модернізації сектору безпеки та правової гармонізації.

Науково-теоретичну основу дослідження склали напрацювання таких науковців, як Авер’янова В.Б., Балтовського О.А., Бандурки О.М., Білоброва Т.В., Бутузова В.М., Воронова І.О., Гнатюка С.О., Грайворонського М.В., Грохольського В.Л., Діордіци І.В., Дороніна І.М., Зінченко О.І., Ісмайлова К.Ю., Калайди А.В., Калюжного Р.А., Корнієнка М.В., Користіна О.Є., Корченко О.Г. Ліпкана В.А., Логінової Н.І., Манжая О.В., Мовчана А.В., Пядишева В.Г., Топчий О.В., Форос Г.В., Хараберюша А.Ф., Хахановського В.Г., Шендрика В.В., Castells M., Maimon D. та інших відомих вчених.

Проте низка питань, пов’язаних із поглибленням методологічного підґрунтя протидії кіберзагрозам у діяльності Національної поліції України, недостатня розробленість на теоретичному рівні організаційно-правових моделей реагування на кіберінциденти та розслідування кіберправопорушень,

потреба у чіткому нормативному визначенні компетенцій і процедур взаємодії НПУ з іншими суб'єктами кібербезпеки (державними органами, CERT/CSIRT, операторами/провайдерами, власниками інформаційних систем), а також наявність колізій і прогалин у регламентації отримання, фіксації, збереження та процесуального використання цифрових доказів зумовили необхідність проведення комплексного дослідження за даною темою.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до основних положень Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 № 392/2020; Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схваленого Указом Президента України від 11.05.2023 № 273/2023; Плану реалізації Стратегії кібербезпеки України, введеним в дію Указом Президента України від 01.02.2022 року № 37/2022; Плану заходів із реалізації Стратегії розвитку Національної поліції України на 2026-2030 роки, затвердженого Наказом Національної поліції України від 21.01.2026 року № 38; Пріоритетних напрямів та завдань (проєктів) цифрової трансформації на 2024-2026 роки, схваленої розпорядженням КМУ від 02.08.2024 № 735-з, Річних планів науково-дослідної діяльності Одеського державного університету внутрішніх справ на період 2023-2028 років «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» № 0123U103538 та кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ на період 2023-2028 років «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період № 0123U103748.

Тема дисертації затверджена на засіданні Вченої ради Одеського державного університету внутрішніх справ (Протокол № 2 від 23 вересня 2024 року).

Мета і завдання дослідження. Метою роботи є розроблення науково обґрунтованих теоретичних положень і практичних рекомендацій

щодо вдосконалення організаційно-правового механізму протидії кіберзагрозам у діяльності Національної поліції України.

Для досягнення зазначеної мети у дисертації поставлено такі **завдання**:

- розкрити правову природу кіберзагроз та їх місце у сучасному правовому полі;
- здійснити класифікацію кіберзагроз і визначити критерії оцінки їх небезпеки у контексті діяльності Національної поліції України;
- проаналізувати міжнародно-правові стандарти боротьби з кіберзагрозами та стан їх імплементації в законодавство України;
- дослідити нормативно-правові засади діяльності Національної поліції у сфері протидії кіберзагрозам;
- оцінити інституційну спроможність та організаційну структуру підрозділів кіберполіції;
- визначити проблеми та виклики організації діяльності Національної поліції у сфері кібербезпеки в умовах воєнного стану;
- обґрунтувати напрями вдосконалення правових та організаційних механізмів протидії кіберзагрозам.

Об'єктом дослідження є суспільні відносини, що виникають у сфері протидії кіберзагрозам у діяльності правоохоронних органів.

Предметом дослідження є організаційно-правовий механізм протидії кіберзагрозам у діяльності Національної поліції України.

Методи дослідження. Методологічну основу дослідження становить сукупність загальнонаукових і спеціально-юридичних методів пізнання. Зокрема, *діалектичний метод* – для комплексного сприйняття і системного опрацювання теоретичних та нормативних положень, що стосуються ґенези та кваліфікації кіберзагроз у сучасному правовому полі (підрозділи 1.1, 1.2); *метод спостереження* – для виявлення й узагальнення закономірностей практики виявлення кіберзагроз (підрозділи 1.2, 3.3); *історико-правовий метод* – для розкриття наукових поглядів на розвиток та правове регулювання інституту кіберзагроз у різні періоди й у різних правових системах (підрозділи 1.1, 1.2, 1.3, 3.1); *компаративний метод* – для порівняльного аналізу

міжнародного досвіду та визначення можливостей його імплементації у національну практику (підрозділи 1.2, 1.3, 3.1, 3.2); *логіко-юридичний метод* – для тлумачення понять, категорій та правових норм, пов'язаних із організаційно-правовими засадами протидії кіберзагрозам НПУ України (підрозділи 1.1, 2.1, 2.2, 3.1, 3.2, 3.3); *метод системного аналізу* – застосовано для дослідження протидії кіберзагрозам Національною поліцією України як цілісного організаційно-правового механізму, що складається з взаємопов'язаних елементів і функціонує в умовах динамічного зовнішнього середовища (кіберпростір, воєнний стан, міжнародні зобов'язання, технічні стандарти реагування) (підрозділи 1.2, 2.2, 2.3, 3.1, 3.2); *догматичний метод* застосовано для дослідження позитивного права у сфері протидії кіберзагрозам – через аналіз змісту правових норм, їх структури, юридичних конструкцій, системних зв'язків, а також правил тлумачення і застосування (підрозділи 1.1, 1.2, 1.3, 2.1, 3.2).

Емпіричну базу дослідження становлять: матеріали правозастосовної та організаційної практики Національної поліції України (узагальнення роботи підрозділів кіберполіції, типові сценарії реагування на інциденти, внутрішні регламенти – у межах доступності); статистичні та аналітичні дані щодо динаміки кіберзлочинності й кіберінцидентів; звіти, методичні матеріали та рекомендації профільних суб'єктів кібербезпеки; результати наукового узагальнення типових проблем взаємодії між правоохоронними та іншими суб'єктами кібербезпеки.

Нормативно-правову основу дослідження склали загальні та спеціальні нормативні джерела: Конституція України, законодавство, що визначає статус, завдання та повноваження Національної поліції України; акти у сфері кібербезпеки, захисту інформації, персональних даних, критичної інфраструктури; міжнародні договори та стандарти, що визначають рамки співпраці, протидії кіберзлочинності та реагування на кіберінциденти.

Наукова новизна одержаних результатів полягає в комплексному обґрунтуванні організаційно-правового механізму протидії кіберзагрозам Національною поліцією України як системи норм, інституцій і процедур, що

має забезпечувати одночасно: оперативність реагування; процесуальну якість доказування; міжвідомчу та міжнародну взаємодію; дотримання прав і свобод людини; адаптацію до умов воєнного стану. У результаті проведеного дослідження сформульовано низку нових концептуальних положень, висновків та рекомендацій, запропонованих особисто здобувачем, які мають важливе теоретичне та практичне значення. Основні з такі:

вперше:

- обґрунтовано комплексне трактування кіберзагроз як самостійного підкласу загроз національній безпеці з подвійною (техніко-юридичною) природою, що поєднує технологічні вектори з юридично значущими наслідками для правового режиму реагування, доказування та комплаєнсу в діяльності НПУ;

- сформульовано авторське визначення «інтероперабельності у кібербезпеці» як системної спроможності технічних, організаційних, процедурних і нормативних компонентів різних суб'єктів забезпечувати узгоджену, безпечну та безперебійну взаємодію на основі гармонізованих стандартів, форматів даних і регламентів обміну інформацією (для створення простору довіри та підтримання кіберстійкості на національному і транскордонному рівнях);

- розроблено концептуальну модель механізму протидії кіберзагрозам у діяльності НПУ як єдиного циклу взаємопов'язаних дій (превенція/моніторинг → виявлення/первинне реагування → оцінювання та пріоритизація → координація → фіксація та збереження цифрових даних → розслідування/процесуальне оформлення → аналіз досвіду та вдосконалення практик), де ключовою умовою результативності визначено стандартизованість первинного реагування та контроль ланцюга збереження;

- доведено доцільність використання превентивних інформаційно-консультаційних онлайн-ресурсів (зокрема chatovi.online) як емпіричного джерела для ідентифікації та уточнення масових соціально-інженерних кіберзагроз із високою латентністю, що має практичне значення для профілактичних і комунікаційних заходів НПУ.

удосконалено підходи:

- до класифікації кіберзагроз для потреб НПУ шляхом операціоналізації багатовимірної моделі (суб'єкт – вектор доступу – тип технічного впливу – об'єкт посягання) із прямою прив'язкою до управлінських рішень (координація, ресурсне планування, пріоритети реагування) та процесуальних вимог (допустимість/доказовість);

- до системи критеріїв оцінювання небезпечності кіберзагроз у поліцейській діяльності через поєднання юридичних та операційних параметрів (імовірність реалізації; організованість/складність; вплив на конфіденційність–цілісність–доступність; швидкість детектування/реагування; потенціал поширення; правові наслідки; репутаційний ефект), що підвищує порівнюваність рішень і прозорість ескалації інцидентів у НПУ;

- до визначення місця НПУ в національній системі кібербезпеки як правоохоронного компонента координаційної моделі, що вимагає процедурно формалізованої взаємодії з іншими суб'єктами кібербезпеки при дотриманні принципів законності, пропорційності та поваги до прав людини;

- до забезпечення процесуальної придатності цифрових даних у протидії кіберзагрозам шляхом акцентування на правомірності способу здобуття й збереження даних, їх відтворюваності та перевірюваності, що обумовлює потребу у стандартизації процедур фіксації, документування та збереження;

- до концептуального вирішення питання допустимості даних, сформованих системами штучного інтелекту, через процесуалізацію таких даних у форматі судової експертизи з виокремленням алгоритмічної (цифрової) експертизи, вимогами до верифікації точності/похибки, умов відтворюваності та документування методик.

дістали подальший розвиток:

- наукові уявлення про співвідношення категорій «загроза», «небезпека» і «ризик» у кіберпросторі через їх прикладне значення для ризик-орієнтованого управління та побудови моделей реагування у публічному управлінні кібербезпекою;

- підходи до гармонізації національного правового регулювання з міжнародними стандартами та практиками (кримінально-правовий, управлінський/ризиковий і правозахисний виміри) через обґрунтування необхідності усунення фрагментарності та термінологічної неузгодженості, а також посилення регулювання щодо ролі приватного сектору, ланцюгів постачання і культури цифрової стійкості;

- організаційно-правові підходи до діяльності кіберполіції у воєнний час через обґрунтування переходу від «ситуативного менеджменту інцидентів» до інституційно закріпленої моделі, що інтегрує: міжвідомчу координацію; внутрішні стандартизовані процедури та мінімальні форензичні вимоги; аналітичне управління ресурсами на основі ILP;

- підходи до інституціалізації «подвійного контуру» управління інцидентом (технічний – безперервність/відновлення; процесуальний – допустимість/доказовість) з розмежуванням ролей і сценаріями залучення слідчих та оперативних працівників НПУ;

- положення щодо нормативного та компетентнісного забезпечення трудових функцій (у парадигмі ILP) шляхом деталізації компетентностей у частині електронних доказів, взаємодії з об’єктами критичної інфраструктури, роботи з криптоактивами, штучним інтелектом, а також NIS2-сумісної взаємодії та ризик-орієнтованих показників результативності;

- підходи до оцінки координаційних ініціатив у кібербезпеці (зокрема проєкт «BRAMA») як практики міжсекторної взаємодії, що має потенціал для нормативного закріплення та інтеграції у загальнодержавну систему протидії кіберзагрозам.

Практичне значення одержаних результатів полягає в тому, що положення, висновки, пропозиції та рекомендації, сформульовані у процесі наукового дослідження, мають прикладний характер і можуть бути використані в низці сфер діяльності державних інституцій. Зокрема:

- *правотворчості* – результати дослідження містять обґрунтовані пропозиції щодо вдосконалення чинного законодавства у сфері протидії кіберзагрозам, зокрема щодо уточнення понятійно-категоріального апарату

(кіберзагроза/кіберінцидент/цифровий слід), розмежування компетенцій Національної поліції України та інших суб'єктів кібербезпеки, а також нормативного закріплення процедур координації, обміну інформацією і реагування на інциденти з дотриманням принципів законності, пропорційності та гарантій прав людини. Реалізація зазначених пропозицій сприятиме підвищенню узгодженості нормативної бази, правової визначеності повноважень і якості правозастосування у секторі безпеки і оборони України;

- *правозастосовній діяльності* – сформульовані у роботі рекомендації можуть бути використані в організації діяльності підрозділів Національної поліції України (насамперед кіберполіції, слідчих та оперативних підрозділів) під час виявлення, припинення та документування кіберінцидентів і кіберзлочинів, удосконалення алгоритмів взаємодії з іншими суб'єктами кібербезпеки, а також стандартизації процесів фіксації цифрових слідів і забезпечення належності, допустимості та достовірності електронних доказів у кримінальному провадженні. Це підвищить оперативність реагування, знизить ризики втрати доказової інформації та посилить керованість міжвідомчих процедур; (акт впровадження Департаменту кіберполіції Національної поліції України від 12.05.2026 року, додаток А);

- *науково-дослідній роботі* – теоретичні узагальнення, методологічні підходи та запропонована модель організаційно-правового механізму протидії кіберзагрозам можуть бути використані як концептуальна основа для подальших досліджень у галузі адміністративно-правового забезпечення діяльності правоохоронних органів у кіберпросторі, зокрема для розроблення критеріїв оцінки небезпеки кіберзагроз, моделей інституційної спроможності кіберпідрозділів, а також для порівняльно-правових досліджень гармонізації національного законодавства з міжнародними стандартами кібербезпеки (акт впровадження Одеського державного університету внутрішніх справ від 01.06.2026 року, додаток А);

- *освітньому процесі* – результати дисертації можуть бути використані при підготовці навчально-методичних матеріалів, спецкурсів і тренінгових модулів для здобувачів юридичної освіти та працівників НПУ (зокрема щодо

правових основ реагування на кіберінциденти, процедур взаємодії, прав людини в цифровому середовищі, роботи з електронними доказами), а також у системі службової підготовки й безперервного професійного розвитку працівників кіберполіції (акт впровадження Одеського державного університету внутрішніх справ від 01.06.2026 року, додаток А).

Особистий внесок здобувача. Дисертаційне дослідження виконано здобувачем самостійно та є завершеною науковою працею. Усі положення, результати, узагальнення й висновки, що виносяться на захист, сформульовані автором особисто. Використання наукових напрацювань інших дослідників здійснено з дотриманням академічної доброчесності: відповідні джерела належним чином процитовано та наведено посилання.

Апробація результатів дисертації. Основні результати дослідження, у тому числі загальні підсумки опрацювання проблематики, її окремі положення, отримані узагальнення та сформульовані висновки, було представлено дисертантом у вигляді доповідей і повідомлень на науково-практичних і науково-теоретичних конференціях: XVI Міжнародній науково-практичній конференції «Роль та місце правоохоронних органів у розбудові демократичної правової держави» (м. Одеса, 29 березня 2024 року); XI Міжнародній науково-практичній онлайн-конференції (м. Одеса, 24 жовтня 2024 року); XII Міжнародній науково-практичній онлайн-конференції (м. Одеса, 24 жовтня 2025 року).

Публікації. Основні положення дисертації опубліковано в 9 працях, серед яких 6 – в наукових фахових виданнях України, визнаних фаховими з юридичних наук, праць апробаційного характеру – 3.

Структура та обсяг дисертації. Дисертація складається із вступу, трьох розділів, що об’єднують 9 підрозділів, висновків, списку використаних джерел (222 найменувань – на 24 сторінці) та 14 додатків – на 24 сторінках. Повний обсяг дисертації становить 233 сторінок, із них основний обсяг тексту – 167 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗАГРОЗ ТА ЇХ ПРАВОВА ПРИРОДА

1.1. Поняття та характеристика кіберзагроз у сучасному правовому полі

Стрімка цифровізація суспільних відносин, гіперзв'язність мережевих середовищ і наростаюча залежність державних та приватних сервісів від інформаційно-комунікаційних технологій породили новий клас ризиків – кіберзагрози, які суттєво відрізняються від традиційних криміногенних явищ нематеріальністю слідів, транскордонністю, масштабованістю та асиметричністю впливу. Невеликі інвестиції з боку зловмисника здатні спричинити системні наслідки для держави або бізнесу, а отже – безпосередньо вплинути на реалізацію конституційних прав і свобод людини, публічну безпеку й національну стійкість. За таких умов кіберзагрози виходять за межі суто технічної проблематики і набувають чітко окресленої правової природи, оскільки саме право встановлює рамки допустимої поведінки, визначає обов'язки суб'єктів цифрових відносин та відповідні санкції за їх порушення.

Відповідно річного Звіту оперативного центру реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України за 2024 рік було приділено особливу увагу 28 тис. критичним подіям інформаційної безпеки, в процесі аналізу яких виявлено та опрацьовано 1042 кіберінцидентів. Найбільш активними у 2024 році були кластери кіберзагроз UAC-0010, UAC-0006 та UAC-0050 згідно з класифікацією Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA. Більш детальна статистика моніторингу кіберінцидентів за категоріями, типами інцидентів, а також технологіями та інструментами виявлення загроз у мережі наведена в Додатку Б[135].

Проведеним аналізом з'ясовано, що серед зафіксованих інцидентів інформаційної безпеки домінують події, пов'язані зі шкідливим програмним забезпеченням, які становлять 58,8% від їх загальної кількості. Частка спроб

несанкціонованого втручання становить 17,6%, а дії зі збору інформації зловмисниками – 12,1%. Інші типи інцидентів формують 8,3%, тоді як порушення цілісності та змісту інформації становлять 2,7%, а інциденти, що впливають на доступність інформаційних ресурсів, – 0,5%. Отримані показники, що характеризують структуру опрацьованих Державним центром кіберзахисту подій у звітний період, дають підстави для визначення ключових пріоритетів у подальшому зміцненні системи кіберзахисту[135].

Тут важливо відмітити, що до кіберінцидентів відносяться події, які входять до Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021. Зазначений перелік призначений для впровадження таксономії як інструменту для обміну інформацією щодо кіберінцидентів та має регулярно переглядатися з урахуванням практики його застосування, появи нових категорій і типів кіберінцидентів, а також інформації, отриманої від суб’єктів забезпечення кібербезпеки[82]. З відповідним переліком кіберінцидентів від CERT-UA та короткої їх характеристикою можна ознайомитися в Додатку В.

Крім того, існує практично одиничний перелік категорій кіберінцидентів Державної служби спеціального зв'язку та захисту інформації України, який може застосовуватись суб’єктами забезпечення кібербезпеки для формування за необхідності власних переліків кіберінцидентів відповідно до специфіки роботи з дотриманням кодування категорій кіберінцидентів, наведених у цьому документі та є обов'язковим для основних суб’єктів забезпечення кібербезпеки при реєстрації, обліку та обміні інформацією про кіберінциденти, передачі звітів до НКЦК, зокрема із використанням автоматизованих платформ обміну інформацією про кіберзагрози. У випадку, коли на початковій стадії реагування кіберінцидент може бути віднесений до декількох категорій, вибирається категорія із більшим рівнем загрози[81].

З відповідним переліком кіберінцидентів Державної служби спеціального зв'язку та захисту інформації України та короткої їх характеристикою можна ознайомитися в Додатку Г[81].

Для порівняння згідно даних Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security, ENISA) в ЄС констатується постійне зростання інцидентів, наприклад у 2012 році їх було 77, в 2020 році – 495, а в 2024 році вже виявлено 1340 інцидентів. З інформацією про типи та секторіальність загроз в ЄС можна додатково ознайомитися в Додатку Є[196].

Для забезпечення правової визначеності важливим є розмежування базових категорій, починаючи в загалі з безпеки до сфери кібербезпеки, а отже і загроз національної безпеки та більш сучасно-технологічних загроз – кіберзагроз.

Категорія «безпека» у сучасному правовому дискурсі розглядається як багатовимірне явище, що охоплює стан захищеності життєво важливих інтересів особи, суспільства і держави від реальних або потенційних загроз. На думку А. Гальчинського та В. Ліпкана безпека трактується як процес постійного збереження балансу між потребами розвитку та здатністю протидіяти ризикам, які можуть ускладнити чи унеможливити цей розвиток. Слушною є думка О.М. Бандурки, який стверджує, що «громадська безпека залежить від виконання спеціальних організаційних правил, встановлених державою з метою попередження тяжких наслідків, які можуть наступити в результаті дій стихійних сил природи або діяльності фізичних та юридичних осіб, пов’язаної з підвищеною небезпекою для життя та здоров’я людей»[1, с. 20].

Сутність національної безпеки охоплює наявність можливості відвернення небезпеки та забезпечення належної захищеності людини, суспільства, держави від будь-яких загроз, а також захист національних інтересів у різних галузях та напрямах. За формою небезпека поділяється на ризики, виклики та загрози[140, с. 94].

У законодавстві України, зокрема в Законі України «Про національну безпеку України», визначається державна безпека, як захищеність державного

суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру[110, ст. 1 п. 4]. Важливо, що вітчизняний законодавець чітко пов'язує безпеку із категорією національних інтересів, які виступають критерієм для ідентифікації загроз та визначення пріоритетів державної політики.

Таким чином, безпека – це не лише статичний стан захищеності, а й динамічна здатність суб'єкта реагувати на нові виклики.

Загрози національній безпеці у науковому вимірі розглядаються як потенційні або реальні чинники, дії чи події, що можуть призвести до підриву стабільності суспільного життя, зниження обороноздатності, економічної спроможності чи рівня правопорядку. Отже, відповідно п. 6 ст. 6 Закону України «Про Національну безпеку України» загроза – це об'єктивно існуюча можливість нанесення шкоди життєво важливим інтересам держави і суспільства, незалежно від того, чи реалізується вона безпосередньо. У законодавчій площині загрози національній безпеці України – це явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України[110, ст. 1, п. 6].

Останні визначаються через систематизовані переліки. Так, у Стратегії національної безпеки України визначено основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації[116, п. 52], а також сформульовані ключові загрози, перерахуємо деякі з них:

- збройна агресія та військові провокації;
- терористична діяльність та гібридні операції;
- кіберзагрози, спрямовані проти критичної інфраструктури;
- корупція, організована злочинність і тіньова економіка;
- інформаційні та психологічні операції, що підривають суспільну довіру та національну єдність[116].

В свою чергу пріоритетами забезпечення кібербезпеки України є:

- убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;
- захист прав, свобод і законних інтересів громадян України у кіберпросторі;
- європейська і євроатлантична інтеграція у сфері кібербезпеки[117, п. 5].

Окрім цього, значна частина поданих визначень кібербезпеки не враховує динамічного характеру кіберзагроз. Більшість підходів орієнтовані на статичні критерії конфіденційності, цілісності та доступності, але не розглядають механізмів адаптації до нових типів атак, таких, які використовують штучний інтелект чи технології квантових обчислень. У цьому контексті українське законодавство виглядає прогресивніше, адже передбачає регулярне оновлення заходів захисту, проте навіть тут не вистачає чітких інструкцій для адаптації політик кібербезпеки до інноваційних технологій[52, с. 57].

Щодо практичної реалізації, то визначення часто сфокусовано на високорівневих принципах, таких, як конфіденційність та цілісність, але проігноровано конкретні механізми їхнього впровадження. Наприклад, Ю.В. Білявська та Я.І. Шестак[4, с. 78-84.] трактують кібербезпеку як систему захисту інформаційної складової, але не пропонують дієвих інструментів для досягнення такого захисту. Це призводить до того, що розуміння стосується переважно теоретичного рівня, а це особливо критично у випадках, коли необхідно швидко реагувати на реальні кіберзагрози[52, с. 57].

Виходячи з вище сказаного кібербезпека виступає одним з ключових пріоритетів у системі національної безпеки України, оскільки забезпечує захист критично важливих інтересів держави та суспільства. Реалізація цього стратегічного напряму здійснюється шляхом інституційного та технологічного посилення національної системи кібербезпеки, спрямованого на ефективне протистояння актуальним і потенційним кіберзагрозам у сучасному динамічному безпековому середовищі. Згідно п. 5 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» термін кібербезпека визначається, як це захищеність життєво важливих інтересів людини і

громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі[114, п. 5 ст. 1].

Забезпечення кібербезпеки є важливим для сталого функціонування інформаційного суспільства, адже воно дає змогу захищати електронні ресурси від несанкціонованого доступу, атак чи порушення їхньої роботи. Це особливо актуально для захисту державної інфраструктури, банківських систем, об'єктів критичної інфраструктури, а також приватних компаній і персональних даних громадян, особливо під час війни[13; 43].

Для зручності розуміння спільного та відмінного в дефініціях «інформаційна безпека» (ІБ) та «кібербезпека» (КБ), розглянемо таблицю нижче[155, с. 556-559].

Параметр аналізу	**Спільне**	**Відмінне**
Онтологічна ідентифікація	Обидва описують стан/спроможність захищеності життєво важливих інтересів	**ІБ:** вся інформаційна сфера (у т. ч. офлайн, медіа). **КБ:** обмежена цифровим середовищем. Орієнтація на виявлення, запобігання й нейтралізацію загроз у кіберпросторі
Логіко-семантичні ознаки	Обидва належать до класу безпеки інформаційної діяльності	**ІБ:** акцент на достовірність/об'єктивність інформації, свобода й права людини в інформаційній сфері, протидія дезінформації та інформаційним операціям. **КБ:** акцент на кіберризиках/інцидентах і стійкості цифрового середовища.
Структурно-реляційний профіль	Мають багаторівневі зв'язки «держава–суспільство–організації–громадяни»	**ІБ:** контентні, правозахисні, інформаційно-комунікаційні відносини. **КБ:** мережеві/технічні відносини, CERT, OT/ICS, IoT.

Контекст і прагматика	Служать цілям нацбезпеки та публічної політики	**ІБ:** протидія дезінформації, забезпечення достовірної інформації. **КБ:** експлуатаційний захист сервісів/мереж, державних і критичних систем, інтернет-екосистеми, реагування на інциденти.
Нормативно-правовий статус	Закріплені в актах державної політики	**ІБ –** значно ширше поняття, ніж **КБ.**
Операціоналізація та вимірюваність	Вимагають індикаторів ефективності та моніторингу	**ІБ:** соціально-правові та контентні показники (доступ/достовірність/захист таємниць). **КБ:** техніко-операційні метрики (MTTD/MTTR, EDR/SIEM, patching, стійкість сервісів).
Темпорально-просторова визначеність	Діють безперервно та системно	**ІБ:** охоплює онлайн- і офлайн-простори. **КБ:** обмежена кіберпростором (мережі, ІКТ, КІК).
Емпіричні приклади	Ілюструються як інцидентами, так і превенцією	**ІБ:** кампанії дезінформації; незаконне розповсюдження секретних даних; обмеження доступу до правдивої інформації. **КБ:** DDoS, фішинг, злам відомчих мереж, атаки.

Таким чином, можна зробити висновок, що інформаційна безпека це широка політико-правова дефініція, яка потребує програмної операціоналізації, кібербезпека ж – чітка просторово-ризикова дефініція, яка легко вимірюється стандартами та процедурами реагування.

Основним критерієм розмежування є середовище та характер загроз: інформаційна безпека охоплює інформаційну сферу (включно з офлайн-контентом і правами людини на інформацію), тоді як кібербезпека стосується ризиків та інцидентів у кіберпросторі та стійкості цифрових сервісів.

Слід зазначити, що процес формування системи кібернетичної безпеки має динамічний, еволюційний характер і за своєю природою не передбачає завершеного стану, оскільки загрозове середовище постійно змінюється під

впливом технологічного прогресу та трансформації моделей злочинної діяльності.

Для державної політики інформаційна безпека визначає стратегічні цілі в комунікаційній та правозахисній площині, а кібербезпека – операційні механізми виявлення/реагування та технічні стандарти[155, с. 256].

При наданні характеристики кіберзагрозам також не можна оминути Закон України «Про критичну інфраструктуру» від 2021 року, який заклав нормативно-правові та організаційні засади функціонування національної системи захисту об'єктів критичної інфраструктури, що є складовою системи національної безпеки. Вказаний акт уперше на законодавчому рівні унормував категоріально-понятійний апарат у сфері забезпечення стійкості, безперервності та захищеності критично важливих об'єктів, інтегрувавши у вітчизняне правове поле сучасні підходи управління ризиками та реагування на загрози. Його положення орієнтовані на формування цілісної моделі захисту, яка поєднує інституційні, технічні та правові механізми. Особливе значення має закріплення принципів моніторингу та своєчасного реагування на інциденти, що створює основу для протидії кіберзагрозам у багатовимірному безпековому середовищі. Таким чином, зазначений закон спрямований не лише на внутрішнє інституційне зміцнення, але й на узгодження українських стандартів із міжнародними підходами у сфері критичної інфраструктури та кібербезпеки[108].

Отже, вразливість системи – це властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи, здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів[102]. Загроза – потенційний механізм або подія, яка за наявності вразливості здатна спричинити шкоду. Інцидент – подія, що вже відбулася та негативно вплинула на CIA-властивості або відповідність встановленим вимогам. Атака – свідомо скоєний інцидент (або їх послідовність), спрямований на досягнення протиправної мети. Таке

розведення понять використовується в аналітичних матеріалах ENISA та закріплене у численних техніко-правових рекомендаціях, забезпечуючи правильну кваліфікацію діяння та розподіл обов'язків між суб'єктами (операторами критичних послуг, провайдерами, уповноваженими органами)[102; 212].

Нині до розгляду питань ризику, загрози та небезпеки застосовують багато різних підходів. У наукових дослідженнях простежується підхід, за якого поняття загроз та небезпек розглядаються як тотожні. Такої думки дотримуються Г.Б. Клейнер[83, с. 31-43], Ю.Г. Лисенко[64].

Професор В.А. Ліпкан характеризує небезпеку як «діяльність, спрямовану на реалізацію загроз, що здатна спричинити дестабілізацію системостворюючих елементів, які самі як такі загрожують функціонуванню та розвитку об'єкту безпеки у момент їх спричинення або при звичайному своєму протіканні закінчуються або можуть закінчитися колапсом його і відповідної системи безпеки»[66, с. 39]. При аналізі визначення, запропонованого В.А. Ліпканом, виникає сумнів, чи завжди небезпеку слід пов'язувати з діяльністю. Вона може бути прогнозуванням наслідків дії стихійних чинників, сил природи, бездіяльності суб'єкта і т.ін. Тому, скоріше, небезпеку слід розглядати як стан, при якому стає можливою реалізація загроз[132, с. 260].

На відміну від небезпеки загроза має більш конкретну форму. Автори теоретико-методологічних досліджень з питань теорії безпеки одностайні у думках, що загроза – це категорія, близька за сутністю до категорії «небезпека», але відмітною особливістю її є більш конкретна форма за рівнем впливу на об'єкт дії. За визначенням А. Кузьменко[63, с. 1-21], «загроза – це кінцева стадія несприятливих умов, після яких спричиняється шкода». В роботі Міжвідомча готовність державного сектору України до ШІ-підсилених кіберзагроз та іноземних інформаційних операцій під авторством Авдєєвої А., Майбороди В., Мисишина А, Ковтуна В., Хрущової Д.[74, с. 7] при формулюванні загрози авторами робиться акцент на обов'язковість настання несприятливих наслідків у випадку відсутності заходів щодо їх запобігання. Становить інтерес визначення загрози, сформульоване В.А. Ліпканом[65; 66], який стверджує, що

загроза, хоча і свідчить про існування або можливість виникнення негативних наслідків, але не переростає у діяльність, безпосередньо спрямовану на її здійснення. Це висловлення не суперечить логічній послідовності формування ступеню ймовірності розвитку негативних подій, але підкреслює обмеженість загрози діями, «які підкріплюють її, але не переростають у діяльність»[65, с. 39].

На відміну від В.А. Ліпкана, А. Пекін вважає, що результатом загрози є порушення структури, функцій, джерел існування об'єкта[83, с. 31-43]. Таке твердження викликає сумніву вже тому, що у такому випадку загроза з потенційно можливої стає дією, здатною вчинити шкоду[132, с. 261].

Серед вітчизняних науковців І.П. Мігус та С.М. Лаптєв розрізняють поняття «загроза» та «ризик». Під загрозою вони розуміють певну подію, що впливає на діяльність суб'єктів господарювання, а ризик є результатом впливу загроз на господарську діяльність суб'єктів господарювання[73].

Навіть якщо брати етимологію цих термінів, то можна побачити, що згідно онлайн-бібліотеки «Горох», в якій зібрані найкорисніші словники української мови, термін «загроза» походить від праслов'янського *groza* – «грім, грозова буря, небезпечне явище природи». У старослов'янській мові слово «гроза» означало як природне явище, так і метафоричне уособлення небезпеки. Префікс «за-» додавав значення наближення, передвісника події. Відтак, «загроза» у семантичному полі означає потенційне наближення небезпечного явища або дії**[**39].

У сучасних тлумачних словниках термін трактується як «потенційна можливість заподіяння шкоди». У правовій доктрині – це «стан, за якого існує ймовірність вчинення дії, здатної завдати шкоди правам, інтересам чи безпеці»[72].

Слово «небезпека» має складену структуру: заперечна частка *«не»* + корінь *«без»* (у значенні «відсутність») + *«пека»* (праслов'янське *рекъ* – «піклування, захист»). Таким чином, етимологічно «небезпека» означає «відсутність захисту», «стан без охорони»[8].

У староукраїнських текстах воно вживалося у значенні «загроза життю, шкода, руйнівна дія». З часом зміст змістився у напрямі позначення будь-якої ситуації, що становить потенційну чи реальну шкоду для людини, суспільства чи держави. У сучасному тлумаченні «небезпека» – це реальний або потенційний стан, що створює умови для шкоди[8]. У кримінально-правовому аспекті – це категорія, яка характеризує суспільно шкідливі явища, здатні порушувати правопорядок[61].

Таким чином, етимологічно «загроза» більше пов'язана з попередженням *і* очікуванням негативної події, тоді як «небезпека» відображає стан вразливості або ризику, а також незважаючи на семантичну схожість категорій «виклик», «ризик», «небезпека» і «загроза», кожна з них визначає різний ступінь можливості заподіяння збитку[5, с. 96].

Правова природа кіберзагроз проявляється у «подвійному» вимірі. З одного боку, це фактичне явище, що характеризується технічною реалізацією впливу: шкідливе програмне забезпечення (ransomware, wipers, spyware), експлуатація вразливостей, DDoS, компрометація ланцюга постачання (supply chain), порушення налаштувань хмарних сервісів, соціальноъ інженерія (фішинг, вішинг, deepfake-маніпуляції). З іншого – це правова категорія, яка отримує нормативний зміст завдяки обов'язкам з управління ризиками, інцидент-репортингу, збереження доказів, аудиту, мінімізації даних і дотримання принципів захисту персональних даних через вбудовання в технології, процеси та системи ще на етапі їх проєктування «privacy by design/default». Саме спосіб реалізації загрози визначає, які норми матеріального й процесуального права будуть застосовані: від кримінально-правових складів (ст. 361-363-1 КК України)[61] до адміністративно-правових і договірних механізмів відповідальності (зокрема у сфері персональних даних та послуг електронної довіри)[89; 104].

У сучасній українській та зарубіжній доктрині термін кіберзагроза не має єдиної канонічної дефініції, так питання дефініції та змістовного наповнення терміну «кіберзагроза» набули особливої актуальності після прийняття Закону України «Про основні засади забезпечення кібербезпеки України»[114], який

закріпив базові правові орієнтири у цій сфері. А отже в національному законодавстві термін кіберзагроза визначається, як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів[114, ст. 1 п. 6].

Хоча слід відзначити, що функціонування національної системи кібербезпеки забезпечується комплексом організаційних, правових та технічних заходів, серед яких особливе місце займає впровадження єдиної (універсальної) системи індикаторів кіберзагроз. Така система дозволяє здійснювати систематизований моніторинг, своєчасне виявлення та реагування на потенційні кіберінциденти. Її запровадження відповідає сучасним тенденціям гармонізації національної нормативно-правової бази з міжнародними стандартами у сфері кібербезпеки та кіберзахисту (зокрема, стандартами ISO/IEC 27000-series, рекомендаціями ЄС та НАТО).

Впровадження універсальної системи індикаторів кіберзагроз має подвійне значення: з одного боку, воно формує єдину методологічну основу для суб'єктів сектору безпеки і оборони України, а з іншого – сприяє інтеграції у світову систему кіберзахисту, що дозволяє забезпечувати сумісність та обмін інформацією з міжнародними партнерами. У цьому контексті варто наголосити, що єдина система індикаторів виступає ключовим інструментом у процесі прогнозування кіберзагроз, підвищення стійкості критичної інфраструктури та зміцнення довіри до національної системи безпеки у цілому.

Українські дослідники розглядають кіберзагрози як складний соціально-правовий і техніко-правовий феномен, що поєднує у собі не лише потенційні деструктивні впливи на інформаційно-телекомунікаційні системи, але й ширший спектр ризиків для публічної безпеки, державного управління та прав людини. Так, В. Цимбалюк розглядає кіберзагрози як сукупність умов і факторів, що створюють можливість заподіяння шкоди інформаційним ресурсам, системам управління та суспільним відносинам у кіберпросторі[153].

О. Довгань та І. Доронін досліджують кіберзагрози як фактори, що ескалюють ризики для національних інтересів України, зумовлюють необхідність правового регулювання та інституційної відповіді[25].

Мазур Я. аналізує кіберзагрози як складову інформаційної війни, пов'язує з поняттями кіберзлочинності, кібертероризму та діяльності кіберполіції[69].

Доцільно розглядати кіберзагрози як постійно еволюціонуючи, адаптивні вектори атак, які потребують постійного оновлення та підвищення заходів захисту для забезпечення надійності та стійкостіцифрового простору[169].

Міжнародні стандарти (див. Додаток О) та практика правозастосування розуміють кіберзагрозу через ризик-орієнтоване управління, технічні та організаційні аспекти, а Доктрина Castells M. розширює категорію до соціально-правового явища[171-174].

У Будапештській конвенція не міститься прямого визначення «кіберзагрози», але криміналізовані діяння (несанкціонований доступ, втручання, використання шкідливих інструментів) фактично окреслюють правову природу загроз[56].

Загальний регламент про захист даних (GDPR ЄС) прямого визначення терміну «кіберзагрози» не надає, але кіберзагрози розглядаються як ризики для прав і свобод суб'єктів персональних даних у контексті безпеки їх обробки[213].

У фундаментальній трилогії The Information Age: Economy, Society and Culture (1996-1998) («The Rise of the Network Society»[174], «The Power of Identity»[173], «End of Millennium»[172]) Castells M. наголошує, що розвиток інформаційних технологій створює нову архітектуру влади та ризиків, в яких підкреслюється, що мережеве суспільство вразливе до загроз у кіберпросторі, оскільки ключові процеси (економічні, політичні, комунікаційні) перемістилися в електронне середовище. Окремо у книзі Communication Power (2009) Castells M.[171] аналізує інформаційні війни, пропаганду, кібератаки як інструменти політичного впливу, тобто Castells M. розглядає кіберзагрози не лише як технічну категорію, а як соціально-правове і політичне явище,

пов’язане з контролем над інформаційними потоками, безпекою особи й держави, а також транснаціональною конкуренцією[9].

Відповідно п. 8 ст. 2 Акту про кібербезпеку ЄС кіберзагроза означає будь-яку потенційну обставину, подію або дію, яка може пошкодити, порушити або інакше негативно вплинути на мережеві та інформаційні системи, користувачів таких систем та інших осіб[130, п. 8 ст. 2].

Отже, проведеним аналізом ми дійшли до висновку, що:

1. Кіберзагрози на сьогодні сформувались як окремий, специфічний різновид загроз національній безпеці, який якісно відрізняється від традиційних криміногенних явищ нематеріальністю слідів, транскордонністю, масштабованістю та асиметричністю впливу. Вони безпосередньо корелюють із рівнем цифровізації публічного управління, економіки та суспільних комунікацій, а відтак здатні істотно впливати на реалізацію конституційних прав і свобод людини, функціонування критичної інфраструктури, стійкість держави в умовах збройної агресії та гібридних загроз.

2. Уточнення базового категоріального апарату («безпека», «національна безпека», «небезпека», «загроза», «ризик») показало, що кіберзагрози слід розглядати як окремий підклас загроз національній безпеці, що поєднує в собі стан вразливості (наявність системних слабких місць) і потенційну можливість реалізації деструктивних подій у кіберпросторі. Етимологічне й доктринальне розмежування понять «загроза» та «небезпека» дозволяє визнати першу більш «динамічною» категорією, пов’язаною з прогнозуванням та ймовірністю настання шкідливих наслідків, тоді як «небезпека» фіксує стан уже наявної вразливості або дефіциту захищеності. Це важливо для побудови адекватних моделей ризик-орієнтованого управління в сфері кібербезпеки.

3. Співвідношення інформаційної безпеки та кібербезпеки свідчить про їхню системну, але не тотожну природу. Інформаційна безпека має ширший, політико-правовий і комунікаційний вимір, охоплюючи як онлайн-, так і офлайн-середовище, права людини на інформацію та протидію дезінформації. Кібербезпека, навпаки, характеризується чіткою просторово-ризиковою

визначеністю, фокусується на стійкості цифрових сервісів, мереж та інформаційно-комунікаційних систем, використовує стандартизовані технічні та організаційні метрики (виявлення, запобігання, реагування, відновлення). Таким чином, кіберзагрози є концентрованим проявом загроз інформаційній безпеці саме в цифровому середовищі, які піддаються формалізованому вимірюванню й регулюванню.

4. Нормативний аналіз засвідчив, що українське законодавство заклало базові правові орієнтири для класифікації кіберзагроз, про які більш детально піде вже у п. 1.2 нашого дослідження. Закон України «Про основні засади забезпечення кібербезпеки України», акти у сфері національної безпеки та захисту критичної інфраструктури, підзаконні акти щодо виявлення вразливостей і категоризації кіберінцидентів, а також профільні стратегії (національної безпеки, кібербезпеки) формують інтегровану, хоча й таку, що продовжує розвиватися, систему правового регулювання. У ній кіберзагроза визначається як явище або чинник, що створює небезпеку життєво важливим національним інтересам у кіберпросторі та негативно впливає на стан кібербезпеки держави і кіберзахист її об’єктів. Таким чином, відбувається «юридизація» технічних феноменів, коли подія в мережі набуває ознак юридичного факту, що тягне відповідні обов’язки та відповідальність.

5. Статистичні дані Державного центру кіберзахисту Держспецзв’язку України та ENISA демонструють не лише сталу тенденцію зростання кількості кіберінцидентів, а й структурну домінанту шкідливого програмного забезпечення, спроб несанкціонованого доступу та інформаційного розвідзбору, що підтверджує перехід до системних, багатоходових атак на державний і приватний сектори. Ці емпіричні показники обґрунтовують необхідність формування єдиної для суб’єктів сектору безпеки та оборони України системи індикаторів кіберзагроз, гармонізованої з міжнародними стандартами (ISO/IEC 27000-series, NIS2, підходи ЄС і НАТО), що є передумовою інтероперабельності та ефективного міжнародного обміну даними про загрози.

6. Правова природа кіберзагроз має подвійний – техніко-юридичний – вимір. З одного боку, кіберзагроза проявляється у конкретних технологічних векторах (шкідливе ПЗ, експлуатація вразливостей, DDoS, компрометація ланцюгів постачання, атаки на хмарні сервіси, соціальна інженерія тощо). З іншого – вона детермінує застосування комплексу матеріально-правових і процесуальних норм: кримінально-правових складів у сфері несанкціонованого доступу й втручання в роботу систем, адміністративно-правових вимог до управління ризиками, інцидент-репортингу, збереження цифрових доказів, аудиту, дотримання принципів захисту персональних даних «за задумом» та «за замовчуванням». Це зближує кіберзагрози з категоріями «правовий ризик» і «регуляторний комплаєнс» та підкреслює їх інтегрованість у сучасну модель верховенства права в цифровому середовищі.

7. Узагальнюючи викладене, кіберзагрози доцільно визначити як зумовлені використанням кіберпростору потенційні або реальні деструктивні впливи на інформаційно-комунікаційні системи, ресурси та пов’язані з ними суспільні відносини, які за наявності вразливостей здатні завдати шкоди життєво важливим інтересам людини, суспільства і держави. Вони виступають результатом взаємодії технічних, організаційних, правових та соціальних факторів, а їхнє належне правове врегулювання потребує узгодженого застосування національних та міжнародних норм, стандартів і практик. Такий підхід створює методологічне підґрунтя для подальшого дослідження механізмів адміністративно-правового забезпечення протидії кіберзагрозам, зокрема – ролі та повноважень підрозділів кримінального аналізу Національної поліції України у системі кібербезпеки держави.

1.2. Класифікація кіберзагроз та критерії оцінки небезпеки кіберзагроз у контексті роботи Національної поліції України

Проаналізувавши основні підходи до визначення змісту самого поняття кіберзагрози, доцільно перейти до їх системної класифікації, оскільки саме вона забезпечує можливість структурованого розуміння природи, джерел та

механізмів реалізації таких загроз. Зазначена класифікація виступає необхідним інструментом для формування ефективної моделі кіберзахисту, визначення пріоритетів реагування та оптимізації розподілу ресурсів Національною поліцією України в сфері забезпечення інформаційної безпеки в цілому.

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

- невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

- недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

- безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

- недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки[22; 116].

У сучасній науковій літературі та нормативно-правових актах виокремлюють низку критеріїв, за якими здійснюється поділ кіберзагроз. До найпоширеніших належать: походження загрози (внутрішні та зовнішні), характер впливу (цілеспрямовані та випадкові), спосіб реалізації (технічні, програмні, соціоінженерні), рівень складності та організованості (індивідуальні, групові, державні), а також наслідки для інформаційних ресурсів (порушення конфіденційності, цілісності чи доступності).

І.В. Діордіца виділяє такі сновні етапи формування системи захисту національної інфраструктури від кіберзагроз:

1) визначення основних понять та їх нормативне закріплення;

2) визначення критеріїв віднесення об’єктів до критично важливих;

3) укладання переліку таких об’єктів;

4) оцінка ризиків безпеки (здійснювалася або централізовано, або галузевими міністерствами відповідно до єдиної методики, розробленої науковими установами на замовлення державних органів);

5) планування заходів безпеки на основі результатів оцінювання ризиків із метою оптимізації витрат[79, с. 96].

У Стратегії кібербезпеки України закріплено 4-ри основні групи кіберзагроз:

1. Загрози державного рівня – дії спецслужб іноземних держав, спрямовані на підрив національної безпеки.

2. Кримінальні кіберзагрози – діяльність організованих злочинних угруповань, фінансові шахрайства, незаконні втручання у роботу інформаційних систем.

3. Терористичні кіберзагрози – використання кіберпростору для дестабілізації суспільно-політичної ситуації або ураження критичної інфраструктури.

4. Соціотехнічні загрози – маніпуляції у соціальних мережах, поширення дезінформації, використання соціальної інженерії[94].

Професор М.В. Грайворонський поділяє кіберзагрози на наступні види:

- таргетовані атаки;

- кібертероризм;

- кібервійни;

- хактивізм;

- атаки на банківські системи;

- атаки на електронний уряд[12, с. 17].

Оцінка небезпеки кіберзагроз здійснюється на основі поєднання кількісних та якісних критеріїв. Серед ключових:

- масштаб впливу – локальний, регіональний, національний або міжнародний рівень інциденту.

- ймовірність реалізації – прогнозна оцінка ймовірності здійснення атаки на основі розвідувальних даних та статистики інцидентів (OSINT, SIGINT).

- рівень збитків – матеріальні, репутаційні, політичні чи соціальні наслідки для держави та громадян.

- об’єкти посягання – чи належить ресурс до об’єктів критичної інфраструктури.

- час відновлення (RTO/RPO) – здатність системи повернутися до нормального функціонування[9].

У сучасному правовому полі України виділяються такі ключові групи кіберзагроз:

1. Кримінально-правові кіберзагрози – протиправні діяння, пов’язані з використанням інформаційних технологій: несанкціонований доступ до інформаційних систем, створення та поширення шкідливого програмного забезпечення, кібершахрайство, незаконне втручання в роботу телекомунікаційних мереж. Відповідальність за такі діяння передбачена у Розділі XVI Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку[61].

2. Національно-безпекові кіберзагрози – деструктивні дії проти державних органів, об’єктів критичної інфраструктури та сектору безпеки й оборони. До цієї категорії належать атаки з боку іноземних держав чи організованих груп, кібершпигунство, дезінформаційні кампанії, гібридні загрози, спрямовані на підрив суверенітету та територіальної цілісності України[114].

3. Економічні кіберзагрози – шахрайство у сфері електронних платежів, атаки фінансових установ, підрив довіри до електронної комерції, використання технологій для відмивання коштів, фінансування тероризму та війни.

4. Соціальні та гуманітарні кіберзагрози – поширення фейкових новин, маніпулятивного контенту та пропаганди в соціальних мережах, що

формує ризики для інформаційної безпеки суспільства, впливає на політичні процеси та громадську думку.

Особливістю сучасного правового поля України є поєднання національних та міжнародних підходів до ідентифікації і класифікації кіберзагроз. Україна активно інтегрує положення Європейського Союзу (Директива NIS2[183], Регламент GDPR[192]), а також практику НАТО та ОБСЄ. Це сприяє гармонізації термінології, уніфікації стандартів і процедур, що дозволяє підвищити ефективність співпраці у сфері кіберзахисту.

В умовах гібридної війни проти України та інтенсивної цифровізації публічного сектору та критичної інфраструктури, побудова єдиного, формально верифікованого підходу до типологізації загроз і їх вимірюваної оцінки є ще більше актуалізується та є необхідною передумовою інтелектуально-керованого поліцейського управління, кримінального аналізу та взаємодії з іншими суб'єктами сектору безпеки і оборони. Нормативні імперативи для такого підходу випливають, з одного боку, із права ЄС (Директива ЄС) 2022/2555 – NIS2)[183], що встановлює вимоги до управління ризиками та інцидент-менеджменту, з іншого – з українського законодавства, яке визначає правові засади кібербезпеки та захисту критичної інфраструктури, включно зі Стратегією кібербезпеки України[117]. Саме ці рамки окреслюють обов'язки суб'єктів у частині ідентифікації, оцінювання і зниження ризиків, а також організацію обміну інформацією про загрози між відомствами, що безпосередньо стосується НПУ як споживача та продуцента розвідувально-аналітичних даних.

Від початку 2025 року CERT-UA фіксує в середньому близько 15 кіберінцидентів на день та відслідковує понад 150 кластерів кіберзагроз (UAC). Основним джерелом кібератак залишається росія. Окрім цього, спостерігається активність з білорусі, Китаю, КНДР та, на жаль, з боку груп, що діють з тимчасово окупованих територій України. Основні типи хакерської кіберактивності містять:

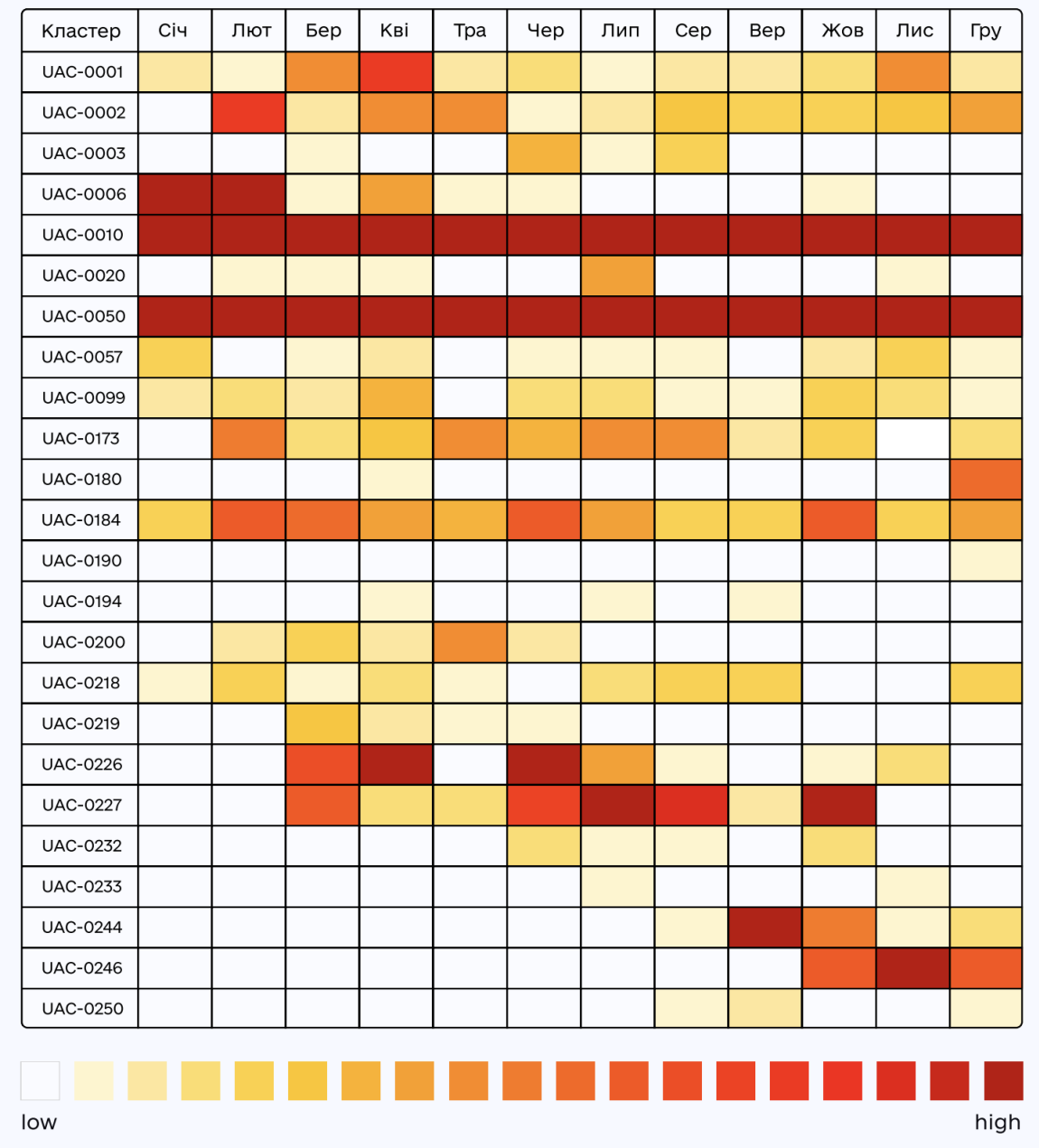
- шпигунство. Переважно російське, спрямоване на будь-які сфери, особливо енергетичну та військову.

- саботаж. Кібертероризм, що впливає на кожного громадянина країни.
- фінансово вмотивовані злочини. Спрямовані на викрадення коштів різними способами та під різноманітними формами.
- інші специфічні атаки, наприклад, атаки на нотаріусів[77].

Згідно аналітичному збірнику Державної служби спеціального зв'язку та захисту інформації України за ІІ півріччя 2025 року – «Кіберзагрози: Україна» інтенсивність кіберінцидентів загалом залишалася на рівні І півріччя 2025 року, хоча їх загальна кількість дещо зменшилася (див. таблицю нижче)[49, с. 9]:

Рівень критичності	H1 2025	H2 2025	Зміна за період
Критичний	1	0	-100%
Високий	6	5	-17%
Середній	2 944	2895	-2%
Низький	67	9	-87%
Загалом	**3 018**	**2 909**	**-4%**

Для наочного відображення розподілу кіберінцидентів за окремими кластерами кіберзагроз нижче наведено теплову карту інтенсивності (HeatMap), яка відображає загальну кількість кіберінцидентів, атрибутованих до відповідних кластерів, та дозволяє оцінити відносну активність різних угруповань (див. таблицю нижче)[49, с. 12]:



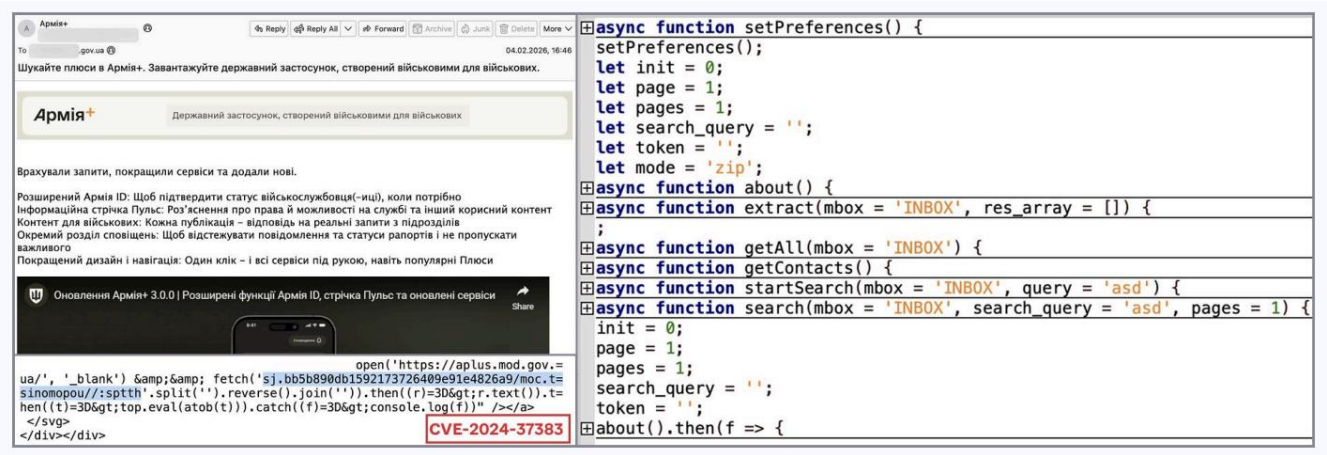
Для відображення тенденцій активності окремих кластерів кіберзагроз в Додатку Е наведено теплову карту, що демонструє динаміку кіберінцидентів, атрибутованих до цих кластерів, у розрізі місяців 2025 року.

На сьогодні фіксується формування нових кластерів кіберзагроз, що продовжує тенденцію початку 2025 року. Зафіксовано як нові підходи до кібершпигунства, так і кібератаки з використанням вірусів-вимагачів (Ransomware). Водночас актуальною залишається активність, пов’язана з експлуатацією zero-click вразливостей.

Так, активність Zero-clickers: UAC-0233, UAC-0250 зафіксована ще у першому півріччі 2025 року, та використання вразливостей Roundcube (CVE-

2024-37383 та CVE-2025-49113) – при відкритті листа через веб-інтерфейс Roundcube код не лише виконається без жодних дій з боку користувача, а ще й не буде відображений. Подібні листи не викликають підозри, якщо не дивитись через поштовий клієнт чи оригінал листа (в форматі eml) в текстовому редакторі[133, с. 17].

Щонайменше з кінця вересня 2025 року зафіксовано серію кампаній, пов'язаних з експлуатацією zero-click вразливостей у поштовому сервері Zimbra. У межах різних атак зловмисники використовували вразливості CVE-2025-48700 та CVE-2025-66376, експлуатація яких забезпечує виконання шкідливого коду без потреби будь-якої взаємодії з боку користувача. У разі успішної компрометації зловмисники отримували доступ до вмісту поштових скриньок, включно з листуванням, яке збиралося у TGZ-архів, резервними кодами багатофакторної автентифікації, паролями застосунків, а також глобальною адресною книгою. Зазначена активність відстежується під ідентифікатором UAC-0250 (див. нижче приклад активності UAC-0233)[49, с. 15-16].



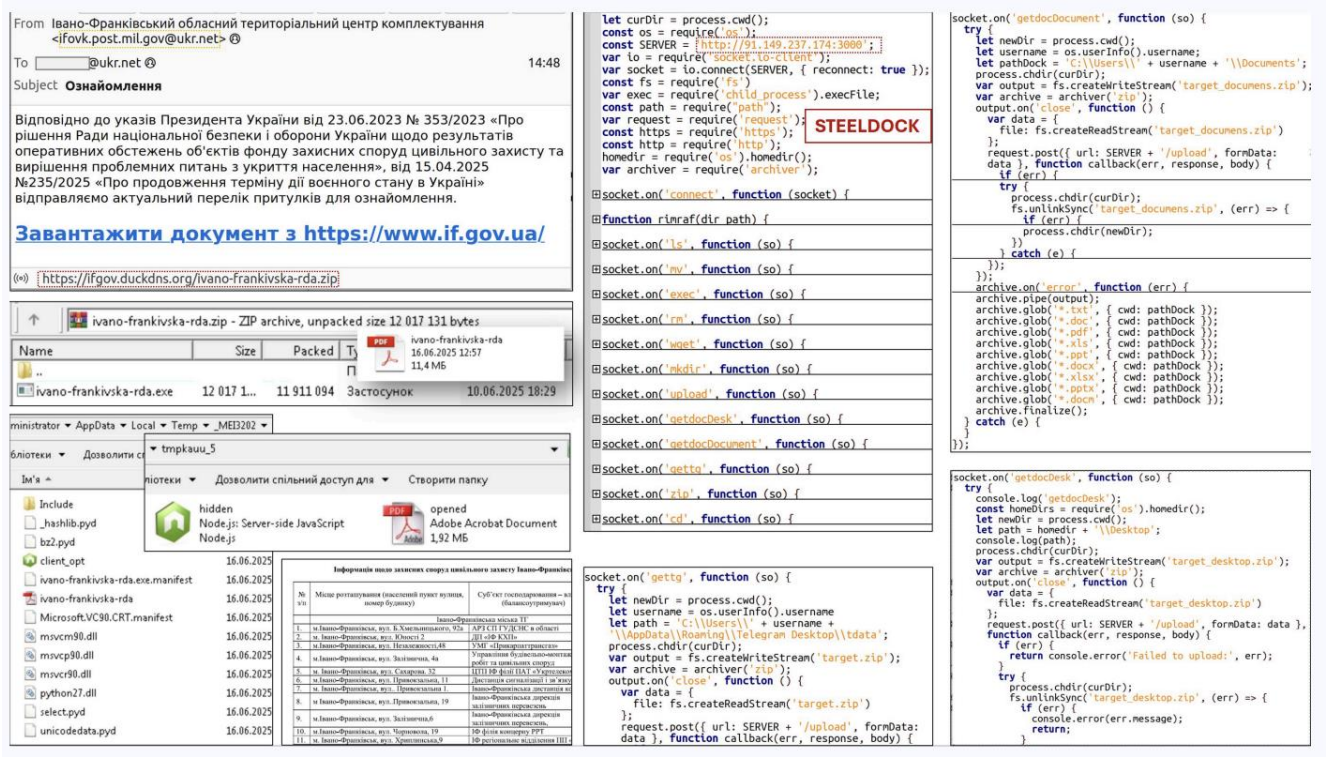
Інший кластер активних кіберзагроз – Кібервимагачі: UAC-0238, UAC-0243 з липня 2025 року здійснювало атаки проти органів місцевого самоврядування, шифруючи дані на ЕОМ з операційною системою Windows за допомогою програм із сімейства Proton. Первинний доступ до інформаційно-комунікаційних систем (ІКС) зловмисники отримували через доступні з мережі Інтернет інтерфейси для адміністрування, переважно RDP. Перед шифруванням файлів хакери видаляли тіньові копії (shadow copies) операційної системи, що

унеможливлювало відновлення даних із їх використанням. Щодо кіберзагрози UAC-0243, точкою входу зазвичай слугує вразливий сервер Microsoft[49, с. 16].

Також, зафіксовано появу нових кіберзагроз – Кібершпигуни: UAC-0232, UAC-0246[49, с. 17], спрямованих на здійснення кібершпигунства. Це свідчить про збереження стратегічної мети росії щодо отримання розвідувальної інформації будь-якими способами.

Основними об’єктами інтересу залишаються інформаційні ресурси сил безпеки та оборони, урядових органів, а також органів місцевого самоврядування.

Цікавим підходом вирізняється угруповання UAC-0232. Кожна з його кампаній була націлена на окремий регіон України. Серед державних установ відповідної області здійснювалася розсилка електронних листів із посиланням на веб-сторінку, що імітує офіційний сайт обласної військової адміністрації, де нібито розміщено перелік захисних споруд. Замість очікуваного документа завантажується архів із виконуваним файлом, що містити шкідливе програмне забезпечення STELLDOCK, яке поєднує функціонал стілера та бекдору (зокрема забезпечує збір даних і виконання обмеженого набору команд на інфікованому комп’ютері). Приклад активності UAC-0232 (див. нижче)[49, с. 17].



Сучасні емпіричні дані, які враховує Національна поліція України в своїй практиці, підтверджують зміщення домінуючих векторів атак у бік соціальної інженерії, фішингових кампаній із використанням скомпрометованої поштової скриньки та зловмисних вкладень/посилань, що ініціюють дистанційне встановлення шкідливого ПЗ, у тому числі з функціоналом віддаленого доступу та деструктивних компонентів[147]. CERT-UA у 2023-2024 роках регулярно фіксувала масштабні хвилі фішингу, у тому числі кампанії UAC-0028/APT28[151] проти органів державної влади та секторів оборони, а також атаки проти окремих професійних груп (наприклад, нотаріусів), що віддзеркалює пріоритет розвідувального та підривного впливу на державні інституції[150].

Як вже зазначалось в нашому дослідженні для Національної поліції України, яка виконує як правоохоронні, так і превентивно-аналітичні функції, питання чіткої класифікації кіберзагроз є ключовим з огляду на необхідність стандартизації оперативно-аналітичної діяльності та розробки ризик-орієнтованих моделей протидії злочинності.

А так як наведене можливо зробити тільки після чіткої типологізації кіберзагроз, що дозволить сформувати структурований підхід до їх виявлення, прогнозування та нейтралізації у діяльності правоохоронних органів, зокрема підрозділів Департаменту кіберполіції Національної поліції України.

Систематизація загроз у кіберпросторі повинна ґрунтуватися не лише на технічних характеристиках атак, але й на суб’єктах їх походження, мотивації та можливих наслідках для державної безпеки, що відповідає сучасним європейським та національним стандартам стратегічного управління ризиками.

Під час дослідження ми дійшли висновку, що кіберзагрози можна поділити на наступні групи, так до першої групи належать *державні (геополітичні) кіберзагрози,* що генеруються іноземними розвідувальними та військово-спеціальними структурами (APT-групами), які застосовують кібершпигунство, підривні операції та інформаційно-психологічний вплив з метою втручання у державне управління, процеси критичної інфраструктури та

стратегічної комунікації. Саме ця категорія становить найвищий рівень ризику, оскільки поєднує технологічний та політичний компоненти впливу.

До другої групи можна віднести *кримінальні кіберзагрози*, які формуються у результаті діяльності організованих злочинних угруповань і транснаціональних кібергруп, що здійснюють фінансові шахрайства, атаки типу програма-вимагач, програма-здирник, програма-шантажист, викрадення персональних даних та несанкціоноване втручання в інформаційно-комунікаційні системи з метою отримання матеріальної вигоди. Для цієї групи характерна динамічна еволюція використовуваних інструментів, високий рівень конспірації та використання тіньових цифрових ринків.

Окремою групою є *терористичні та екстремістські кіберзагрози*, які передбачають використання кіберпростору для планування, координації або реалізації атак на об’єкти критичної інфраструктури, поширення радикальної ідеології, вербування та дестабілізації суспільно-політичної ситуації. Такі загрози орієнтовані не лише на фізичне завдання шкоди, а й на створення атмосфери страху, паніки чи недовіри до державних інститутів. Наприклад, вербування для здійснення підривної діяльності на ТЦК.

Не менш значущими є *соціотехнічні та інформаційно-психологічні кіберзагрози*, які проявляються у формах маніпуляцій у соціальних мережах, дезінформаційних кампаніях, використанні технологій соціальної інженерії, включно з фішингом та deepfake. Ця категорія загроз є найбільш складною для ідентифікації, оскільки спрямована на вплив на когнітивну сферу громадян та підрив інформаційної довіри в суспільстві.

Також суттєву небезпеку становлять і *внутрішні (інсайдерські) кіберзагрози,* пов’язані з діями співробітників, підрядників або інших осіб, які мають законний доступ до інформаційних систем. Такі загрози можуть мати як умисний, так і ненавмисний характер, призводячи до витоку конфіденційної інформації, саботажу або порушення цілісності процесів інформаційної безпеки.

З огляду на зростаючу складність технічного середовища, окремо виокремлюються *технологічні та техногенні кіберзагрози*, зумовлені

вразливостями програмного забезпечення, помилками конфігурації, з перебоями в роботі автономних систем, штучного інтелекту та інтернету речей. Їх особливість полягає у можливості спричинення каскадних інцидентів, які впливають одночасно на значну кількість об’єктів.

Отже, для співробітників НПУ, на наш погляд доцільно використовувати багатовимірну класифікацію кіберзагроз, яка забезпечує як таксономічну повноту, так і придатність до оперативного застосування.

Перший напрям класифікації – за природою та мотивацією правопорушника: державні й квазідержавні структури, організовані кіберзлочинні угрупування, ідеологічно мотивовані об’єднання та одиночні виконавці.

Другий напрям – за способом проникнення: соціальна інженерія/фішинг, компрометація ланцюгів постачання, використання вразливостей у публічних сервісах, зловмисні макроси/скрипти, «living-off-the-land». Цей напрям безпосередньо корелює з рекомендаціями ENISA щодо домінантних трендів.

Третій напрям – за типом технічного впливу: кібершпигунство та збір даних, криптографічне або логічне блокування ресурсів (ransomware, wiper), підміна даних та маніпуляція доказовою інформацією, порушення доступності сервісів (DDoS), підрив довіри через цільові інформаційні операції у соціальних медіа.

Четвертий напрям – за об’єктом посягання: інформаційні системи та реєстри, цифрові канали комунікації, мобільні пристрої, вузли взаємодії з іншими органами (прокуратура, суд, міграційні служби), а також об’єкти критичної інфраструктури, де НПУ виконує функції досудового розслідування та координації реагування. Зазначена класифікація узгоджується з європейським тенденціями про міжсекторальний характер ризиків і вимогу NIS2 до впровадження «appropriate and proportionate technical, operational and organizational measures» з урахуванням профілю загроз[185].

Окремої уваги потребує динамічний розподіл загроз за рівнями – від мікрорівня (таргетовані атаки на окремого працівника або підрозділ) через мезорівень (секторні та міжвідомчі інциденти, що зачіпають взаємодію НПУ з

іншими органами) до макрорівня (кризові події на критичній інфраструктурі національного масштабу). Саме мезо- і макрорівень уможливлюють правове застосування категорій «суттєвих/важливих суб'єктів» за NIS2 та критеріїв критичності за українським законом про критичну інфраструктуру, що визначають вимоги до обов'язкової звітності, безперервності надання послуг і стійкості. У цьому розрізі діяльність НПУ як координатора слідчих дій і як провайдера аналітики для ситуаційних центрів має спиратися на єдину термінологічну базу і пороги ескалації[183].

Також, для оцінювання небезпечності кіберзагроз у поліцейському середовищі ключовим є перехід від дескриптивної типології до кількісно-якісної оцінки ризику з визначеними метриками, порогами та процедурами ухвалення рішень. На методологічному рівні доцільно поєднувати підходи ISO/IEC 27005 (ідентифікація активів, джерел загроз, вразливостей, сценаріїв впливу та визначення обсягу ризику)[32] та NIST SP 800-30 (оцінювання імовірності загрози та величини впливу на трьох рівнях управління)[208] з адаптацією до завдань НПУ.

За методологією оцінки ризиків NIST ієрархія управління ризиками представляється як спрощений трирівневий підхід, який полегшує розуміння процесу оцінки ризиків NIST:

Рівень 1. Організаційний, який розглядає всю організацію, включаючи бізнес-моделі, організаційну структуру та довгострокові цілі. Основні елементи:

- формування корпоративної стратегії управління ризиками;
- визначення ролей і відповідальності;
- затвердження політик, стандартів, рамкових підходів;
- інтеграція ризик-менеджменту в систему управління організацією;
- встановлення критеріїв прийнятності ризиків.

Рівень 2. Місії та бізнес-процесів, який досліджує конкретні сфери, такі як продажі та маркетинг для компаній, отже, надає контекстуальну інформацію, яка часом може бути дуже корисною. Основні елементи:

- моделювання бізнес-процесів з урахуванням ризиків;

- визначення критичності кожного процесу;
- формування вимог до інформаційних систем.

Рівень 3. Інформаційних систем, який зосереджений на технічних аспектах, таких як інформаційні системи, програми та потоки даних. На цьому рівні проводяться:

- ідентифікація активів;
- оцінка загроз і вразливостей;
- розрахунок ризиків;

впровадження технічних і процедурних заходів безпеки;

- моніторинг та реагування на інциденти.

Таким чином, NIST забезпечує єдину методологічну логіку ризик-менеджменту, де стратегія, процеси та технології взаємопов’язані й взаємозалежні.

Складність полягає в забезпеченні узгодженості цих рівнів один з одним, оскільки розуміння контекстуально релевантних ризиків на кожному рівні є важливою передумовою для проведення ефективного аналізу ризиків[78].

Крім того, емпіричні показники для налаштування порогових значень критеріїв можуть базуватися на офіційній статистиці кіберінцидентів та загальновизнаних індикаторах загроз. Аналітичні звіти ENISA за 2023-2024 роки засвідчують домінування фішингу як основного способу первинного доступу, зростання використання легітимних системних інструментів у зловмисних цілях, посилення атак на ланцюги постачання та поєднання кібероперацій з інформаційно-психологічним впливом. Зазначені тенденції відповідають українській практиці, що підтверджується попередженнями CERT-UA та статистикою опрацьованих інцидентів.

Для НПУ це означає, що вага критеріїв «детектовність» та «скритність до фіксації події» має підвищуватися, а індикатори – охоплювати не лише сигнатурні події, а й поведінкові аномалії у хмарних офісних пакетах, месенджерах і мобільних ОС.

Впровадження запропонованої моделі для співробітників НПУ потребує єдиного глосарію, матриці відповідності категорій загроз до TTPs, карти активів

поліцейських інформаційних систем, а також регламентів ескалації за порогами оцінки. Джерелом первинних даних виступають як відкриті звіти (ENISA Threat Landscape), так і національні попередження CERT-UA та внутрішня телеметрія; їх інтеграція здійснюється через процеси SIEM/SOAR із підтримкою таксономій STIX/TAXII та MITRE ATT&CK. Методологічно обґрунтовано періодичний перегляд ваг критеріїв залежно від тенденцій загроз і змін у нормативному середовищі. Для цілей доказового права у кримінальному провадженні окремо регламентується зберігання метаданих оцінки ризику й артефактів детектування, що забезпечує відтворюваність та аудит[183].

З огляду на євроінтеграційний курс, класифікація та критерії оцінювання, які застосовуються співробітниками НПУ, мають бути сумісними з підходами ЄС та НАТО, що полегшує транскордонний обмін даними про інциденти та взаємодію з CSIRT-мережами. Стратегічний орієнтир на відповідність NIS2 та розвиток національної системи захисту критичної інфраструктури створює підґрунтя для уніфікації протоколів реагування та навчання персоналу, а також для побудови показників зрілості ризик-менеджменту, які можуть бути інспектовані зовні. Така уніфікація, у свою чергу, підвищує доказову силу цифрових слідів і знижує ризик процесуальних втрат при документуванні кіберзлочинів[183].

Актуальність дослідження ШІ-посилених кіберзагроз зумовлена тим, що використання генеративного штучного інтелекту істотно підвищило масштабованість, персоналізацію та переконливість соціально-інженерних атак і фішингу. Європейське агентство з кібербезпеки (ENISA) відносить штучний інтелект до елементів сучасного ландшафту загроз, а британський NCSC підкреслює, що в останні півтора року дослідники фіксують нові техніки, пов’язані з повністю автоматизованими цільовими фішинговими, автоматизацією посткомпрометаційних стадій та ексфільтрації даних[185; 186; 200].

У змістовому аспекті ШІ-посилені кіберзагрози доцільно розглядати як різновид гібридних загроз, у межах яких алгоритми штучного інтелекту використовуються для автоматизованого збору відомостей про цільову особу,

побудови її цифрового профілю, генерування переконливого синтетичного контенту, імітації реальної комунікації та масштабування злочинного впливу. Найбільш поширеними формами таких загроз є ШІ-посилена соціальна інженерія та ШІ-посилений фішинг. ENISA окремо наголошує, що новітні технології, зокрема штучний інтелект і машинне навчання, спрощують аналіз поведінки користувачів і дають змогу здійснювати більш таргетовані фішингові атаки[184].

Для України ця проблематика має додаткову актуальність у зв'язку з необхідністю одночасної протидії кіберзагрозам та інформаційним операціям в умовах війни. Офіційні міжнародні безпекові домовленості України 2024-2026 років прямо фіксують потребу зміцнення стійкості до інформаційних загроз, дезінформації та кібербезпеки штучного інтелекту. Це означає, що ШІ-посилені кібератаки мають розглядатися не ізольовано як технічний феномен, а як елемент ширшого комплексу гібридних впливів на державні інституції, критичну інфраструктуру та суспільну довіру[143; 144; 147].

Отже, хочемо виділити насьогодні специфічні форми загроз:

1. Планування та проведення інформаційних атак за допомогою ШІ.

В рамках таких атак ШІ використовують, перш за все, для збору інформації та планування інформаційних операцій. Це включає як вивчення інформаційного простору і популярних наративів, так і профілювання аудиторії, категоризацію груп залежно від їх вразливостей. Не менш небезпечною є соціальна інженерія, підсилена ШІ, та створення чат-ботів, основним завданням яких є введення користувачів платформ в оману для отримання різного роду інформації. Існує багато випадків, коли за допомогою технологій клонування голосу та дипфейків створювалися фейкові персони, що маскувалися під відомих людей з метою виманити комерційну чи секретну інформацію (для прикладу голосовий клон мера Києва Віталія Кличка, чи екс-президента України Петра Порошенка).

2. Генерування підробленого та маніпулятивного контенту за допомогою ШІ.

ШІ використовується для підробки будь-якого виду контенту: візуального та аудіовізуального (фото та відео), аудіального (звукозаписи) та текстового. При цьому, часто різні способи комбінують для створення клонів – сторінок реальних людей і навіть цілих ресурсів, на кшталт популярних медіа. Окрім клонів реальних особистостей ШІ використовується і для створення підробних сторінок, зображення та вся інформація на яких ніколи не існувала насправді. Вони можуть використовуватися для подальшого масштабування FIMI-кампаній. Важливо розуміти, що найчастіше потерпілими від діпфейків стають публічні особи, відомі блогери і журналісти. Щодо текстових підробок, небезпечна тенденція спостерігається у підвищенні якості автоматизованого перекладу FIMI-наративів різними мовами.

3. Використання ШІ для здійснення інфраструктурних атак та атак на ШІ-системи.

Такі атаки передбачають пошук вразливостей на різних етапах життєвого циклу систем ШІ та експлуатація таких прогалин. Наприклад, їх можуть націлювати на навчальні дані або навпаки – спробувати «отруїти» інформацію, серед якої ШІ-система здійснює пошук (наприклад, створюючи тисячі фейкових сторінок та вебсайтів з дезінформацією у Google та інших пошуковиках). Популярними також є «злами» обмежувачів ШІ за допомогою правильно введених промптів, внаслідок чого генеративні системи починають видавати заборонений контент. Крім того, інфраструктурні атаки часто містять шкідливе або шпигунське програмне забезпечення, яке за допомогою ШІ стає більш адаптивним та здатним обходити захист програмного забезпечення. Часто такі файли розміщуються у відкритих джерелах та оснащуються додатковими спроможностями обходити детектори (як-от проходити Captcha та інші верифікатори). Зрештою, ШІ часто використовується для поширення та масштабування фішингових атак, спрямованих як на отримання конфіденційної інформації, так і віддаленого доступу до пристроїв. Інколи такі ШІ-фішингові атаки здійснюються на державних службовців за допомогою методу імперсоніфікації високопосадовців[74, с. 26-27].

У процесі аналізу сучасних форм кіберзагроз доцільним є використання матеріалів відкритих інформаційно-аналітичних онлайн-ресурсів превентивного спрямування, які систематизують типові сценарії онлайн-шахрайства та інших ризиків цифрового середовища. До таких ресурсів належить, зокрема, спеціалізована онлайн-платформа chatovi.online, що функціонує як консультаційний та інформаційний майданчик з питань безпеки онлайн-комунікацій та протидії шахрайським практикам у мережі Інтернет[127].

Матеріали зазначеного ресурсу мають прикладний характер і ґрунтуються на узагальненні найбільш поширених схем соціальної інженерії, фішингових атак, маніпулятивних цифрових сервісів та інших форм неправомірного впливу на користувачів. У науково-дослідницькому контексті такі матеріали можуть розглядатися не як нормативне чи доктринальне джерело, а як емпіричний індикатор актуальних типів кіберзагроз, з якими стикаються громадяни та правоохоронні органи у повсякденній практиці[127].

З огляду на це, інформація, що міститься на платформі chatovi.online, є релевантною для уточнення класифікації кіберзагроз за критеріями способу вчинення, спрямованості впливу та характеру заподіяної шкоди. Особливу цінність такі ресурси становлять для ідентифікації масових соціально-інженерних кіберзагроз, що характеризуються високим рівнем латентності та потребують поєднання правоохоронних і превентивно-інформаційних заходів реагування з боку Національної поліції України.

Підсумовуючи, науково обґрунтована класифікація кіберзагроз для НПУ має виходити з багатовимірної моделі, що поєднує учасників, вектори доступу, типи технічного впливу та об’єкти посягання, і бути операціоналізованою через критерії оцінювання небезпечності, узгоджені з міжнародними стандартами ризик-менеджменту та національним/європейським правовим полем. Пропонована система критеріїв – імовірність, організованість впливу на CIA і довіру до даних, часові параметри детектування й реагування, потенціал поширення, правові наслідки, репутаційний ефект – забезпечує порівнюваність рішень, прозорість ескалації та підвищує якість кримінально-аналітичного

процесу. Її регулярне оновлення на основі звітів ENISA, попереджень CERT-UA та статистики інцидентів дозволяє підтримувати актуальність у мінливому середовищі загроз і одночасно забезпечувати відповідність вимогам NIS2 та українського законодавства щодо стійкості та безперервності надання послуг.

1.3. Міжнародно-правові стандарти боротьби з кіберзагрозами та механізми їх імплементації в законодавство України

У попередніх розділах ми вже торкалися питань дії міжнародних нормативних документів, що регулюють відносини у сфері інформаційної безпеки та ролі поліції в її забезпеченні, але для висвітлення можливих прогалин у минулих підрозділах та сприйняття більш цілісною картини, присвятим цей пункт нашого дослідження аналізу основних міжнародно-правових актів і стандартів у сфері протидії кіберзагрозам та визначим їх вплив на формування національної системи кібербезпеки України. А також розглянемо механізми адаптації та імплементації цих стандартів у українське законодавство з метою гармонізації з європейським та глобальним правовим полем із відповідними рекомендаціями до національного законодавства.

Необхідно зазначити, що міжнародно-правові стандарти у сфері кібербезпеки сформувалися як відповідь на транснаціональний характер кіберзлочинності та уразливість глобальної цифрової інфраструктури.

У колективній монографії «Світова гібридна війна: український фронт», підготовленій експертами Національного інституту стратегічних досліджень, звертається увага на те, що частка кібертероризму в світі зростає, а його вплив на національну та міжнародну безпеку стає все більш відчутним. DDoS-атаки на сайти урядів (США, Канади, Південної Кореї, Ізраїлю, Естонії та ін.), державних і приватних компаній (NASA, Delta Air Lines, Dell, Yahoo, Amazon, E-bay, Sony, CNN) та міжнародних організацій (ООН, МОК)[134] відбуваються все частіше.

Міжнародний досвід правового регулювання кібербезпеки, представлений у звіті IFES Ukraine «Cybersecurity in Ukraine: Legal Framework

Analysis», демонструє необхідність адаптації кращих світових практик до українських реалій[181]. Дослідження підкреслює важливість гармонізації національного законодавства з європейськими директивами та міжнародними конвенціями у сфері кібербезпеки. Особливо актуальним є впровадження стандартів звітності про кіберінциденти та створення національної системи сертифікації засобів кіберзахисту відповідно до міжнародних стандартів [68, с. 168].

Особливо актуальним є впровадження стандартів звітності про кіберінциденти та створення національної системи сертифікації засобів кіберзахисту відповідно до міжнародних стандартів:

Критерій	**Міжнародні стандарти / акти**	**Ключовий акцент**	**Адаптація для України**
Гармонізація законодавства	ЄС: NIS2, GDPR, ENISA; РЄ: Будапештська конвенція (+2-й протокол); США: NIST CSF 2.0; НАТО: Tallinn Manual	Перехід до ризик-орієнтованої моделі + «governance»	– імплементація NIS2 та GDPR у національне законодавство – вдосконалення закону «Про основні засади кібербезпеки України» – узгодження з Будапештською конвенцією для міжнародного співробітництва – впровадження NIST-подібних стандартів для критичної інфраструктури
Звітність про інциденти	NIS2, ISO/IEC 27035; підходи CISA/CIRCIA	Строки NIS2: 24h/72h/≤1 місяць	– впровадження обов’язкового повідомлення про атаки для держорганів та критичних об’єктів – використання ISO/IEC 27035 для національних протоколів реагування
Сертифікація / довіра до ІТ	ЄС Cybersecurity Act + схеми сертифікації (EUCC);	Сертифікація як умова закупівель і доказ безпеки	– розробка національної системи сертифікації з урахуванням ENISA та Common Criteria

	ISO/IEC 15408 (CC); крипто-стандарти (FIPS-підхід)		– впровадження стандартів для державних за-купівель IT-рішень – партнерство з НАТО для сертифікації військових кіберсистем
Міжнародна співпраця	НАТО CCDCOE; європейські координаційні мережі; Будапештська конвенція + 2-й протокол	Прискорення доступу до е-доказів та обміну	– участь у міжнародних платформах (наприклад, CCDCOE) – підписання угод про кіберрозслідування з ЄС та США – інтеграція з системами раннього попередження NATO (на кшталт Malware Information Sharing Platform)
Критична інфраструктура	ЄС: CER + NIS2; практики CISA; PPP-моделі	CER = стійкість критичних суб'єктів ширше за кібер	– впровадження сегментації мереж за зразком NERC CIP (США) – розвиток Public-Private Partnerships (PPP) для захисту енергосистеми – використання рекомендацій Світового банку для реформ у фінансовому секторі
Управління та відповідальність	NIS2, NIST CSF 2.0 (GOVERN)	Відповідальність керівництва, навчання, контроль виконання	закріпити ролі власника ризику, KPI/аудит, обов'язкове навчання управлінців у держсекторі/КІ
Фінансовий сектор	DORA (ЄС)	Операційна цифрова стійкість, контроль ІКТ-аутсорсингу	виділити фінсектор окремо: тестування стійкості, вимоги до провайдерів, інцидент-менеджмент
Безпека цифрових продуктів	Cyber Resilience Act (CRA)	«Security-by-design», управління вразливостями, supply-chain	вимоги до продуктів з цифровими елементами для держзакупівель/КІ; контроль ланцюгів постачання

Одним із перших комплексних документів, що сформували уніфіковані підходи до криміналізації діянь у кіберпросторі, стала Конвенція Ради Європи

про кіберзлочинність 2001 р. (Будапештська конвенція)[56]. Вона встановила мінімальні стандарти щодо криміналізації неправомірного доступу до комп'ютерних систем, незаконного перехоплення даних, умисного втручання в дані та системи, комп'ютерного шахрайства, а також окреслила процесуальні повноваження правоохоронних органів щодо збереження, вилучення та міжнародного обміну електронними доказами. Основними положеннями Конвенції є[56]:

1. Уніфікація складів кіберзлочинів, таких як:

- незаконний доступ до інформаційних систем (ст. 2 Конвенції Про кіберзлочинність ЄС);
- незаконне перехоплення (ст. 3 Конвенції Про кіберзлочинність ЄС);
- втручання в дані та системи (ст. 4-5 Конвенції Про кіберзлочинність ЄС);
- підробка та комп'ютерне шахрайство (ст. 7-8 Конвенції Про кіберзлочинність ЄС)[56].

2. Процесуальні повноваження для розслідування, включно з:

- швидким збереженням трафіку та даних;
- вилученням цифрової інформації;
- міжнародним доступом до даних.

3. Механізми міжнародного співробітництва, зокрема через мережі 24/7 контактних пунктів.

Кількісні показники діяльності Європолу відображаються у щорічних звітах про оперативні результати, що містять дані щодо підтриманих розслідувань, арештів, вилучень активів та обміну інформацією. У 2024 році агентство підтримало 3324 операції, вилучено активів на 1,4 млрд євро та збільшено обмін інформацією SIENA на 18% в таких пріоритетних сферах, як організована злочинність, тероризм, кіберзлочинність та фінансові злочини, що перевищує внутрішні цілі та відображає розширену координацію з державами-членами ЄС та третіми країнами[177]. Це включало сприяння діяльності 65 оперативних цільових груп, які об'єднують розвідувальні дані та ресурси для боротьби з мережами з високим рівнем загрози[36].

Як слушно підкреслює M. Gercke, Будапештська конвенція стала «глобальною моделлю кримінально-правової реакції на кіберзлочинність», оскільки поєднала три компоненти: гармонізацію складів злочинів, розширення процесуальних інструментів та інституціалізацію міжнародної співпраці[190]. Аналогічного висновку дотримуються F. Calderoni та інші дослідники, наголошуючи, що цінність Конвенції полягає не лише у встановленні переліку кіберзлочинів, а й у створенні сталої основи для взаємної правової допомоги між державами у справах про кіберзлочини. Для України участь у Будапештській конвенції означає обов'язок адаптувати кримінальне законодавство (насамперед розділ XVI КК України)[61] до її стандартів та забезпечити можливість використання спеціальних процесуальних інструментів у розслідуванні кіберправопорушень.

Наступними міжнародно-правовими документами є акти Європейського Союзу, які спрямовані на забезпечення кіберстійкості мереж та інформаційних систем, насамперед Директива ЄС 2022/2555 (NIS2). Документ встановлює вимоги до управління ризиками та безпеки мереж і інформаційних систем для «суттєвих» та «важливих» суб'єктів у критичних секторах (енергетика, транспорт, фінанси, охорона здоров'я, державне управління, цифрові послуги тощо), запроваджує обов'язкові внутрішні політики кіберзахисту, процедури інцидент-репортингу, вимоги до корпоративного управління та персональної відповідальності керівництва[183].

Наукові та експертні джерела зазначають, що Директива NIS2 фактично формує «європейський периметр кібербезпеки», у межах якого держава та приватний сектор зобов'язані діяти за єдиними стандартами ризик-менеджменту, моніторингу та реагування на кіберінциденти. NIS2 стала першою директивою, яка встановила обов'язкову кіберстійкість не тільки держави, а й бізнесу, що означає вихід за межі класичного державоцентричного підходу[215].

Значною мірою NIS2 вписується у ширший блок регуляторних ініціатив ЄС, спрямованих на безпеку цифрових продуктів і даних. До нього належить, зокрема, Regulation (EU) 2023/2854 (Data Act)[215] та Cyber Resilience Act

(CRA)[180], які встановлюють вимоги до «продуктів з цифровими елементами»: принцип «security-by-design», обов'язкове усунення вразливостей протягом усього життєвого циклу продукту, прозорість щодо кіберризиків та відповідальність виробників за заподіяну шкоду[213]. На думку європейських дослідників, ці акти переводять кібербезпеку із площини суто організаційних заходів у площину регулювання ринку цифрових товарів і послуг, змушуючи виробників інтегрувати вимоги безпеки у процес розроблення й експлуатації програмного забезпечення та обладнання.

Доцільно докладніше проаналізувати Закон ЄС Про кіберстійкість (CRA)[180], який набрав чинності 11 грудня 2024 року та спрямований на покращення кібербезпеки та кіберстійкості в ЄС, шляхом запровадження спільних стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, таких як обов'язкові звіти про інциденти та автоматичні оновлення безпеки[180].

Основними вимогами та принципами CRA є:

- принцип «security by design» – продукція має проєктуватися, розроблятися й створюватися з урахуванням безпеки з самого початку;
- «Secure by default» – заводські/стандартні налаштування пристроїв не повинні створювати вразливостей (наприклад, заборона слабких паролів, наявність механізмів автооновлення і т. ін.);
- обов'язкова обробка вразливостей протягом усього життєвого циклу продукту: від моніторингу, повідомлення про знайдені (особливо – експлуатовані) вразливості до випуску патчів/оновлень;
- прозорість: виробники / дистриб'ютори мають розкривати характеристики безпеки продуктів, що дасть змогу споживачам – бізнесам і кінцевим користувачам – обирати безпечні рішення[180].

Особливої актуальності в сучасних умовах набуває Регламент ЄС про дані (Data Act), що зумовлено цифровізацією економіки, публічного управління та безпекового сектору, а також зростанням ролі даних як стратегічного ресурсу розвитку держави. В умовах поширення Інтернету речей, хмарних сервісів, штучного інтелекту та платформних рішень виникає потреба у чіткому

правовому врегулюванні доступу, використання та повторного використання даних, зокрема промислових і неперсональних. Data Act формує нову модель «економіки даних», спрямовану на забезпечення справедливого розподілу цінності даних між виробниками, користувачами та державою, що є особливо важливим для України в контексті відновлення економіки, розвитку інновацій та інтеграції у Єдиний цифровий ринок ЄС[215].

Додаткової наукової та практичної значущості Data Act набуває у процесі гармонізації законодавства України з правом Європейського Союзу та формування правових засад цифрової стійкості держави. Впровадження підходів Data Act сприятиме підвищенню прозорості договірних відносин у сфері обігу даних, зменшенню асиметрії між великими цифровими платформами та споживачами, а також створенню правових механізмів доступу державних органів до даних у надзвичайних ситуаціях. Для України це має особливе значення з огляду на потреби забезпечення національної безпеки, відбудови критичної інфраструктури та розвитку data-driven управління, що вимагає сучасного, європейсько орієнтованого правового регулювання обігу даних[215].

Окремий блок міжнародних стандартів охоплює питання захисту персональних даних і приватності, які безпосередньо пов’язані з проблематикою кібербезпеки. Центральне місце тут посідає Регламент ЄС 2016/679 (GDPR)[213], який установлює уніфіковані принципи обробки персональних даних, права суб’єктів даних та обов’язки контролерів і операторів[205]. Паралельно Рада Європи модернізувала Конвенцію № 108 (1981)[54], яка є першим у світі юридично обов’язковим міжнародним договором у сфері захисту персональних даних, ухваливши Конвенцію 108+, що розширює вимоги щодо міжнародної передачі даних, запроваджує додаткові гарантії прозорості та відповідальності держав і приватних суб’єктів за обробку даних[192]. Г. Greenleaf та C. de Terwangne оцінюють Конвенцію 108+ як потенційну «глобальну рамку» для уніфікації стандартів захисту даних, сумісну з GDPR, але відкриту для приєднання держав за межами ЄС[193]. Для України це відкриває наступні можливості:

- для євроінтеграції;
- для реформування законодавства про персональні дані;
- для адаптації до стандартів GDPR;
- для забезпечення кібербезпеки та довіри у транснаціональних даних[205].

Треба відмітити, що Загальний регламент про захист даних (GDPR)[211] відповідно законопроєкту № 8153 «Про захист персональних даних» планувалось імплементувати в законодавство України ще у IV кварталі 2025 року[105];

13 лютого 2025 року Комісія та Європейська рада з цифрових послуг схвалили офіційну інтеграцію добровільного Кодексу поведінки щодо дезінформації в рамки Закону про цифрові послуги (DSA), який спрямований на боротьбу з ризиками дезінформації, одночасно повністю дотримуючись свободи слова та підвищуючи прозорість. Підписанти Кодексу , включаючи тих, хто визначений як Дуже великі онлайн-платформи (VLOP) та великі онлайн-пошукові системи (VLOS) згідно з DSA (Facebook, Instagram, LinkedIn, Bing, TikTok, YouTube та Google Search), подали необхідні документи на підтвердження свого запиту на його перетворення на Кодекс поведінки згідно з DSA. На цій підставі Європейська рада з цифрових послуг та Комісія прийняли свої позитивні висновки, дійшовши висновку, що Кодекс відповідає умовам, зазначеним у DSA, та схваливши його офіційну інтеграцію в систему DSA. Таким чином, Кодекс стане відповідним орієнтиром для визначення дотримання DSA щодо ризиків дезінформації для постачальників VLOP та VLOS, які дотримуються його зобов'язань та виконують їх[52].

Наступний нормативний документ – Акт про свободу медіа (European Media Freedom Act, EMFA) формує комплексну рамкову модель регулювання діяльності медіа у цифровому середовищі, зокрема в частині протидії інформаційним загрозам, що походять від онлайн-ресурсів. Його положення спрямовані на забезпечення балансу між свободою вираження поглядів і необхідністю мінімізації деструктивних інформаційних впливів, включаючи дезінформацію, маніпулятивний контент та інші форми інформаційного

втручання. Водночас EMFA передбачає посилення ролі національних регуляторів у здійсненні нагляду за дотриманням медіа-суб'єктами зобов'язань, зокрема в межах механізмів саморегулювання, таких як Кодекс поведінки щодо протидії дезінформації[52]. Окрему увагу приділено встановленню вимог щодо прозорості структури власності у сфері медіа, що є важливим інструментом запобігання прихованому впливу на інформаційний простір та підвищення довіри до онлайн-медіа в умовах сучасних гібридних загроз[215].

Крім того, Рада ЄС у травні 2024 року затвердило два документи: Майбутнє цифрової політики ЄС та Висновки Ради щодо демократичної стійкості: захист виборчих процесів від іноземного втручання. Перший документ стосується 5-річного плану у сфері розробки цифрових політик, де серед пріоритетів значиться протидія дезінформації. Другий документ, своєю чергою, надає огляд законодавчих, виконавчих та інституційних ініціатив, впроваджених в ЄС для захисту виборчого процесу. Хоча ці інструменти є радше рекомендаційними актами, вони актуальні для посилення української інфраструктури, в тому числі в контексті проведення повоєнних виборів. Документи надають як огляд актуальних загроз, так і пропозиції щодо колективної протидії таким викликам: шляхом співпраці з платформами, міждержавної співпраці, та оновлення інформаційних політик. Для України ці документи є практично актуальними з двох причин. По-перше, вони формують спільну європейську рамку вимог до платформ і державних органів щодо виявлення та обмеження контенту – що дозволяє Україні апелювати до цих стандартів у переговорах з платформами та міжнародними партнерами. По-друге, в умовах підготовки до повоєнних виборів досвід ЄС із захисту виборчих процесів від іноземного втручання є безпосередньо застосовним: зокрема, механізми міждержавної співпраці та оновлення інформаційних політик можуть бути адаптовані до українського контексту без необхідності розробляти їх з нуля[74, с. 24].

Системний міждисциплінарний аналіз цих стандартів демонструє, що вони взаємодоповнюють один одного. Праці M. Gercke, T. Holt, D. Maimon та інших дослідників показують, що Будапештська конвенція забезпечує

кримінально-правову основу для боротьби з кіберзлочинами, NIS2 та пов’язані з нею регламенти – організаційно-управлінську та технічну стійкість інформаційних систем, а GDPR і Конвенція 108+ – належний рівень захисту персональних даних у цифровому середовищі[190; 203].

З метою виявлення трансформації підходів до забезпечення кібербезпеки у відповідь на еволюцію загроз у кіберпросторі доцільним стало проведення компаративного аналізу нормативно-правових і стратегічних засад кіберзахисту в окремих європейських державах, зокрема у Німеччині, Франції, Великій Британії, Нідерландах та Польщі. Вибір зазначених країн зумовлений тим, що вони належать до держав із високим рівнем технологічного розвитку, розвиненою цифровою інфраструктурою та інституційно оформленими механізмами реагування на кіберзагрози. Крім того, кожна з них виробила власну модель правового та організаційного забезпечення кібербезпеки, що дає змогу виявити як спільні європейські тенденції, так і специфічні національні особливості. Німеччина та Франція як провідні політико-економічні центри Європи послідовно розбудовують комплексні механізми захисту від кіберзагроз, насамперед у сфері критичної інфраструктури. Велика Британія, спираючись на значний інституційний і стратегічний досвід, зосереджує увагу на інноваційних інструментах протидії кібертероризму та іншим формам деструктивної кібердіяльності. Нідерланди демонструють високий рівень технологічної готовності та активну участь у міжнародних ініціативах у сфері кібербезпеки, тоді як Польща вирізняється системним нормативним підходом до визначення самої сутності кібербезпеки та побудови національної системи її забезпечення[41, с. 62].

Первинний аналіз нормативного матеріалу засвідчив, що в більшості європейських держав поняття «кібербезпека» не завжди закріплене в законодавстві як автономна та вичерпно визначена правова категорія. Натомість відповідні положення здебільшого інтегруються до ширших правових конструкцій, пов’язаних з інформаційною безпекою, захистом критичної інфраструктури, безпекою мережевих та інформаційних систем, а також управлінням ризиками. Такий підхід свідчить про міжгалузевий характер

кібербезпеки, її функціональний зв’язок із різними компонентами національної безпеки та складність формування універсального нормативного визначення. Водночас саме ця багатовимірність зумовлює необхідність комплексного правового, організаційного та технічного осмислення кібербезпеки як об’єкта державного управління й правового регулювання.

Показовим у цьому аспекті є досвід Німеччини. Закон «Про ІТ-безпеку» (IT-Sicherheitsgesetz)[222] встановлює підвищені вимоги до захисту інформаційних систем, насамперед тих, що належать до об’єктів критичної інфраструктури, зокрема в енергетичній, транспортній та медичній сферах. Хоча закон не містить окремого легального визначення терміна «кібербезпека», його змістовне наповнення розкривається через систему технічних і організаційних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформаційних систем. Така модель свідчить про пріоритет практико-орієнтованого підходу, в основі якого лежить управління кіберризиками, впровадження сучасних технологій захисту та підвищення стійкості критично важливих цифрових сервісів. Водночас аналіз німецького підходу дає підстави стверджувати, що його подальший розвиток об’єктивно пов’язаний із потребою посилення політико-правової координації та інституційної узгодженості між безпековим, технологічним і регуляторним компонентами[41, с. 63].

Французький підхід характеризується виразною стратегічною та оборонною орієнтацією. Закон щодо військової програми на 2019-2025 роки[202] розглядає кібербезпеку як сукупність заходів, технологій і політик, спрямованих на захист національної цифрової інфраструктури, з особливим наголосом на безпеці військових комунікацій. У такий спосіб кібербезпека виводиться на рівень одного з ключових елементів національної оборони, а кіберпростір фактично визнається окремим середовищем потенційного конфлікту. Подібне нормативне позиціонування обумовлює посилену увагу до захисту критичної інфраструктури, забезпечення стійкості державних інформаційних систем та розвитку інституцій спроможності держави протидіяти високоризиковим кіберінцидентам. Отже, французька модель

демонструє, що кібербезпека в сучасних умовах дедалі більше набуває ознак стратегічного елемента оборонної політики.

Для Великої Британії характерним є більш розширений підхід до правового осмислення кібербезпеки, за якого пріоритет надається захисту інформаційних систем і даних від несанкціонованого доступу, використання, розголошення, зміни, порушення чи знищення[77]. У цьому контексті кібербезпека охоплює захист апаратного та програмного забезпечення, мереж, інформаційних ресурсів і пов'язаних із ними процесів функціонування. Важливою особливістю британського підходу є поєднання двох взаємопов'язаних завдань: гарантування належного рівня захисту персональних даних та забезпечення безперервності функціонування державних і суспільно значущих інформаційних процесів. Такий баланс відповідає сучасному розумінню кібербезпеки як сфери, у якій інтереси безпеки не можуть реалізовуватись із відривом від прав людини, а цифрова стійкість держави має поєднуватися з належним рівнем правових гарантій.

Законодавство Нідерландів, зокрема Закон «Про безпеку мережевих та інформаційних систем»[78], розглядає кібербезпеку як один із фундаментальних елементів національної безпеки. У центрі уваги перебувають питання захисту від несанкціонованого доступу, витоків даних і збоїв у роботі інформаційно-комунікаційних систем як у державному, так і в приватному секторах. Водночас нідерландський підхід має виразну методологічну специфіку: він ґрунтується на чіткому розмежуванні окремих типів загроз, зокрема кібервійни, шпигунства, терористичної діяльності в кіберпросторі, хактивізму та кіберзлочинності. Така класифікація є важливою не лише з аналітичної, а й із нормативно-прикладної точки зору, оскільки дає змогу розробляти диференційовані моделі реагування залежно від природи загрози, її цілей, суб'єктного складу та очікуваних наслідків. Саме тому нідерландський досвід видається особливо цінним для України, оскільки він сприяє уникненню термінологічної невизначеності в політико-правових дискусіях та створює підґрунтя для формування більш структурованої й функціонально ефективної національної стратегії кібербезпеки[41, с. 64].

Перша Національна стратегія кібербезпеки Великої Британії[181], ухвалена у 2009 році, була зорієнтована передусім на підвищення стійкості об'єктів критично важливої інфраструктури до кіберзагроз. Подальший розвиток стратегічного підходу до забезпечення кібербезпеки знайшов відображення у наступних стратегічних документах, зокрема 2011 та 2016 років, у яких акцент було зміщено на посилення партнерської взаємодії між державою, приватним сектором і міжнародними суб'єктами співробітництва[182; 183].

Сучасний етап розвитку британської політики у сфері кібербезпеки пов'язаний із реалізацією Національної стратегії кібербезпеки на 2022-2030 роки, яка сформована з урахуванням умов глобальної нестабільності та зростання інтенсивності кіберзагроз. У цьому документі центральне місце відведено захисту критичної інфраструктури, підвищенню готовності держави до потенційних конфліктів у кіберпросторі, а також зміцненню спроможності реагувати на складні й масштабні кібератаки, зокрема ті, що пов'язуються з агресивною діяльністю росії[184]. Важливим напрямом реалізації зазначеної стратегії визначено розвиток партнерських відносин з Україною, європейськими державами та НАТО у сфері обміну розвідувальною інформацією, координації безпекових зусиль і посилення оборонних механізмів.

У цілому кібербезпека у Великій Британії розглядається як невід'ємна складова національної безпеки, у структурі якої особлива увага приділяється не лише цивільним, а й військовим та квазівійськовим загрозам. Як і інші провідні європейські держави, Велика Британія системно інвестує у розвиток технологічних рішень, удосконалення механізмів управління ризиками та підвищення готовності до кібератак, зокрема шляхом поглиблення взаємодії з міжнародними партнерами. Важливою рисою британського підходу є також орієнтація на міжнародні стандарти у сфері кібербезпеки, що свідчить про здатність держави адаптувати власну політику до трансформації сучасного кібернетичного середовища. Інституційно ключову роль у централізації системи кіберзахисту Великої Британії відіграє Національний центр кібербезпеки (NCSC), створений у 2016 році[200]. Цей орган забезпечує координацію зусиль у протидії кіберзагрозам, надає експертну та практичну підтримку державним

інституціям і приватному сектору, а також сприяє налагодженню ефективного обміну інформацією між основними суб'єктами національної системи кібербезпеки. Поряд із NCSC, вагоме місце у британській моделі кіберзахисту посідає Управління комісара з питань інформації (ICO)[195], яке забезпечує нагляд у сфері захисту персональних даних, уповноважене здійснювати розслідування порушень конфіденційності та застосовувати санкції за недотримання законодавчих вимог, зокрема положень Data Protection Act та UK GDPR. Додатково важливі повноваження щодо забезпечення безпеки телекомунікаційних мереж покладено на телекомунікаційного регулятора OFCOM[194], компетенція якого була розширена у зв'язку з ухваленням Закону про телекомунікації 2021 року, що загалом посилило інституційні механізми забезпечення кібербезпеки в державі.

Отже, Велика Британія послідовно розвиває національну систему кібербезпеки з урахуванням високого рівня залежності суспільства, економіки та державного управління від цифрової інфраструктури, а також зростання спектра кіберзагроз. У державі сформовано комплексну правову та інституційну основу, яка охоплює питання захисту персональних даних, безпеки критичної інфраструктури та розвитку партнерства між державним і приватним секторами. Ключовими інституціями у цій сфері виступають Національний центр кібербезпеки та Управління комісара з питань інформації. Водночас Велика Британія активно залучена до міжнародної співпраці, зокрема з Україною та НАТО, що сприяє посиленню її кіберзахисного потенціалу та підвищенню ефективності протидії сучасним загрозам, у тому числі пов'язаним із кіберактивністю росії[41, с. 121-122].

Не менш показовим є і польський досвід. Закон Республіки Польща від 5 липня 2018 року «Про національну систему кібербезпеки» (USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa)[221] визначає кібербезпеку через категорію стійкості інформаційних систем до дій, що порушують конфіденційність, цілісність, доступність і достовірність оброблюваних даних або пов'язаних із ними послуг. Таке нормативне формулювання видається достатньо змістовним і концептуально виваженим,

оскільки поєднує функціональне розуміння кібербезпеки з інституційним баченням національної системи її забезпечення. Польський підхід демонструє, що чітка структуризація понятійного апарату та законодавче закріплення елементів системи кібербезпеки створюють передумови для ефективної організації управління в цій сфері. Саме цим значною мірою пояснюється те, що Польща нині посідає помітне місце серед регіональних лідерів у сфері організації кіберзахисту[41, с. 64-65].

В загальних положеннях Закону України «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу» ще з 2004 року зазначалось, що загальнодержавна програма адаптації законодавства України до законодавства Європейського Союзу визначає механізм досягнення Україною відповідності третьому Копенгагенському та Мадридському критеріям набуття членства в Європейському Союзі. Цей механізм включає адаптацію законодавства, утворення відповідних інституцій та інші додаткові заходи, необхідні для ефективного правотворення та правозастосування[90].

Але особливо в останні роки законодавець став проводити активну політику щодо адаптації законодавства України до законодавства Європейського Союзу. Так, в ЄС функціонує Рада OECD (Організації економічного співробітництва та розвитку), яка виділяє дві основні площини: міжнародно-протиправна поведінка держави та індивідуальна кримінальна відповідальність за злочин.

Проте проведений нами аналіз чинного українського законодавства, норм міжнародного права та практики застосування кіберзасобів у міждержавних конфліктах свідчить, що така дихотомія є звуженою й не охоплює повного спектра суспільно небезпечних проявів кіберагресії.

По-перше, відповідно до статей про відповідальність держав за міжнародно-протиправні діяння (ARSIWA, 2001), держава несе відповідальність за будь-які дії у кіберпросторі, що порушують її міжнародні зобов’язання, зокрема:

- принцип суверенної рівності всіх (п. 1 ст. 2 Статут ООН);

- заборону погрози силою або її застосування проти територіальної цілісності, або політичної незалежності будь-якої держави (п. 4 ст. 2 Статут ООН);
- базові права людини[139].

Більш сучасним не нормативним актом, в якому кіберзброя зазначається вже як засіб ведення війни, є Талліннський Посібник (Tallinn Manual on the International Law Applicable to Cyber Warfare). У ньому засобам та методам ведення війни присвячено окремий розділ. Зокрема, ним забороняється використовувати засоби та способи, що спричиняють зайві травми або непотрібні страждання[204, с. 119].

Застосування кіберзброї допускається лише у воєнних цілях. Посібник також наводить заборону на воєнні репресалії проти полонених, цивільних осіб, які знаходяться hors de combat, а також проти медичних працівників, установ, транспорту та обладнання, також забороняються атаки проти різноманітних цивільних об'єктів, об'єктів природнього середовища та критичної інфраструктури. Варто також погодитися з наведеним у Посібнику твердженням, відповідно до якого держави зобов'язані оцінювати власні наявні засоби ведення кібервійни, а також приводити їх у відповідність до Додаткового Протоколу І до Женевських конвенцій 1949 року, а саме ст. 36, що стосується нових видів озброєнь[27; 46, с. 215].

Наприклад, атака NotPetya у 2017 році, офіційно приписана російській військовій розвідці, призвела до масштабних руйнувань інформаційних систем в Україні та у світі, що розцінюється низкою держав як міжнародно-протиправний акт держави-агресора[130]. Або кібератаки рф по енергетичній інфраструктурі України (зокрема атаки на «Київенерго» у 2015-2016 роках, критичної інфраструктури у 2022-2026 роках) продемонстрували здатність кібератак спричиняти фізичні наслідки, що наближає їх до застосування сили у розумінні міжнародного права.

Повертаючись до положень Ради Організації економічного співробітництва та розвитку, імплементацією яких в українське законодавство

займається Міністерство цифрової трансформації України, то нами було розглянуто останні три аналітичні таблиці щодо рекомендації Ради:

- щодо цифрової безпеки критично важливих видів діяльності (OECD/LEGAL/0456)[210];
- щодо управління ризиками цифрової безпеки (OECD/LEGAL/0479)[211];
- щодо національних стратегій цифрової безпеки (OECD/LEGAL/0480)[212].

В процесі дослідження зазначених рекомендацій можна надати наступні рекомендації щодо внесення змін в законодавство України з метою відповідності Рекомендаціям OECD[158, с. 124-128]:

1. Виходячи з положень щодо цифрової безпеки критично важливих видів діяльності (OECD/LEGAL/0456):

відповідно розділу II OECD:

- додати до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»[114] або Закону України «Про критичну інфраструктуру»[108] визначення *«критична функція» та «цифрова екосистема»*. Розглянувши *цифрову екосистему*, як цифрове середовище, яке підтримує критичні функції оператора вздовж ланцюжка створення вартості критично важливих видів діяльності. Воно включає цифрові активи, такі як апаратне забезпечення, програмне забезпечення, мережі та дані, операційні технології, що виявляють або викликають зміни у фізичних процесах, а також внутрішні та зовнішні суб'єкти, осіб та процеси, які їх проєктують, підтримують та експлуатують, та взаємозв'язки між ними;
- доповнити Постанову КМУ від 28.04.2023 № 415[99] пунктами: критичні функції, ключові цифрові активи/системи, основні залежності та постачальники[158, с. 124].

відповідно розділу IV OECD:

- закріпити в Законі України «Про основні засади забезпечення кібербезпеки України»[114] та/або Закону України «Про критичну інфраструктуру»[108] пороги значущості та строки повідомлення

(первинне/уточнене) для операторів КІІ і визначених ризик-орієнтованих категорій приватних суб'єктів обов'язкові;

- закріпити рамки/методики управління ризиками та безперервності для держсектору;

- упровадити добровільно-обов'язкові (за рівнем ризику) схеми кіберсертифікації продуктів і послуг; створити реєстр сертифікованих провайдерів (MSSP/SOC/CSIRT);

- адаптувати вимоги публічних закупівель: пріоритет сертифікованих рішень/постачальників.

відповідно розділу VIII OECD:

- доповнити Закон України «Про основні засади забезпечення кібербезпеки України»[114] окремою статтею про транскордонну оперативну взаємодію операторів;

- закріпити у зазначених вище законах принцип «win-win» партнерства: оператори отримують від держави не лише обов'язки, а й переваги (аналітика, попередження, пільги на інноваційні заходи безпеки)[160, с. 147-155; 158, с. 124].

2. Виходячи з положень щодо управління ризиками цифрової безпеки (OECD/LEGAL/0479):

відповідно розділу I OECD:

- необхідно оновити (уточнити) визначення «ризику» в Законі України «Про основні засади забезпечення кібербезпеки» та Постанові КМУ № 367 від 01.04.2025[91]. Виходячи з терміну *Ризик цифрової безпеки/стійкості* – це категорія ризику (тобто впливу невизначеності на досягнення цілей), що пов'язаний із використанням, розробкою та управлінням цифровим середовищем у ході будь-якої діяльності, який: - може виникати внаслідок поєднання загроз і вразливостей у цифровому середовищі; - може перешкоджати досягненню економічних і соціальних цілей, зокрема фізичній безпеці, шляхом порушення доступності, цілісності та конфіденційності даних, інформаційних систем і мереж; - має динамічний характер; - охоплює аспекти,

пов’язані з цифровим і фізичним середовищем, залученими особами та організаційними процесами, що підтримують діяльність;

- попри наявність доволі вузького визначення *«управління ризиками безпеки»* для КІ-І у постанові Кабінету Міністрів України від 01.04.2025 року № 367[91], необхідно закріпити дефініцію *«управління ризиками цифрової безпеки»* – це сукупність скоординованих дій, що здійснюються в межах організації та/або між організаціями для реагування на ризик цифрової безпеки із одночасним використанням можливостей, які: - є невід’ємною частиною ухвалення рішень і загального підходу до управління ризиками для економічної та соціальної діяльності; - ґрунтуються на комплексному, системному та гнучкому циклічному процесі, що є максимально прозорим і чітко визначеним; - спрямовані на забезпечення того, щоб заходи цифрової безпеки відповідали рівню ризику та економічним і соціальним цілям;

- поняття *«цифрова безпека/стійкість»* значно ширше понять «кібербезпека» та «кіберзахист». Тому необхідно: по-перше Закон України «Про основні засади забезпечення кібербезпеки України»[114] доповнити ст. 1 новим визначенням: *«цифрова безпека/стійкість»* – це сукупність організаційних, технічних, правових та соціально-економічних заходів, спрямованих на управління ризиками цифрової безпеки та забезпечення здатності держави, суспільства, бізнесу та громадян протистояти загрозам у цифровому середовищі, адаптуватися до них і швидко відновлюватися після інцидентів». По-друге, в Законі України «Про критичну інфраструктуру»[108, ст. 1] розширити визначення «стійкість критичної інфраструктури» (ст. 1) з урахуванням цифрової складової, підкресливши її залежність від інформаційно-комунікаційних систем та цифрового середовища;

- в Законі України «Про основні засади забезпечення кібербезпеки України» доповнити ст. 1 новими визначеннями[114]:

♦ *«заінтересовані сторони (стейкхолдери)»* – уряд, публічні та приватні організації, а також фізичні особи, які залежать від цифрового середовища для здійснення повністю або частково своєї економічної чи

соціальної діяльності; можуть поєднувати різні ролі, зокрема як учасники ланцюгів постачання;

- *«керівники та особи, що приймають рішення (ОПР)»* – представники заінтересованих сторін на найвищому рівні керівництва;
- «культура цифрової безпеки/стійкості» як сукупність знань, навичок, поведінкових практик і управлінських процедур, спрямованих на усвідомлене прийняття рішень з урахуванням власних ризиків і впливу на інших;
- *«власник ризику цифрової безпеки»* – посадова особа організації, відповідальна за прийняття рішень щодо оброблення конкретного ризику, у т.ч. за визначення й документоване прийняття прийнятного рівня залишкового ризику[158, с. 125-126].

відповідно розділу II OECD:

- доповнити та уточнити Закон України «Про основні засади забезпечення кібербезпеки України»:
  - ст. 7. *«застосування ризик-орієнтованого підходу до цифрової безпеки/стійкості на всіх рівнях органів державної влади, органів місцевого самоврядування та інших публічних організацій незалежно від виду інформації, що обробляється»;*
  - до ст. 7 додати новий абзац: «Інклюзивність співпраці, що забезпечує залучення учасників ланцюгів постачання цифрових продуктів і послуг, у тому числі постачальників хмарних сервісів, розробників програмного забезпечення та інтеграторів, до управління ризиками цифрової безпеки/стійкості»;
  - ст. 8 «…, що центральний орган виконавчої влади у сфері кібербезпеки затверджує методичні настанови для публічних організацій щодо впровадження такого узгодження;
  - до ст. 8 додати нові пункти повноважень: «… забезпечує функціонування національної політики відповідального повідомлення про вразливості (VDP) та безпечних каналів взаємодії з технічною спільнотою;

організовує галузеві осередки обміну кіберінформацією за участю приватного сектору, МСП та постачальників»;

- ст. 7 або ст. 8 «держава заохочує приватні організації до впровадження принципів управління ризиками цифрової безпеки/стійкості шляхом запровадження добровільних рамок і програм;
- додати нову статтю *«Відповідальність і підзвітність за управління ризиками»*, в якій визначити - обов'язок призначати власників ризиків для ключових активів/процесів; - обов'язок вести реєстр ризиків, план оброблення; - вимоги враховувати міжорганізаційний вплив (ланцюги постачання, клієнти);
- у ст. 9 додати пункт «Оцінювання ризиків цифрової безпеки здійснюється на безперервній основі як циклічний процес, що включає ідентифікацію, аналіз, оцінку, обробку, моніторинг і перегляд ризиків, із періодичним та тригерним переглядом»;
- додати спеціальну статтю «Права людини, етичність та прозорість заходів кібербезпеки»;

- в Законі України «Про критичну інфраструктуру»[108] уточнити та доповнити:

- ст. 19 ч. 1 п. 8(в) щодо організації системи підготовки персоналу, яка здійснюється в контексті ризик-орієнтованого управління цифровою стійкістю секторів КІ;
- зробити уточнення суб'єктного складу в ст. 19: «… система обміну інформацією та взаємодії обов'язково охоплює операторів об'єктів, їхніх постачальників і підрядників, які надають цифрові продукти/послуги, що впливають на стійкість об'єктів КІ»;
- ст. 21 ч. 1 «формування та постійне підтримання культури цифрової безпеки/стійкості, у т.ч. через рольову підготовку керівників/ОПР, регулярні вправи з прийняття рішень та оцінку зовнішніх ефектів»;
- ст. 23 додати: «Управління ризиками обов'язково охоплює ризики ланцюгів постачання цифрових продуктів і послуг; оператори КІ впроваджують

процедури SCRM, у т.ч. оцінку постачальників, вимоги до договірних умов безпеки, контроль оновлень та залежностей»;

- в Закон «Про інформацію»[107] додати поняття *«прозорість практик управління цифровою безпекою»* і поширити його на приватних осіб, що надають інформаційні послуги значному колу користувачів або є операторами КІ[158, с. 126-127].

3. Виходячи з положень щодо національних стратегій цифрової безпеки (OECD/LEGAL/0480):

відповідно розділу I OECD:

- необхідно в законодавстві про кібербезпеку закріпити положення про цифрову трансформацію, а саме підкреслити, що заходи з кібербезпеки мають сприяти, а не стримувати цифровізацію економіки та суспільства, а також закріпити принцип відкритості цифрового середовища та посилити акцент на економічному та соціальному процвітанні (розвиток цифрової економіки та суспільства є не менш важливим, ніж захист від ризиків);

- необхідно передбачити вимогу гармонізації цифрової безпеки з економічною, соціальною, безпековою та правоохоронною політикою.

відповідно розділу III OECD:

- Закон України «Про основні засади забезпечення кібербезпеки України»[114]:

♦ ст. 7 (Принципи) доповнити: принципом стейкхолдер-орієнтованості та пропорційності вимог для МСП і фізичних осіб, а також принципом технологічної нейтральності ініціатив, адресованих цим групам;

♦ ст. 8 ч. 3 доповнити пунктом: «… здійснення технологічно нейтральних ініціатив із підвищення обізнаності та спроможності до управління ризиками цифрової безпеки, адаптованих до потреб різних категорій заінтересованих сторін, зокрема малих і середніх підприємств та окремих осіб»;

♦ ст. 8 ч. 3 доповнити пунктом: «… забезпечення інклюзивності освітніх і просвітницьких програм, у т.ч. за гендерною ознакою, з охопленням усіх рівнів освіти та як технічних, так і нетехнічних спеціальностей»;

♦ ст. 8 ч. 3 доповнити пунктом: «Національна програма кіберстійкості МСП»: безкоштовні базові курси, ваучери на аудит/впровадження МФА/резервування/керування оновленнями, типові політики; галузеві профілі ризиків для мікро- та малих підприємств;

- до Закону України «Про критичну інфраструктуру»[108], ст. 16 ч. 2 – розширення мандату, додати, що уповноважений орган у сфері КІ, у взаємодії з ЦОВВ у сфері освіти та цифрової трансформації, «… поширює типові програми та стандарти компетентностей управління цифровими ризиками для суб'єктів поза КІ, з урахуванням потреб МСП»[158, с. 126].

Таким чином, результати проведеного аналізу міжнародно-правових актів і стандартів у сфері протидії кіберзагрозам дозволяють сформулювати такі узагальнюючі висновки.

По-перше, міжнародна система протидії кіберзагрозам сформувалася як багаторівнева та комплексна, що зумовлено транснаціональним характером кіберзлочинності, гібридністю сучасних загроз і високою залежністю держав та суспільства від цифрової інфраструктури. Будапештська конвенція про кіберзлочинність заклала кримінально-правову й процесуальну основу міжнародної співпраці, тоді як акти Європейського Союзу (NIS2[181], GDPR[190], Data Act[215], Cyber Resilience Act[180]) і документи Ради Європи (Конвенція 108+)[205] розвинули організаційно-управлінський, технічний та правозахисний виміри кібербезпеки. У сукупності ці інструменти формують цілісну модель, що поєднує кримінально-правове реагування, управління ризиками, забезпечення стійкості інформаційних систем і захист прав людини у цифровому середовищі

По-друге, дослідження показало, що традиційна дихотомія між міжнародно-правовою відповідальністю держав і індивідуальною кримінальною відповідальністю осіб є недостатньою для адекватного реагування на сучасні прояви кіберагресії. Практика застосування норм міжнародного права, зокрема положень Статуту ООН, свідчить про поступове визнання кібератак як таких, що можуть досягати порогу застосування сили або міжнародно-протиправного діяння держави[139]. Це зумовлює необхідність

розширеного правового підходу, який охоплює як міждержавний, так і внутрішньодержавний рівні регулювання.

По-третє, рекомендації Ради OECD щодо цифрової безпеки критично важливих видів діяльності, управління ризиками цифрової безпеки та національних стратегій цифрової безпеки відображають сучасний зсув від вузького технократичного розуміння кібербезпеки до концепції цифрової безпеки/стійкості, інтегрованої в економічну, соціальну та управлінську політику держави. Вони акцентують увагу на ризик-орієнтованому підході, ролі заінтересованих сторін, відповідальності керівництва, стійкості ланцюгів постачання та необхідності поєднання безпекових заходів із цілями цифрової трансформації

По-четверте, аналіз стану імплементації міжнародних стандартів у законодавство України засвідчує наявність позитивної динаміки, однак водночас виявляє фрагментарність і термінологічну неузгодженість правового регулювання. Чинні норми законів України «Про основні засади забезпечення кібербезпеки України»[114] та «Про критичну інфраструктуру»[108] не повною мірою відображають підходи OECD і ЄС щодо управління ризиками цифрової безпеки, ролі приватного сектору, ланцюгів постачання та культури цифрової стійкості. Це обумовлює необхідність системного перегляду законодавства з метою його гармонізації з європейськими та світовими стандартами[158, с. 126-127].

Висновок до розділу 1

Узагальнення результатів, отриманих у трьох підрозділах, дає підстави стверджувати, що кіберзагрози сформувалися як самостійний, динамічний і комплексний різновид загроз національній безпеці, який якісно відрізняється нематеріальністю слідів, транскордонністю, масштабованістю та асиметричністю впливу, а також здатністю безпосередньо впливати на реалізацію конституційних прав і свобод, функціонування критичної інфраструктури та стійкість держави в умовах гібридних викликів.

Встановлено, що їх правова природа має подвійний (техніко-юридичний) характер: кіберзагроза проявляється у конкретних технологічних векторах, але водночас детермінує застосування комплексу матеріально-правових і процесуальних норм, зокрема щодо управління ризиками, інцидент-репортингу, збереження цифрових доказів, аудиту та дотримання стандартів захисту даних, що переводить технічні події у площину юридично значущих фактів і комплаєнсу.

Обґрунтовано, що ефективна протидія кіберзагрозам у діяльності НПУ потребує науково вивіреної багатовимірної класифікації, яка інтегрує суб'єктний склад (учасників), вектори доступу, типи технічного впливу та об'єкти посягання, і має бути операціоналізована через систему критеріїв оцінювання небезпечності, узгоджених із міжнародними стандартами ризик-менеджменту та національним/європейським правовим полем. Запропонована сукупність критеріїв (імовірність реалізації, організованість і складність атаки, вплив на конфіденційність/цілісність/доступність і довіру до даних, часові параметри детектування та реагування, потенціал поширення, правові наслідки й репутаційний ефект) забезпечує порівнюваність управлінських рішень, прозорість ескалації інцидентів і підвищення якості кримінально-аналітичного процесу. Її регулярне оновлення на підставі звітів ENISA, попереджень CERT-UA та інцидентної статистики дозволяє підтримувати актуальність оцінювання в умовах мінливого середовища загроз і одночасно корелювати практику НПУ з вимогами NIS2 щодо кіберстійкості та безперервності надання послуг.

Доведено, що міжнародно-правові стандарти протидії кіберзагрозам утворюють багаторівневу та комплексну модель, яка поєднує кримінально-правове реагування (Будапештська конвенція), управління ризиками й кіберстійкість (акти ЄС, зокрема NIS2, Cyber Resilience Act, Data Act), а також правозахисний вимір і захист персональних даних (GDPR, Конвенція 108+). Водночас встановлено, що традиційна дихотомія між міжнародно-правовою відповідальністю держав і індивідуальною кримінальною відповідальністю осіб є недостатньою для сучасних проявів кіберагресії: практика застосування норм міжнародного права (зокрема в контексті Статуту ООН) демонструє

тенденцію до визнання кібератак такими, що за певних умов можуть досягати порогу застосування сили або міжнародно-протиправного діяння держави, що потребує розширеного підходу, синхронізованого з внутрішньодержавним регулюванням.

У підсумку, аналіз імплементації міжнародних стандартів у законодавство України засвідчує позитивну динаміку, але водночас виявляє фрагментарність і термінологічну неузгодженість, а також неповне відображення ризик-орієнтованих підходів OECD і ЄС щодо ролі приватного сектору, ланцюгів постачання, відповідальності керівництва та формування культури цифрової стійкості. Це обумовлює необхідність системного перегляду й гармонізації нормативної бази України з європейськими та світовими стандартами, а також подальшого методичного закріплення для НПУ (зокрема підрозділів кримінального аналізу) уніфікованих підходів до класифікації, оцінювання небезпечності та ескалації кіберінцидентів як передумови підвищення ефективності протидії кіберзагрозам і забезпечення стійкості державних сервісів.

Проведено аналіз рекомендацій Ради Організації економічного співробітництва та розвитку щодо цифрової безпеки критично важливих видів діяльності, управління ризиками цифрової безпеки та національних стратегій цифрової безпеки, що дає підстави стверджувати, що чинне законодавство України у сфері кібербезпеки, захисту критичної інфраструктури та цифрової стійкості потребує подальшого системного оновлення. Йдеться не лише про техніко-юридичне уточнення окремих норм, а про концептуальне переосмислення предмета правового регулювання – від вузького розуміння кібербезпеки як захисту інформаційно-комунікаційних систем до ширшої моделі цифрової безпеки/стійкості як комплексної категорії, що охоплює організаційні, технологічні, правові, економічні та соціальні аспекти функціонування держави, суспільства і критично важливих секторів.

Обґрунтовано, що одним із ключових напрямів удосконалення законодавства України має стати нормативне закріплення базових категорій, без яких подальша гармонізація національного права з підходами ОЕСР є

неповною. Передусім це стосується дефініцій «критична функція», «цифрова екосистема», «ризик цифрової безпеки/стійкості», «управління ризиками цифрової безпеки», «культура цифрової безпеки/стійкості», «власник ризику цифрової безпеки», а також пов'язаних понять, що описують сучасну багаторівневу цифрову взаємозалежність. Уведення таких категорій до законодавства має не лише термінологічне значення, а й створює правову основу для ризик-орієнтованого управління, персоналізації відповідальності, формування системи підзвітності та побудови сучасної моделі цифрової стійкості держави.

Встановлено, що українське законодавство потребує переходу від фрагментарного регулювання кіберзахисту окремих об'єктів до інтегрованої моделі управління цифровими ризиками, яка має поширюватися на державний сектор, операторів критичної інфраструктури, постачальників цифрових продуктів і послуг, а також інші суб'єкти, діяльність яких впливає на стійкість цифрового середовища. Такий підхід передбачає закріплення безперервного циклу управління ризиками, що включає їх ідентифікацію, аналіз, оцінку, обробку, моніторинг і перегляд, а також установлення обов'язку ведення реєстрів ризиків, призначення відповідальних осіб і врахування міжорганізаційних залежностей, зокрема ризиків ланцюгів постачання цифрових продуктів та послуг.

З урахуванням проведеного дослідження зроблено загальний висновок, що гармонізація законодавства України з рекомендаціями OECD має здійснюватися не шляхом механічного перенесення окремих норм, а через послідовне формування нової правової парадигми цифрової безпеки/стійкості. Її сутність полягає у переході від об'єктоцентричної моделі захисту до функціоцентричної та ризик-орієнтованої моделі, у центрі якої перебувають критичні функції, цифрові екосистеми, міжсекторальна взаємодія, відповідальне управління ризиками, стійкість ланцюгів постачання та поєднання безпекових, економічних і соціальних інтересів. Саме така модель є найбільш перспективною для подальшого розвитку українського законодавства та правозастосовної практики.

Аналіз матеріалів інформаційно-консультаційного онлайн-ресурсу превентивного спрямування chatovi.online свідчить про доцільність використання таких платформ як емпіричного джерела для ідентифікації та уточнення класифікації масових соціально-інженерних кіберзагроз, що характеризуються високою латентністю та мають істотне значення для формування пріоритетів діяльності Національної поліції України у сфері протидії кіберзлочинності.

РОЗДІЛ 2.
Організаційно-правовий механізм протидії кіберзагрозам Національною поліцією України

2.1. Нормативно-правові засади діяльності Національної поліції України у сфері протидії кіберзагрозам

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням ролі цифрових технологій у функціонуванні держави, економіки та повсякденному житті людини, що водночас зумовлює появу нових, складних і динамічних форм загроз у кіберпросторі. Кіберзагрози набувають системного, транскордонного та гібридного характеру, поєднуючи, як ми розібрали в першому розділі нашої роботи, – кримінальні, терористичні та інформаційні. Саме тому протидія кіберзагрозам у правовій державі не може розглядатися виключно як технічне реагування або суто управлінська функція, а має характеризуватися як комплекс правових і організаційних заходів, у межах яких правоохоронна складова спрямована на захист людини, суспільства і держави від кримінально протиправних посягань у кіберпросторі[57].

Прикладом запровадження елементів штучного інтелекту в відеоналітики може бути місто Чернігів, в якому з грудня 2025 року почав працювати центр із сучасною системою відеоспостереження. За словами начальника ГУ Нацполіції в Чернігівській області Івана Іщенка, реалізація цього проєкту має практичне значення для безпеки мешканців міста: «Головним управлінням Нацполіції в Чернігівській області реалізовано цей великий проєкт, і я переконаний, що він принесе багато користі жителям міста, особливо в цей непростий час. Система відеоспостереження спрямована насамперед на підвищення рівня особистої безпеки чернігівців», – зазначив Іщенко. У поліції зазначають, що система дозволяє не лише фіксувати правопорушення, а й працювати на випередження. Начальник Департаменту інформаційно-аналітичної підтримки НПУ Олексій Григорович наголосив, що впровадження таких систем є важливим елементом формування безпечного середовища: «Система побудована на програмному

забезпеченні українського виробництва, що забезпечує технологічну незалежність, гнучкість у розвитку та можливість масштабування під потреби територіальних громад», – зазначив він. За його словами, відеоаналітика підвищує якість ситуаційного моніторингу, дозволяє своєчасно виявляти ризики та ухвалювати обґрунтовані управлінські рішення. Очільник Департаменту кримінального аналізу НПУ Роман Бутко підкреслив, що: «Такі системи відеоспостереження – це інструмент, який не лише допомагає правоохоронним органам, а й забезпечує безпеку громадян в умовах війни»[7].

Нормативно-правові засади протидії кіберзагрозам Національною поліцією України становлять багаторівневу систему, в якій поєднуються конституційні приписи, спеціальне законодавство про поліцію та кібербезпеку, процесуальні вимоги кримінального провадження, а також підзаконні акти, що визначають порядок реагування та взаємодії суб’єктів національної системи кібербезпеки. Вихідною основою є конституційний принцип діяльності органів державної влади лише на підставі, у межах повноважень та у спосіб, що передбачені Конституцією і законами України, а також пріоритет прав і свобод людини як змістовний орієнтир будь-яких владних втручань[57].

Національну систему кібербезпеки визначено положеннями статті 8 Закону України «Про основні засади забезпечення кібербезпеки України». Зокрема, ч. 1 зазначеної норми передбачено, що під такою системою розуміється сукупність суб’єктів забезпечення кібербезпеки, а також пов’язаних з нею науково-технічних, політичних, інформаційних, освітніх, правових, організаційних, розвідувальних, процесуальних, оперативно-розшукових, оборонних, контррозвідувальних, інженерно-технічних, криптографічного і технічного захисту заходів, спрямованих на захист національних інформаційних ресурсів та кіберзахист об’єктів критичної інформаційної інфраструктури[114, ч. 2, ст. 8].

Необхідно відмітити, що правова модель діяльності Національної поліції України у кіберпросторі формується:

- по-перше, Законом України «Про Національну поліцію», який визначає поліцію як орган, що служить суспільству шляхом охорони прав і свобод

людини, протидії злочинності та підтримання публічної безпеки і порядку, а також закріплює принципи й вимоги до застосування поліцейських заходів[96];

- по-друге, законодавство про кібербезпеку встановлює національну систему кібербезпеки та інструменти міжвідомчої взаємодії, у межах яких поліцейська діяльність виступає правоохоронною складовою загальнодержавного механізму забезпечення захищеності у кіберпросторі[114];

- по-третє, стратегічні засади державної політики у цій сфері деталізуються рішенням РНБО, введеним у дію Указом Президента України, що задає пріоритети розвитку спроможностей і координації у сфері кібербезпеки[117].

- по-четверте, урядові процедури реагування на кіберінциденти, кібератаки та кіберзагрози, включно з національним плануванням реагування та визначенням порядку взаємодії національної системи реагування із суб'єктами забезпечення кібербезпеки і правоохоронними органами. Такі акти є ключовими для зниження ризиків «розриву» між технічним реагуванням і правоохоронною діяльністю, оскільки закріплюють процесуальні особливості: хто, коли, у якій формі та з яким мінімально необхідним обсягом відомостей здійснює інформування, залучення, узгодження дій та передавання відповідних матеріалів[20; 100; 101].

Отже, законодавство про кібербезпеку формує національну систему кібербезпеки як сукупність суб'єктів і заходів різної природи (правових, організаційних, оперативно-розшукових, технічних та інших), спрямованих на забезпечення захищеності життєво важливих інтересів у кіберпросторі. У межах цієї системи Національна поліція України прямо віднесена до основних суб'єктів, що зумовлює її не ізольовану, а системну участь у державному механізмі забезпечення кібербезпеки[114, п. 4 ч. 4 ст. 5]. Водночас стратегічне визначення пріоритетів і напрямів державної політики у цій сфері здійснюється через рішення Ради національної безпеки і оборони України, введені в дію актами Президента України, зокрема Стратегією кібербезпеки України, яка задає рамку розвитку спроможностей сектору безпеки і оборони та інших суб'єктів системи кібербезпеки[117; 47, с. 338-341].

Межі компетенції Національної поліції у кіберпросторі розкривається передусім через її загальні завдання, визначені законом про Національну поліцію, – забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядок, належить Національній поліції України, а саме по управлінський вертикалі – міжрегіональному територіальному органу Національної поліції – Департаменту кіберполіції[122].

Загальні завдання та повноваження працівників підрозділів кіберполіції як поліцейських визначено у Законі України «Про Національну поліцію»[111] та у Постанові Кабінету Міністрів України «Про затвердження Положення про Національну поліцію» від 28 жовтня 2015 № 8772[97]. За специфікою діяльності відповідно до Положення про Департамент кіберполіції Національної поліції України, затвердженого Наказом Національної поліції України від 10 жовтня 2015 № 85, основними завданнями кіберполіції є такі[96]:

- участь у формуванні та забезпеченні реалізації державної політики у сфері протидії кіберзлочинності щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку;
- сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень у сфері інформаційної безпеки, використання платіжних систем, електронної комерції та господарської діяльності;
- завчасне інформування населення про появу новітніх кіберзлочинів;
- упровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини;
- реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів;
- участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності;

- участь у міжнародних операціях та співпраця в режимі реального часу, забезпечення діяльності мережі контактних пунктів між країнами світу[96; 50].

На рівні підзаконного регулювання у 2025 році Кабінет Міністрів України затвердив Національний план реагування на кіберінциденти, кібератаки та кіберзагрози та визначив загальні засади реагування, включно з узгодженням термінів, ролей і процедур у межах національної системи реагування[20]. Ці положення мають принципове значення для діяльності Національної поліції, оскільки створюють нормативну основу для своєчасного залучення правоохоронного компонента у випадках, коли подія у кіберпросторі набуває ознак кримінально протиправного посягання або потребує процесуально значущого документування.

Додатково Кабінет Міністрів України у 2025 році затвердив спеціальний порядок взаємодії суб'єктів національної системи реагування із суб'єктами забезпечення кібербезпеки, правоохоронними та іншими уповноваженими органами, який прямо орієнтує взаємодію на функціонування національної системи реагування і національної системи обміну інформацією та прив'язує процедури до національного плану реагування[100]. Для Національної поліції України це означає нормативно закріплену основу участі в міжвідомчих процедурах отримання та передавання інформації про кіберінциденти, а також можливість узгоджувати правоохоронні дії з технічними заходами реагування без порушення меж компетенції інших суб'єктів.

Важливою позитивною ініціативою Уряду України у сфері забезпечення кібербезпеки та підвищення кіберстійкості публічного управління стало ухвалення Постанови Кабінету Міністрів України від 08.10.2025 № 1281 «Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни». Зазначений нормативно-правовий акт закріплює комплексний та превентивний підхід до формування базових і спеціалізованих компетентностей у сфері безпечного користування засобами інформатизації та мережі Інтернет серед суб'єктів державного управління. Його нормативне значення полягає у переході від фрагментарних інформаційно-роз'яснювальних

заходів до системної моделі регулярного навчання з кібергігієни, орієнтованої на запобігання, своєчасне виявлення та належне реагування на кіберінциденти і кібератаки, а також на забезпечення захисту персональних даних і дотримання вимог законодавства у сфері кібербезпеки[103].

Постанова № 1281 формує обов'язкову організаційну рамку для проведення первинних та періодичних інструктажів і тренінгів, визначає коло суб'єктів, на яких поширюється її дія, та закладає підґрунтя для уніфікації підходів до кібергігієни у різних секторах публічної служби. У контексті діяльності Національної поліції України цей акт має особливе значення, оскільки сприяє підвищенню загального рівня кіберобізнаності поліцейських та інших працівників системи МВС, що безпосередньо впливає на зниження вразливостей людського фактору як одного з ключових джерел кіберризиків[103].

Подальший розвиток і практична деталізація положень зазначеної постанови здійснені у Наказі Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 21.10.2025 № 661 «Про затвердження Методичних рекомендацій щодо проведення інструктажів і тренінгів щодо кібергігієни…». Цей підзаконний нормативний акт виконує методико-організаційну функцію та забезпечує практичну реалізацію урядового Порядку шляхом встановлення змістовних, процедурних і дидактичних орієнтирів для проведення навчальних заходів[94].

Методичні рекомендації визначають цільові аудиторії (державні службовці, працівники органів державної влади, військовослужбовці, керівники та працівники державних підприємств, установ і організацій), типові теми інструктажів і тренінгів, рекомендовані формати навчання, а також мінімальні вимоги до їх змісту (нараховують 12 тем, які містять 47 підтем, а також 3 додаткові теми). Їх нормативна цінність полягає у стандартизації підходів до формування практичних навичок кібергігієни, узгоджених із чинними політиками безпеки, національними та міжнародними стандартами у сфері кібербезпеки[94; 103].

У системному вимірі всі зазначені вище акти свідчать про еволюцію адміністративно-правових механізмів протидії кіберзагрозам в Україні у напрямі людиноцентричної та ризик-орієнтованої моделі, в якій підготовка персоналу розглядається як ключовий елемент забезпечення кіберстійкості. Для Національної поліції України вони створюють нормативні передумови для інституціоналізації кібергігієни як обов'язкової складової службової підготовки та як інструменту попередження як зовнішніх, так і внутрішніх кіберзагроз, що відповідає сучасним тенденціям розвитку національної та європейської систем кібербезпеки.

Проведення тренінгів у рамках службової підготовки НПУ окрім основної функції – підвищення рівня обізнаності поліцейських, забезпечую виконання загальну превентивну роль недопущення випадків кіберінцидентів.

У межах національної системи кібербезпеки ключова роль у виявленні, припиненні та документуванні кіберзагроз належить Національній поліції України, зокрема підрозділам кіберполіції. Реалізація покладених на поліцію повноважень у цій сфері безпосередньо пов'язана з обігом цифрової інформації, яка набуває статусу доказів у кримінальному провадженні або використовується як аналітична основа для прийняття управлінських і процесуальних рішень.

Нормативно-правові засади діяльності Національної поліції України у сфері протидії кіберзагрозам формуються на перетині Закону України «Про Національну поліцію», кримінального процесуального законодавства, спеціальних актів у сфері кібербезпеки та міжнародно-правових актів. Водночас практика досудового розслідування свідчить, що навіть за наявності формального визнання електронних доказів у законодавстві України питання їх допустимості, належності та достовірності залишаються одними з найбільш спірних питань.

Ще більш ситуація ускладнюється впровадженням у поліцейську діяльність автоматизованих систем аналізу даних, алгоритмів машинного навчання та штучного інтелекту, результати роботи яких дедалі частіше використовуються для ідентифікації кіберінцидентів, кореляції цифрових слідів

та прогнозування злочинної активності. За відсутності спеціального нормативного регулювання постає питання правової природи таких результатів та можливості їх використання як доказів у кримінальному процесі.

Професор Солдатенко О.А. у контексті швидкого розвитку цифрових технологій та активного використання електронних доказів у кримінальному процесі пропонує наступні напрями вдосконалення:

1. Кодифікація електронних доказів у КПК України. Доцільно передбачити окрему статтю, яка б регулювала визначення поняття електронних доказів, порядок їх збирання, перевірки та оцінки, з урахуванням наявної судової практики.

2. Запровадження єдиної централізованої платформи для зберігання електронних доказів, що передбачає фіксацію оригіналів інформації з використанням електронного підпису.

3. Організація систематичного навчання та підвищення кваліфікації слідчих, прокурорів і суддів з питань роботи з електронними доказами, зокрема щодо сучасних технологій, методів верифікації та правових аспектів їх застосування[136, с. 775].

Окремі норми Будапештської Конвенції спрямовані на здійснення заходів, які б забезпечували збереження файлів протоколів провайдерів та операторів телекомунікаційних послуг (ст. 16) та встановлення повноважень компетентних органів щодо отримання такої інформації (ст. 18), а також здійснення окремих слідчих (розшукових) дій (обшук і арешт комп’ютерних даних, які зберігаються) та оперативно-розшукових або негласних слідчих (розшукових) дій (збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації)[56, ст. 18, ст. 18].

Цифрові докази за міжнародним стандартами ISO/IEC здобуваються в процесі реагування на інциденти інформаційної безпеки. Стандарти ISO/IEC, які або безпосередньо регламентують управління інцидентами інформаційної безпеки або впливають на цю діяльність можна зазначити як в ISO/IEC 27035-1 через класифікацію фаз процесу розслідування інцидентів (див. Додаток Е)[6, с. 11].

Якщо узагальнено скласти в один ланцюг всі Стандарти, то отримаємо наступне 27035-2 (готовність)[33] → 27035-1 (керування інцидентом як процес)[33] → 27043 (організація розслідування)[31] → 27037 (правильне отримання/збереження доказів)[29] → 27042[30] (аналіз/інтерпретація) під методичним «контролем якості» 27041[34].

В Україні методом «підтвердження за позначенням» була прийнята наступна низка національних стандартів (ДСТУ), що гармонізовані з міжнародними (ISO/IEC) стандартами, які стосуються саме електронних доказів. Важливо, що ISO лише нещодавно почала рухатися в напрямку розробки стандартів, що стосуються ШІ (див. Додаток И).

Актуальність проблеми допустимості та належності цифрових, зокрема AI-згенерованих, даних у діяльності Національної поліції України обумовлена такими конкретними обставинами:

- по-перше, хоча законодавство України визнає електронні відомості джерелом доказів (ст. 96 Господарського процесуального кодексу України[11], ст. ст. 100-101 Цивільного процесуального кодексу України[152, ст. 100-101], ст. ст. 99-100 Кодексу адміністративного судочинства України[51, ст. 99-100]), закон не містить вичерпного регулювання порядку формування, збереження та перевірки цифрових доказів, отриманих у мережевому середовищі або шляхом автоматизованої обробки інформації. Це створює для слідчих і оперативних підрозділів поліції ризик втрати доказового значення результатів їхньої роботи на стадії судового розгляду.
- по-друге, судова практика Верховного Суду неодноразово фіксувала випадки визнання електронних доказів недопустимими через порушення процедури їх отримання або відсутність можливості перевірити автентичність цифрових даних. Зокрема, у постановах Касаційного кримінального суду звертається увага на необхідність забезпечення безперервності ланцюга збереження електронних носіїв та належного документування дій правоохоронних органів при їх вилученні й дослідженні;
- по-третє, діяльність підрозділів кіберполіції Національної поліції України все більше орієнтується на превентивне виявлення кіберзагроз, що

передбачає використання систем моніторингу мережевого трафіку, аналізу лог-файлів, OSINT-даних, аналізу даних та алгоритмічних моделей виявлення аномалій. Проте результати такої аналітичної діяльності, включно з висновками, сформованими за допомогою штучного інтелекту, наразі мають невизначений процесуальний статус і фактично використовуються лише як допоміжна інформація, без чітких критеріїв їх трансформації у допустимі докази;

- по-четверте, Закон України «Про основні засади забезпечення кібербезпеки України»[114] покладає на Національну поліцію обов'язок участі у виявленні та розслідуванні кіберінцидентів, однак не деталізує правові механізми фіксації та процесуального використання цифрових слідів, отриманих у ході міжвідомчої інформаційної взаємодії. Це створює нормативний розрив між функціональною роллю поліції в системі кібербезпеки та її процесуальними можливостями у кримінальному провадженні;

- по-п'яте, в умовах імплементації європейських стандартів кібербезпеки та цифрових прав (зокрема положень Будапештської конвенції про кіберзлочинність і практики ЄСПЛ щодо допустимості електронних доказів) відсутність національних правил щодо використання AI-згенерованих даних у діяльності поліції може призвести до порушення принципів законності, пропорційності та передбачуваності втручання у права людини[160, с. 144].

Тому, виходячи з Концепції розвитку штучного інтелекту в Україні (2020), в якій зазначено, що одним з пріоритетних напрямків у сфері науково-технологічних досліджень є розвиток технологій штучного інтелекту[58] та «Білій книзі з регулювання ШІ» (2024) Міністерства цифрової трансформації України, яка пропонує поетапну модель регулювання: від м'якого саморегулювання та стандартів відповідальності розробників – до обов'язкових вимог і державного нагляду, із курсом на гармонізацію українського підходу з правом ЄС[3], а також Європейського підходу (AI Act, 2024), що базується на людино-центриському підході та ризик-орієнтованій моделі: системи AI поділяються за рівнями ризику (неприйнятний, високий, обмежений, мінімальний), а до високоризикових систем висуваються підвищені вимоги

щодо прозорості, якості даних, управління ризиками, людського контролю та простежуваності[123], слід констатувати об'єктивну необхідність нормативного визначення правового статусу даних, згенерованих або оброблених із застосуванням систем штучного інтелекту, у діяльності правоохоронних органів, зокрема Національною поліцією України, а також встановлення чітких процесуальних критеріїв їх допустимості, належності та перевірюваності як доказів у кримінальному провадженні.

Наприклад, ст. 5 Закону ЄС «Про штучний інтелект» забороняє використовувати AI у тому числі у пунктах: d) для проведення оцінки ризиків фізичних осіб з метою оцінки або прогнозування ризику вчинення фізичною особою кримінального правопорушення, виключно на основі профілювання фізичної особи або оцінки її рис особистості та характеристик; e) які створюють або розширюють бази даних розпізнавання обличь шляхом нецільового збору зображень обличь з Інтернету або записів із камер відеоспостереження[123].

В загалі більшість векторів, де українська правоохоронна система може застосувати ШІ, згідно AI Act ЄС підпадає під неприйнятний рівень ризику.

Водночас сучасні підходи до використання ШІ у кримінальній юстиції США (2024) вимагають інвентаризації всіх застосувань ШІ, оцінки впливу на права людини, постійного тестування на упередженість, документування алгоритмів та безперервного моніторингу їх ефективності й ризиків[165].

На наш погляд, для надання результатам, сформованим із застосуванням систем штучного інтелекту, процесуально визначеного статусу доказів та забезпечення їх допустимості за умов прозорості, відтворюваності й експертної верифікації, доцільно реалізувати поетапну модель імплементації.

Етап 1. Пілотне впровадження:

- Міністерство цифрової трансформації України та МВС України мають розробити й затвердити спільні технічні вимоги до прозорості, протоколювання (логування) та людського нагляду для всіх AI-рішень, що застосовуються підрозділами досудового розслідування та оперативними підрозділами (біометрична ідентифікація, аналітика великих масивів даних, автоматизоване зіставлення цифрових слідів тощо). Окремо повинні бути

визначені обов’язкові вимоги до кіберзахисту, конфіденційності, обліку, аудиту та контролю доступу до даних і моделей;

- створюється реєстр застосувань AI у правоохоронній діяльності та розробка типової методики проведення судових експертизи, передбачивши аудит для забезпечення того, щоб аналіз проводився для зазначених цілей, постійний моніторинг і пом'якшення ризиків (відповідно практики США).

Етап 2. Нормативна імплементація (середньострокова перспектива):

- внесення змін до процесуального законодавства (зокрема КПК України, ЦПК України, КАС України) шляхом закріплення «висновку експерта щодо аналізу результатів застосування AI» як процесуального джерела доказів, а також встановлення умов допустимості (вимоги до прозорості, перевірюваності, людського нагляду);

- законодавче визначення класифікації застосувань AI за рівнями ризику з урахуванням сфери використання, чутливості даних та потенційного впливу на права людини;

- розроблення спеціалізованих методик криміналістичних (судово-експертних) досліджень для різних напрямів застосування AI (біометрія, аналіз цифрових слідів, мережеві події, текстова аналітика тощо);

- атестація та державна реєстрація методик проведення судових експертиз відповідно до наказу Міністерства юстиції України від 02.10.2008 № 1666/5 «Про затвердження Порядку ведення Реєстру методик проведення судових експертиз»[98];

- внесення змін до Закону України «Про судову експертизу» з метою інституціоналізації алгоритмічної (AI-орієнтованої) експертизи та встановлення вимог до кваліфікації експертів, включно з технічною компетентністю у сфері машинного навчання й обробки даних[119].

Етап 3. Повна гармонізація з правом ЄС (довгострокова перспектива):

- закріплення в українському законодавстві категорій ризику AI, наближених до AI Act (у т.ч. поняття «високоризикової системи»);

- обов’язковий людський нагляд і протоколювання процедури отримання кожного алгоритмічного результату, що потім використовується як доказ;

- періодична переатестація та аудит таких систем на предмет точності, недискримінаційності та пропорційності застосування[160, с. 146].

Окрім того, що алгоритмічний результат повинен бути закріплений на рівні закону та процесуальних інструкцій МВС, Мін’юсту, ОГП) приведемо вимоги допустимості результатів АІ як доказів:

1. Ідентифікованість та відтворюваність:

- має бути зафіксована конкретна версія АІ (модель, дата навчання, конфігурація);

- для реалізації принципу вимоги до простежуваності та прозорості має бути збережений алгоритмічний протокол (лог прозорості) для конкретної генерації результату.

2. Перевірка якості та упередженості:

- перед використанням система має пройти тестування на точність, чутливість, показники хибнопозитивних/хибнонегативних збігів, а також оцінку дискримінаційних перекосів за захищеними ознаками;

- результати тестування додаються до матеріалів справи. Такий підхід відповідає практиці Міністерства юстиції США, яке вимагає оцінювати вплив АІ на права людини, включаючи виявлення упередженості та постійний моніторинг ризиків.

3. Людський нагляд:

- має бути визначена посадова особа (слідчий, експерт, аналітик), що приймає кінцеве рішення про інтерпретацію результату АІ;

- у матеріалах справи фіксується, що результат не був автоматично прийнятий без критичної оцінки людини. Це є прямою вимогою до високоризикових систем АІ в ЄС: людина повинна мати можливість запобігти або мінімізувати ризики для фундаментальних прав. Також, в ст. 14 Законі України «Про судову експертизу» зазначається відповідальність судового експерта за вчинення дисциплінарного проступку[119, ст. 14].

4. Законність отримання вхідних даних:

- дані, на основі яких модель зробила висновок, мають бути отримані законним шляхом і з дотриманням процесуальних гарантій);
- це має фіксуватися в окремому процесуальному документі (аналог ланцюга збереження речових доказів).

5. Можливість контрперевірки стороною захисту:

- захист повинен мати право доступу до методики, логів прозорості та метрик якості в межах, які не розкривають державну таємницю в повному обсязі, але достатні для ефективного оскарження надійності результату;
- суд зобов'язаний забезпечити реальну, а не формальну можливість поставити під сумнів алгоритмічний результат.

6. Пропорційність і цільове використання:

- збір та аналіз даних повинен бути конкретно обґрунтованим потребами провадження, а не використовуватись для невибіркового масового спостереження та здійснюватися під людським наглядом;
- застосування AI не може порушувати право на приватність, захист персональних даних та недоторканність приватного життя (Розділ II Конституція України)[57];
- будь-які алгоритми прогнозування поведінки особи / «ймовірності вчинення злочину» без фактичних даних про конкретні події будуть кваліфікуватися як такі, що створюють неприйнятний рівень ризику і, за європейською логікою, підлягають забороні (тобто апріорі не можуть бути джерелом допустимого доказу);
- передбачити право сторони захисту на альтернативну алгоритмічну експертизу.

З двох нормативних моделей, кожна з яких має право на існування:

Модель 1. Цифрового джерела доказу:

Суть: внести до процесуальних кодексів окрему категорію «алгоритмічний результат ШІ як цифрове джерело доказу», за аналогією з електронними доказами.

Тобто сам результат AI вважається електронним доказом, але обов'язково вимагається додатковий «сертифікат достовірності» від акредитованого суб'єкта (аналог технічного свідоцтва), який підтверджує, що файл є оригінальним, не зміненим, отриманим у визначених умовах, а алгоритм пройшов аудит якості.

Модель 2. Оперативно-орієнтована інформація:

Суть: результати AI офіційно не визнаються доказом, але можуть бути використані: для ініціювання слідчих (розшукових) дій; для обґрунтування клопотань; як орієнтувальна інформація для призначення експертизи.

Тобто результати AI не можуть виступати підставою, а служать оперативно-орієтируючою інформацією.

На наш погляд, перша модель найбільш сприятлива для українського правозастосування на сьогодні.

Отже, місце Національної поліції України в національній системі кібербезпеки полягає у виконанні нею функції правоохоронного компонента державного механізму протидії кіберзагрозам, спрямованого на охорону прав і свобод людини, а також захист інтересів суспільства та держави від кримінально протиправних посягань у кіберпросторі. Реалізація зазначених повноважень має здійснюватися на засадах законності, із неухильним дотриманням принципу пропорційності та стандартів поваги до прав людини, у межах координаційної моделі національної системи реагування, яка забезпечує узгодження дій поліції з іншими суб'єктами кібербезпеки й підсилює здатність держави до своєчасного та правомірного реагування на актуальні кіберзагрози.

У підсумку адміністративно-правові інструменти протидії кіберзагрозам у діяльності Національної поліції повинні забезпечувати цілісний і послідовний цикл управлінських та процесуальних дій – від превенції і виявлення до реагування, фіксації та належного документування – за умови чіткого дотримання меж компетенції, режимів обігу інформації та процедурних гарантій кримінального провадження. Вирішальне значення при цьому має процесуальна «придатність» отриманих цифрових даних, тобто можливість їх перевірки, відтворення та оцінки судом, а також правомірність способу їх

здобуття і збереження, що визначає результативність поліцейської діяльності не лише на етапі оперативного реагування, а й у площині досягнення кінцевого юридичного ефекту – доведення обставин правопорушення та притягнення винних осіб до відповідальності у встановленому законом порядку.

Насьогодні вбачається, що найбільш реалістичним механізмом розв'язання питання допустимості даних, сформованих системами штучного інтелекту, є їх процесуалізація через інститут судової експертизи із нормативним виокремленням алгоритмічної (цифрової) експертизи. Такий підхід має супроводжуватися обов'язковою верифікацією параметрів точності й похибки, встановленням умов отримання та відтворюваності результатів, а також належним документуванням застосованих методик і процедур, що забезпечить перевірюваність відповідних даних як доказів у кримінальному провадженні[160, с. 145-146].

2.2. Інституційна спроможність протидії кіберзагрозам у системі Національної поліції України

Інституційна спроможність Національної поліції України у протидії кіберзагрозам доцільно розглядати як здатність органу виконувати покладені законом функції (попередження, виявлення, припинення та розкриття кримінальних правопорушень у кіберпросторі, захист прав і свобод людини, забезпечення публічної безпеки), забезпечуючи водночас належну координацію, процесну дисципліну, кадрову компетентність, ресурсну оснащеність і внутрішню підзвітність. Базовий контур такої спроможності формується на перетині:

- загальних засад поліцейської діяльності та організації НПУ, визначених Законом України «Про Національну поліцію»[111];

- спеціального правового поля кібербезпеки, закріпленого Законом України «Про основні засади забезпечення кібербезпеки України»[114];

- режимів обігу інформації (персональні дані, державна таємниця, захист інформації в ІКС) та антикорупційних обмежень[54; 86; 87; 88; 104];

- підзаконних та відомчих актів, які конкретизують структуру, підпорядкування та функції спеціалізованих підрозділів, насамперед Департаменту кіберполіції, Департаменту кримінального аналізу, а також інших підрозділів НПУ.

Початковою умовою інституційної спроможності є чітке визначення місця спеціалізованих підрозділів у структурі НПУ, їх функцій і юрисдикції. Структурне закріплення Департаменту кіберполіції як міжрегіонального територіального органу НПУ здійснено постановою Кабінету Міністрів України від 13 жовтня 2015 року № 831, що закріпило організаційну модель, в якій Департамент кіберполіції функціонує як спеціалізований елемент кримінальної поліції з «горизонтальною» (міжрегіональною) логікою реагування на кіберзлочинність, яка за своєю природою часто виходить за межі адміністративних кордонів[96]. У науковій літературі справедливо підкреслюється, що така модель покликана зменшити фрагментацію реагування, забезпечити концентрацію експертизи та уніфікацію підходів до цифрових доказів і технічних методів протидії. Зокрема В.В. Береза, аналізуючи теоретико-правові аспекти діяльності Департаменту кіберполіції, акцентує на значенні принципів поліцейської діяльності (верховенство права, законність, повага до прав людини) як нормативної «рамки» для спеціалізованої кіберфункції, що має особливо високий ризик втручання у приватність і інформаційні права[2, с. 44-48].

Поряд із кіберполіцією інституційна спроможність НПУ у кіберпросторі підтримується іншими функціональними компонентами. По-перше, це підрозділи кримінального блоку та оперативні підрозділи, які розслідують «змішані» склади правопорушень, коли кіберкомпонент є способом або середовищем вчинення. По-друге, це Департамент кримінального аналізу, який інституційно орієнтований на впровадження аналітичних методів та підвищення ефективності протидії злочинності загалом – ІОСТА, що забезпечує перетворення великих масивів даних у розвідувально-аналітичні висновки для управлінських рішень і пріоритизації[128].

Функціональна юрисдикція кіберполіції в Україні має подвійний вимір:

1. Предметний – за видами кіберзлочинів;

2. Процедурний – за участю у кримінальному провадженні (оперативно-розшукові та слідчі дії у межах повноважень, участь у проведенні оглядів, обшуків, вилучення техніки, забезпечення цифрової криміналістики тощо).

Відомчі та наукові джерела демонструють прагнення до конкретизації завдань кіберполіції як реалізації державної політики у сфері протидії кіберзлочинності, попередження, реагування, інформування громадян та взаємодії з іншими суб'єктами. При цьому практична «пріоритизація» діяльності нерідко зміщується у бік протидії організованим формам кіберзлочинності, оскільки саме вони створюють найбільший сукупний ризик для економіки та критичних сервісів. Така управлінська логіка відображалася й у публічних комунікаціях НПУ: зокрема повідомлялося, що виявлення організованих злочинних хакерських угруповань визначалося як пріоритет у певні періоди. Водночас більш сучасні звіти кіберполіції демонструють перехід до кількісно вимірюваних результатів на напрямі організованої кіберзлочинності (знешкодження організованих груп тощо), що важливо для оцінювання «виходу» інституційної спроможності[23].

Окремий, системоутворювальний аспект спроможності – це підпорядкування та розподіл завдань між підрозділами так, щоб мінімізувати дублювання і «розриви» відповідальності. У кіберпросторі це особливо складно через перетин компетенцій між правоохоронним блоком НПУ, спеціальним суб'єктом технічного реагування у державному секторі (CERT-UA у системі Держспецзв'язку) та іншими суб'єктами національної системи кібербезпеки. CERT-UA офіційно визначає свої завдання як накопичення та аналіз даних про кіберінциденти, ведення державного реєстру кіберінцидентів, надання допомоги власникам об'єктів кіберзахисту, міжнародну взаємодію тощо, що формує «технічний контур» реагування і обміну інформацією, тоді як НПУ реалізує правоохоронну функцію та процесуальне оформлення доказів[124]. Для організаційної стійкості НПУ критично важливою є формалізація каналів взаємодії з CERT-UA/CSIRT та іншими структурами, включно з оперативним обміном індикаторами компрометації, технічними звітами та координацією дій

під час масштабних інцидентів. Нормативний розвиток державних механізмів реагування (зокрема у 2025 році) додатково підсилює вимоги до швидкого повідомлення та координації, що прямо впливає на внутрішні процедури НПУ (чергова служба, первинна фіксація, маршрутизація подій, взаємодія з технічними командами)[20].

З огляду на викладене, організація діяльності підрозділів НПУ у протидії кіберзагрозам має базуватися на керованому циклі управління:

планування → моніторинг/виявлення → оцінювання та пріоритизація → координація реагування → документування → висновки та удосконалення

У корпоративному вимірі цей цикл концептуально корелює з міжнародними стандартами управління інцидентами інформаційної безпеки (зокрема ISO/IEC 27035-1), де підкреслюється структурований підхід до підготовки, виявлення, звітування, оцінювання, реагування та врахування висновків[33]. Хоча поліцейська діяльність регулюється насамперед публічним правом і процесуальними нормами, інтеграція «стандартизованого» підходу до інцидент-менеджменту є методологічно виправданою: вона забезпечує передбачуваність рішень, зіставність практик між регіонами, якісне документування і керованість ризиків. У цьому контексті наукові джерела з адміністративно-правового регулювання інформаційної безпеки в діяльності обґрунтовують необхідність усунення нормативних прогалин, уточнення повноважень і посилення організаційних процедур, щоб правоохоронна реакція була одночасно ефективною та правомірною[44].

Регламентація процедур та стандартизація роботи у кіберпідрозділах НПУ охоплює щонайменше три блоки:

- блок 1. процедури первинного реагування та фіксації події;
- блок 2 процедури роботи з цифровими доказами;
- блок 3 процедури координації і взаємодії (внутрішньої та міжвідомчої).

Метою першого блоку є забезпечення оперативності, законності та цілісності даних на початку реагування, щоб подальші слідчі та аналітичні дії спиралися на коректно задокументовані факти, артефакти та часові мітки. Ключовим ядром другого блоку є належне поводження з цифровими доказами від ідентифікації потенційних джерел до збирання/здобуття, копіювання та збереження з гарантуванням цілісності. Тут методологічною опорою виступає міжнародний стандарт ISO/IEC 27037:2022, який прямо визначає ці процеси як базові дії у роботі з потенційними цифровими доказами та наголошує на збереженні їх цілісності[44]. Для НПУ практичне значення стандартоподібного підходу полягає не лише у технічній коректності вилучення/копіювання (форензичні образи, контрольні суми, ланцюг зберігання), а й у підвищенні процесуальної стійкості доказів, зменшенні ризику визнання їх недопустимими через порушення порядку отримання або сумніви щодо автентичності. Саме тому питання процесуальної допустимості цифрових даних у кіберпровадженнях доцільно пов’язувати з організаційною дисципліною та внутрішніми стандартами виконання, а не лише з рівнем технічної кваліфікації окремого спеціаліста.

Кадрова складова інституційної спроможності охоплює компетентності, спеціалізацію та безперервну підготовку. Розглянемо нормативні орієнтири трудових функцій оперуповноваженого. Так, правовий статус, обсяг повноважень і засади діяльності Національної поліції України визначаються Конституцією України[57], законом України «Про Національну поліцію» (ст. ст. 2, 5, 17, 18, 23, 25, 30, 31)[111], а також спеціальним законодавством – насамперед законом України «Про оперативно-розшукову діяльність»[112], Кримінальним процесуальним кодексом України (ст. ст. 36, 40, 41, 104, 107, 208 глава 21)[62] та законом України «Про основні засади забезпечення кібербезпеки України» (ст. ст. 8-10)[114] та іншими актами. У сукупності ці документи формують цілісну нормативну рамку, в межах якої оперуповноважений поліції як посадова особа оперативного підрозділу реалізує свої функції, взаємодіючи зі слідчими підрозділами, іншими органами публічної влади та інститутами громадянського суспільства[161, с. 99].

Кіберкомпонент трудових функцій кіберполіцейського – це інтегрований контур від аналітичної розвідки та реагування з CSIRT до процесуального збору електронних доказів і міжнародної координації. В нього входять:

- моніторинг кіберпростору та аналітична розвідка;
- реагування на кіберінциденти та міжвідомча взаємодія (CERT/CSIRT, НКЦК);
- оперативно-розшукове забезпечення кіберпроваджень (НСРД);
- електронні докази та цифрова криміналістика;
- протидія кіберзлочинам у сегментах критичної інфраструктури;
- криптоактиви та фінансово-технічні[161, с. 100].

В умовах швидкої еволюції технік атак і зростання ролі шкідливого ПЗ, соціальної інженерії, криптоактивів і хмарної інфраструктури «разова» підготовка персоналу не забезпечує стійкої спроможності; потрібна модель безперервного професійного розвитку, у якій формуються як технічні навички (мережевий аналіз, цифрова криміналістика, робота з логами, реверс-інжиніринг, аналіз шкідливого коду), так і правові/процесуальні компетентності (дотримання прав людини, межі втручання, режим доступу до даних).

Також Україна поступово стає на колії стандартизованого підходу до різних державних процесів. Підготовка та підвищення кваліфікації співробітників поліції не є винятком. Так, у 2020 році впроваджено Державний освітній стандарт зі спеціальності 262 «Правоохоронна діяльність» другого (магістерський) рівня[137], а в 2024 році ввели Державний освітній стандарт зі спеціальності 262 «Правоохоронна діяльність», першого (бакалаврський) рівня[138] та Державний освітній стандарт професії 5162 «Поліцейський (за спеціалізаціями)» для системи професійної (професійно-технічної) освіти[17]. Поряд із державними стандартами розвиваються і професійні стандарти. Зокрема, Професійний стандарт «Слідчий (поліція)» – використовується для проектування програм перепідготовки/підвищення кваліфікації та оцінювання результатів навчання поліцейських[125].

Нині триває активна фаза розробки проєкту професійного стандарту «Оперуповноважений (поліція)»[113], у межах наукового дослідження узагальнено та систематизовано перелік трудових дій у складі відповідних трудових функцій, що відображають як нормативно-правові вимоги до посади, сучасні організаційно-професійні підходи до її реалізації, так і потреби ILP.

У контексті ескалації гібридних загроз і поглиблення цифровізації публічних сервісів професійний профіль кіберполіцейського потребує чіткої систематизації кіберкомпонентів трудових функцій. Нижче узагальнено ключові функції, структуровані за принципами ILP і узгоджені з національним законодавством та міжнародними стандартами, що забезпечує доказовість і пропорційність.

Трудова функція 1. Виконання завдань та повноважень поліції відповідно до правових засад та принципів діяльності поліції:

- знати та вміти застосовувати Конституцію України[57], закон України «Про Національну поліцію»[111], Кримінальний кодекс України[61], Кримінальний процесуальний кодекс України[62], закон «Про запобігання корупції» та інші нормативно-правові акти;
- дотримуватись і втілювати основоположні принципи: верховенства права, пропорційності, законності, недискримінації, публічності, прозорості, поваги до людської гідності;
- дотримуватись антикорупційного законодавства, уникати в своїх діях відносно громадян погроз, принижень, сленгу, ненормативної лексики[161, с. 103].

Трудова функція 2. Виконання письмових доручень слідчого, вказівки прокурора та ухвали слідчого судді суду і запитів повноважних державних органів, установ та організацій про проведення оперативно-розшукових заходів:

- планувати заходи та здійснювати підготовку до реалізації доручення слідчого, дізнавача, прокурора в порядку, передбаченому Кримінальним процесуальним кодексом України, вживає ряд заходів щодо підвищення ефективності зазначеного напрямку діяльності;

- безпосереднє проводити слідчі (розшукові) дії та негласні (розшукові) дії[161, с. 103].

Трудова функція 3. Здійснення комплексу оперативно-розшукових заходів щодо попередження, своєчасного виявлення і припинення кримінальних правопорушень та викриття причин і умов, які сприяють вчиненню кримінальних правопорушень, здійснювати профілактику правопорушень:

- проводити оперативно-розшукові заходи щодо попередження своєчасного виявлення і припинення кримінальних правопорушень (кіберзлочинів) та викриття причин та умов, які спричиняють їх вчиненню;
- виконувати гласні та негласні оперативно-розшукові дії;
- встановлювати зв'язки, канали поширення злочинної інформації;
- брати участь у проведенні слідчих дій[161, с. 104].

Трудова функція 4. Здійснювати оцінку оперативної обстановки, ризик-аналіз та аналітичну розвідку:

- проводити збір інформації про оперативну обстановку;
- застосовувати аналітичну розвідку (ILP) та прогнозно-аналітичну діяльність для ухвалення рішень;
- проводити ідентифікацію загроз та ризиків з подальшим ризик-аналізом та типізацією загроз[161, с. 103-104].

Трудова функція 5. Вживати заходи, які спрямовані на попередження та протидію злочинам і правопорушенням (механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку) у сфері комп'ютерних систем:

- здійснювати ідентифікацію кіберзагроз у межах оперативної обстановки;
- моніторити кіберпростір та виявляти кіберзагрози на предмет виявлення ознак підготовки або вчинення кіберзлочинів;
- проводити слідчі (розшукові) дії та негласні (розшукові) дії у сфері комп'ютерних систем;

- проводити інформаційно-профілактичні заходи в сфері комп’ютерних систем[161, с. 104].

Трудова функція 6. Здійснювати моніторинг та аналіз відкритих джерел з метою подальших аналітичних досліджень, у тому числі руху віртуальних активів:

- ідентифікувати релевантні відкриті джерела;
- застосовувати інструменти OSINT для дослідження, у тому числі криптоактивів;
- встановлювати первинні характеристики об’єктів дослідження та документувати результати моніторингу;
- ідентифікувати гаманці/адреси, кластеризувати транзакції, здійснювати запити до VASP/бірж щодо збереження й надання даних, ініціювати арешт активів і документувати ланцюжок володіння електронними доказами з подальшою інтеграцією *on-chain* та *off-chain* матеріалів у доказову базу;
- виявляти та документувати використання міксерів, cross-chain bridges і криптоанонімайзерів;
- застосовувати та валідувати моделі ШІ для аналітичної підтримки розслідувань і реагування, тобто будувати пайплайни виявлення аномалій і класифікації (фішинг, бот-мережі та інше), забезпечує прозорість і відтворюваність (логування даних/версій, оцінка похибок та упередженості)[161, с. 104].

Трудова функція 7. Набуття нових або вдосконалення раніше набутих знань, умінь, навичок своєї професійної діяльності або галузі знань:

- регулярно проходити тренінги, семінари, курси підвищення кваліфікації, перевірки знань в системі службової підготовки;
- здійснювати поточне вивчення та систематизацію змін у законодавстві, нормативно-правовій базі й спеціалізованій літературі з метою вдосконалення професійної компетентності.

Таким чином, по-перше, перехід до інтелектуально-керованої моделі робить аналітичні спроможності оперуповноваженого

системоутворювальними; без ILP-циклу функції залишаються фрагментарними. По-друге, нормативна база України забезпечує достатні рамки (Нацполіція, ОРД, КПК, кібербезпека), однак професійний стандарт доцільно деталізувати: включити ILP-компетентності, електронні докази, криптоактиви, NIS2-сумісну взаємодію та KPI ризик-орієнтованого типу. По-третє, кіберкомпоненти трудових функцій кіберполіцейського формують наступну взаємодоповнювану систему: аналітика дає змогу приймати обґрунтовані рішення; реагування – трансформувати події у процесуально значущі кейси; процесуальне забезпечення та цифрова криміналістика – перетворювати технічні знахідки на допустимі докази; робота з критичною інфраструктурою – зберігати стійкість життєво важливих послуг; компетентність у криптоактивах – протидіяти фінансовим і технологічним зловживанням у цифровій економіці[161, с. 104-105].

Українські науковці приділяють цьому напрямові окрему увагу. Так, О.М. Бандурка, аналізуючи особливості підготовки поліцейських кіберполіції, підкреслює необхідність врахування специфіки кіберсередовища і тенденцій відомчої освіти, що зумовлює запит на сучасні засоби навчання і цільову спеціалізацію[16, с. 233-237]. Додатково цінним є приклад інституційної підтримки підготовки з боку міжнародних організацій: ОБСЄ запускала та підтримувала програми перепідготовки кіберполіцейських, зокрема 100-годинний курс (жовтень 2016 року) та подальші цикли навчання і оснащення, що в сукупності охоплювали значну кількість співробітників[59; 141; 142]. Для дисертаційного аналізу це важливо як свідчення того, що кадрова спроможність є результатом поєднання внутрішньої кадрової політики, відомчої освіти та зовнішньої партнерської підтримки, причому у майбутньому вагомість саме внутрішніх механізмів безперервного навчання має зростати, аби зменшувати залежність від ситуативних проєктів допомоги.

У межах нормативно-правового аналізу доцільно розглянути технології, що забезпечують ідентифікацію та виявлення аномальної активності у веб-середовищі, оскільки саме веб-сервіси є одним із ключових напрямів сучасних кіберпосягань (бот-мережі, фішинг, обхід автентифікації тощо). Однією з таких

технологій виступає browser fingerprinting, що формує технічний ідентифікатор на основі параметрів клієнтського середовища і може використовуватися як допоміжний інструмент кіберзахисту та інцидент-менеджменту за умови дотримання вимог законодавства про захист персональних даних і принципів пропорційності обробки[163, с. 45-47].

Browser fi ngerprinting може бути частиною таких систем, тому може активно виявляти кіберзагрози та може вправно документувати обхідні дані та сесійні атаки.

Відповідно до наказу ДССЗЗІ № 600 від 2017 року «Про затвердження вимог з технічного захисту інформації» використання browser fi ngerprinting може бути інструментом комплексу організаційних заходів кіберзахисту. Впровадження заходів контролю доступу, моніторингу та журналювання є обов'язковим у захищених інформаційних системах. Browser fi ngerprinting відповідає цим вимогам, оскільки забезпечує:

- неперсоніфікований, але стабільний індикатор користувацької активності;

- виявлення аномалій, включно з підміною сесії, бот-атаками, використанням VPN/Tor/анонімізаторів,

- додатковий фактор ризик-орієнтованої аутентифікації, рекомендований міжнародними стандартами (NIST SP 800-63B).

Доктрина інформаційної безпеки України (Указ Президента № 47/2017) визначає сумісність browser fi ngerprinting із національною системою кіберзахисту. У документі встановлено необхідність:

- впровадження сучасних систем аналізу трафіку;

- моніторингу кіберінцидентів;

- виявлення загроз у реальному часі.

Fingerprinting виконує роль низькорівневої поведеневої телеметрії, що дозволяє:

- виявляти шкідливу автоматизовану поведінку;

- фіксувати спроби обходу автентифікації;

- підсилювати інструменти threat intelligence[163, с. 45].

Browser fingerprinting є перспективним інструментом кіберзахисту в Україні, проте його використання має бути врегульоване через:

- розробку методичних рекомендацій,

- юридичні обмеження щодо приватності,

- чітке визначення правового режиму даних,

- інтеграцію з національною системою кібербезпеки[163, с. 49].

Практичні застосування браузерних відбитків:

1. Безпека та боротьба з шахрайством – верифікація пристрою при авторизації та аналіз транзакцій для виявлення ботів або підозрілих дій.

2. Аналітика та персоналізація – ідентифікація повторних відвідувачів для накопичення анонімної статистики.

3. Цільова реклама та трекінг – створення профілів для рекламних мереж.

4. Вимірювання ефективності та обмеження відбитку браузера досліджена на унікальність, стабільність, продуктивність та прихильність до приватності.

Відбиток браузера є якісним інструментом, але його надійність не абсолютна. Відповідність одного відбитка одному пристрою не гарантується: однакові конфігурації утворюють однаковий відбиток, а часті оновлення програмного забезпечення або зміна обладнання можуть змінити результати. Водночас застосування нечітких хешів та комбінування кількох джерел даних (IP, час, поведінкові патерни) значно підвищує точність, що робить технологію привабливою для захисту від ботів та шахрайства. Розробникам та законодавцям необхідно збалансувати користь (безпека, боротьба з ботами) і ризики (порушення приватності, можливість демографічного профілювання) та встановити чіткі обмеження щодо використання браузерного відбитку[163, с. 48-49].

Окремим, напрямком, який активно розвивається останні роки є використання криптоактивів як інструменту обходу міжнародних санкцій у системі сучасних кіберзагроз[162, с. 122-124].

Сучасна практика обходу санкційних обмежень із використанням криптоактивів демонструє формування кількох стійких типологічних моделей,

які відрізняються за організаційною структурою, видом задіяних цифрових активів, масштабом операцій та рівнем інтегрованості у міжнародні нелегальні фінансові мережі. Узагальнення відповідних підходів дає підстави стверджувати, що криптоактиви вже не є лише допоміжним інструментом тіньового обігу, а перетворилися на окремий елемент інфраструктури ухилення від санкцій, який поєднує фінансові, технологічні та кіберзлочинні компоненти (див. Додаток К).

Першою поширеною типологією є державно афілійована стейблкоїн-інфраструктура. Її сутність полягає у використанні токенів, прив'язаних до національної валюти, випущених або контрольованих структурами, пов'язаними з державними фінансовими інститутами. У наведеному прикладі йдеться про токен, прив'язаний до рубля, емітований або забезпечений структурами для трансакцій поза традиційною системою міжбанківських розрахунків SWIFT. Базовим активом у цій моделі виступає рублевий стейблкоїн, а задекларований масштаб застосування сягає 93,3 млрд доларів США за 10 місяців. Такий формат свідчить про прагнення підсанкційних суб'єктів сформувати альтернативні канали розрахунків, менш залежні від класичних банківських механізмів контролю та міжнародного фінансового моніторингу[162, с. 126-127].

Другою типологією є KBR-орієнтована інфраструктура, під якою слід розуміти використання криптоактивів у зовнішньоекономічних і торговельних схемах, зорієнтованих на обхід експортно-імпортних обмежень. У таблиці як приклад наведено діяльність біржі Garantex, пов'язаної з використанням стейблкоїна USDT, а також згадано обробку значних обсягів транзакцій для Ірану. Окремо підкреслено санкційне реагування OFAC у січні 2026 року Масштаби цієї інфраструктури оцінено приблизно в 1 млрд доларів США. У науковому розумінні така модель відображає поєднання криптовалютних сервісів із міжнародними ланцюгами постачання, що дозволяє мінімізувати прозорість платежів і знижує ефективність санкційних бар'єрів у сфері міжнародної торгівлі[162, с. 127].

Третьою моделлю виступає експлуатація VASP-посередників. Її ключовою ознакою є використання постачальників послуг, пов'язаних з обігом віртуальних активів, які свідомо або через прогалини у комплаєнсі забезпечують маршрутизацію транзакцій через різні юрисдикції. Як приклад наводиться підсанкційний брокер Garantex, а також здійснення маршрутизації через біржу Exved з подальшим спрямуванням активів у суміжних VASP. Основними активами тут виступають USDT і BTC, а масштаб операцій оцінюється у 100 млрд доларів США, не враховуючи строк функціонування самої Garantex. З правової точки зору дана типологія є особливо небезпечною, оскільки демонструє, як легально зареєстровані або напівлегальні сервіси можуть бути інтегровані у схеми санкційного обходу, залишаючись формально частиною міжнародного крипторинку[162, с. 127].

Четверта типологія представлена IT-схемами Корейської Народно-Демократичної Республіки, що поєднують елементи кіберзлочинності, цифрового шахрайства та криптовалютних розрахунків. Її зміст зводиться до використання північнокорейських IT-фахівців у нелегальних компаніях за підробленими особами, де заробітна плата або винагорода конвертується у криптоактиви та далі репатріюється через ETH, USDT або BTC. У таблиці обсяг такої діяльності оцінено у 800 млн доларів США лише за 2024 року Ця типологія є особливо показовою з позицій кібербезпеки, оскільки демонструє взаємодію санкційного обходу з кіберопераціями, підставною цифровою ідентичністю, віддаленим працевлаштуванням та транснаціональними мережами прихованого фінансування[162, с. 127].

П'ятою моделлю є використання міксерів, тумблерів і крос-чейн-мостів. Вона ґрунтується на багатоетапному розщепленні та переміщенні криптоактивів через сервіси, покликані ускладнити трасування транзакцій. У таблиці зазначено, що подвоєне розщеплення відбувається через Tornado Cash з подальшим використанням російськомовних містків; підкреслено також зростання обсягів таких мостів до 2,01 млрд доларів США у 2025 р. До основних активів належать BTC, ETH і USDC. У кримінально-аналітичному вимірі ця типологія становить одну з найбільш проблемних для правозастосування,

оскільки саме міксери та міжмережеві мости забезпечують високий рівень анонімізації, ускладнюють атрибуцію кінцевих бенефіціарів і фрагментують цифровий слід у кількох блокчейн-екосистемах одночасно[162, с. 127].

Шостою типологією є платформні гарантійні сервіси типу Huione, які виконують функцію інфраструктурних вузлів для шахрайства, відмивання доходів і проведення розрахунків між нелегальними учасниками ринку. Їх особливість полягає у наданні гарантійного або посередницького механізму для тіньових транзакцій, включно з розрахунками у стейблкоїнах. Основним активом виступає USDT, а обсяги надходжень, зафіксовані у таблиці, перевищують 98 млрд доларів США за 2021-2025 рр. Значення цієї типології полягає в тому, що такі платформи формують не окрему злочинну операцію, а цілу сервісну екосистему, придатну для системного обслуговування схем санкційного обходу[162, с. 127].

Сьомою типологією є DeFi-шарування, тобто багатоетапне приховування походження активів через децентралізовані кредитні та ліквідні протоколи, свопи, пули ліквідності у поєднанні з крос-чейн-мостами. У таблиці йдеться про використання ETH, USDC та DAI, а також зазначено, що перша санкція щодо DeFi-протоколу була застосована OFAC у січні 2025 року. Ця типологія ілюструє новий етап еволюції санкційного обходу, коли суб’єкти використовують не централізовані біржі чи обмінники, а децентралізовані протоколи без єдиного оператора, що істотно ускладнює як встановлення юрисдикції, так і реалізацію класичних регуляторних важелів впливу[162, с. 127].

Окремі відібрані кейси ДКП НПУ у сфері крипто-злочинності (2024-2026 р.р.) приведені в Додатку И[23; 24; 197; 209; 162, с. 130-131].

Отже, наведені типології свідчать, що ухилення від санкцій із застосуванням криптоактивів є багаторівневим і технологічно адаптивним явищем. Воно охоплює як державно підтримувані стейблкоїн-механізми, так і приватні або напівлегальні біржові та сервісні структури, децентралізовані фінансові протоколи, інструменти анонімізації та кіберзлочинні мережі. Сукупно це підтверджує, що блокчейн-екосистема дедалі частіше

використовується не лише як засіб переказу активів, а як комплексна інфраструктура для маскування фінансових потоків, збереження ліквідності підсанкційних суб'єктів та підтримки суміжних кіберзагроз. Саме тому протидія таким практикам потребує не ізольованого фінансового контролю, а поєднання санкційного комплаєнсу, блокчейн-аналітики, цифрової криміналістики, міжнародної координації та спеціалізованого правового регулювання[162, с. 130].

У зв'язку з чим ми пропонуємо модель Аналітичного Життєвого Циклу Крипто-Санкцій (АЖЦКС) (див. Додаток М), яка передбачає безперервну розвідувальну функцію, інтегровану на усіх фазах – від моніторингу до пост-правозастосовчої стійкості. Модель відображає регуляторні рубежі 2026 року та забезпечує системне поєднання аналітичних, правозастосовних і комплаєнс-механізмів у сфері протидії обходу санкцій із використанням криптоактивів.

На першому етапі здійснюється виявлення аномальних патернів у блокчейні, крос-чейн та мультиактивних потоків у режимі реального часу із застосуванням автоматизованих KYT-рішень, скорингових систем і моніторингових платформ, що формує первинний сигнал підозрілої активності.

Другий етап охоплює атрибуцію псевдоанонімних адрес до реальних суб'єктів через поєднання OSINT, даних VASP, механізмів міжнародного інформаційного обміну та спеціалізованих інструментів аналітичної ідентифікації, результатом чого стає аналітичний звіт, придатний для використання як доказова основа.

На третьому етапі формується пакет розвідки у вигляді аналітичних меморандумів, форензичних висновків та адресних списків, підготовлених для санкційного позначення компетентними органами. Четвертий етап пов'язаний із безпосередньою правозастосовчою дією, що включає замороження активів, арешт, вилучення доменів і запити до емітентів стейблкоїнів та інших посередників (див. Додаток М).

Завершальний, п'ятий етап передбачає постмоніторинг, спрямований на відстеження інфраструктури наступників, міграції користувачів і трансформації схем обходу санкцій, що дає змогу оцінити стійкість санкційного

виконання та своєчасно реагувати на появу нових ризиків[178; 179; 184; 191; 217].

Таким чином, модель АЖЦКС репрезентує перехід від фрагментарного реагування до цілісного аналітико-правового циклу, адаптованого до сучасних кіберзагроз, розвитку ринку віртуальних активів і новітніх вимог міжнародного санкційного регулювання[162, с. 133].

1.3. Координація та взаємодія Національної поліції з іншими суб'єктами кібербезпеки в Україні та на міжнародному рівні

Координація та взаємодія Національної поліції України з іншими суб'єктами кібербезпеки в Україні та на міжнародному рівні є не допоміжною формою діяльності, а однією з ключових організаційно-правових умов ефективної протидії кіберзагрозам. Такий висновок зумовлений природою сучасних кіберзагроз, для яких характерні транскордонність інфраструктури атак, висока швидкість зникнення або трансформації цифрових слідів, використання розподілених хмарних середовищ, доменної інфраструктури, криптосервісів і систем штучного інтелекту, а також накладання кількох правових режимів одночасно – кримінально-процесуального, оперативно-розшукового, адміністративно-правового, інформаційного та режиму захисту персональних даних. Саме тому спроможність держави до належного реагування на кіберінциденти визначається не лише ресурсами окремого органу, а й якістю міжвідомчої та міжнародної взаємодії[100; 114].

У системі національної кібербезпеки України Національна поліція України виконує спеціальну правоохоронну функцію, пов'язану з виявленням, припиненням і розслідуванням кримінальних правопорушень, учинених у кіберпросторі або з використанням інформаційно-комунікаційних технологій. Нормативну основу такої взаємодії становлять, насамперед, Закон України «Про Національну поліцію»[111], який передбачає міжнародне співробітництво поліції в межах її повноважень, Закон України «Про основні засади забезпечення кібербезпеки України»[114], яким Національну поліцію віднесено

до суб’єктів національної системи кібербезпеки, а також норми кримінального процесуального законодавства щодо міжнародного співробітництва у кримінальному провадженні. У цьому контексті координація виступає не лише управлінською категорією, а й юридичним механізмом узгодження компетенцій, процедур та режимів обміну інформацією.

Ключовими партнерами Національної поліції України на внутрішньодержавному рівні є Державна служба спеціального зв’язку та захисту інформації України, Національний координаційний центр кібербезпеки при РНБО України, Служба безпеки України, Міністерство оборони України, Міністерство цифрової трансформації України, а також урядова команда реагування на комп’ютерні надзвичайні події CERT-UA.

Якщо Національна поліція зосереджена переважно на доказуванні, кримінально-правовій кваліфікації та процесуальному супроводі справ, то CERT-UA і галузеві CSIRT-команди забезпечують технічний аналіз інцидентів, реагування, збирання телеметрії, виявлення індикаторів компрометації та координацію технічного стримування. Саме на стику цих функцій виникає одна з центральних науково-практичних проблем: яким чином узгодити потребу в оперативному технічному реагуванні з необхідністю збереження цифрових слідів у формі, придатній для подальшого використання як електронних доказів[100].

Важливим кроком у нормативній інституціоналізації такої взаємодії стало ухвалення Кабінетом Міністрів України постанови від 13 листопада 2025 року № 1471, якою затверджено Порядок взаємодії суб’єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб’єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб’єктами оперативно-розшукової діяльності[100]. Значення цього акта полягає в тому, що він переводить координацію з площини ситуативних контактів у площину формалізованих процедур, зокрема щодо невідкладного інформування, спільного технічного дослідження інцидентів, доступу до технічних деталей кібератак, фіксації та збереження відомостей в електронній формі з урахуванням вимог кримінального

процесуального законодавства. Отже, законодавець фактично закріпив модель, за якої технічне реагування і правоохоронна діяльність мають здійснюватися паралельно, а не послідовно.

Додаткового значення координаційному компоненту надає Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки[53]. У межах цього документа координація між правоохоронними органами, суб'єктами кібербезпеки та іншими інституціями сектора безпеки і оборони розглядається як елемент підвищення спроможності держави до комплексного реагування на нові загрози. Для Національної поліції України це означає необхідність переходу від відомчо замкненої моделі до інституціоналізованої мережевої взаємодії, що передбачає уніфіковані канали комунікації, процедури ескалації інцидентів, узгоджені стандарти документування та спільні підходи до оцінки ризиків.

До числа ключових суб'єктів у зазначеній сфері належить також Служба безпеки України, компетенція якої охоплює протидію кібертероризму, окремим проявам кіберзлочинності та іншим посяганням на державну безпеку в кіберпросторі. Водночас Міністерство оборони України здійснює координацію питань, пов'язаних із кібероборoною держави, тоді як Національна поліція України забезпечує виявлення, припинення та розслідування кримінальних правопорушень, учинених із використанням інформаційно-комунікаційних технологій або спрямованих на цивільний сектор.

Окрему роль у формуванні та реалізації державної політики у сфері цифрової безпеки відіграє Міністерство цифрової трансформації України, діяльність якого пов'язана з розвитком цифрової інфраструктури, упровадженням електронних сервісів та нормативно-організаційним супроводом окремих напрямів цифрової трансформації держави.

Важливим практичним елементом національної системи кібербезпеки є також Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка здійснює моніторинг кіберінцидентів, їх технічний аналіз, а також організовує реагування на відповідні загрози в межах національного кіберпростору[41, с. 144].

У міжнародній науці про кіберзлочинність і поліцейське реагування це описується як перехід від ізольованої відомчої моделі до мережевих конфігурацій безпеки, де правоохоронні органи є одним із вузлів системи, що включає органи кіберзахисту, контррозвідку, регуляторів, критичну інфраструктуру й провайдерів; зокрема Д.С. Волл обґрунтовує, що реальна протидія кіберзлочинності фактично здійснюється в мережах взаємодії та розподілу спеціалізацій, а не в межах організаційної самодостатності. Для України ця методологія додатково актуалізується в умовах воєнного часу та гібридної війни, коли кібератаки можуть одночасно мати кримінальну, диверсійну й воєнну природу, що вимагає не ситуативної, а інституціоналізованої координації між правоохоронними і оборонними органами.

Нормативним підґрунтям координації та взаємодії НПУ виступає, по-перше, загальне правило про міжнародне співробітництво поліції, закріплене Законом України «Про Національну поліцію», відповідно до якого взаємовідносини поліції з компетентними органами інших держав та міжнародними організаціями ґрунтуються, по-перше, на міжнародних договорах і правилах міжнародних організацій, членом яких є Україна[111]. Традиційною основою міжнародного співробітництва у сфері протидії кіберзлочинності залишається Будапештська конвенція про кіберзлочинність[56], включно з мережею контактних пунктів 24/7, а також Другий додатковий протокол до неї[28], спрямований на посилення співробітництва та розкриття електронних доказів. Значення цього інструментарію для України полягає в тому, що він забезпечує правові рамки для прискореного збереження даних, отримання електронних доказів та міждержавної процесуальної взаємодії. Водночас нова Конвенція ООН проти кіберзлочинності формує додатковий універсальний рівень кооперації, який у перспективі може розширити інструментарій міжнародної правової допомоги, але водночас потребує особливої уваги до гарантій прав людини, пропорційності та захисту даних.

По-друге, спеціальний правовий режим задає Закон України «Про основні засади забезпечення кібербезпеки України», який визначає національну систему кібербезпеки, коло суб'єктів забезпечення кібербезпеки та логіку їх взаємодії, а також закріплює НПУ як одного із суб'єктів національної системи кібербезпеки з фокусом на протидії кримінально протиправним посяганням у кіберпросторі[114].

По-третє, практичний вимір міжнародної взаємодії НПУ реалізується у процесуальних формах міжнародного співробітництва під час кримінального провадження, системно врегульованих Розділом IX КПК України[62]. Саме тут виникає ключова наукова проблема: як узгодити технологічну швидкість реагування на інцидент і обмін технічними даними (індикатори компрометації, телеметрія, журнали подій) із вимогами процесуального законодавства (збереження електронних доказів, ланцюг зберігання, контроль доступу, допустимість), не знижуючи ні оперативності, ні гарантій прав та свобод людини[156, с. 308-309].

У рамках питання, що досліджується, важливою подією для української системи в 2025 році є ухвалення Кабінетом Міністрів України у 2025 році спеціального Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти/кібератаки/кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності (постанова КМУ від 13.11.2025 № 1471)[100]. Змістовно це означає перехід від «домовленостей і контактів» до нормативно визначених координаційних процедур: каналів обміну інформацією, правил ескалації, визначення ролей у реагуванні та взаємного залучення.

Також, гарною практикою є утворення Координаційної ради з питань моніторингу реалізації плану заходів, спрямованих на виконання Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки[121], яка виступає інституційно-управлінським інструментом посилення міжвідомчої узгодженості та підзвітності в секторі безпеки і оборони: вона формалізує «центральний вузол»

регулярного нагляду за виконанням реформ, забезпечує синхронізацію дій ключових виконавців та створює процедурну основу для консолідованого контролю результатів і коригування заходів. Це має прикладне значення для НПУ, оскільки такі координаційні механізми підсилюють керованість взаємодії з іншими суб'єктами кібербезпеки (CERT-UA/CSIRT, органами сектору безпеки і оборони, регуляторами, операторами критичної інфраструктури) через уніфікацію управлінських «очікувань» і прозорі контури моніторингу виконання заходів, що випливають із Комплексного стратегічного плану, схваленого актом Президента України[53].

Однак інституціоналізація не усуває, а загострює доктринальні питання про межі та юридичну природу міжвідомчого обміну даними: що передається як «технічна інформація про інцидент», а що становить відомості досудового розслідування; як забезпечити пропорційність обробки персональних даних; якими мають бути стандарти фіксації отриманих «зовнішніх» даних, щоб вони могли набути доказового значення або, принаймні, правомірна підтримувати оперативні рішення. Ця проблематика співвідноситься з висновками Стратегії кібербезпеки України щодо необхідності підсилення планування, координації та вимірюваності політики кібербезпеки, що у практичній площині означає дефіцит керованості комплексної взаємодії та потребу метрик і процедур[117].

На внутрішньодержавному рівні координація НПУ з іншими суб'єктами кібербезпеки об'єктивно вибудовується навколо розмежування сфер технічного реагування та процесуального доказування та механізмів їх синхронізації. У цьому сенсі ключовим вузлом є CERT-UA, завдання якого накопичення й аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів, надання допомоги власникам об'єктів кіберзахисту та міжнародну взаємодію[124; 19]. Для НПУ взаємодія з CERT-UA є не лише обміном інформацією, а питанням узгодження форензічно-обережного реагування: якщо технічна команда концентрується на відновленні сервісів і видаленні шкідливих артефактів, вона може мимоволі змінити або знищити цифрові сліди; якщо ж правоохоронний блок затримує відновлення задля огляду/фіксації, зростають ризики для безперервності критичних функцій.

Відтак, координаційні процедури мають бути спрямовані на мінімізацію конфлікту цілей через стандартизовані алгоритми: первинне «заморожування» релевантних даних, забезпечення контрольованого доступу, логування дій, погодження моментів відновлення, використання інструментів швидкого збереження доказового матеріалу паралельно з технічною мітигацією[156, с. 309-310].

Окремий контур взаємодії НПУ з безпековими та контррозвідувальними суб'єктами актуалізується, коли кібератака потенційно пов'язана з діяльністю іноземних спецслужб, кібертероризмом, диверсією або воєнними діями. Тут проявляється структурна напруга між пріоритетами: для кримінального провадження вирішальною є доказова перспектива (допустимість і відтворюваність), тоді як для безпекового блоку – негайна нейтралізація загрози та режим секретності. Науково це постає як проблема процесуалізації розвідувально-контррозвідувальної інформації: за яких умов і в яких межах результати безпекових заходів можуть бути трансформовані в юридично придатні докази, не порушуючи правових гарантій та режимів охорони інформації, а також як уникнути дублювання дій і некерованого перетоку чутливих даних між органами.

У національній адміністративно-правовій доктрині координаційний характер міжнародної та міжвідомчої взаємодії поліції концептуально підкреслюється низкою робіт українських учених. Зокрема А.В. Калайда у дисертаційному дослідженні доводить, що міжнародне співробітництво органів і підрозділів НПУ має погоджувальний і координаційний характер, потребує визначеного механізму реалізації та інструментів адміністративно-правового регулювання[45]. У контексті кіберзагроз це безпосередньо переноситься на координацію як управлінську функцію: стандарти контактних точок, порядок обміну даними, алгоритми спільних дій, критерії відповідальності та підзвітності. В.М. Бабакін, аналізуючи проблематику міжнародного співробітництва у розслідуванні кіберзлочинів, підкреслює залежність результативності від транснаціональних каналів правової допомоги та конвенційних механізмів – тобто від того, наскільки «юридична швидкість»

координації відповідає швидкості втрати доказів. У прикладній площині Д.Й. Никифорчук показує значення взаємодії підрозділів НПУ й суміжних суб'єктів у протидії злочинам у сфері електронних платежів і банківських розрахунків, що для сучасних кіберзагроз трансформується у постійну потребу координації з фінансовим сектором, телеком-операторами та провайдерами цифрових сервісів[45; 218].

Міжнародна координація та взаємодія НПУ в кіберпросторі має опиратися на поєднання:

- універсальних/регіональних конвенційних механізмів;

- мережевих поліцейських платформ (Europol/EC3, Eurojust, Interpol);

- процедур електронних доказів, які еволюціонують у бік прискорених форм допустимості і належності.

Традиційною основою залишається Будапештська конвенція про кіберзлочинність, яка запроваджує уніфікацію підходів до криміналізації та механізми міжнародного співробітництва, включно з мережею контактних пунктів 24/7 (ст. 35) для надання негайної допомоги – інструментом, що критично важливий саме для координації збереження даних у перші години інциденту[56, ст. 35]. Проте «класична» модель міжнародної правової допомоги часто не відповідає темпу кіберрозслідувань і факту, що значна частина релевантних даних перебуває у приватних провайдерів за кордоном. Саме тому Другий додатковий протокол до Будапештської конвенції спрямований на посилення співробітництва та розкриття електронних доказів, зокрема через прискорені режими й форми прямішої взаємодії, а також підсилення функціоналу 24/7 мережі контактних пунктів[28]. Для НПУ це створює перспективу «координаційного прискорення», але водночас формує складну правову задачу: інституційно визначити відповідальні контактні точки, забезпечити документування й верифікацію отриманих даних, а також гарантувати пропорційність і судовий контроль там, де це потрібно, щоб швидкість не знизила стандарти прав людини.

Окремого аналізу потребує нова Конвенція ООН проти кіберзлочинності, яка, за даними UNODC, була прийнята Генеральною Асамблеєю 24 грудня 2024

року, відкрита для підписання 25 жовтня 2025 року в Ханої й залишатиметься відкритою до 31 грудня 2026 року; набрання чинності прив’язане до набуття статусу учасника 40 державами[220]. Паралельно ця конвенція стала предметом публічної критики щодо потенційних ризиків правам людини через можливість широкого тлумачення окремих положень, що підкреслювали як медіа, так і представники технологічної індустрії та правозахисного середовища[219]. Для України це означає, що міжнародна координація в межах нових універсальних режимів має бути юридично «запобіжена»: приєднання/імплементація повинні супроводжуватися національними гарантіями пропорційності, належної правової процедури й захисту даних, щоб інструменти кооперації не перетворювалися на механізми надмірного втручання.

Інституційний вимір міжнародної взаємодії Національної поліції України посилюється через співпрацю з Europol, насамперед у межах European Cybercrime Centre (EC3), місією якого є зміцнення правоохоронного реагування на кіберзлочинність у Європейському Союзі. Практика міжнародних операцій, координованих Europol, переконливо демонструє, що сучасна протидія кіберзлочинності дедалі більше набуває форми багатоюрисдикційної синхронізованої діяльності, в якій національні поліції виконують функцію елементів єдиної оперативно-аналітичної мережі. Для України це має не лише прикладне, а й концептуальне значення, оскільки в умовах повномасштабної війни кібератаки можуть поєднувати ознаки загальнокримінального правопорушення, диверсійної діяльності, інформаційно-психологічної операції та елементу воєнної агресії[35].

Практика міждержавних операцій, координованих Європолом, демонструє тенденцію до «операційної інтернаціоналізації» протидії кіберзлочинності, коли результат залежить не від одиничного органу, а від синхронізації дій багатьох юрисдикцій. Так, 16 липня 2025 року Європол повідомив, що скоординована міжнародна операція знищила інфраструктуру проросійської мережі кіберзлочинності, пов'язаної з серією атак типу «відмова в обслуговуванні», спрямованих проти України та її союзників. Операція під кодовою назвою «Іствуд» була спрямована проти так званої групи

NoName057(16)[148], яку голландська влада ідентифікувала як таку, що стоїть за серією атак типу «відмова в обслуговуванні» на кілька муніципалітетів та організацій, пов'язаних із самітом НАТО в Нідерландах у 2025 році. Європол заявив, що мережа кіберзлочинності також була причетна до атак у Швеції, Німеччині та Швейцарії. Правоохоронні та судові органи Франції, Фінляндії, Німеччини, Італії, Литви, Польщі, Іспанії, Швеції, Швейцарії, Чехії, Нідерландів та Сполучених Штатів одночасно вжили заходів проти правопорушників та інфраструктури[10].

Також Україна продовжує поглиблювати співпрацю з партнерами у сфері кіберзахисту. Адже досвід України в боротьбі з кібератаками російського агресора допомагає не тільки Україні, а й нашим партнерам у побудові дієвих національних та міжнародних систем кіберзахисту. Про зазначене свідчить інтерес міжнародної спільноти до інформації від українських фахівців на міжнародних заходах із кібербезпеки[70, с. 312].

Треба відмітити, що у міжнародному вимірі кібербезпека України формується як інституціоналізована система договірних і меморандумних зв’язків, що поєднує політико-правові зобов’язання держав, міжвідомчу технічну взаємодію та публічно-приватне партнерство з глобальними технологічними компаніями. Сукупність цих документів створює багаторівневу рамку забезпечення кіберстійкості держави в умовах гібридної війни та подальшої євроінтеграції.

Ключове місце у цій системі займає двостороння безпекова угода між Україною та Сполученими Штатами Америки від 13 червня 2024 року, яка вперше закріплює кібербезпеку як самостійний і довгостроковий напрям міждержавної безпекової співпраці. Угода виходить за межі декларативної підтримки й орієнтована на практичне нарощення спроможностей України щодо захисту державних інформаційних ресурсів і критичної інфраструктури, насамперед енергетичного сектору. Її значення полягає у формуванні стабільної основи для технічної допомоги, обміну інформацією про загрози, спільного реагування на кібератаки та відновлення після інцидентів, що переводить кіберзахист у площину стратегічного безпекового партнерства[15].

На інституційному рівні важливу роль відіграють меморандуми про співпрацю Державної служби спеціального зв'язку та захисту інформації України з профільними органами іноземних держав. Зокрема, меморандум з Агентством з кібербезпеки та інфраструктурної безпеки США (CISA) 2022 року заклав основу для системної міжвідомчої взаємодії у сфері реагування на кіберінциденти, захисту критичної інфраструктури та розвитку національних CERT/CSIRT-спроможностей. Його науково-практичне значення полягає у формалізації каналів обміну технічною інформацією та кращими практиками, що сприяє підвищенню зрілості процесів управління кіберінцидентами в Україні[18].

Аналогічну функцію виконують меморандуми Держспецзв'язку з компетентними органами держав – членів Європейського Союзу, зокрема зі Словенією[145] та Фінляндією[146]. Ці документи спрямовані на гармонізацію підходів до кіберзахисту, обмін досвідом і розвиток спільних ініціатив у сфері стійкості державних систем. Особливий акцент у фінському напрямі робиться на концепції resilience, тобто здатності державних і суспільно важливих функцій безперервно діяти та швидко відновлюватися в умовах криз, що є критично важливим для України в період воєнних і післявоєнних трансформацій.

Окрему групу становлять домовленості України з інституціями Європейського Союзу та НАТО. Важливим кроком у цьому напрямі стало укладення 13 листопада 2023 року Робочої угоди про співпрацю між Національним координаційним центром кібербезпеки при РНБО України, Адміністрацією Державної служби спеціального зв'язку та захисту інформації України та Агентство Європейського Союзу із мережевої та інформаційної безпеки (ENISA)[126]. Для Національної поліції України це має важливе значення з огляду на необхідність адаптації власних підходів до фіксації, збереження й використання цифрових даних відповідно до сучасних європейських вимог щодо ситуаційної обізнаності, інцидент-репортингу та управління кіберризиками. У цьому ж контексті слід враховувати положення Директиви NIS2, яка посилює вимоги до управління кіберризиками, звітування

про інциденти та координації між компетентними органами, формуючи для України нормативний орієнтир у процесі євроінтеграції.

Особливого значення у цьому контексті набуває участь правоохоронного компоненту, насамперед Національна поліція України, у процесах, що формуються в межах взаємодії з ENISA. Хоча ENISA не є правоохоронною інституцією, її рекомендації та аналітичні напрацювання безпосередньо впливають на організацію реагування на кіберінциденти, зокрема у частині взаємодії між технічними командами реагування (CERT/CSIRT) та органами досудового розслідування. Для Національної поліції України це означає необхідність адаптації власних підходів до фіксації, збереження та використання цифрових даних з урахуванням європейських стандартів ситуаційної обізнаності, інцидент-репортингу та управління кіберризиками.

Прийняття у 2022 році Директиви NIS2[183] стало важливим етапом у розвитку правових та організаційних засад забезпечення кібербезпеки Європейського Союзу. Її ухвалення зумовлене необхідністю посилення захисту критичної інфраструктури, мережевих та інформаційних систем держав-членів ЄС, а також адаптації європейської безпекової політики до нових викликів і загроз, що формуються в умовах динамічної цифровізації суспільних відносин.

Порівняно з попередньою редакцією, Директива NIS2 істотно розширює сферу свого застосування. Вона поширюється не лише на традиційно визначені ключові сектори, зокрема енергетику, транспорт і фінансову сферу, а й охоплює нові напрями, серед яких цифрові послуги, водопостачання, виробництво харчових продуктів та сектор інформаційних технологій. Такий підхід свідчить про поглиблення розуміння інституціями Європейського Союзу сучасної природи кіберзагроз, які нині мають комплексний, транссекторальний характер і однаковою мірою впливають як на публічний, так і на приватний сегменти суспільних відносин.

У політико-правовому вимірі NIS2 доцільно розглядати як інструмент стратегічного посилення колективної кіберстійкості Європейського Союзу. Значення такого підходу зумовлене тим, що сучасні кіберзагрози мають транскордонний характер, а отже, потребують узгоджених механізмів

міждержавної взаємодії, обміну інформацією та координації реагування. У цьому контексті формування спільного європейського безпекового простору, в межах якого кожна держава-член виконує визначену функцію у забезпеченні загальної стійкості, є об'єктивно необхідною умовою ефективної протидії кіберризикам[183].

Окрему увагу в Директиві приділено обов'язку суб'єктів господарювання повідомляти про кіберінциденти. Така модель має важливе превентивне та координаційне значення, оскільки сприяє оперативному реагуванню на загрози, забезпечує формування цілісного уявлення про стан кібербезпеки в межах Європейського Союзу та мінімізує ризики фрагментації у сфері кризового реагування. Крім того, запровадження цього механізму створює передумови для більш швидкої мобілізації ресурсів у разі масштабних кіберінцидентів та підвищує ефективність функціонування загальноєвропейської системи кіберзахисту[41, с. 95-96].

Вагомим складником сучасної європейської архітектури кібербезпеки є також Європейська схема сертифікації кібербезпеки на основі загальних критеріїв – EUCC[187]. Зазначений механізм установлює уніфіковані правила та стандарти оцінювання рівня захищеності ІКТ-продуктів, послуг і процесів, що має на меті забезпечення належного рівня довіри до цифрових рішень, які функціонують у межах Єдиного цифрового ринку Європейського Союзу. Упровадження такої схеми сприяє формуванню спільних підходів до підтвердження відповідності засобів кіберзахисту встановленим вимогам, а також підвищує прозорість і передбачуваність у сфері цифрової безпеки.

Водночас слід зауважити, що добровільний характер застосування сертифікації в межах EUCC, а також відмінності у практиках її сприйняття та реалізації державами-членами ЄС зумовлюють низку організаційно-правових викликів. Такі обставини можуть ускладнювати досягнення належного рівня уніфікації у сфері сертифікації кібербезпеки та, відповідно, потребують посилення координації на рівні європейської політики й вироблення узгоджених підходів до практичного застосування цього інструменту.

У цілому EUCC доцільно розглядати як важливий елемент інституційного зміцнення кібербезпеки Європейського Союзу, що сприяє підвищенню рівня довіри, посиленню нормативної єдності та реалізації стратегічних цілей ЄС у сфері захисту кіберпростору[41, с. 96].

Ще одним значущим елементом європейської системи кібербезпеки виступає Європейська організація з кібербезпеки (ECSO), яка функціонує як приватний партнер Європейської Комісії та відіграє важливу роль у розвитку державно-приватного партнерства у цій сфері. Її діяльність відображає сучасну тенденцію до інституціоналізації взаємодії між державними органами, бізнесом, науковими установами та іншими заінтересованими суб'єктами з метою формування узгодженої політики кібербезпеки на рівні Європейського Союзу.

Інтеграція приватного сектору до механізмів реалізації безпекової політики ЄС видається стратегічно обґрунтованою, з огляду на те, що значна частина об'єктів критичної інфраструктури перебуває саме у приватній власності або експлуатується за участю приватних операторів. За таких умов ефективність кібербезпекової політики значною мірою залежить від урахування інтересів приватних компаній, а також від їх фактичної спроможності бути повноцінними учасниками системи запобігання, виявлення та реагування на кіберзагрози. Залучення приватного сектору, у свою чергу, створює передумови для вироблення більш адаптивних, технологічно гнучких та практично орієнтованих механізмів захисту.

Значення співпраці між Європейським Союзом та ECSO полягає також у тому, що таке партнерство демонструє здатність ЄС консолідувати державні й приватні ресурси для реагування на актуальні виклики цифрової епохи. Водночас воно сприяє формуванню нової моделі політичної взаємодії між національними урядами, інституціями Європейського Союзу та приватними заінтересованими сторонами, що в перспективі підвищує загальний рівень стійкості європейського кіберпростору.

Окремого значення набуває той факт, що ECSO об'єднує широке коло суб'єктів з усього Європейського Союзу, включаючи представників бізнесу,

академічного середовища та публічної влади. Така багаторівнева взаємодія не лише сприяє підвищенню рівня кіберзахисту, а й формує інституційне підґрунтя для зміцнення політичної солідарності, розвитку спільного простору вироблення рішень та узгодження підходів до цифрової безпеки.

Разом із тим слід зазначити, що реалізація такої моделі не позбавлена суттєвих труднощів. Взаємодія між державним і приватним секторами об'єктивно потребує досягнення політико-правового компромісу, насамперед у питаннях управління інформаційною безпекою, розподілу відповідальності за захист критичної інфраструктури, а також визначення меж доступу до чутливої інформації. Додатковим ускладнювальним чинником виступає різноманітність національних правових режимів і технічних систем держав-членів, що ускладнює координацію, стандартизацію процедур та ефективний обмін інформацією. У зв'язку з цим Європейський Союз стикається з необхідністю формування по-справжньому скоординованого підходу, реалізація якого потребує високого рівня політичної узгодженості, інституційної довіри та сталої міжсекторальної співпраці[41, с. 98-99].

Проблемним аспектом такої взаємодії залишається узгодження технічної логіки реагування на кіберінциденти, що домінує у практиках ENISA, з процесуальними вимогами кримінального провадження, за які відповідає Національна поліція. У європейській моделі пріоритет надається швидкому обміну інформацією про інциденти, мінімізації шкоди та відновленню функціонування систем, тоді як для правоохоронних органів ключовим є забезпечення допустимості та належності цифрових доказів. Це створює ризик конфлікту цілей, коли оперативне технічне втручання може призвести до втрати або модифікації цифрових слідів, що мають доказове значення. Саме тому співпраця з ENISA має супроводжуватися розробленням і впровадженням в Україні форензічно-орієнтованих протоколів реагування, які дозволяють поєднати інтереси кіберзахисту та кримінального переслідування. У ширшому безпековому контексті взаємодія з ENISA логічно доповнюється співпрацею України з інституціями НАТО, зокрема через меморандуми та технічні угоди з відповідними структурами Альянсу, включно з NATO Communications and

Information Agency (NCIA). Ці домовленості формують підґрунтя для досягнення сумісності та стандартизації у сфері кібербезпеки, що є критично важливим для сучасних систем командування, управління та зв'язку. На відміну від ENISA, яка фокусується на цивільному та регуляторному вимірі кібербезпеки, структури НАТО інтегрують кіберкомпонент у воєнне планування та оборонні операції, що вимагає від України синхронізації цивільних і правоохоронних механізмів реагування з воєнними та оборонними підходами.

Для Національної поліції України це означає розширення функціонального поля діяльності в умовах гібридних загроз, коли кіберінцидент може одночасно мати ознаки кримінального правопорушення, акту воєнної агресії та елементу інформаційної операції. У такій ситуації взаємодія з ENISA та структурами НАТО опосередковано впливає на трансформацію ролі поліції – від класичного суб'єкта досудового розслідування до повноправного учасника національної та міжнародної системи кіберстійкості.

Важливим напрямом є співпраця з міжнародними та донорськими організаціями, зокрема з CRDF Global та Luxembourg House of Cybersecurity. Відповідні меморандуми орієнтовані на розвиток людського капіталу, освітніх і науково-технічних програм, обмін інформацією про кібератаки та підтримку практичних проєктів із підвищення кіберспроможностей. Такі документи доповнюють міждержавні угоди, забезпечуючи гнучкість і швидке реагування на нові типи загроз[84].

Суттєве значення для економічної безпеки держави має меморандум між Міністерством фінансів США та Національним банком України, спрямований на посилення кібербезпеки й операційної стійкості фінансового сектору. Він відображає усвідомлення того, що банківська система є критичним об'єктом кіберзахисту, а її стійкість безпосередньо впливає на макрофінансову стабільність і довіру до державних інституцій[76].

Окремий вимір формують меморандуми України з провідними глобальними технологічними компаніями, зокрема Amazon Web Services та

Microsoft. Хоча ці документи мають переважно рамковий і програмний характер, їх значення для кібербезпеки полягає у створенні інфраструктурної основи цифрової держави, доступі до хмарних технологій, threat intelligence та експертизи з реагування на масштабні кібератаки. У поєднанні з державними гарантіями захисту даних вони сприяють підвищенню стійкості державних інформаційних систем і забезпеченню безперервності цифрових сервісів[120].

Прикладом сучасного інструменту міжсекторальної координації у сфері протидії кіберзагрозам в Україні є національний проєкт «BRAMA», створено Консультативною місією Європейського Союзу в Україні за ініціативи Департаменту кіберполіції Національної поліції України, у партнерстві з громадською організацією МІНЗМІН та компанією Yedynka. Зазначена ініціатива спрямована на протидію фінансовому шахрайству, дезінформації, фішинговим кампаніям, діяльності шахрайських онлайн-ресурсів, а також на підвищення рівня цифрової обізнаності населення[48].

Концептуально проєкт «BRAMA» ґрунтується на моделі публічно-приватного партнерства та залучення громадянського суспільства до забезпечення кібербезпеки, що відповідає сучасним підходам Європейського Союзу до побудови стійких кіберекосистем. Його функціонування передбачає інтеграцію інформаційних потоків від користувачів, фінансових установ, телекомунікаційних операторів і правоохоронних органів, що дозволяє оперативно ідентифікувати загрози та мінімізувати шкоду від кіберінцидентів.

У контексті діяльності Національної поліції України проєкт «BRAMA» має подвійне значення. З одного боку, він виступає додатковим джерелом аналітичної інформації для підрозділів кіберполіції щодо актуальних схем кіберзлочинної діяльності. З іншого – сприяє профілактиці кіберзлочинів, що відповідає превентивній функції поліції, закріпленій у законодавстві України.

Важливо підкреслити, що реалізація таких проєктів актуалізує питання нормативного закріплення механізмів взаємодії між Національною поліцією, приватним сектором та громадськістю у сфері кібербезпеки. У перспективі це потребує формування чітких процедур обміну інформацією, гарантій захисту

персональних даних та визначення правового статусу громадських ініціатив у системі протидії кіберзагрозам[48].

Окремо слід наголосити, що подальший розвиток координації та взаємодії Національної поліції України з іншими суб'єктами кібербезпеки потребує не лише інституційного розширення, а й методологічного доопрацювання. Насамперед ідеться про необхідність розроблення форензічно орієнтованих протоколів реагування на кіберінциденти, які б забезпечували одночасно безперервність технічної мітигації та належне збереження цифрових доказів; нормативного визначення меж і режимів міжвідомчого обміну технічною інформацією; посилення ролі спільних аналітичних продуктів; упровадження узгоджених метрик оцінки ефективності координації; а також розвитку механізмів взаємодії з приватним сектором і громадянським суспільством. У цьому аспекті перспективними видаються моделі, що поєднують функції поліцейського реагування, технічної кібероборони, міжнародного обміну даними та превентивної цифрової просвіти населення.

Узагальнюючи, міжнародні договори та меморандуми України у сфері кібербезпеки формують цілісну багаторівневу модель, в якій поєднуються стратегічні безпекові зобов'язання, міжвідомчі механізми координації та публічно-приватні інструменти технологічної підтримки. Їх наукове та практичне значення полягає у тому, що вони переводять кібербезпеку з площини ситуативного реагування у сферу системного публічного управління, забезпечуючи підвищення стійкості держави, сумісність із міжнародними партнерами та правову визначеність дій суб'єктів національної системи кібербезпеки.

Висновок до розділу 2

Проведений у розділі аналіз підтверджує, що кіберзагрози в Україні слід розглядати як комплексний об'єкт публічно-правового регулювання та правоохоронного реагування, який одночасно зачіпає сферу національної безпеки, захист критичної інфраструктури, публічну безпеку і правопорядок, а

також реалізацію конституційних прав і свобод людини. У цьому контексті ключовим завданням є забезпечення балансу між ефективністю протидії кіберзлочинності та додержанням принципів законності, пропорційності, поваги до прав людини і належної правової процедури, що визначають межі втручання держави у цифровій сфері.

Встановлено, що нормативна основа протидії кіберзагрозам в Україні має багаторівневий характер і включає: по-перше, конституційні засади захисту прав і свобод та безпеки особи; по-друге, профільне законодавство у сфері кібербезпеки та захисту інформації; по-третє, кримінально-правові та кримінально-процесуальні механізми, які визначають підстави відповідальності та правила збирання/фіксації цифрових даних; по-четверте, адміністративно-правові інструменти організації діяльності суб'єктів кібербезпеки і міжвідомчої взаємодії. Така багатокомпонентність зумовлює, що механізм протидії кіберзагрозам з боку Національної поліції України не зводиться до розслідування окремих правопорушень, а охоплює сукупність превентивних, організаційних, аналітичних, оперативних і процесуальних дій у межах компетенції, визначеної законодавством.

Обґрунтовано, що місце Національної поліції України в національній системі кібербезпеки визначається її правоохоронною функцією – виявлення, припинення та розслідування кіберзлочинів, захист прав і законних інтересів фізичних і юридичних осіб, реагування на повідомлення про кіберінциденти, а також участь у міжвідомчих механізмах координації. При цьому дієвість НПУ напряму залежить від чіткого розмежування компетенції між суб'єктами сектору безпеки і оборони, наявності формалізованих процедур взаємодії (обмін інформацією, спільні заходи реагування, спільні аналітичні продукти) та узгодженості дій під час інцидентів, що мають ознаки гібридних загроз або посягань на критичну інфраструктуру.

Доведено, що для практичних потреб НПУ найбільш придатною є ризик-орієнтована класифікація кіберзагроз, яка забезпечує уніфіковану оцінку небезпеки та коректну пріоритизацію реагування. Така класифікація має включати:

- об’єкт посягання (персональні дані, державні інформаційні ресурси, інформаційно-комунікаційні системи, об’єкти критичної інфраструктури);

- спосіб та вектор атаки (фішинг/соціальна інженерія, шкідливе ПЗ, експлуатація вразливостей, DDoS тощо);

- суб’єкт і мотивацію (злочинні групи, інсайдери, квазідержавні актори);

- масштаби та наслідки (локальні/масові, із значною суспільною шкодою, із ризиком порушення прав людини). Саме така багатовимірність відповідає реальній структурі повноважень НПУ і дозволяє узгоджувати управлінські рішення (ресурси, координація, комунікація) з процесуальними вимогами (фіксація, допустимість, доказовість).

Визначено, що критерії оцінювання небезпеки кіберзагроз у діяльності НПУ мають поєднувати юридичні та операційні параметри. До вирішальних належать:

- рівень суспільної значущості та масштаб потенційної шкоди (особливо у випадках, що стосуються критичної інфраструктури, державних реєстрів, масового витоку персональних даних);

- імовірність реалізації загрози та швидкість її розвитку;

- наявність ознак організованості, повторюваності або зовнішнього впливу;

- ступінь уразливості цільових систем та можливість подальшого поширення;

- можливість належного документування та отримання цифрових даних у спосіб, який забезпечує їх процесуальну придатність. У такий спосіб ризик-орієнтованість виступає не лише управлінською категорією, а й інструментом правової обґрунтованості втручання, що мінімізує ризики непропорційних заходів та підсилює стійкість доказової бази.

Системно доведено, що механізм протидії кіберзагрозам НПУ доцільно описувати як послідовний цикл взаємопов’язаних дій: профілактика та моніторинг → виявлення і первинне реагування → оцінювання та пріоритизація ризиків → координація з іншими суб’єктами кібербезпеки → фіксація та збереження цифрових даних → розслідування і процесуальне оформлення →

аналіз уроків та удосконалення практик. Ключовою умовою ефективності такого циклу є стандартизація процедур первинного реагування (щоб уникати втрати даних, порушення ланцюга збереження та подальших сумнівів у доказовості), а також інституційна взаємодія з профільними суб'єктами у сфері кібербезпеки і захисту інформації.

Окремо обґрунтовано, що імплементація міжнародних стандартів і практик має здійснюватися через призму українського правового поля: будь-які технологічні або організаційні рішення повинні бути узгоджені з національними процедурами, компетенцією органів, процесуальними вимогами щодо доказів, а також гарантіями прав людини. Для НПУ це означає пріоритет розвитку правових та організаційних інструментів, які забезпечують одночасно: оперативність реагування; якість міжвідомчої координації; належність і доказовість цифрових даних; прозорість та контрольованість втручання.

Встановлено, що кадрова складова інституційної спроможності кіберпідрозділів охоплює не лише питання укомплектування посад, а насамперед спеціалізацію, компетентнісну модель та безперервний професійний розвиток персоналу. Умови стрімкої еволюції кіберзагроз, поширення шкідливого програмного забезпечення, використання криптоактивів, соціальної інженерії та хмарної інфраструктури зумовлюють потребу переходу від моделі разової підготовки до моделі безперервного професійного розвитку. Така модель має інтегрувати як технічні компетентності – мережевий аналіз, цифрову криміналістику, роботу з логами, аналіз шкідливого коду, реверс-інжиніринг, – так і правові та процесуальні компетентності, пов'язані з дотриманням прав людини, межами втручання, режимом доступу до даних та правилами процесуалізації цифрової інформації.

Аргументовано, що чинна нормативно-правова база України загалом формує достатні правові рамки для діяльності кіберполіцейських, оскільки поєднує положення Конституції України, Закону України «Про Національну поліцію», Закону України «Про оперативно-розшукову діяльність», Кримінального процесуального кодексу України та Закону України «Про

основні засади забезпечення кібербезпеки України». Водночас ці акти мають переважно загальний характер і потребують подальшої функціональної деталізації через професійні стандарти, типові процедури, методичні рекомендації та компетентнісні профілі, адаптовані до сучасних умов цифрової злочинності та розвитку інтелектуально-керованої моделі поліцейської діяльності.

Доведено, що кіберкомпонент трудових функцій кіберполіцейського становить інтегрований функціональний контур, який поєднує аналітичну розвідку, реагування на кіберінциденти, взаємодію з CERT/CSIRT та НКЦК, оперативно-розшукове забезпечення, роботу з електронними доказами, цифрову криміналістику, захист критичної інфраструктури, а також протидію злочинним практикам, пов’язаним із криптоактивами. Такий підхід дозволяє розглядати кіберполіцейського не як вузького технічного виконавця, а як спеціалізованого суб’єкта правоохоронної діяльності, здатного діяти одночасно в аналітичній, процесуальній, координаційній та превентивній площинах.

Обґрунтовано, що впровадження філософії Intelligence-Led Policing трансформує функціональне призначення оперуповноваженого та кіберполіцейського, надаючи аналітичним спроможностям системоутворювального значення. Без повноцінного ILP-циклу – збору, оцінювання, аналізу, інтерпретації та використання інформації для прийняття рішень – функції оперативного працівника залишаються фрагментарними та реактивними. Саме тому ризик-аналіз, аналітична розвідка, типізація загроз, прогнозування та оцінка оперативної обстановки повинні бути не додатковими елементами підготовки, а ядром професійного профілю сучасного кіберполіцейського.

Встановлено, що перспективна модель професійного стандарту «Оперуповноважений (поліція)» має бути істотно розширена за рахунок включення компетентностей, пов’язаних із ILP, електронними доказами, OSINT, цифровою криміналістикою, криптоактивами, застосуванням моделей штучного інтелекту в аналітичній підтримці розслідувань, а також NIS2-сумісною взаємодією у сфері кібербезпеки. Така деталізація дасть змогу

привести професійні вимоги до посади у відповідність із сучасними організаційно-правовими викликами та міжнародними тенденціями розвитку поліцейської діяльності в цифровому середовищі.

Доведено, що особливого значення набуває інституціоналізація трудових функцій, пов’язаних з моніторингом відкритих джерел, документуванням результатів OSINT, відстеженням руху віртуальних активів, кластеризацією транзакцій, взаємодією з постачальниками послуг віртуальних активів, виявленням криптоанонімізаторів та використанням моделей штучного інтелекту для виявлення аномалій. Це свідчить про якісне розширення предмета правоохоронної діяльності, у межах якого цифрова аналітика, on-chain/off-chain інтеграція та відтворюваність аналітичних процедур перетворюються на складові належного доказового забезпечення.

Проєкт «BRAMA» засвідчує можливість ефективної реалізації координаційної функції держави у сфері кібербезпеки шляхом інституційної взаємодії органів публічної влади, правоохоронних структур, приватного сектору та громадянського суспільства, а також демонструє потенціал для подальшого нормативного закріплення, інституційного розвитку та інтеграції таких ініціатив у загальнодержавну систему протидії кіберзагрозам.

РОЗДІЛ 3.
ПРОБЛЕМИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У СФЕРІ ПРОТИДІЇ КІБЕРЗАГРОЗАМ

В Розділі 1 нами було розкрито правову природу кіберзагроз, їх ознаки та класифікаційні підходи в сучасному правовому полі, у Розділі 2 – охарактеризовано чинний організаційно-правовий механізм протидії кіберзагрозам у системі Національної поліції України, тому Розділ 3 буде спрямований на виявлення системних «вузьких місць» у нормативному, інституційному та процедурному забезпеченні діяльності НПУ і формулювання обґрунтованих напрямів удосконалення.

Актуальність такого фокусу зумовлена тим, що протидія кіберзагрозам у правоохоронній сфері є динамічним процесом, який залежить одночасно від темпів технологічної еволюції загроз, від здатності інституцій діяти в режимі високої невизначеності та від рівня правової визначеності управлінських і процесуальних процедур.

3.1. Проблеми правового регулювання протидії кіберзагрозам у діяльності Національної поліції України

Правове регулювання такої динамічної сфери, як протидія кіберзагрозам, об’єктивно перебуває у стані постійного оновлення, оскільки законодавець змушений реагувати на зміну технологічного середовища, еволюцію тактик порушників та трансформацію самої архітектури публічного управління у цифровій державі. На користь цього свідчить і емпірична динаміка загроз: за офіційними даними Держспецзв’язку, у 2024 році CERT-UA опрацювала 4 315 кіберінцидентів, що приблизно на 70 % більше, ніж у 2023 році, а від початку 2025 року фіксувала в середньому близько 15 кіберінцидентів на день та відслідковувала понад 150 кластерів кіберзагроз. Така інтенсивність підтверджує, що проблема полягає вже не лише у наявності окремих правових

норм, а у здатності права забезпечити безперервне, скоординоване й процесуально коректне реагування на масивні та різнотипні кіберподії[77; 176].

Наприклад, 11-12 березня 2025 року відбувся другий Київський міжнародний форум кіберстійкості 2025 під гаслом «На захисті демократії». Захід під егідою Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України об'єднав українських та міжнародних представників державного сектору, міжнародних організацій, бізнесу, кіберспільноти, технологічних компаній і провідних експертів галузі для обговорення ключових викликів кібербезпеки. За результатами було підписано Меморандум про співпрацю між Європейським центром компетенцій у кібербезпеці (ECCC) та НКЦК, який сприятиме розвитку інновацій та політик у сфері кібербезпеки, інтеграції українських компаній до європейської кібербезпекової спільноти та посиленню їх конкурентоспроможності завдяки обміну інформацією та спільним дослідженням. «Налагодження співпраці між НКЦК та ключовими агенціями ЄС в сфері кібербезпеки – ENISA та ECCC – є важливим кроком на шляху інтеграції України в Європейський Союз», – підкреслив Сергій Демедюк, заступник Секретаря РНБО України, заступник керівника НКЦК. Також понад 100 експертів з різних секторів обговорювали стратегії кібербезпеки на майбутнє, роль міжнародного співробітництва у глобальному кіберстримуванні, кібероперації у військових конфліктах, гібридні та інформаційні загрози, виклики новітніх технологій та інноваційні рішення для кіберстійкості, розвиток партнерств та екосистеми, ландшафт та аналітика кіберзагроз, кібербезпека регіонів тощо[26].

Також, Службою безпеки України 24 жовтня 2025 року за підтримки міжнародних партнерів проведено форум «Кібертероризм як виклик державі в умовах війни» та командно-штабні кібернавчання «Оберіг 2025», які стали першими в Україні масштабними заходами, спрямованими на обговорення теоретико-правових засад та практичне відпрацювання алгоритмів реагування на кросдоменні загрози терористичного характеру, що поєднують фізичну та кіберскладові. За результатами зазначених заходів встановлено, що наразі бракує належних організаційно-правових інструментів для системної протидії

кібертероризму та кібердиверсіям, а чинна нормативно-правова база не враховує сучасних викликів і загроз, оскільки була розроблена до кристалізації відповідних проблем і потребує невідкладної актуалізації.

Проблеми правового регулювання кібербезпеки впродовж останніх років активно опрацьовуються представниками різних наукових шкіл і напрямів. Базові теоретико-методологічні підходи до інформаційної безпеки та правової природи інформаційних відносин сформовано, зокрема, у працях В.А. Ліпкана, О.О. Баранова, І.В. Діордіци, які заклали концептуальні засади розуміння принципів їх правового регулювання. Вагомий внесок у розвиток зазначеної проблематики зробили дослідження В.М. Фурашєва, В.Л. Грохольського, К.Ю. Ісмайлова, А.І. Марущака, С.Г. Петрова, присвячені аналізу адміністративно-правових механізмів забезпечення інформаційної безпеки. Зарубіжні автори, зокрема М. Шмітт, Т. Рід, Д. Кларк, зосереджують увагу на міжнародно-правових вимірах кібербезпеки та складнощах застосування традиційних норм міжнародного права до кіберпростору.

Водночас значна частина наявних напрацювань має фрагментарний характер і не формує цілісної, комплексної моделі вирішення окреслених проблем. Окремий напрям сучасних досліджень становить аналіз кібератак на критичну інфраструктуру та обґрунтування правових механізмів її захисту. Зокрема, роботи Р.А. Калюжного, О.В. Логінової, М.В. Гуцалюка спрямовані на висвітлення питань правового регулювання охорони державних інформаційних ресурсів і критичних об’єктів інформаційної інфраструктури. Значний науковий інтерес також становлять праці європейських дослідників (Н. Цагурія, П. Маурер, А. Флоріді), у яких розкривається досвід імплементації Директиви ЄС про мережеву та інформаційну безпеку (NIS) і оцінюються можливості його адаптації в національних правових системах[68, с. 166].

Разом із тим недостатньо розробленими залишаються питання узгодження європейських стандартів кібербезпеки зі специфікою українського нормотворення та особливостями функціонування національного законодавства в умовах гібридних загроз. Ця проблема є особливо відчутною з огляду на те, що європейський регуляторний підхід уже перейшов до моделі

безперервного управління ризиками, інцидент-звітності, стійкості ланцюгів постачання та безпеки цифрових продуктів упродовж їх життєвого циклу, що прямо відображено у Директиві NIS2 та Cyber Resilience Act. Для України це означає, що адаптація європейських стандартів не може обмежуватися декларативним запозиченням термінології: вона потребує процесуального «перекладу» цих стандартів у діяльність конкретних суб'єктів, насамперед Національної поліції, яка діє одночасно в межах адміністративно-правового, оперативно-розшукового та кримінально-процесуального режимів[183].

Як підкреслює професор Н.І. Логінова у монографії «Кібернетична безпека держави: теоретико-правовий аспект», стратегічне планування є основою для формування дієвої системи протидії кіберзагрозам та забезпечення національної безпеки в кіберпросторі[67].

Імплементація Стратегії кібербезпеки України здійснюється через затверджені плани заходів, які оновлюються кожного року відповідно до змін безпекового середовища, наприклад Розпорядження КМУ від 07.03.2025 № 204-р «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України»[95].

Принципово важливо, що цей план передбачив не лише загальні політичні орієнтири, а й конкретні завдання, релевантні для правоохоронного сегмента: розроблення механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони, а також проведення щонайменше одного командно-штабного кібернавчання стратегічного рівня за участі, серед інших, Національної поліції. У розвиток цього підходу у 2025 році було ухвалено низку нормативних актів, що свідчать про поступовий перехід від декларативного змісту до процедурної конкретизації: Закон України від 27.03.2025 № 4336-IX щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури[86], який модернізував підходи до кіберзахисту державних інформаційних ресурсів і критичної інформаційної інфраструктури; постанову КМУ від 08.10.2025 № 1281 щодо систематичних тренінгів з кібергігієни[103]; постанову КМУ від 13.11.2025 № 1471, якою затверджено Порядок взаємодії суб'єктів національної

системи реагування з правоохоронними органами[100]; а також постанову КМУ від 26.11.2025 № 1533, що затвердила Національний план реагування на кіберінциденти, кібератаки та кіберзагрози[20]. Сам по собі цей нормативний масив є сильним аргументом на користь висновку, що правове поле кібербезпеки в Україні вже входить у стадію інституційної деталізації, однак саме на цьому етапі найбільш виразно проявляються прогалини його внутрішньої узгодженості.

В.В. Шемчук та О.Л. Костенко у дослідженні «Кіберпростір як сфера національної безпеки: правові засади забезпечення» аналізують специфіку правового регулювання кіберпростору в умовах воєнного стану та приходять до висновку, що правові аспекти забезпечення кібербезпеки в умовах збройного конфлікту потребують особливої уваги з боку законодавця та правозастосовних органів[164, с. 167-174.]. Та підкреслюють необхідність розробки спеціальних норм, які враховують особливості кібероперацій під час збройного конфлікту та забезпечують адекватну правову відповідь на гібридні загрози[68, с. 167].

Отже, щодо різних аспектів правового реагування зазначеної сфери необхідно виділити, по-перше, присутність недостатньої узгодженості між загальними рамками кібербезпеки та конкретними правоохоронними процедурами. На рівні доктрини це постає як розрив між регуляторною моделлю «публічної адміністрації у сфері кібербезпеки» і регуляторною моделлю «кримінальної юстиції», що працюють за різною логікою: перша – за логікою превенції, управління ризиками та реагування, друга – за логікою доказування, процесуальних гарантій і судового контролю. Саме тут і локалізується головна проблема діяльності НПУ: поліція є суб’єктом, який повинен одночасно реагувати швидко, координуватися технічно, фіксувати цифрові сліди, забезпечувати допустимість доказів і не порушувати стандарти прав людини. За відсутності належної процедурної взаємодії між цими режимами будь-яка помилка на ранньому етапі реагування породжує або втрату доказової інформації, або дефекти процесуальної форми, або затримку реагування на інцидент[21; 22].

У практичній площині зазначений розрив концентрується щонайменше у трьох взаємопов’язаних площинах:

1. Дефініційна площина: відсутність уніфікованого, операційно придатного тлумачення категорій «кіберінцидент», «кібератака», «кіберзагроза» в міжвідомчій взаємодії зумовлює різні режими реагування, різні пороги ескалації та, як наслідок, різні юридичні рішення.

2. Процедурна площина: розмежування технічного реагування (локалізація, відновлення, нейтралізація) та процесуальної фіксації (збирання/закріплення відомостей, забезпечення ланцюга збереження) часто залишається не деталізованим, а ситуативним, що знижує передбачуваність і відтворюваність практик.

3. Організаційно-компетенційна площина: межі відповідальності різних суб’єктів у спільних діях (CERT-UA/галузеві CSIRT/власники систем/НПУ/інші органи) не завжди чіткі алгоритми рішень, що породжує ризики дублювання або прогалин відповідальності.

Суттєвим кроком до нормативної узгодженості технічного та правоохоронного контурів стало ухвалення постанови Кабінету Міністрів України від 13.11.2025 № 1471[100], якою затверджено Порядок взаємодії суб’єктів національної системи реагування на кіберінциденти/кібератаки/кіберзагрози із суб’єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб’єктами оперативно-розшукової діяльності. Його нормативна цінність полягає в тому, що він прямо передбачає обмін інформацією про кіберінциденти, проведення спільних заходів під час реагування, надання доступу до технічних деталей кіберінциденту для проведення слідчих (розшукових) дій, а також функціонування міжвідомчих груп реагування. Більше того, Порядок зобов’язує невідкладно інформувати НКЦК про всі значні кіберінциденти та кібератаки, а Національну поліцію – про значні кіберінциденти та кібератаки щодо об’єктів критичної інформаційної інфраструктури. Отже, законодавець фактично визнав, що кіберреагування і

правоохоронне документування більше не можуть існувати як автономні процеси.

Водночас саме поява такого Порядку робить очевидним другий блок проблем – проблему деталізації: хто і на якій правовій підставі ініціює спільні дії; як синхронізуються цілі безперервності функціонування системи та цілі збереження цифрових слідів; які стандарти документування застосовуються для забезпечення ланцюга збереження даних; як фіксуються ролі учасників і межі доступу до даних; хто несе відповідальність за рішення щодо «зачистки» артефактів або відновлення сервісів до завершення первинної фіксації. Постановою КМУ № 1533 від 26.11.2025 ці питання частково конкретизовано через Національний план реагування: він визначає загальні процедури реагування, механізм координації та взаємодії, а також передбачає документування інциденту шляхом формування звіту про реагування. Проте навіть ця новела ще не усуває повністю головної проблеми для НПУ – яким саме чином технічні дані, зібрані у змішаних режимах реагування, мають трансформуватися у процесуально придатний масив доказової інформації[20].

Центральним теоретико-правовим питанням у цьому вузлі є правовий режим технічних даних, зібраних під час реагування на кіберінцидент. Порядок взаємодії фактично визнає, що збір технічних даних і «збирання, фіксація та збереження відомостей в електронній формі» мають співіснувати, але останні повинні здійснюватися з урахуванням вимог кримінального процесу.

Проте КПК України, визначаючи загальну рамку доказування та процесуальних дій, не дає сам по собі технологічно деталізованих відповідей щодо форензичної надійності даних, отриманих поза класичними слідчими діями або в межах змішаних процедур реагування[62]. Звідси виникає прикладна проблема: одна й та сама категорія «технічні дані» може виступати як:

- інформація для управлінського реагування;

- орієнтуюча інформація для оперативно-розшукових заходів;

- фактичні дані, що потенційно набувають статусу доказів у кримінальному провадженні.

Без розмежування цих режимів та їх процесуального закріплення зростає ризик: або втратити оперативність через надмірну формалізацію, або отримати процесуально вразливий доказовий масив.

На рівні вирішення цієї проблеми доцільним є впровадження у відомчих і міжвідомчих стандартних операційних процедур модельного алгоритму «первинного реагування з форензичним запобіганням», який уніфікує мінімально необхідні кроки документування та журналювання дій, розподіл ролей і контроль доступу. Тут доречно спиратися на міжнародно визнані підходи до обігу цифрових доказів, зокрема на ISO/IEC 27037 (настанови щодо ідентифікації, збирання, придбання та збереження цифрових доказів)[29]. Такі стандарти не замінюють КПК, але дозволяють уніфікувати технічну сторону збереження даних, щоб знизити ризики їх компрометації та забезпечити відтворюваність процедур.

Третій блок проблем пов’язаний із балансом між оперативністю протидії кіберзагрозам і гарантіями прав та свобод людини. У правоохоронній площині це означає чітку нормативну визначеність підстав і меж доступу до інформації, пропорційність втручання та належну процесуальну форму. Загальноєвропейський стандарт у цій сфері задається ст. 8 Європейської конвенції з прав людини (право на повагу до приватного і сімейного життя), яка допускає втручання лише за умов законності, необхідності та пропорційності[55, ст. 8]. Практика ЄСПЛ у справі Roman Zakharov v. Russia має тут не загальнотеоретичне, а безпосередньо прикладне значення: Суд констатував, що режими прихованого доступу до комунікацій, які не містять достатніх гарантій проти свавілля та зловживань, несумісні з вимогами статті 8 Конвенції. Для НПУ це означає, що будь-які механізми доступу до трафікових даних, логів, ідентифікаторів пристроїв, журналів авторизації чи інших цифрових слідів мають бути не лише ефективними, а й належно обмеженими законом, процедурно контрольованими і підзвітними. Інакше ризик полягає не лише у порушенні прав людини, а й у подальшій процесуальній дискредитації зібраних матеріалів[170].

Для НПУ це має пряме значення, бо кіберрозслідування часто оперують даними про трафік, комунікації, ідентифікатори пристроїв, логами доступу, а також персональними даними жертв, свідків, адміністраторів і потенційних підозрюваних. Відповідно, додаткові обмеження та вимоги задає Закон України «Про захист персональних даних»[170].

Проблема тут має саме ефективний процесуальний характер: без належного оформлення правових підстав доступу та обробки даних виникає ризик не лише порушення прав, а й процесуальної дискредитації результатів (оспорюваність, визнання недопустимими, неможливість використання). Саме тому у дисертаційному вимірі доцільно ставити питання про адміністративно-правові гарантії якості втручання: внутрішні політики доступу, аудит, розмежування прав, протоколи передачі даних, контроль за дотриманням режимів інформації та службова підзвітність. Нормативну основу режимів доступу до інформації та її захисту задають також Закон України «Про інформацію»[107] та Закон України «Про захист інформації в інформаційно-комунікаційних системах», які формують загальні рамки правомірного обігу й охорони інформації у публічному секторі.

Окремим проблематикою правовому регулюванні є міжнародний компонент кіберрозслідувань: значна частина даних зберігається у провайдерів за межами України, а строк збереження логів часто обмежені. Тому ефективність НПУ залежить від здатності діяти у правових механізмах міжнародної взаємодії. У цьому сенсі ст. 35 Конвенції про кіберзлочинність закріплює модель 24/7 мережі контактних пунктів для надання негайної допомоги у розслідуваннях і збиранні електронних доказів[56, ст. 35].

Важливо, що у профілі України в системі Ради Європи прямо зазначено: функції 24/7 контактного пункту виконує Департамент кіберполіції Національної поліції України; водночас такий канал призначений насамперед для police-to-police запитів щодо кіберзлочинності та електронних доказів. Це підсилює висновок, що міжнародна кооперація у кіберсправах для НПУ не є факультативним елементом, а становить структурну частину правового

механізму протидії кіберзагрозам, яка також потребує чіткішого внутрішньодержавного процедурного забезпечення[154].

Втім на національному рівні це знову актуалізує питання нормативної узгодженості: внутрішньодержавні правила розмежування компетенцій і процедурні механізми мають забезпечувати для НПУ можливість оперативно ініціювати законне збереження даних, водночас гарантуючи належне оформлення підстав, обсягу та меж такого звернення з метою подальшої процесуальної придатності отриманих матеріалів.

Наукове підґрунтя для критичного аналізу цих проблем формують і роботи українських дослідників. Так, І.Д. Казанчук підкреслює наявність особливостей і проблем правового регулювання діяльності НПУ у сфері забезпечення інформаційної безпеки, що методологічно релевантно і для кіберпростору як її частини[44]. Праці І.В. Діордіци, присвячені сутності та призначенню системи забезпечення кібербезпеки, є важливими для розуміння адміністративно-правової логіки національної кібербезпеки як системи з розподілом функцій і координаційним управлінням[21; 22]. А.В. Калайда у дисертаційному дослідженні про міжнародне співробітництво НПУ концептуалізує координаційний характер взаємодії поліції, що прямо переноситься у кіберконтекст як потреба процедурної інституціоналізації співпраці та визначення контактних механізмів[45].

Отже, проблематику правового регулювання протидії кіберзагрозам у діяльності НПУ слід інтерпретувати передусім не як кількісний дефіцит нормативних приписів, а як фрагментарність і неузгодженість регулювання між різними правовими «контурами» – кібербезпековим, інформаційним, кримінально-процесуальним, оперативно-розшуковим і міжнародним – а також як недостатню процедурну конкретизацію спільних техніко-правових дій під час реагування та документування. Відповідно, розв’язання найбільш актуальних питань має бути зосереджене на:

- гармонізації дефініцій і встановленні чітких порогів ескалації у міжвідомчих регламентах;

- упровадженні уніфікованих стандартних операційних процедур первинного реагування із форензичними запобіжниками та контролем ланцюга збереження даних;

- нормативному окресленні правового режиму технічних даних і процедур їх процесуальної інтеграції («легалізації») у кримінальному провадженні;

- посиленні гарантій пропорційності, режимів доступу та підзвітності при обробці персональних даних і роботі з інформацією;

- інституційному забезпеченні прискорених каналів міжнародної взаємодії із належним документуванням правових підстав кожної дії.

Саме такий підхід забезпечує перехід від декларативного нормативного «каркасу» до дієвого правового механізму, здатного гарантувати передбачуваність, відтворюваність і організаційну стійкість правоохоронних практик у кіберпросторі з урахуванням українських реалій.

3.2. Виклики в організації діяльності підрозділів кіберполіції України в умовах воєнного стану

Розглянувши різні аспекти правового регулювання протидії кіберзагрозам у діяльності Національної поліції України, перейдемо в своєму дослідженні до другого блоку проблем – організаційний – в умовах воєнного стану.

Наведені виклики організації діяльності підрозділів кіберполіції України в умовах воєнного стану доцільно концептуалізувати як інтегровану управлінсько-правову проблему, в межах якої взаємодіють і взаємообумовлюються:

- стрімким зростанням інтенсивності та скоординованості кібератак;

- об’єктивною потребою в безперервному технічному реагуванні й підтриманні стійкості сервісів;

- додержанням норм кримінального процесу щодо належності, допустимості та достовірності доказів, а також забезпечення гарантій прав і свобод людини;

- інформаційно-психологічними операціями;

- ресурсним обмеження та підвищені ризики для особового складу й критичної інфраструктури.

Організаційний підхід зосереджується на формуванні ефективної структури управління кібербезпекою та налагодженні взаємодії між різними підрозділами. Розподіл відповідальності та повноважень між суб'єктами забезпечення кібербезпеки здійснюється відповідно до їх компетенції та функціональних обов'язків. Процесний підхід до управління кібербезпекою передбачає стандартизацію процедур реагування на інциденти та 15 впровадження систем управління безперервністю бізнесу. Розвиток механізмів координації та обміну інформацією сприяє підвищенню ефективності протидії кіберзагрозам[66; 71, с. 14-15].

Основні суб'єкти національної системи кібербезпеки України наведені нижче в таблиці[71, с. 36]:

Суб'єкт	**Ключові функції у сфері кібербезпеки**	**Нормативно-правова основа діяльності**
РНБО України	Координація та контроль діяльності суб'єктів сектору безпеки і оборони.	Закон України «Про національну безпеку України»[110].
Національний координаційний центр кібербезпеки	Координація та контроль діяльності у сфері кібербезпеки.	Указ Президента України від 07.06.2025 № 242/2016[109].
Держспецзв'язок	Формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації.	Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»[87].
СБУ	Контррозвідувальний та оперативно-розшуковий захист кіберпростору.	Закон України «Про Службу безпеки України»[118].
Кіберполіція	Протидія кіберзлочинності та забезпечення кібербезпеки.	Положення про Департамент кіберполіції НПУ[96].

Воєнний стан як особливий правовий режим (запроваджений Указом Президента України № 64/2022 та надалі продовжуваний у визначеному законом порядку) об'єктивно трансформує оперативне середовище правоохоронних органів й змінює параметри реагування на кіберзагрози, однак не нівелює вимоги законності та підзвітності владних рішень і дій[85; 115]. Навпаки, за таких умов зростає значущість процедурної бездоганності, оскільки будь-які процесуальні дефекти здатні спричинити втрату доказової спроможності матеріалів, а кіберінциденти воєнного часу нерідко мають прямі наслідки для безперервності критичних функцій держави, безпеки громадян та набувають суспільного резонансу.

З огляду на це, ми нажаль сьогодні маємо можливість в реальному часі спостерігати дію правової системи України в максимально «екстремальних» умовах. Організація діяльності повинно передбачати можливість обмеження прав людини, гарантованих такими нормами Конституції України, на які ми звернем увагу не тільки простим перерахуванням статей, а і зазначаючи їх назви, так як, вважаємо, що це вкрай важливо та чутливо для громадян та країн демократичного вибору сьогодні[57; ст. ст. 30-34, 38, 39, 41-44, 53]:

- ст. 30 «Кожному гарантується недоторканність житла»;

- ст. 31 «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції»;

- ст. 32 «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України»;

- ст. 33 «Кожному, хто на законних підставах перебуває на території України, гарантується свобода пересування, вільний вибір місця проживання, право вільно залишати територію України, за винятком обмежень, які встановлюються законом»;

- ст. 34 «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань»;

- ст. 38 «Громадяни мають право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування»;

- ст. 39 «Громадяни мають право збиратися мирно, без зброї і проводити збори, мітинги, походи і демонстрації, про проведення яких завчасно сповіщаються органи виконавчої влади чи органи місцевого самоврядування»;

- ст. 41 «Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності»;

- ст. 42 «Кожен має право на підприємницьку діяльність, яка не заборонена законом»;

- ст. 43 «Кожен має право на працю, що включає можливість заробляти собі на життя працею, яку він вільно обирає або на яку вільно погоджується»;

- ст. 44 «Ті, хто працює, мають право на страйк для захисту своїх економічних і соціальних інтересів»;

- ст. 53 «Кожен має право на освіту»[57].

Також відповідно до ч. 2 ст. 64 Конституції України, «в умовах воєнного або надзвичайного стану можуть установлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень. Не можуть бути обмежені права і свободи, передбачені статтями 24, 25, 27, 28, 29, 40, 47, 51, 52, 55, 56, 57, 58, 59, 60, 61, 62, 63 цієї Конституції»[57].

Як бачимо у переліку статей, що закріплюють права, які не можуть бути обмеженими в умовах воєнного або надзвичайного стану не має ст. 34, що закріплює право на інформацію. Відтак, влада у цій війні отримує повну законну можливість обмежувати нас в інформаційній свободі і тим самим стримувати розвиток інформаційного суспільства. Однак, в реаліях ми стикаємося з унікальнішою в світі ситуацією, коли саме воєнний стан стає каталізатором розвитку новітніх інституцій інформаційного суспільства[38, с. 167].

Таким чином, проголошується дійсність та дієвість усього комплексу прав, що проголошуються для громадян України в рамках Конституції, у тому числі під час дії воєнного стану. Звісно, комплекс проголошених Конституцією прав та спосіб їх законодавчого формулювання підлягає певній критиці, але більш ґрунтовно ми будемо розглядати це у наступних пунктах нашої

роботи. На цьому ж етапі роботи слід зазначити, що в Україні діє режим свободи слова на найвищому – конституційному рівні[38, с. 71].

Професор М. Корнієнко розглядає воєнний стан як засіб відновлення умов, за яких людина може ефективно реалізувати свої права та свободи. Відповідно, права людини визначають межі діяльності публічної влади щодо введення воєнного стану та засоби, що нею використовуються. При цьому низка прав не може бути обмежена, а обмеження інших прав не може знищувати їх сутність. Окрім визначення прав людини, які не можуть бути обмежені в умовах воєнного стану, конституційно-правові норми визначають особливості реалізації окремих прав за досліджуваних обставин: права на власність та права на працю[60, с. 30].

Також, провідною організаційною проблемою стає розрив між реагуванням і розслідуванням у часі. Реагування вимагає безперервності, інколи – оперативного внесення змін до конфігурацій, ізоляції сегментів мережі, відновлення сервісів, тоді як розслідування потребує стабільного середовища для форензичного зняття копій, збереження журналів подій, фіксації ланцюга збереження та чіткого визначення ролей осіб, що здійснювали втручання. Ця дилема особливо загострюється в атаках на державні реєстри, телеком-інфраструктуру, енергетику та інші критичні системи, де «час простою» має суспільно небезпечні наслідки. Аналітичні огляди українського кіберсередовища та міжнародні звіти неодноразово підкреслювали, що атакуюча сторона у війні проти України поєднує руйнівні інструменти з кампанійністю та синхронізацією з кінетичними/інформаційними діями, що підвищує вимоги до швидкості рішень.

Тому доцільно сформувати і впровадити стандартизовану модель первинного реагування кіберполіції у воєнний час, яка вбудована в міжвідомчу взаємодію й одночасно процесуально придатна. Для цього необхідно спиратися не лише на національні акти, а й на міжнародні стандарти поводження з цифровими доказами та інцидент-менеджменту. ISO/IEC 27037:2022 визначає базові керівні підходи до ідентифікації, збирання, здобуття та збереження цифрових доказів, що дозволяє уніфікувати мінімальні форензичні вимоги

навіть у «гарячому» середовищі інциденту[29]. Для координації реагування між організаціями релевантними є принципи ISO/IEC 27035 (керування інцидентами)[33], який прямо присвячений координації реагування кількох організацій – тобто саме тому, що у воєнний час жоден суб'єкт не може ефективно діяти ізольовано.

Управлінська логіка такої моделі має передбачати «подвійний контур» документування:

1. Технічний журнал інциденту (що зроблено для стримування/відновлення, ким, коли, на підставі якого рішення)$

2. Процесуальний мінімум фіксації (що саме збережено як потенційно доказове: логи, образи носіїв, мережеві дампи, артефакти шкідливого ПЗ, з яких систем, у якому стані, якими засобами, хто мав доступ).

Без цього у воєнний період закономірно виникає друга організаційна проблема – «ефект втрати доказів під час порятунку системи»: швидкі технічні дії, які виправдані з погляду захисту сервісу, можуть знищувати або змінювати сліди, а відтак знижувати доказову перспективу кримінального провадження. Тому в організаційній системі підрозділів кіберполіції слід закріплювати ролі та відповідальність за рішення щодо допустимого рівня «втручання без форензики», а також визначати, які дії можна виконувати негайно, а які – лише після мінімальної фіксації.

Друга група організаційних викликів пов'язана з кадровою спроможністю та відповідними стандартами. Воєнний стан супроводжується мобілізаційними процесами, ротаціями, підвищеним емоційним і професійним вигоранням, що критично впливає на підрозділи, де компетентності формуються роками. Водночас підрозділи кіберполіції мають покривати широкий спектр завдань: від цифрової криміналістики до оперативної аналітики та міжнародної взаємодії.

Оперативно-розшукова ж діяльність детермінується законом як система правових і організаційних засобів здобуття інформації про злочини та осіб, причетних до їх учинення, що для оперуповноваженого означає ініціювання й проведення оперативно-розшукових заходів, застосування оперативно-технічних засобів, роботу з конфіденційними джерелами, забезпечення

належного режиму секретності та доказової верифікації зібраних доказів. Організація взаємодії органів досудового розслідування з іншими підрозділами поліції для запобігання кримінальним правопорушенням, їх виявлення та розслідування, притягнення до встановленої законодавством відповідальності осіб, які їх учинили, відшкодування завданої кримінальними правопорушеннями шкоди, відновлення порушених прав та інтересів фізичних і юридичних осіб здійснюється відповідно до наказу МВС України «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні»[92] та Інструкції щодо реагування на заяви і повідомлення[93].

Своєю чергою кіберкомпонент і міжвідомча координація вибудовуються відповідно до Стратегії кібербезпеки України: Департамент кіберполіції НПУ забезпечує протидію кіберзлочинності, превенцію та взаємодію з приватним сектором і населенням, а CERT-UA, як урядова команда реагування на комп'ютерні інциденти, виступає ключовим партнером поліції у повідомленні, обміні технічною інформацією (показники компрометації, типології атак), первинному реагуванні та ескалації інцидентів[117].

Кіберкомпонент трудових функцій кіберполіцейського – це інтегрований контур від аналітичної розвідки та реагування з CSIRT до процесуального збору електронних доказів і міжнародної координації. В нього входять:

- Моніторинг кіберпростору та аналітична розвідка;
- Реагування на кіберінциденти та міжвідомча взаємодія (CERT/CSIRT, НКЦК);
- Оперативно-розшукове забезпечення кіберпроваджень (НСРД);
- Електронні докази та цифрова криміналістика;
- Протидія кіберзлочинам у сегментах критичної інфраструктури;
- Криптоактиви та фінансово-технічні[161, с. 100].

Третя група організаційних викликів стосується стійкості матеріально-технічної бази та безпечної комунікації. Воєнний контекст означає ризики фізичної недоступності об'єктів, перебої електроживлення та зв'язку,

необхідність резервування, розосередження, евакуаційних планів, а також підвищені вимоги до захисту службової інформації й режимів доступу. Тут з'являється «парадокс воєнного часу»: підрозділи кіберполіції мають ділитися даними швидше і з більшою кількістю партнерів, але одночасно зростає ціна витоку та компрометації каналів. Відповідно, організаційні рішення мають включати не лише закупівлю інструментів, а й побудову архітектури безпечного обміну (контрольовані середовища, журналювання доступу, розмежування прав, шифрування, політики мінімально необхідного доступу) і процедурний порядок передачі артефактів та даних між підрозділами/відомствами. Саме така логіка узгоджується з ідеєю національної системи обміну інформацією про кіберінциденти, яку підкреслює Порядок, затверджений постановою КМУ від 13.11.2025 № 1471[100].

Четверта група викликів – міжвідомча координація у високому темпі подій, коли декілька інцидентів можуть розгортатися паралельно, а загроза має серійний характер. Воєнні кіберкампанії відрізняються повторюваними патернами (інфраструктура, інструменти, групи), тому організаційна ефективність залежить від того, чи здатна кіберполіція перетворити розрізнені епізоди у цілісну картину, придатну для прогнозування та попередження. Саме тут методологічно доречно застосовувати парадигму Intelligence-Led Policing (ILP) як управлінсько-аналітичну рамку: вона дозволяє вибудовувати циклічність «завдання → збір → обробка → аналіз → поширення → зворотний зв'язок» і раціоналізувати ресурси в умовах множинних загроз[128, с. 53-67].

У міжнародній науково-прикладній традиції ILP пов'язують із ризик-орієнтованим управлінням та роллю аналітики у впливі на рішення, що концептуалізовано у працях Дж. Ретклiфа та відображено в сучасних поліцейських настановах з управління розвідданими/аналітикою. Для українського контексту важливо, що існує і національна науково-методична база з цієї проблематики: О.Є. Користін та співавтори розвивають підхід до кримінального аналізу й ILP у сучасних моделях поліцейської діяльності, а також публікують праці, присвячені реалізації філософії ILP у системі кримінального аналізу НПУ. У воєнний період це має прикладний зміст: ILP

може бути організаційною «мовою» для пріоритизації інцидентів, формування «портфеля загроз», планування профілактичних операцій і синхронізації дій між регіонами.

П’ята група викликів – міжнародний вимір інцидентів і доказів. Значна частина інфраструктури (хмарні сервіси, платформи, провайдери, доменні реєстратори) знаходиться поза юрисдикцією України, а «вікна збереження» технічних даних у комерційних провайдерів можуть бути короткими. Тому організаційна спроможність кіберполіції включає готовність до швидких запитів на збереження даних, ефективної комунікації через канали міжнародної взаємодії та документування правових підстав таких дій. На рівні організаційного дизайну це означає: наявність спеціалізованих груп/офіцерів міжнародної взаємодії з цифрових доказів, типові шаблони запитів, внутрішній контроль якості обґрунтувань, а також взаємну «сумісність» з каналами партнерів.

Узагальнюючи, виклики організації діяльності підрозділів кіберполіції у воєнний час можна звести до ключової дилеми: швидкість та безперервність реагування проти процесуальної якості та відтворюваності доказової бази. Вирішення цієї дилеми у дисертаційному вимірі доцільно обґрунтовувати як перехід від «ситуативного менеджменту інцидентів до інституційно закріпленої моделі, у якій взаємодіють три елементи:

1. Міжвідомча рамка координації (національна система реагування/обміну, постанови та процедури взаємодії);

2. Внутрішні стандарти НПУ/кіберполіції (SOP, ролі, тригери ескалації, мінімальні форензичні вимоги);

3. Аналітичне управління ресурсами (ILP як механізм пріоритизації, прогнозування, оцінки ризиків і розподілу сил). Нормативне підґрунтя першого елемента формують Стратегія кібербезпеки України та Порядок взаємодії, затверджений постановою КМУ № 1471; емпіричне підґрунтя другого і третього елементів дають дані CERT-UA та звіти кіберполіції про масштаб і структуру навантаження.

Звідси випливають практично орієнтовані напрями вдосконалення, які одночасно «закривають» проблематику і формують рішення.

По-перше, необхідно створити та затвердити уніфіковані відомчі стандартні операційні процедури первинного реагування кіберполіції у воєнний час, які містять мінімальний стандарт форензичного збереження, алгоритми документування дій та правила взаємодії з CERT-UA/CSIRT у типових сценаріях. Обґрунтуванням для їх структури мають бути міжнародні керівні підходи до цифрових доказів і координації реагування (ISO/IEC 27037; ISO/IEC 27035-4).

По-друге, доцільно інституціалізувати «подвійний контур» управління інцидентом: технічний (безперервність/відновлення) і процесуальний (допустимість/доказовість), із чітким розподілом ролей і сценаріями залучення слідчих та оперативних працівників.

По-третє, слід розвивати кадрову модель через ролеорієнтовані компетентнісні стандарти й безперервну підготовку, спираючись на українські науково-методичні напрацювання з кримінального аналізу та ILP у НПУ.

По-четверте, потрібна технологічно-процедурна інфраструктура безпечного обміну даними, яка забезпечує контроль доступу, журналювання і можливість аудиту, що прямо відповідає логіці національної системи обміну інформацією про кіберінциденти.

По-п’яте, організаційна архітектура має бути аналітично керованою: ILP-цикл повинен впроваджений у щоденне управління, що особливо важливо за умов організованих кібератак і обмежених ресурсів. Міжнародні керівні документи з ILP та кримінальної аналітики (зокрема напрацювання ОБСЄ та UNODC) підтверджують релевантність цього підходу саме для ситуацій високого навантаження, коли потрібні стандартизовані аналітичні продукти для управлінських рішень.

3.3. Напрями вдосконалення правових та організаційних механізмів протидії кіберзагрозам Національною поліцією України

Питання удосконалення механізмів протидії кіберзагрозам у діяльності Національної поліції України набуло системного значення в умовах воєнного стану та стійкого зростання організаційних кібервпливів на державні інформаційні ресурси, критичну інфраструктуру і суспільно значущі сервіси. Нормативно-правову основу української кібербезпеки закріплює базову термінологію, принципи та коло суб'єктів, а також визначає спеціальні ролі на кшталт національної команди реагування CERT-UA. Водночас ефективність саме правоохоронних органів у протидії залежить не стільки від «наявності норм», скільки від здатності трансформувати рамкові приписи у відтворювані управлінські й процесуальні практики НПУ, які одночасно забезпечують швидке реагування та процесуальну придатність цифрових відомостей для кримінального провадження відповідно до вимог КПК України[183].

У сучасній моделі протидії кіберзагрозам НПУ діє не ізольовано: законодавець визначає її як складову національної системи кібербезпеки, де функції розподіляються між органами сектору безпеки і оборони, спеціальними службами, регуляторами, власниками/операторами критичної інфраструктури, а також спеціалізованими CSIRT/CERT[114]. Це означає, що інституційна спроможність поліції в кіберпросторі вимірюється двома взаємопов'язаними параметрами: якістю внутрішньої організаційно-правової архітектури та якістю зовнішньої взаємодії і сумісності (інтероперабельності) із суб'єктами національної системи реагування та міжнародними партнерами. Саме тому, на наш модернізацію механізмів протидії кіберзагрозам доцільно реалізовувати у двох площинах: ILP-орієнтована трансформація трудових функцій оперативного працівника з інтегрованим кіберкомпонентом і розбудова інтероперабельності в кібербезпеці як умови швидкої міжвідомчої взаємодії й доказового обміну.

Вихідною передумовою першої площини є те, що класична реактивна модель оперативної роботи у кіберпросторі об'єктивно програє проактивній моделі.

Кіберкомпонент трудових функцій кіберполіцейського – це інтегрований контур від аналітичної розвідки та реагування з CSIRT до процесуального збору електронних доказів і міжнародної координації. В нього входять:

Моніторинг кіберпростору та аналітична розвідка;

- реагування на кіберінциденти та міжвідомча взаємодія (CERT/CSIRT, НКЦК);
- оперативно-розшукове забезпечення кіберпроваджень (НСРД);
- електронні докази та цифрова криміналістика;
- протидія кіберзлочинам у сегментах критичної інфраструктури;
- криптоактиви та фінансово-технічні активи[161, с. 100].

Усе це зумовлює потребу системної інтеграції трудових функцій у діяльність оперуповноваженого, уніфікації процедур доступу до електронних інформаційних систем та хмарних сервісів, а також закріплення у внутрішніх регламентах вимог до пропорційності втручання, захисту персональних даних, прозорого аудиту НСРД і регулярного підвищення кваліфікації персоналу на стику оперативної, процесуальної та кібербезпекової компетентностей. Отже, сьогодні ми вже спостерігаємо створення нових аналітичних підрозділів у державі, так і в структурі Національної поліції України, а також поступовий перехід інших підрозділів поліції на використання інноваційного інформаційно-аналітичного програмного забезпечення та сучасних методик (SOCTA, IOCTA), що, безумовно, підвищує ефективність діяльності органів та підрозділів поліції. Впроваджується модель проактивної діяльності, яка замінює домінуючу парадигму реактивної поліцейської діяльності, створюючи нову сферу[198, с. 36-37].

Також, українська правоохоронна система поступово стає на колії стандартизованого підходу до різних державних процесів. Підготовка та підвищення кваліфікації співробітників поліції не є винятком. Так, у 2020 році впроваджено Державний освітній стандарт зі спеціальності 262

«Правоохоронна діяльність» другого (магістерський) рівня[137], а в 2024 році ввели Державний освітній стандарт зі спеціальності 262 «Правоохоронна діяльність», першого (бакалаврський) рівня[138] та Державний освітній стандарт професії 5162 «Поліцейський (за спеціалізаціями)» для системи професійної (професійно-технічної) освіти[17]. Поряд із державними стандартами розвиваються і професійні стандарти. Зокрема, Професійний стандарт «Слідчий (поліція)» – використовується для проектування програм перепідготовки/підвищення кваліфікації та оцінювання результатів навчання поліцейських[125].

Як в п.п. 2.2 вже зазначалось нині триває активна фаза розробки проєкту професійного стандарту «Оперуповноважений (поліція)»[113], у межах наукового дослідження узагальнено та систематизовано перелік трудових дій у складі відповідних трудових функцій, що відображають як нормативно-правові вимоги до посади, сучасні організаційно-професійні підходи до її реалізації, так і потреби ILP.

Отже, з урахуванням положень, обґрунтованих у попередніх розділах дисертації, функціональне наповнення діяльності працівників підрозділів кіберполіції доцільно розглядати не як механічну сукупність окремих службових повноважень, а як цілісну систему взаємопов’язаних правових, аналітичних, оперативно-розшукових, процесуальних і профілактичних компонентів. Така система формується на засадах Intelligence-Led Policing, узгоджується з вимогами національного законодавства та міжнародних стандартів і орієнтована на забезпечення законності, пропорційності, доказовості та ефективності правоохоронної діяльності в цифровому середовищі.

Узагальнення проведеного дослідження дає підстави стверджувати, що зміст діяльності кіберполіції охоплює декілька взаємообумовлених функціональних блоків.

Перший із них пов’язаний із реалізацією загальних правових засад поліцейської діяльності, що передбачає дію виключно в межах Конституції та законів України, дотримання принципів верховенства права, законності,

пропорційності, недискримінації, публічності, прозорості та поваги до людської гідності[161, с. 103].

Другий блок становить виконання процесуально визначених доручень слідчого, прокурора, слідчого судді та інших уповноважених суб'єктів, що забезпечує належне поєднання оперативно-розшукової та кримінальної процесуальної діяльності[161, с. 103].

Третій функціональний блок охоплює безпосереднє попередження, виявлення, припинення і документування кримінальних правопорушень, зокрема у сфері використання комп'ютерних систем, мереж та електронних комунікацій. У цьому вимірі діяльність кіберполіції поєднує превентивну, оперативну та доказову складові[161, с. 103].

Четвертий блок формує аналітичний контур її функціонування, що включає оцінювання оперативної обстановки, ідентифікацію загроз, ризик-аналіз, типізацію кримінальних проявів, використання інструментів аналітичної розвідки та прогнозно-аналітичного супроводу прийняття управлінських і процесуальних рішень. Саме цей блок забезпечує перехід від реактивної моделі правоохоронної діяльності до інтелектуально керованої[161, с. 103-104].

Окремого значення набуває функціональний напрям, пов'язаний із моніторингом відкритих джерел, використанням OSINT-інструментів, аналізом руху віртуальних активів, виявленням цифрових зв'язків, документуванням on-chain та off-chain даних, а також застосуванням моделей штучного інтелекту для аналітичної підтримки розслідувань. У сучасних умовах саме цей напрям свідчить про якісне розширення професійного профілю кіберполіцейського, який має володіти не лише класичними правоохоронними компетентностями, а й спеціальними навичками у сфері цифрової криміналістики, аналізу електронних доказів, криптоактивів та алгоритмічних систем підтримки рішень[161, с. 104].

Поряд із цим, невід'ємним елементом професійної моделі є безперервний розвиток компетентностей, що охоплює систематичне оновлення знань, проходження спеціалізованої підготовки, засвоєння змін у законодавстві, оволодіння новими технічними інструментами та адаптацію до нових способів

учинення кіберзлочинів. Такий підхід дає підстави розглядати професійну підготовку не як допоміжний, а як системоутворювальний елемент інституційної спроможності кіберполіції.

Таким чином, із попередньо проведеного аналізу випливає, що діяльність підрозділів кіберполіції повинна будуватися на інтегрованій функціональній моделі, у межах якої правова визначеність, аналітична спроможність, оперативно-розшукова активність, процесуальна коректність, технологічна підготовленість і безперервний професійний розвиток утворюють єдиний організаційно-правовий механізм протидії кіберзагрозам. Саме така модель найбільш повно відповідає сучасним потребам забезпечення кібербезпеки, розслідування кіберзлочинів і зміцнення доказової спроможності Національної поліції України.

Таким чином, можна виділити, шо:

- по-перше, перехід до інтелектуально-керованої моделі робить аналітичні спроможності оперуповноваженого системоутворювальними; без ILP-циклу функції залишаються фрагментарними;

- по-друге, нормативна база України забезпечує достатні рамки (Нацполіція, ОРД, КПК, кібербезпека), однак професійний стандарт доцільно деталізувати: включити ILP-компетентності, електронні докази, криптоактиви, NIS2-сумісну взаємодію та KPI ризик-орієнтованого типу;

- по-третє, кіберкомпоненти трудових функцій кіберполіцейського формують наступну взаємодоповнювану систему: аналітика дає змогу приймати обґрунтовані рішення; реагування – трансформувати події у процесуально значущі кейси; процесуальне забезпечення та цифрова криміналістика – перетворювати технічні знахідки на допустимі докази; робота з критичною інфраструктурою – зберігати стійкість життєво важливих послуг; компетентність у криптоактивах – протидіяти фінансовим і технологічним зловживанням у цифровій економіці[161, с. 104-105].

Друга площина удосконалення – інтероперабельність – є відповіддю на структурну проблему української кібербезпеки: різні суб’єкти часто володіють «частинами пазлу» (індикатори компрометації, телеметрія, мережеві журнали,

артефакти шкідливого ПЗ, відомості про інфраструктуру, фінансові сліди), але відсутність єдиних форматів, узгоджених таксономій і процедур маршрутизації призводить до втрати часу та якості даних. У фаховій роботі з інтероперабельності прямо підкреслено, що українські дослідники фіксують нормативно-правовий розрив: нестачу чітких стандартів для обміну кіберінформацією, неоднорідність відповідальності між держструктурами та слабке законодавче закріплення механізмів автоматизованої взаємодії.

У цьому контексті інтероперабельність у кібербезпеці постає як визначальний чинник забезпечення цілісності, надійності та стійкості кіберпростору. Вона передбачає здатність різних інформаційно-комунікаційних систем, органів державного управління та суб'єктів господарювання діяти узгоджено, на основі спільних стандартів, протоколів і правових норм. Саме інтероперабельність забезпечує безперервний обмін кіберінформацією, координацію реагування на інциденти, спільне управління ризиками та взаємну довіру між національними й міжнародними учасниками системи кіберзахисту[157, с. 107].

Для України питання розвитку інтероперабельності має подвійне значення. З одного боку, воно визначає внутрішню спроможність національної системи кібербезпеки діяти як єдиний координаційний механізм у взаємодії між державними структурами, сектором безпеки та приватними операторами критичної інфраструктури. З іншого – інтеграція до європейського цифрового безпекового простору вимагає адаптації національного законодавства, технічних стандартів і управлінських процесів до норм і практик ЄС, зокрема NIS2[183] та ISO/IEC 27001[199].

На рівні Європейського Союзу зазначений принцип закріплено у Директиві ЄС 2022/2555 (NIS2)[183], Регламенті ЄС 2019/881 (Cybersecurity Act)[214], а також у діяльності Європейської агенції з кібербезпеки (ENISA)[188], яка є ключовою структурою Євросоюзу, що формує політику та стандарти кібербезпеки, включно з механізмами спільного реагування. Ці документи та ініціативи демонструють, що інтероперабельність уже стала базовою умовою кіберстійкості на рівні ЄС[199].

Для підсилення дефініційного апарату дослідження та чіткішого окреслення змістовних меж терміну «інтероперабельність» як системної властивості кібербезпекового середовища здійснено її відмежування від суміжних категорій – «сумісності», «координації» та «стандартизації» (див. Додаток Н)[157, с. 110].

У контексті української інфраструктури слід відзначити роль CERT-UA – центрального елементу національної системи кібербезпеки, відповідальним за виявлення, аналіз і реагування на кіберінциденти в інформаційно-комунікаційних системах країни. CERT-UA функціонує як спеціалізований структурний підрозділ Державної служби спеціального зв’язку та захисту інформації України і координується через Державний центр кіберзахисту[124].

Демонструє активну роль у відслідковуванні й протидії кіберзагрозам. Наприклад, у 2025 році організація повідомляла про щонайменше три кібератаки з використанням шкідливого програмного забезпечення WRECKSTEEL із метою викрадення державних даних[175]. Крім того, CERT-UA виявляє масштабні плани групи Sandworm, спрямовані на порушення функціонування систем критичної інфраструктури у сфері енергетики, водопостачання та теплопостачання в різних регіонах України[157, с. 111].

Якщо розглядати бар’єри впровадження інтероперабельності в Україні, до них належать технічні: відсутність уніфікованих API у багатьох системах, застаріле програмне забезпечення, недостатній рівень інтеграційної інфраструктури; організаційні: слабка координація між державними й приватними суб’єктами, небажання ділитися даними через побоювання юридичної або репутаційної відповідальності; нормативні: законодавча невизначеність, відсутність стандартів обміну кіберінформацією, розбіжності між нормативними актами різних відомств; а також ризики безпеки: відкриті інтерфейси можуть бути використані для атак, і недбале управління доступом може призвести до витоків інформації[157, с. 111].

Для цілісного розуміння феномену інтероперабельності в системі кібербезпеки України представимо її у вигляді багаторівневої моделі, що відображає взаємозалежність технічних, організаційних, правових і

стратегічних компонентів. Така модель дозволяє не лише систематизувати чинники, що визначають ефективність взаємодії суб'єктів кібербезпеки, але й оцінити рівень зрілості держави у забезпеченні цифрової стійкості (див. таблицю «Рівні інтероперабельності у кібербезпеці»)[157, с. 112].

Рівень	Характеристика	Ключові елементи / приклади
Технічний	Забезпечує сумісність IT-систем, мереж, платформ і засобів кіберзахисту шляхом використання узгоджених стандартів і протоколів	Протоколи обміну даними (STIX, TAXII), стандарти ISO/IEC 27001, 27035, засоби SIEM, SOC, CSIRT
Семантичний	Передбачає єдине тлумачення даних, подій і кіберіндикаторів між різними суб'єктами	Єдина система індикаторів кіберзагроз, довідники подій (MITRE ATT&CK, ENISA taxonomy)
Організаційний	Визначає узгодження процедур, політик і процесів між органами державної влади, приватним сектором та міжнародними партнерами	Спільні операційні протоколи CERT-UA, НКЦК, СБУ, НПУ; участь у MISP-мережах; кібернавчання з ENISA
Правовий	Забезпечує нормативне узгодження регламентів, повноважень і вимог до обміну даними, реагування та розслідування інцидентів	Закон України «Про основні засади забезпечення кібербезпеки України», NIS2 Directive, GDPR, Cybersecurity Act
Стратегічний (політичний)	Відображає інтеграцію державної політики у сфері кібербезпеки з європейськими та глобальними стандартами, а також узгодження на рівні управління ризиками	Угода Україна-ENISA (2023), імплементація NIS2, участь у програмі EU Cyber Solidarity Act, стратегія кіберстійкості 2030

Таблиця. Рівні інтероперабельності у кібербезпеці

Узагальнюючи вище викладене, можна зробити наступні висновки та сформулювати перспективи розвитку інтероперабельності в кібербезпеці України та в міжнародному контексті.

По-перше, інтероперабельність є стратегічним інструментом підвищення колективної кіберстійкості: здатність швидко поширювати інформацію про

загрози, корелювати дані з різних джерел і координувати реагування має вирішальне значення у протистоянні сучасним складним атакам. Однак вона несе зі собою нові ризики, серед яких – збільшення площі атаки через інтерфейси, складність контролю доступу та необхідність підтримки довіри між організаціями[157, с. 111-112].

По-друге, український контекст додає специфічні виклики: нестача усталених стандартів обміну кіберінформацією, фрагментарність координації між державою та приватним сектором, юридична невизначеність, а також потреба в міжнародній інтеграції з європейськими системами кібербезпеки. Науковці України вже відзначають ці проблеми та вказують шляхи вирішення через законодавчі оновлення, удосконалення інституційної архітектури та підтримку відкритих даних[157, с. 112].

По-третє, для ефективної реалізації інтероперабельності слід акцентувати увагу не лише на технічних рішеннях, але й на соціальних, організаційних та нормативних компонентах. Важливо формувати мережу довіри між учасниками, розробляти механізми стимулів до участі в обміні кіберінформацією (напр. через страхування ризиків, схеми винагород) і закріплювати відповідальність та правила в законодавстві[157, с. 112].

На наш погляд, перспективи розвитку можна окреслити таким чином:

- удосконалення стандартів «secure-by-design» – кожен стандарт обміну має містити вбудовані механізми автентифікації, шифрування, перевірки цілісності даних та контролю доступу;
- адаптивні моделі довіри – системи, які з урахуванням контексту (рівень ризику, довіра між учасниками), можуть динамічна змінювати рівень доступу та автоматично коригувати правила обміну;
- гібридні підходи обміну – поєднання централізованих і децентралізованих архітектур (наприклад, із використанням блокчейн) для балансування ефективності та безпеки;
- розширення міжнародної інтеграції – активна участь України в європейських та міжнародних ініціативах обміну кіберрозвідданими, узгодження стандартів і правових механізмів, інтеграція з CSIRT-мережами,

участь у відомчих проєктах НАТО/ЄС (що вже частково реалізується (проєкт Трастового фонду Україна – НАТО з питань кіберзахисту). Також, інтеграція з системами ЄС підвищить довіру до українських партнерів у кібербезпеці;

- навчання й розвиток кадрів – створення освітніх програм, тренінгів і симуляційних середовищ, щоб фахівці розуміли як технічні, так і організаційні аспекти інтероперабельності;

- експериментальні пілотні проєкти та тестування – впровадження пробних середовищ, де державні, приватні та академічні установи можуть тестувати обмін кіберінформацією, перевіряти на міцність механізми контролю, верифікації та реагування;

- моделювання економічних взаємодій – розробка економічних моделей, які враховуватимуть стимули й ризики для учасників обміну, щоб уникнути ситуації, коли один учасник «перекладає ризик» на інших[157, с. 112-113].

Реалізація окреслених заходів сприятиме підвищенню національної кіберстійкості України, зокрема шляхом розширення механізмів міжнародного реагування та посилення санкційного впливу на ворожі кіберугруповання, що здійснюють деструктивну діяльність у кіберпросторі. Це стане важливим чинником у зміцненні цифрового суверенітету держави, який визначає здатність України самостійно формувати, контролювати й захищати власний цифровий простір, забезпечуючи незалежність стратегічних інформаційних ресурсів і технологічних процесів.

Водночас, досвід України у протидії масштабним кібератакам російського походження має значний практичний і методологічний потенціал для вдосконалення системи кіберзахисту Європейського Союзу та НАТО. Адаптація та інтеграція цих напрацювань у спільну європейську архітектуру безпеки сприятимуть зміцненню глобальної кіберстійкості і забезпеченню стійкості критичної інфраструктури на міждержавному рівні.

У цьому контексті подальша інтеграція України до європейської системи кібербезпеки має залишатися одним із пріоритетних напрямів державної

політики. Такий підхід не лише підвищить ефективність протидії актуальним загрозам, а й сприятиме стратегічної цифрової автономії України.

Отже, інтероперабельність є фундаментальним поняттям у сфері кібербезпеки, яке означає здатність різних систем, пристроїв або додатків взаємодіяти, обмінюватись даними та ефективно використовувати обміняну інформацію задля полегшення співпраці різних систем, навіть якщо вони розроблені різними постачальниками або організаціями. По-перше, інтероперабельність інструментів кіберзахисту виступає передумовою ефективного функціонування комплексної системи безпеки. Узгоджена взаємодія між різними засобами – такими як міжмережеві екрани, антивірусне програмне забезпечення, системи виявлення та запобігання вторгненням – забезпечує формування цілісного багаторівневого захисного середовища, здатного протидіяти широкому спектру кібератак.

По-друге, інтероперабельність протоколів безпеки гарантує узгодженість механізмів автентифікації, шифрування, контролю доступу та обміну службовими повідомленнями між різними компонентами цифрової інфраструктури. Така координація дозволяє досягти уніфікації процесів захисту інформації, сприяючи безпечній передачі даних і зменшенню ризиків втручання в комунікаційні канали.

По-третє, інтероперабельність у контексті обміну даними розглядається як здатність різнорідних систем здійснювати взаємодію в межах єдиних стандартів і протоколів з метою забезпечення безперервного, надійного та безпечного інформаційного обміну. Застосування таких міжнародно визнаних стандартів, як STIX, TAXII, OpenC2, або моделей сумісності, визначених Європейською агенцією з кібербезпеки (ENISA), створює основу для гармонізації процесів виявлення інцидентів, реагування на них та обміну кіберзагрозами між організаціями[42; 80; 157, с. 112-113].

Все вище сказане дозволяє зробити авторське визначення терміна «інтероперабельність у кібербезпеці», сформульоване відповідно до сучасних підходів Європейської агенції з кібербезпеки (ENISA), директив NIS2, ISO/IEC 27000, а також практик Європейського Союзу щодо створення єдиного

цифрового простору безпеки. А отже інтероперабельність у кібербезпеці – це інтеграційна системна властивість та спроможність технічних, організаційних, процедурних і нормативно-правових компонентів кібербезпекового середовища різних суб'єктів (державних органів, інституцій, підприємств, мережевих інфраструктур) забезпечувати узгоджену, безпечну та безперебійну взаємодію між собою на основі гармонізованих стандартів, протоколів, форматів даних і регламентів обміну інформацією. Її сутність полягає у створенні спільного простору довіри, який уможливлює ефективний обмін даними, координацію дій під час виявлення, реагування та нейтралізації кіберінцидентів, а також підтримання єдиного рівня кіберстійкості та оперативної сумісності у національному й транскордонному цифровому середовищі[157, с. 113].

Висновок до розділу 3

Наведений у розділі аналіз засвідчує, що проблеми організаційно-правової діяльності Національної поліції України у сфері протидії кіберзагрозам мають не стільки нормативно недостатньо врегульований, скільки системний характер. Ключовий виклик полягає у розриві між двома регуляторними контурами: кібербезпековим (превенція, управління ризиками, технічне реагування, безперервність сервісів) та нормами процесуального характеру (доказування, процесуальні гарантії, судовий контроль). Унаслідок цього навіть за наявності значного масиву учасників у сфері кібербезпеки та інформаційних відносин зберігаються дефініційні розбіжності, неоднакові пороги ескалації, ситуативність процедур первинного реагування, а також недостатня процесуальна визначеність правового режиму технічних даних, зібраних під час інциденту.

Дослідження проблем правового регулювання (підрозділ 3.1) дозволяє констатувати, що найбільш вразливою ланкою є процедурна конкретизація спільних «техніко-правових» дій під час інцидентів: хто і на якій підставі ініціює взаємодію; як синхронізуються цілі відновлення працездатності

системи та завдання збереження цифрових слідів; які стандарти документування забезпечують ланцюг збереження; як розмежовуються режими використання технічних даних (управлінський, оперативно-розшуковий, доказовий). Окрему групу становлять питання прав людини та захисту персональних даних: у кіберрозслідуваннях ризики непропорційного втручання та процесуальної вразливості матеріалів зростають, а отже потрібні внутрішні політики доступу, аудит, розмежування ролей і підзвітність як адміністративно-правові гарантії «якості втручання». Водночас міжнародний компонент кіберрозслідувань підсилює вимогу до швидких каналів збереження даних і належного документування правових підстав кожної дії, оскільки значна частина доказово значущої інформації перебуває у провайдерів за межами юрисдикції України та має обмежені строки зберігання.

Виклики організації діяльності підрозділів кіберполіції у воєнний час (підрозділ 3.2) показали центральну дилему: необхідність безперервного, швидкого технічного реагування на інциденти протиставляється потребі забезпечити процесуальну якість та відтворюваність цифрових доказів. Воєнний стан об’єктивно підвищує інтенсивність і «кампанійність» атак та актуалізує питання простою критичних систем, однак не знімає вимог законності, пропорційності та підзвітності. Отже, організаційна ефективність кіберполіції має будуватися на інституційно закріпленій моделі, що поєднує міжвідомчу координацію, внутрішні стандартні операційні процедури (SOP), мінімальні форензичні вимоги і аналітично кероване управління ресурсами. Додатково окреслено кадрові та матеріально-технічні обмеження, ризики безпечної комунікації та обміну даними, а також необхідність перетворювати сукупність інцидентів на цілісну аналітичну картину для прогнозування та попередження, що методологічно узгоджується з підходами Intelligence-Led Policing.

У підрозділі 3.3 обґрунтовано, що напрями вдосконалення мають реалізовуватися у двох взаємодоповнюваних площинах. Перша – ILP-орієнтована трансформація трудових функцій і компетентностей працівників, з інтеграцією кіберкомпонента (OSINT-аналітика, реагування в координації з

CERT/CSIRT, робота з електронними доказами та цифровою криміналістикою, міжнародна взаємодія, протидія злочинам щодо критичної інфраструктури, криптоактиви, штучний інтелект), а також із систематичним підвищенням кваліфікації та деталізацією професійних стандартів. Друга – розбудова інтероперабельності у кібербезпеці як умови швидкої взаємодії та доказово коректного обміну даними: йдеться про технічну, семантичну, організаційну, правову та стратегічну сумісність, що забезпечує створення «простору довіри», зниження втрат часу і якості даних, а також інтеграцію України до європейської кібербезпекової екосистеми.

Таким чином, розв’язання окреслених проблем доцільно спрямувати на перехід від рамкового нормативного «каркасу» до відтворюваних управлінських і процесуальних практик у НПУ. Пріоритетними є: гармонізація дефініцій та порогів ескалації у міжвідомчих регламентах; упровадження уніфікованих SOP первинного реагування із форензичними запобіжниками та контролем ланцюга збереження; нормативне окреслення правового режиму технічних даних і процедур їх процесуальної інтеграції у кримінальному провадженні; посилення гарантій пропорційності, режимів доступу та підзвітності при обробці персональних даних; інституційне забезпечення прискорених каналів міжнародної взаємодії з належним документуванням підстав кожної дії; а також аналітичне управління ресурсами на основі ILP-циклу. Реалізація цих напрямів формує підґрунтя для підвищення кіберстійкості держави, зміцнення доказової спроможності кіберрозслідувань і забезпечення належного балансу між безпекою та правами людини в умовах воєнних і гібридних загроз.

ВИСНОВКИ

Проведене дисертаційне дослідження забезпечило комплексне теоретико-методологічне та організаційно-правове осмислення протидії кіберзагрозам у діяльності правоохоронного компонента національної системи кібербезпеки. Узагальнені результати дисертаційного дослідження дозволяють сформулювати такі основні висновки:

1. Показано нетотожність дефініцій «інформаційна безпека» та «кібербезпека» й обґрунтовано, що кібербезпека має більш визначений операційний контур (стійкість мереж і систем, реагування та відновлення), тоді як інформаційна безпека охоплює ширші політико-правові та комунікаційні аспекти, унаслідок чого кіберзагрози постають концентрованим проявом загроз в інформаційній сфері саме у цифровому середовищі.

2. Концептуалізовано кіберзагрози як самостійний різновид загроз національній безпеці та встановлено, що, характеризуючись нематеріальністю слідів, транскордонністю, масштабованістю й асиметричністю впливу, вони в умовах загальної цифровізації держави та гібридних/воєнних викликів набувають підвищеної суспільної небезпечності, що зумовлює їх прямий вплив на реалізацію прав і свобод людини, функціонування критичних сервісів і стійкість держави.

3. Уточнено категоріально-понятійний апарат і методологічні засади ризик-орієнтованого підходу та доведено, що принципове розмежування понять «загроза» як динамічної ймовірнісної категорії і «небезпека» як стану наявної вразливості/дефіциту захищеності є необхідною передумовою формування правових і управлінських механізмів оцінювання, пріоритизації та ескалації кіберінцидентів.

4. Сформульовано комплексне техніко-юридичне визначення поняття «кіберзагроза» і сформовано науково придатну для практики Національної поліції України модель їх класифікації, доведено, що кіберзагрози, з одного боку, проявляються як технологічні вектори (шкідливе ПЗ, експлуатація вразливостей, DDoS, компрометація ланцюгів постачання, атаки на хмарні

сервіси, соціальна інженерія тощо), а з іншого – детермінують застосування матеріально-правових і процесуальних норм (управління ризиками, інцидент-репортинг, режими доступу, аудит, збереження цифрових доказів), у зв'язку з чим ефективна класифікація має бути багатовимірною (суб'єкт, вектор доступу, тип впливу, об'єкт посягання, масштаби та наслідки) та придатною до використання в управлінських і процесуальних рішеннях.

5. Запропоновано систему критеріїв оцінювання небезпечності кіберзагроз і прозорої ескалації інцидентів та встановлено, що для управлінських і процесуальних рішень визначальними є: імовірність реалізації, організованість, вплив на конфіденційність–цілісність–доступність і довіру до даних, часові параметри детектування/реагування, потенціал поширення та правові наслідки, тоді як регулярне оновлення цих критеріїв з урахуванням практик ENISA і національних попереджень CERT-UA підвищує актуальність оцінювання в мінливому середовищі загроз.

6. Уточнено методологічні основи ризик-орієнтованого підходу та визначено, що принципове розмежування категорій «загроза» як ймовірнісної, прогнозної й динамічної та «небезпека» як стану наявної вразливості/дефіциту захищеності є необхідною передумовою правомірної пріоритизації реагування, обґрунтованого вибору інструментів втручання й побудови прозорих механізмів ескалації.

7. Доведено доцільність використання превентивних онлайн-ресурсів як емпіричного джерела та обґрунтовано, що консультаційно-попереджувальні платформи (зокрема chatovi.online) можуть застосовуватися для ідентифікації й уточнення масових соціально-інженерних загроз із високою латентністю, що посилює превентивний компонент діяльності Національної поліції України та підвищує якість кримінально-аналітичної пріоритизації.

8. Систематизовано міжнародно-правові та стандартотворчі підходи до протидії кіберзагрозам і встановлено, що сучасна міжнародна модель має багаторівневий характер, поєднуючи кримінально-правове та процесуальне реагування (конвенційні механізми співпраці), управління ризиками й кіберстійкість (організаційні європейські вимоги) та правозахисний вимір

(захист персональних даних та гарантії прав людини), при цьому окремо зафіксовано зсув до концепції «цифрової стійкості», характерний для підходів Організації економічного співробітництва та розвитку (OECD).

9. Проведено аналіз рекомендацій Ради Організації економічного співробітництва та розвитку щодо цифрової безпеки критично важливих видів діяльності, управління ризиками цифрової безпеки та національних стратегій цифрової безпеки, що дає підстави стверджувати, що чинне законодавство України у сфері кібербезпеки, захисту критичної інфраструктури та цифрової стійкості потребує подальшого системного оновлення. Йдеться не лише про техніко-юридичне уточнення окремих норм, а про концептуальне переосмислення предмета правового регулювання – від вузького розуміння кібербезпеки як захисту інформаційно-комунікаційних систем до ширшої моделі цифрової безпеки/стійкості як комплексної категорії, що охоплює організаційні, технологічні, правові, економічні та соціальні аспекти функціонування держави, суспільства і критично важливих секторів.

10. Обґрунтовано, що одним із ключових напрямів удосконалення законодавства України має стати нормативне закріплення базових категорій, без яких подальша гармонізація національного права з підходами OECD є неповною. Передусім це стосується дефініцій «критична функція», «цифрова екосистема», «ризик цифрової безпеки/стійкості», «управління ризиками цифрової безпеки», «культура цифрової безпеки/стійкості», «власник ризику цифрової безпеки», а також пов’язаних понять, що описують сучасну багаторівневу цифрову взаємозалежність. Уведення таких категорій до законодавства має не лише термінологічне значення, а й створює правову основу для ризик-орієнтованого управління, персоналізації відповідальності, формування системи підзвітності та побудови сучасної моделі цифрової стійкості держави.

11. Виявлено ключові проблеми імплементації міжнародних стандартів у національне правове поле та, констатовано загальну позитивну динаміку розвитку регулювання, а також встановлено його фрагментарність і термінологічну неузгодженість, крім того неповне відображення ризик-

орієнтованих підходів щодо ланцюгів постачання, ролі приватного сектору, відповідальності керівництва й культури цифрової стійкості, що додатково обґрунтовує потребу системної гармонізації з європейськими підходами.

12. Визначено функціональне місце поліції в національній системі кібербезпеки та її адміністративно-правовий інструментарій, яке полягає у виконанні нею функції правоохоронного компонента державного механізму протидії кіберзагрозам, спрямованого на охорону прав і свобод людини. Також, доведено, що ефективність правоохоронного реагування зумовлюється чітким розмежуванням компетенцій між суб'єктами сектору безпеки, наявністю формалізованих процедур взаємодії (обмін інформацією, спільні аналітичні продукти, координація під час інцидентів) та неухильним дотриманням стандартів законності, пропорційності й прав людини як меж втручання у цифровій сфері.

13. Обґрунтовано пріоритет процесуальної придатності цифрових даних як передумови результативності кіберрозслідувань та встановлено, що її забезпечення визначається перевірюваністю й відтворюваністю, безперервністю ланцюга збереження, правомірністю здобуття та належним документуванням, тоді як стандартизація первинного реагування є критичною для недопущення втрати даних і мінімізації ризику визнання доказів недопустимими.

14. Запропоновано перспективний механізм процесуалізації даних, сформованих системами штучного інтелекту, та обґрунтовано, що практично реалістичним є їх залучення через судову експертизу із нормативним виокремленням алгоритмічної (цифрової) експертизи, за умови верифікації точності/похибки й відтворюваності результатів та належного опису застосованих методик, що забезпечує перевірюваність і допустимість відповідних даних.

15. Проведене дослідження дає підстави стверджувати, що інституційна спроможність кіберпідрозділів Національної поліції України має розглядатися не лише як сукупність організаційних ресурсів і технічних засобів, а як цілісна система нормативно визначених процедур, професійних компетентностей,

стандартів поводження з цифровими доказами та моделей міжвідомчої взаємодії. Саме така системна конструкція забезпечить спроможність поліції ефективно реагувати на кіберінциденти, належно документувати цифрові сліди та перетворювати інформаційні дані на процесуально допустимі докази. Отже, інституційна спроможність кіберпідрозділів є не допоміжною організаційною характеристикою, а одним із ключових елементів організаційно-правового механізму протидії кіберзагрозам.

16. Обґрунтовано, що регламентація процедур та стандартизація діяльності кіберпідрозділів НПУ повинні охоплювати щонайменше три взаємопов’язані блоки: первинне реагування і фіксацію події; роботу з цифровими доказами; координацію та взаємодію як усередині системи НПУ, так і на міжвідомчому рівні. Такий поділ має не лише методичне, а й правове значення, оскільки дозволяє забезпечити послідовність дій, збереження цілісності інформації, прозорість процедур та належну доказову перспективу кримінального провадження. Встановлено, що саме процедурна впорядкованість на початкових етапах реагування значною мірою визначає якість подальшого слідчого, оперативного та аналітичного забезпечення.

17. Встановлено, що кадрова складова інституційної спроможності кіберпідрозділів охоплює не лише питання укомплектування посад, а насамперед спеціалізацію, компетентнісну модель та безперервний професійний розвиток особового складу. Умови стрімкої еволюції кіберзагроз, поширення шкідливого програмного забезпечення, використання криптоактивів, соціальної інженерії та хмарної інфраструктури зумовлюють потребу переходу від моделі разової підготовки до моделі безперервного професійного розвитку, у тому числі із залученням міжнародних експертів. Така модель має інтегрувати як технічні компетентності – мережевий аналіз, цифрову криміналістику, роботу з логами, аналіз шкідливого коду, реверс-інжиніринг, – так і правові та процесуальні компетентності, пов’язані з дотриманням прав людини, межами втручання, режимом доступу до даних та правилами процесуалізації цифрової інформації.

18. Встановлено, що перспективна модель професійного стандарту «Оперуповноважений (поліція)» має бути істотно розширена за рахунок включення компетентностей, пов’язаних із ILP, електронними доказами, OSINT, цифровою криміналістикою, криптоактивами, застосуванням моделей штучного інтелекту в аналітичній підтримці розслідувань, а також NIS2-сумісною взаємодією у сфері кібербезпеки. Така деталізація дасть змогу привести професійні вимоги до посади у відповідність із сучасними організаційно-правовими викликами та міжнародними тенденціями розвитку поліцейської діяльності в цифровому середовищі.

19. Доведено, що особливого значення набуває інституціоналізація трудових функцій, пов’язаних з моніторингом відкритих джерел, документуванням результатів OSINT, відстеженням руху віртуальних активів, кластеризацією транзакцій, взаємодією з постачальниками послуг віртуальних активів, виявленням криптоанонімізаторів та використанням моделей штучного інтелекту для виявлення аномалій. Це свідчить про якісне розширення предмета правоохоронної діяльності, у межах якого цифрова аналітика, інтеграція та відтворюваність аналітичних процедур перетворюються на складові належного доказового забезпечення.

20. Результати дослідження дозволяють дійти висновку, що проєкт «BRAMA» є показовим прикладом практичної реалізації координаційної функції держави у сфері кібербезпеки, оскільки підтверджує ефективність міжінституційної взаємодії органів публічної влади, правоохоронних органів, приватного сектору та інститутів громадянського суспільства. Водночас його функціонування свідчить про доцільність подальшого нормативного оформлення, організаційного зміцнення та інтеграції подібних механізмів до цілісної загальнодержавної системи запобігання і протидії кіберзагрозам.

21. Узагальнення проблем організації діяльності підрозділів кіберполіції дає підстави констатувати, що ключовим організаційно-правовим викликом є часовий розрив між первинним реагуванням на кіберінцидент і подальшим процесуальним розслідуванням. Такий розрив зумовлений різною правовою природою, темпом і функціональним призначенням цих видів діяльності:

реагування вимагає безперервності, оперативності та технічної негайності, тоді як досудове розслідування підпорядковується процесуальним формам, вимогам фіксації, допустимості доказів і судового контролю. Відтак, одним із визначальних напрямів удосконалення організації діяльності кіберполіції є нормативне та процедурне зближення контурів реагування і розслідування, що має забезпечити безперервність переходу від технічного виявлення події до процесуального закріплення цифрових слідів.

22. Встановлено, що виклики організації діяльності підрозділів кіберполіції мають комплексний характер і охоплюють часово-процесуальний, кадрово-компетентнісний, матеріально-технічний, координаційний та міжнародно-правовий виміри. Саме тому їх подолання потребує не ізольованих адміністративних рішень, а системного вдосконалення організаційно-правового механізму функціонування кіберполіції, що має включати стандартизацію процедур, розвиток кадрового потенціалу, зміцнення технічної стійкості, формалізацію міжвідомчої взаємодії та підвищення спроможності до міжнародного обігу цифрових доказів. Такий підхід забезпечує не лише підвищення ефективності діяльності кіберполіції, а й зміцнення загальної спроможності держави реагувати на сучасні кіберзагрози в умовах цифрової трансформації.

23. Сформульовано авторське визначення інтероперабельності у кібербезпеці та обґрунтовано її системоутворювальну роль, визначивши інтероперабельність як інтеграційну властивість і спроможність технічних, організаційних, процедурних і нормативно-правових компонентів різних суб’єктів забезпечувати узгоджену, безпечну та безперебійну взаємодію на основі гармонізованих стандартів, форматів даних і регламентів обміну, що формує «простір довіри» для координації дій і підтримання єдиного рівня кіберстійкості з урахуванням стандартотворчих практик ISO та підходів NATO.

24. Поглиблено організаційні підходи до реагування у воєнний час та обґрунтовано ILP-орієнтовану модель управління, встановивши центральну дилему «швидкість/безперервність реагування – процесуальна якість/відтворюваність доказів» і довівши доцільність інституційно закріпленої

моделі, що поєднує міжвідомчу координацію, внутрішні стандартизовані процедури реагування (мінімальні форензичні вимоги, тригери ескалації) та аналітично кероване управління ресурсами (ILP-цикл) із посиленням ролеорієнтованих компетентностей персоналу.

25. Встановлено, що використання криптоактивів для обходу міжнародних санкцій набуло системного та технологічно адаптивного характеру, інтегрувавшись у структуру сучасних фінансових і кіберзагроз. Це зумовлює необхідність комплексної протидії, що має ґрунтуватися на поєднанні санкційного комплаєнсу, блокчейн-аналітики, цифрової криміналістики, міжвідомчої координації та вдосконалення спеціалізованого правового регулювання.

26. Запропонована удосконалена п’ятиетапна модель Аналітичного Життєвого Циклу Крипто-Санкцій (АЖЦКС), яка відображає регуляторні рубежі 2026 року та забезпечує системне поєднання аналітичних, правозастосовних і комплаєнс-механізмів у сфері протидії обходу санкцій із використанням криптоактивів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бандурка О.М. Роль адміністративного законодавства в зміцненні правопорядку. *Проблеми охорони громадського порядку і вдосконалення законодавства: матеріали науково-практичної конференції. Харків* : Рубікон, 2001. С. 19-21.

2. Береза В.В. Принципи діяльності Департаменту кіберполіції Національної поліції України: теоретико-правові аспекти. *Forum Prava.* № 5. 2017. С. 44-48.

3. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. 2024. URL: https://storage.thedigital.gov.ua/files/a/ba/d5da75c2613e331bb89258f950adcbae.pdf

4. Білявська Ю.В. Використання бенчмаркінгу в операційному процесі туристичного підприємства. Науковий вісник Полтавського університету економіки і торгівлі. Серія : Економічні науки. Полтава. 2014. № 2. С. 78-84.

5. Бойко І.В. Дефініції «ризик», «загроза», «небезпека» як об'єкти наукових досліджень у напрямі економічної безпеки підприємства. Приазовський економічний вісник. Випуск 5(05) 2017. С. 94-98. URL: http://pev.kpu.zp.ua/journals/2017/5_05_uk/20.pdf

6. Бутко Р.Ю., Манжай О.В., Носов В.В., Мальцев В.В., Роговий А.П. Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у кримінальному аналізі: науково-методичні рекомендації. Харків : ХНУВС, 2024. 36 с.

7. В Україні вперше запустили ШІ-відеоспостереження для безпеки: де запрацювали камери. РБК-Україна. 24.12.2025. URL: https://www.rbc.ua/rus/news/chernigiv-pershim-ukrayini-zapustiv-shi-videosposterezhennya-1766584522.html

8. Великий тлумачний словник сучасної української мови / уклад. В. Бусел. К.: Перун, 2009. 1700 с.

9. Гайдук О.В., Звєрєв В.П. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Електронне фахове наукове видання*

«Кібербезпека: освіта, наука, техніка». № 3(23). 2024. С. 225-236. https://csecurity.kubg.edu.ua/index.php/journal/article/view/552/451

10. Глобальна операція, скоординована Європолом, знищує проросійську мережу кіберзлочинців. – Майк Кордер. 16.07.2025. URL: https://apnews.com/article/europol-hackers-cybercrime-russia-ukraine-42d98dabdc0182dac4bd4c80d880cdb4

11. Господарський процесуальний: кодекс України від 06.11.1991 № 1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text

12. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки: матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених *«Теоретичні і прикладні проблеми фізики, математики та інформатики»*, м. Київ, 21-23 травня 2015. Київ : НТУУ «КПІ». 2015. С. 10-17.

13. Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д.юн., проф. В.Л. Грохольського. Одеса: ОДУВС, 2020. 142 с.

14. Гуленко К.І., Манжай О.В. Прогнозування та запобігання кібератакам за допомогою інструментів штучного інтелекту. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів*: матеріали Всеукр. наук.-практ. конф.(м. Вінниця, 16 травня 2025 року). Вінниця: ХНУВС, 2025. С. 481-185.

15. Двостороння безпекова Угода між Україною та Сполученими Штатами Америки: Угода, Міжнародний документ від 13.06.2024. URL: https://zakon.rada.gov.ua/laws/show/840_001-24#Text

16. Денищук Д.Є. Особливості підготовки поліцейських кіберполіції в умовах сьогодення на прикладі Харківського національного університету внутрішніх справ. *Підготовка поліцейських в умовах реформування системи МВС України*. Харків, 2020. С. 233-237.

17. Державний освітній стандарт з професії 5162 «Поліцейський (за спеціалізаціями)». Затверджено наказом МОН від 07.11.2024 № 1592. URL:

https://mon.gov.ua/static-objects/mon/sites/1/pto/standarty/2024/11/07/nakaz-mon-1592-vid-07-11-2024-politseyskyy-za-spetsializatsiyamy.pdf

18. Держспецзв’язок та американське Агентство з кібербезпеки підписали меморандум про співпрацю. 28.07.2022. URL: https://detector.media/infospace/article/201415/2022-07-28-derzhspetszvyazku-ta-amerykanske-agentstvo-z-kiberbezpeky-pidpysaly-memorandum-pro-spivpratsyu/

19. Держспецзв'язок: Як CERT-UA реагує на кіберінциденти – від повідомлення до ліквідації наслідків. Державна служба спеціального зв’язку та захисту інформації України, 10.02.2025. URL: https://www.kmu.gov.ua/news/derzhspetszviazku-iak-cert-ua-reahuie-na-kiberintsydenty-vid-povidomlennia-do-likvidatsii-naslidkiv?

20. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/go/1533-2025-%D0%BF

21. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки. дисертація на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.07. 2018. 521 с.

22. Діордіца І.В. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України Підприємництво, господарство і право. № 10. 2017. С. 206-211.

23. ДКП НПУ Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році. Київ: Департамент кіберполіції НПУ. 2025. URL: https://cyberpolice.gov.ua

24. ДКП НПУ Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік. Київ: Департамент кіберполіції НПУ, 16 лютого 2026 р. URL: https://cyberpolice.gov.ua

25. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ : Артек, 2017. 312 с

26. Довгострокова підтримка ЄС та посилення ролі України як регіонального лідера в сфері кібербезпеки: В Києві відбувся Міжнародний форум кіберстійкості 2025. https://www.rnbo.gov.ua/ua/Diialnist/7142.html

27. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року щодо захисту жертв міжнародних збройних конфліктів: https://www.icrc.org/rus/assets/files/2013/ ap_i_rus.pdf

28. Другий додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах : Протокол Ради Європи від 08.11.2001 р. № 994_518 : ратифіковано Законом України від 01.06.2011 р. № 3449-VI.

29. ДСТУ EN ISO/IEC 27037:2022 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (EN ISO/IEC 27037:2016, IDT; ISO/IEC 27037:2012, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=100063

30. ДСТУ EN ISO/IEC 27042:2022 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (EN ISO/IEC 27042:2016, IDT; ISO/IEC 27042:2015, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=67149

31. ДСТУ EN ISO/IEC 27043:2022 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів (EN ISO/IEC 27043:2016, IDT; ISO/IEC 27043:2015, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=103327

32. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400

33. ДСТУ ISO/IEC 27035-1:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес (ISO/IEC 27035-1:2023, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112378

34. ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захиту. Керівництво щодо забезпечення прийнятності та адекватності методів

розслідування (ISO/IEC 27041:2015, IDT). URL: https://online.budstandart.com/ru/catalog/doc-page.html?id_doc=67147

35. Європейський центр кіберзлочинності – EC3. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

36. Європол. URL: https://grokipedia.com/page/Europol

37. Желновач Є.Г. Адміністративно-правові аспекти функціонування інформаційного суспільства в умовах воєнного стану в Україні : монографія / за заг. ред. д.ю.н., проф. М. В. Корнієнка. Одеса : Видавництво «Юридика», 2024. 212 с.

38. Желновач Є.Г. Війна як каталізатор формування нових складових інформаційного суспільства в Україні. Правові новели. № 21/2023. С. 163-171.

39. Загроза – етимологія. URL: https://surl.li/unaxyd

40. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році. URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074

41. Зінченко О.І. Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 052 «Політологія». – Харківський національний університет імені В.Н. Каразіна, Харків, Україна, 2025. 275 с.

42. Інтероперабельність: Підвищення обміну даними та комунікації. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/interoperability?srsltid=AfmBOoohLvvIz98H2zsHiHGOfoSCy2ENjmLeVaNWl7TOqjhjFqhm1b0Q

43. Ісмайлов К.Ю. Поняття «кібербезпека» та «інформаційна безпека». *Типологія безпеки. Актуальні проблеми автоматизації та управління*: матеріали Міжнародної науково-практичної інтернет-конференції, 25 листопада 2016 р. Луцьк: Луцький національний технічний університет, 2016. № 4. С. 32-33.

44. Казанчук І.Д., Яценко В.П. Особливості правового регулювання діяльності Національної поліції України у сфері забезпечення інформаційної безпеки в Україні. *Право і безпека.* 2020. № 4 (79). С. 32-38.

45. Калайда А.В. Адміністративно-правові засади міжнародного співробітництва органів та підрозділів Національної поліції України. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю: 081 Право. Київ. 2021. 214 с.

46. Камчатий М. Заборонені засоби ведення кібервійни. *Підприємство, господарство і право.* № 9. 2017. С. 211-217.

47. Карпанець О. Сучасний стан та пріоритети вдосконалення нормативно-правового регулювання діяльності органів МВС України у сфері забезпечення кібербезпеки в умовах протидії збройній агресії. Матеріали VIII Міжнародної науково-практичної конференції (ДДУВС, 15.03.2024). Частина II. 2024. С. 338-341.

48. Кібер Брама Твоя міць в інтернеті. URL: https://stopfraud.gov.ua

49. Кіберзагрози: Україна. Аналітика за II півріччя 2025. Державна служба спеціального зв'язку та захисту інформації України. 2025. 23 с.

50. Кіберполіція України. URL: https://cyberpolice.gov.ua

51. Кодекс адміністративного судочинства України від 06.07.2005 № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text

52. Кодекс поведінки щодо дезінформації. 13.02.2025. URL: https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

53. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки: Указ Президента України від 11.05.2023 № 273/2023.

54. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : міжнародний документ Ради Європи від 28.01.1981 р. № 994_326. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

55. Конвенція про захист прав людини і основоположних свобод (з протоколами) : Конвенція Ради Європи, міжнародний документ, Протокол від 04.11.1950 р. : ст. 8.

56. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. № 994_575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

57. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

58. Концепція розвитку штучного інтелекту в Україні: Розпорядження КМУ від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

59. Координатор проектів ОБСЄ навчає та оснащує українську кіберполіцію. ОБСЄ. 19/07.2017. URL: https://www.osce.org/project-coordinator-in-ukraine/330471

60. Корнієнко М.В. Права людини в умовах воєнного стану: загальноправовий дискурс. *Південноукраїнський правничий часопис.* 2022. № 1-2. С. 27-31.

61. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

62. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

63. Кузьменко А. Проблеми відповідності стратегії та системи забезпечення безпеки України національним потребам. *Юридичний Журнал.* 2006. № 10. С. 1-21.

64. Лисенко Ю.Г., Мінц А.Ю., Стасюк В.П. Пошук ефективних рішень в економічних задачах. Донецк: ДонНУ, 2002. 101 с.

65. Ліпкан В.А. Національна безпека України. Навчальний посібник. Кондор. 2006. 552 с.

66. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

67. Логінова Н.І. Кібернетична безпека держави: теоретико-правовий аспект: монографія. Харків: Право, 2023. 224 с.

68. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства.* № 2 (42). С. 164-171.

69. Мазур Я.П. Аналіз основних кіберзагроз в умовах інформаційної війни. *Актуальні проблеми правознавства.* 2024. № 4. С. 100-108.

70. Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 3(31). С. 309-322.

71. Марчак Я.В. Особливості, механізми та напрями вдосконалення діяльності силових структур із захисту кіберпростору України в умовах повномасштабної війни : робота на здобуття кваліфікаційного ступеня магістра : спец. 281 Публічне управління та адміністрування / наук. кер. Г.Т. Панишко; Волинський національний університеті імені Лесі Українки. Луцьк, 2024. 91 с.

72. Мельничук О.С. Етимологічний словник української мови. Т. 4. К.: Наук. думка, 2003.

73. Мігус І.П., Лаптєв С.М. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання: URL: http://www.economy.nayka.com.ua/ index.php?operation=1&iid=821

74. Міжвідомча готовність державного сектору України до ШІ-підсилених кіберзагроз та іноземних інформаційних операцій / Авдєєва А., Майборода В., Мисишин А, Ковтун В., Хрущова Д. Інститутом Інноваційного Врядування в рамках Партнерства України та Великої Британії. 2026. 100 с.

75. Мороз О.В. Концепція економічної безпеки сучасного підприємства: монографія / О.В. Мороз, Н.П. Карачина, А.А. Шиян. Вінниця : ВНТУ, 2010. 259 с.

76. Національний банк України та Міністерство фінансів США продовжать обмін досвідом у сфері кібербезпеки. НБУ. 08.04.2024. URL: https://bank.gov.ua/ua/news/all/natsionalniy-bank-ukrayini-ta-ministerstvo-finansiv-ssha-prodovjat-obmin-dosvidom-u-sferi-kiberbezpeki

77. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. URL: https://cip.gov.ua/ua/faqs/cyber-threat-overview-and-defense-strategies-in-2025-cert-ua-s-experience

78. Оцінка ризиків NIST: Виявлення та управління ризиками безпеки. 19.09.2024. URL: https://surl.li/estylk

79. Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз. *Інформаційна безпека людини, суспільства, держави*: наук.-практ. журн. К. № 3 (10). 2012. С. 100-109.

80. Пасько В.П., Гасанов В.А., Гришко А.С., Максимюк А.В. Інтероперабельність матриці прийняття рішень для оцінювання ризиків інформаційної безпеки. *Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління».* № 2 (33). 2018. С. 75-85.

81. Перелік категорій кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. 26.10.2021. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

82. Перелік категорій кіберінцидентів. CERT-UA. 2021. URL: https://cert.gov.ua/recommendation/16904

83. Перерва П.Г. Інноваційна складова реінжинірингу у забезпеченні економічної безпеки підприємства / П.Г.Перерва, Т.В.Романчик . Реінжиніринг бізнеспроцесів маркетингової сфери промислових підприємств: монографія / за заг. ред. докт. екон. наук, проф. Л.М. Таранюка. Суми: Видавець СНАУ, 2018. С. 31-43.

84. Посилення співпраці для реагування на кіберзагрози: Держспецзв'язку та CRDF Global підписали Меморандум про взаєморозуміння. 10.04.2025. URL: https://cip.gov.ua/ua/news/posilennya-spivpraci-dlya-reaguvannya-na-kiberzagrozi-derzhspeczv-yazku-ta-crdf-global-pidpisali-memorandum-pro-vzayemorozuminnya

85. Про введення воєнного стану в Україні. Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text

86. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон

України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text

87. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 10.12.2015 № 889-VIII. URL: https://zakon.rada.gov.ua/laws/show/889-19#Text

88. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

89. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

90. Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу: Закон України від 18.03.2004 № 1629-IV. URL: https://zakon.rada.gov.ua/laws/show/1629-15#Text

91. Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності: Постанова Кабінету Міністрів України від 01.04.2025 № 367. URL: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text

92. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: наказ МВС України від 07.07.2017 № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text

93. Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: наказ МВС України від 27.04.2020 № 357. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text

94. Про затвердження Методичних рекомендацій щодо проведення інструктажів і тренінгів щодо кібергігієни на період призначення на посади державних службовців, працівників органів державної влади та інших державних органів, військовослужбовців, керівників та працівників державних підприємств, установ та організацій: Наказ Адміністрації Держспецзв'язку від 21.10.2025 № 661. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-21-10-2025-661-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-provedennya-instruktazhiv-i-treningiv-shodo-kibergigiyeni-na-period-priznachennya-na-posadi-derzhavnikh-sluzhbovciv-pracivnikiv-organiv-derzhavnoyi-vladi-ta-inshikh-derzhavnikh-organiv-viiskovosluzhbovciv-kerivnikiv-ta-pracivnikiv-derzhavnikh-pidpriyemstv-ustanov-ta-organizacii

95. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: Розпорядження КМУ від 07.03.2025 № 204-р.

96. Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10.11.2015 № 85.

97. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28.10.2015 № 877. URL: https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text

98. Про затвердження Порядку ведення Реєстру методик проведення судових експертиз: наказ Міністерства юстиції України від 02.10.2008 № 1666/5. URL: https://zakon.rada.gov.ua/laws/show/z0924-08#Text

99. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього: Постанова Кабінету Міністрів України від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

100. Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності:

Постанова КМУ від 13.11.2025 № 1471. URL: https://zakon.rada.gov.ua/laws/show/1471-2025-%D0%BF#Text

101. Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури: Постанова КМУ від 31 грудня 2025 року №1799. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-otsiniuvannia-stanu-kiberzakhystu-informatsiinykh-s1799311225

102. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: Постанова КМУ від 16 травня 2023 року № 497. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text

103. Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни: Постанова Кабінету Міністрів України від 08.10.2025 № 1281. URL: https://zakon.rada.gov.ua/laws/term/1281-2025-%D0%BF/name

104. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

105. Про захист персональних даних: проєкт Закону від 25.10.2022 № 8153. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707

106. Про захист прав людини і основоположних свобод (з протоколами). Конвенція Ради Європи від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

107. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

108. Про критичну інфраструктуру Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

109. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2025 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

110. Про національну безпеку України: Закон України від 21.06.2018

№ 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

111. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

112. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

113. Про організацію розроблення проєкту професійного стандарту: наказ Національної поліції України від 29 05.2025 № 610.

114. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

115. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19

116. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України; Стратегія від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020

117. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

118. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

119. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text

120. Про укладення Меморандуму про взаєморозуміння у розвитку інновацій Україні між Комітетом Верховної Ради України з питань цифрової трансформації та Амазон Веб Сервісес ЕМЕА САРЛ. Комітет ВРУ з питань цифрової трансформації. 19.02.2025. URL: https://komit.rada.gov.ua/uploads/documents/31767.pdf

121. Про утворення Координаційної ради з питань моніторингу реалізації плану заходів, спрямованих на виконання Комплексного стратегічного плану

реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки: Постанова КМУ від 21.01.2026 № 65. URL: https://ips.ligazakon.net/document/KP260065?an=1

122. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13.10.2015 № 831. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text

123. Про штучний інтелект: Закон ЄС від 2020 № 1828. URL: https://artificialintelligenceact.eu/ai-act-explorer

124. П

р 125. Професійний стандарт «Слідчий (поліція)». Затверджено наказом Національною поліцією України від 28.06.2024 № 724 URL: https://register.nqa.gov.ua/uploads/0/629-profesijnij_standart_slidcij_policia.pdf

С 126. Разом – на захисті кіберпростору: Держспецзв'язок, НКЦК та ENISA Підписали угоду про співпрацюю ДССЗЗІ. 31.11.2023. URL: Https://cip.gov.ua/ua/news/razom-na-zakhisti-kiberprostoru-derzhspeczv-yazku-Nkck-ta-enisa-pidpisali-ugodu-pro-spivpracyu

- 127. Разом проти дезінформації та спаму. 2026. URL: https://chatovi.online

U 128. Реалізація філософії «Intelligence-led Policing» в системі Аримінального аналізу Національної поліції України: монографія / Користін О., Бутко Р., Денисенко Б., Ісмайлов К.Ю. та ін., за заг. ред. Користіна О.Є. Київ: «BAITE», 2024. 444 с.

U 129. Регламент (ЄС) 2024/2847 Європейського Парламенту і Ради від 23 Rжовтня 2024 року про горизонтальні вимоги до кібербезпеки продуктів з Iцифровими елементами та про внесення змін до Регламенту (ЄС) № 168/2013 і https://eur-(ЄС) 2020/1828 (Закон ЄС про кіберстійкість). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847

130. Регламент європейського парламенту і ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку): Європарламент, Рада ЄС; Регламент,

Міжнародний документ, Вимоги від 17.04.2019 № 2019/881. URL: https://zakon.rada.gov.ua/laws/show/984_024-19/ed20190417#n143

131. РНБО звинуватила Росію в хакерській атаці на Україну. URL: https://www.bbc.com/ukrainian/news-56179424

132. Романчик Т.В. Небезпека, загроза, ризик: аналіз термінологічного апарату теорії економічної безпеки. *Економічний вісник.* НТУУ «КПІ», 2020. С. 257-267.

133. Російські кібероперації. Аналітика за І півріччя. Державна служба спеціального зв'язку та захисту інформації України. 2025. 24 с.

134. Світова гібридна війна: український фронт / за заг. ред. В.П. Горбуліна. Національний інститут стратегічних досліджень. К.: НІСД, 2017. 89 с.

135. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: річний звіт оперативного центру реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України за 2024 рік. 24 с. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006

136. Солдатенко О.А., Яровий О.Ю. Проблема допустимості електронних доказів у кримінальному провадженні. *Актуальні питання у сучасній науці.* № 9(39). 2025. С. 768-778.

137. Стандарт вищої освіти України: другий (магістерський) рівень вищої освіти, галузь знань 26 «Цивільна безпека», спеціальність 262 «Правоохоронна діяльність». Затверджено і введено в дію наказом Міністерства освіти і науки України від 22.10.2020 р. № 1294. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/262-Pravookhor.diyaln-mag.31.01.22.pdf

138. Стандарт вищої освіти України: перший (бакалаврський) рівень вищої освіти, галузь знань 26 Цивільна безпека, спеціальність 262 Правоохоронна діяльність. Затверджено і введено в дію наказом Міністерства освіти і науки України від 28 05 2024 р. № 769. URL: https://mon.gov.ua/static-

objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/28.05.2024/262-Pravookhor.Diyaln-bak.769.V%C3%ADd.28.05.24.pdf

139. Статут Організації Об'єднаних Націй : міжнародний договір від 26 черв. 1945 р., ратифікований Україною 22 серп. 1991 р. // Офіційний вісник України. 2006. № 45. Ст. 3021.

140. Тимошенко В.І. Внутрішні загрози національній безпеці україни. *Електронне наукове видання «Аналітично-порівняльне правознавство».* № 2 2024. С. 94-99.

141. Тренінг з основ кібергігієни у рамках проєкту «Програма підтримки ОБСЄ для України». ОБСЄ. 02.12.2024. URL: https://nubip.edu.ua/news/treninh-z-osnov-kiberhihiyeny-u-ramkakh-proyektu-prohrama-pidtrymky-obsye-dlya-ukrayiny

142. У Харкові розпочато програму перепідготовки сертифікованих українських співробітників кіберполіції за підтримки ОБСЄ. ОБСЄ. 03.10.2016. URL: https://www.osce.org/ukraine/271166

143. Угода про співробітництво в галузі безпеки між Україною та Італією від 24 лютого 2024 року. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-89245

144. Угода про співробітництво в галузі безпеки між Україною та Республікою Польща від 08 липня 2024 року. URL: https://www.president.gov.ua/en/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-92009

145. Угода про співробітництво у сфері безпеки та довгострокову підтримку між Україною та Республікою Словенія. 18.07.2024. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-ta-dovgostrokovu-p-92241

146. Угода про співробітництво у сфері безпеки та довгострокову підтримку між Україною та Фінляндською Республікою від 03 квітня 2024 року. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-ta-dovgostrokovu-p-90021

147. Угода про співробітництво у сфері безпеки та довгострокову підтримку між Україною та Чеською Республікою від 18 липня 2024 року. URL: https://www.president.gov.ua/en/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-ta-dovgostrokovu-p-92237

148. Уряд Нідерландів заявив, що проросійські хакери атакували муніципалітети, пов'язані з самітом НАТО цього тижня. 23.06.2025. URL: https://apnews.com/article/nato-summit-cybersecurity-hack-russia-netherlands-fa97bbf8797a51c2885d47f5f83691be

149. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

150. Фішингова афера спрямована на українські оборонні компанії. Бет Маундрілл Редактор журналу «Інфобезпека». 09.12.2024. URL: https://www.infosecurity-magazine.com/news/phishing-scam-targets-ukrainian

151. Фішингові атаки групи APT28 (UAC-0028) для отримання даних автентифікації для публічних поштових служб (CERT-UA#6975). https://csirt.csi.cip.gov.ua/en/posts/apt28-group-uac-0028

152. Цивільний процесуальний: кодексу України від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

153. Цимбалюк В. Інформаційна безпека України: адміністративно-правові засади : монографія. Київ : НАВС, 2019. 280 с.

154. Цілодобова мережа, створена відповідно до Конвенції про кіберзлочинність. URL: https://www.coe.int/en/web/cybercrime/24/7-network-new

155. Шаронов А.П. Дефініційний аналіз суміжних понять «інформаційна безпека» та «кібербезпека». *Роль та місце правоохоронних органів у розбудові демократичної правової держави*: матеріали XVI міжнар. наук.-практ. Інтернет конф., м. Одеса, 29 березня 2024 р. Одеса : ОДУВС, 2024. С. 556-559.

156. 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.

157. Шаронов А.П. Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. *Морська безпека та оборона.* № 2 (6). 2025. С. 106-115.

158. 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.

159. 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 р. Одеса : ОДУВС, 2024. С. 215-216.

160. Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. *Юридичний бюлетень.* № 39. 2025. С. 147-155.

161. Шаронов А.П. Трудові функції оперуповноваженого в парадигмі ILP: нормативно-практичні ориси та кіберкомпонент. *Юридичний бюлетень.* № 37. 2025. С. 97-106.

162. 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.* № 41. 2026. С. 120-136.

163. Шаронов А.П., Самойлов С.В., Крайнічук (Шелепало) Г.В. Організаційно-правовий аспект використання відбитку браузера для заходів кіберзахисту. *Наше право*. № 1. 2026. С. 42-52.

164. Шемчук В.В., Костенко О.Л. Кіберпростір як сфера національної безпеки: правові засади забезпечення. *Науковий вісник публічного та приватного права.* 2024. Вип. 3. С. 167-174.

165. Штучний інтелект та кримінальне правосуддя. Заключний звіт. США. 2024. URL: https://www.justice.gov/olp/media/1381796/dl?fbclid=IwY2xjawNoCplleHRuA2FlbQIxMQABHmRHDTcegNebZwJcoC4Inv-

RzRXpAHHz7Oj7s1YCUOfVej7Gn_feQMGP3Slq_aem_kwlPmUuGdGuwWtws_LtAsg

166. Cabinet Office, 2009. Cyber Security Strategy of the United Kingdom. London : TSO. URL: https://assets.publishing.service.gov.uk/media/5a7c69fb40f0b62aff6c17fc/7642.pdf

167. Cabinet Office, 2011, National security and intelligence. The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. London. URL: https://isc.independent.gov.uk/wp-content/uploads/2021/01/2010-2011_ISC_AR.pdf

168. Cabinet Office, National security and intelligence, HM Treasury (2021). National Cyber Security Strategy 2016 to 2021. URL: https://www.gov.uk/government/publications/national-security-and-investment-act-2021-annual-report-2024-25/national-security-and-investment-act-2021-annual-report-2024-25-html

169. Callejas J., Afifi A., Lozinskiy N. Cybersecurity in the united nations systemorganizations.United Nations. 2021. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

170. CASE OF ROMAN ZAKHAROV v. RUSSIA. *Application no. 47143/06)*. JUDGMENT. STRASBOURG. 4 December 2015. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]}

171. Castells M. Communication Power. Oxford University Press, 2009. 571p.

172. Castells M. End of Millennium. Oxford: Blackwell, 1998. 448 p.

173. Castells M. The Power of Identity. Oxford: Blackwell, 1997. 461 p.

174. Castells M. The Rise of the Network Society. Oxford: Blackwell, 1996. 556 p.

175. CERT-UA повідомляє про кібератаки, спрямовані на українські д

е 176. CERT-UA recorded 4,315 cyber incidents in 2024. URL: https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

ж 177. Consolidated Annual Activity Report 2024. Europol Public Information. 25 June 2025. P. 96. URL: https://www.europarl.europa.eu/cmsdata/296825/Europol%20CAAR%202024.pdf

а

н

178. Crypto Crime Report 2026. Сан-Франциско: TRM Labs Inc. 2026. URL: https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

179. Crystal Intelligence Platform Capabilities and Regulatory Engagement Overview. Амстердам: Crystal Intelligence B.V. 2025. URL: https://crystalintelligence.com

180. Cyber Resilience Act (CRA): Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) № 168/2013 and Directive (EU) 2020/1828. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847

181. Cybersecurity in Ukraine: Legal Framework Analysis. IFES Ukraine Report, 2024.

182. Data Protection Act 2018: Act. URL: https://www.legislation.gov.uk/ukpga/2018/ 12/enacted/data.pdf

183. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union.* L 333/80. 27.12.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

184. Elliptic Sanctions Compliance in Cryptocurrencies: 2026 Update. Лондон: Elliptic Enterprises Ltd. 2026. URL: https://elliptic.co

185. ENISA THREAT LANDSCAPE 2024. European Union Agency for Cybersecurity (ENISA), 2024. URL: https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

186. ENISA THREAT LANDSCAPE 2025. European Union Agency for Cybersecurity (ENISA), 2025. URL: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

187. EUCC Certification Scheme. European Union Cybersecurity Certification. URL: https://certification.enisa.europa.eu/certification-library/eucc-certificationscheme_en

188. European Union Agency for Cybersecurity (ENISA). *Interoperability Framework for Cybersecurity and Incident Management.* Athens: ENISA, 2023. 54 p. URL: https://www.enisa.europa.eu

189. E

u 190. Gercke M. Understanding Cybercrime: A Guide for Developing Countries. Geneva : ITU, 2012. 303 p.

o 191. Global Ledger Crypto Hacks and the Laundering Race: Industry Report 2025. Женева: Global Ledger SA. 2025. URL: https://globalledger.io

e 192. Greenleaf G. «Modernised» Data Protection Convention 108 and the GDPR // UNSW Law Research Paper. 2018. № 18-39.

n 193. Holt T.J. Regulating Cybercrime through Law Enforcement and Industry Mechanisms. Annals of the American Academy of Political and Social Science. 2018. Vol. 679. P. 140-157.

n 194. Home OFCOM. 2026. URL: https://www.ofcom.org.uk

i 195. ICO. Information Commissioner's Office (ICO). URL: https://ico.org.uk

o 196. Incident reporting. ENISA. 2025. URL: https://ciras.enisa.europa.eu

n 197. Interfax Україна «Правоохоронці України та країн-партнерів викрили транснаціональне хакерське угруповання». 15 січня 2026. URL: https://interfax.com.ua

g 198. Ismailov K.Y. Peculiarities of human rights and freedom while applying intelligence-led policing (ILP). *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2019. Special Issue № 1. P. 36-37.

c 199. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection Information security management systems Requirements. Geneva: International Organization for Standardization, 2022. 35 p.

f 200. It's time to act. Open your eyes to the imminent risk to your economic security. National Cyber Security Centre a part of GCHQ. Annual Review 2025. 100 p. URL: https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf

C

201. L_2016194NL.01000101.XM July 19, 2016. URL: https://eurlex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016L1148&from=EN

202. Loi de programmation militaire 2019-2025. Ministère Des Armées. (2022, September 27). URL: https://www.defense.gouv.fr/ministere/dossiersevenementiels-thematiques-du-ministere-armees-anciens-combattants/loiprogrammation-militaire

203. Maimon D., Louderback E.R. Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology.* 2019. Vol. 2. P. 191-216.

204. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare // *Cambridge University Press.*

205. Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+) / Council of Europe. Strasbourg, 2018. URL: https://www.coe.int/en/web/data-protection/convention108/modernised

206. National Cyber Security Centre – NCSC.GOV.UK. National Cyber Security Centre. URL: https://www.ncsc.gov.uk

207. National Cyber Strategy 2022 (HTML). (2022, December 15). GOV.UK. URL: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

208. National Institute of Standards and Technology Special Publication 800-61 Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-61 Revision 2, 79 pages (Aug. 2012) CODEN: NSPUE2. URL: http://dx.doi.org/10.6028/NIST.SP.800-61r2

209. RBC-Україна «Псевдоромантика та криптобіржі у Дніпрі: викрили любовні кол-центри». 01 квітня 2026. URL: https://www.rbc.ua

210. Recommendation of the Council on Digital Security of Critical Activities: adopted 11 Dec. 2019, OECD/LEGAL/0456 (provides guidance on strengthening continuity, resilience and safety of digitally-dependent critical economic and social activities). OECD Legal Instruments. OECD, Paris. 2019.

211. Recommendation of the Council on Digital Security Risk Management: adopted 26 Sept. 2022, OECD/LEGAL/0479 (aims to assist adherents in devising or

updating digital security strategies and policies without inhibiting digital transformation). OECD Legal Instruments. OECD, Paris. 2022.

212. Recommendation of the Council on National Digital Security Strategies : adopted 26 Sept. 2022, OECD/LEGAL/0480 (provides guidance for development of comprehensive national digital security strategies). *OECD Legal Instruments*. OECD, Paris. 2022.

213. Regulation (EU) 2016/679 (GDPR). OJ L 119, 4.5.2016, p. 1-88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

214. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity (ENISA) and on Information and Communications Technology Cybersecurity Certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union.* L 151/15. 7.06.2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881

215. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the EU.

216. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

217. The Chainalysis 2026 Crypto Crime Report. Нью-Йорк: Chainalysis Inc. 2026. URL: https://www.chainalysis.com/reports/crypto-crime-2026

218. UN Convention against Cybercrime opens for signature in Hanoi. CADE. 2025. URL: https://cadeproject.org/updates/un-convention-against-cybercrime-opens-for-signature-in-hanoi

219. UN cybercrime pact to be signed in Hanoi raises hopes, concerns. Reuters. 23.10.2025. URL: https://www.reuters.com/sustainability/society-equity/un-cybercrime-pact-be-signed-hanoi-raises-hopes-concerns-2025-10-22

220. United Nations Convention against Cybercrime. Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of

Evidence in Electronic Form of Serious Crimes. URL: https://www.unodc.org/unodc/cybercrime/convention/home.html

221. USTAWA z dnia 5 lipca 2018 r. o krajowymsystemiecyberbezpieczeństwa. Kancelaria Sejmu. URL:https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf

222. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Bundesamt Für Sicherheit in Der Informationstechnik. URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-undVerordnungen/IT-SiG/2-0/it_sig-2-0_node.html

ДОДАТКИ

Додаток А

АКТИ ВПРОВАДЖЕННЯ

ЗАТВЕРДЖУЮ
Начальник Департаменту кіберполіції
(міжрегіональний територіальний орган)
Національної поліції України
генерал поліції третього рангу

Юрій ВИХОДЕЦЬ

12.05.2026

АКТ №1
про впровадження наукових розробок
аспіранта Одеського державного університету внутрішніх справ
Шаронова Андрія Павловича
на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект», викладених у наукових статтях, у практичну діяльність Департаменту кіберполіції (міжрегіональний територіальний орган) Національної поліції України

Комісія у складі:

тимчасово виконуючого обов'язки начальника 2-го відділу (кадрового забезпечення) 2-го управління (організаційно-аналітичної роботи та забезпечення діяльності Департаменту кіберполіції (міжрегіональний територіальний орган) Національної поліції України полковника поліції Молчанського Віталія Михайловича;

начальника 2-го відділу (прогнозування ризиків та реагування) Департаменту кіберполіції (міжрегіональний територіальний орган) Національної поліції України підполковника поліції Рогута Семена Андрійовича;

старшого інспектора з особливих доручень 4-го відділу (організації роботи та планування) 2-го управління (організаційно-аналітичної роботи та забезпечення діяльності Департаменту кіберполіції (міжрегіональний територіальний орган) Національної поліції України майора поліції Феденко Романа Віталійовича,

склала цей акт з приводу того, що наукові розробки, рекомендації та пропозиції викладені у наукових статтях Шаронова А. П. Трудові функції оперуповноваженого в парадигмі ILP: нормативно-практичні ориси та кіберкомпонент. *Юридичний бюлетень.* № 37. 2025. С. 97-106; Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. *Морська безпека та оборона.* № 1 (5). 2025.С. 106-115; Міжнародні правові стандарти протидії кіберзагрозам: імплементація та розвиток цифрової стійкості в правовій системі України. *Актуальні проблеми вітчизняної юриспруденції.* № 6. 2025. С. 125-134; Протидія кіберзагрозам Національною

поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. *Юридичний бюлетень.* № 39. 2025. С. 147-155; Організаційно-правовий аспект використання відбитку браузера для заходів кіберзахисту. *Наше право*. № 1. 2026. С. 42-52; Криптоактиви як інструмент обходу санкцій у системі кіберзагроз: блокчейн-аналітика, регуляторно-правові рамки та українська практика. Юридичний бюлетень. № 41. 2026. С. 139-148, оприлюднених у межах підготовки дисертаційного дослідження на тему «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» впроваджено в практичну діяльність Департаменту кіберполіції (міжрегіональний територіальний орган) Національної поліції України, з метою використання під час підготовки тематичних планів занять зі службової підготовки, проведення занять у системі службової підготовки, а також у безпосередній практичній діяльності Департаменту.

Підсумки практичного використання зазначених наукових розробок та пропозицій автора підтвердили їх ефективність щодо адміністративно-правового забезпечення діяльності Департаменту кіберполіції та Національної поліції України в цілому.

Старший інспектор з особливих доручень
4-го відділу (організації роботи та планування)
2-го управління (організаційно-аналітичної роботи
та забезпечення діяльності) Департаменту кіберполіції
(міжрегіональний територіальний орган)
Національної поліції України
майор поліції **Роман ФЕДЕНКО**

Начальник 2-го відділу (прогнозування ризиків
та реагування) Департаменту кіберполіції
(міжрегіональний територіальний орган)
Національної поліції України
підполковник поліції **Семен РОГУТ**

Т. в. о. начальника 2-го відділу (кадрового забезпечення)
2-го управління (організаційно-аналітичної роботи
та забезпечення діяльності) Департаменту кіберполіції
(міжрегіональний територіальний орган)
Національної поліції України
полковник поліції **Віталій МОЛЧАНСЬКИЙ**
12.05.2026 року

ЗАТВЕРДЖУЮ
Перший проректор
Одеського державного
університету внутрішніх справ
доктор юридичних наук, професор
полковник поліції

Максим КОРНІЄНКО

«01» 06 2026 року

АКТ
про впровадження результатів дисертаційного дослідження
Шаронова Андрія Павловича
«Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» у наукову діяльність
Одеського державного університету внутрішніх справ

Комісія у складі:

1) начальника відділу організації наукової діяльності ОДУВС, кандидата юридичних наук, доцента Домброван Наталії;

2) ученого секретаря секретаріату Вченої ради ОДУВС, кандидата педагогічних наук Ісаєнка Максима;

3) начальника відділу аспірантури (ад'юнктури) і докторантури ОДУВС, кандидата юридичних наук Теслюк Ірини склала цей акт про те, що комісією вивчені наукові положення, пропозиції і рекомендації Шаронова Андрія Павловича щодо впровадження результатів дисертаційного дослідження на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право» у наукову діяльність Одеського державного університету внутрішніх справ при проведенні наукових досліджень за темою НДР ОДУВС, а саме: загальноуніверситетською темою «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (реєстраційний номер 0123U103538).

Комісія дійшла висновку, що дисертаційне дослідження Шаронова Андрія Павловича щодо впровадження результатів дисертаційного дослідження на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» становить цінність для наукової діяльності, а надані матеріали мають високий теоретичний рівень, зокрема, наступні публікації:

1. Шаронов А.П. Трудові функції оперуповноваженого в парадигмі ILP: нормативно-практичні ориси та кіберкомпонент. *Юридичний бюлетень.* № 37. 2025. С. 97-106.

2. Шаронов А.П. Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. *Морська безпека та оборона.* № 1 (5). 2025. С. 106-115.

3. Шаронов А.П. Міжнародні правові стандарти протидії кіберзагрозам: імплементація та розвиток цифрової стійкості в правовій системі України. *Актуальні проблеми вітчизняної юриспруденції.* № 6. 2025. С. 125-134.

4. Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. *Юридичний бюлетень.* № 39. 2025. С. 147-155.

5. Шаронов А.П., Самойлов С.В., Крайнічук (Шелепало) Г.В. Організаційно-правовий аспект використання відбитку браузера для заходів кіберзахисту. *Наше право.* № 1. 2026. С. 42-52.

6. 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. № 41. 2026. С. 139-148.

7. 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.

8. 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.

9. 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.

Результати дисертаційного дослідження Шаронова Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» впроваджені у наукову діяльність Одеського державного університету внутрішніх справ.

Члени комісії:

Начальник відділу організації наукової діяльності ОДУВС кандидат юридичних наук, доцент підполковник поліції — **Наталія ДОМБРОВАН**

Учений секретар секретаріату Вченої ради ОДУВС кандидат педагогічних наук — **Максим ІСАЄНКО**

Начальник відділу аспірантури (ад'юнктури) і докторантури ОДУВС, кандидат юридичних наук — **Ірина ТЕСЛЮК**

ЗАТВЕРДЖУЮ
Перший проректор
Одеського державного
університету внутрішніх справ
доктор юридичних наук, професор
полковник поліції

Максим КОРНІЄНКО

«01» 06 2026 року

АКТ
впровадження результатів дисертаційного дослідження Шаронова Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» в освітній процес Одеського державного університету внутрішніх справ

Комісія у складі:

1) начальника відділу забезпечення якості освіти, кандидата історичних наук, доцента Камінської Олени;

2) завідувача кафедри кримінального аналізу та інформаційних технологій, кандидата юридичних наук, доцента, підполковника поліції Форос Ганни;

3) старшого наукового співробітника науково-дослідної лабораторії з актуальних питань кримінального аналізу, кандидата юридичних наук, старшого дослідника, майора поліції Пилипенко Євгенії склала цей акт про те, що результати дисертаційного дослідження Шаронова Андрія Павловича на тему: «Протидія кіберзагрозам Національною поліцією України: організаційно-правовий аспект» використовуються в освітньому процесі Одеського державного університету внутрішніх справ, зокрема під час проведення семінарських і практичних занять зі здобувачами вищої освіти при вивченні наступних навчальних дисциплін: «Актуальні питання інформаційного права», «Адміністративна діяльність поліції», «Інформаційні та комунікаційні технології», «Кримінальний аналіз».

Зокрема, використовуються основні положення та висновки, які викладені у наступних публікаціях Шаронова А.П.:

1. Шаронов А.П. Трудові функції оперуповноваженого в парадигмі ILP: нормативно-практичні ориси та кіберкомпонент. *Юридичний бюлетень.* № 37. 2025. С. 97-106.
2. Шаронов А.П. Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. *Морська безпека та оборона.* № 1 (5). 2025. С. 106-115.
3. Шаронов А.П. Міжнародні правові стандарти протидії кіберзагрозам: імплементація та розвиток цифрової стійкості в правовій системі України. *Актуальні проблеми вітчизняної юриспруденції.* № 6. 2025. С. 125-134.
4. Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. *Юридичний бюлетень.* № 39. 2025. С. 147-155.

5. Шаронов А.П., Самойлов С.В., Крайнічук (Шелепало) Г.В. Організаційно-правовий аспект використання відбитку браузера для заходів кіберзахисту. *Наше право*. № 1. 2026. С. 42-52.

6. 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. № 41. 2026. С. 139-148.

7. 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.

8. 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.

9. 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.

Члени комісії:

Начальник відділу
забезпечення якості освіти
кандидат історичних наук, доцент **Олена КАМІНСЬКА**

Завідувач кафедри
кримінального аналізу та інформаційних технологій
кандидат юридичних наук, доцент
підполковник поліції **Ганна ФОРОС**

Старший науковий співробітник
науково-дослідної лабораторії
з актуальних питань кримінального аналізу
кандидат юридичних наук, старший дослідник
майор поліції **Євгенія ПИЛИПЕНКО**

Додаток Б

Опис організаційної структури, технологій та інструментів виявлення вразливостей і реагування на кіберінциденти за 2024 рік


Розподіл кіберінцидентів за секторами
71
Протягом 2024 року така кількість об'єктів кіберзахисту зазнала кібератак і/або кіберінцидентів
5
Оборонний
65
Урядовий
1
Енергетичний
Розподіл кіберінцидентів за місяцями
200
150
100
50
0
179
101
56
54
65
72
66
99
92
98
70
90
Січень
Лютий
Березень
Квітень
Травень
Червень
Липень
Серпень
Вересень
Жовтень
Листопад
Грудень


Розподіл кіберінцидентів за секторами
61
Протягом 2024 року така кількість об'єктів кіберзахисту зазнали кібератак чи кіберінцидентів, що були пов'язані з відомими кластерами кіберзагроз
5
Оборонний
55
Урядовий
1
Енергетичний
Розподіл за джерелом виявлення
EDR
40,8%
EDR
NDR/IDS
59,2%
NDR/IDS

Додаток В

ПЕРЕЛІК
категорій кіберінцидентів CERT-UA[81; 82]

Код xx	**Категорія інциденту**	**Код xx**	**Тип інциденту**	**Тип інциденту англійською**	**Опис типу інциденту**
01.	Шкідливий (образливий) вміст (Abusive content)	01	Спам	Spam	Надсилання небажаних повідомлень або великої кількості повідомлень (флуд)
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection	У системі виявлено ШПЗ.
		02	Розповсюдження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містятять вкладення з шпз або посилання на його завантаження.
		03	Командно-контрольний центр (C2)	Command & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами.
		04	Шкідливе підключення	Malicious connection	Спроби з’єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов’язаних із активністю певної бот-мережі.
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning	Збір інформації про системи або мережі.
		02	Сніфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіку.

		03	Фішинг	Phishing	Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти)
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt	Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі
		02	Спроби авторизації/входу в систему	Login attempts	Спроба входу до служб або механізмів автентифікації / доступу. Невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних.
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compromise	Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу.
06.	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні	DoS/DDoS	Вплив на нормальне функціонування системи чи сервісу що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів.
		02	Саботаж / шкідливі дії	Sabotage	Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо.
		03	Збій	Outage, no malice	Збій в роботі системи чи її компоненту без зловмисного втручання.

07.	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації	Unauthorised access to information	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації.
		02	Несанкціонована модифікація	Unauthorised modification of info	Несанкціонована зміна або видалення певного набору інформації.
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних.
09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability	Наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації
		02	Некоректна конфігурація	Misconfiguration	Недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо)
10.	Інше (Other)	01	Невизначений інцидент	Undetermined incident	Недостатньо даних для обробки інциденту

Додаток Г

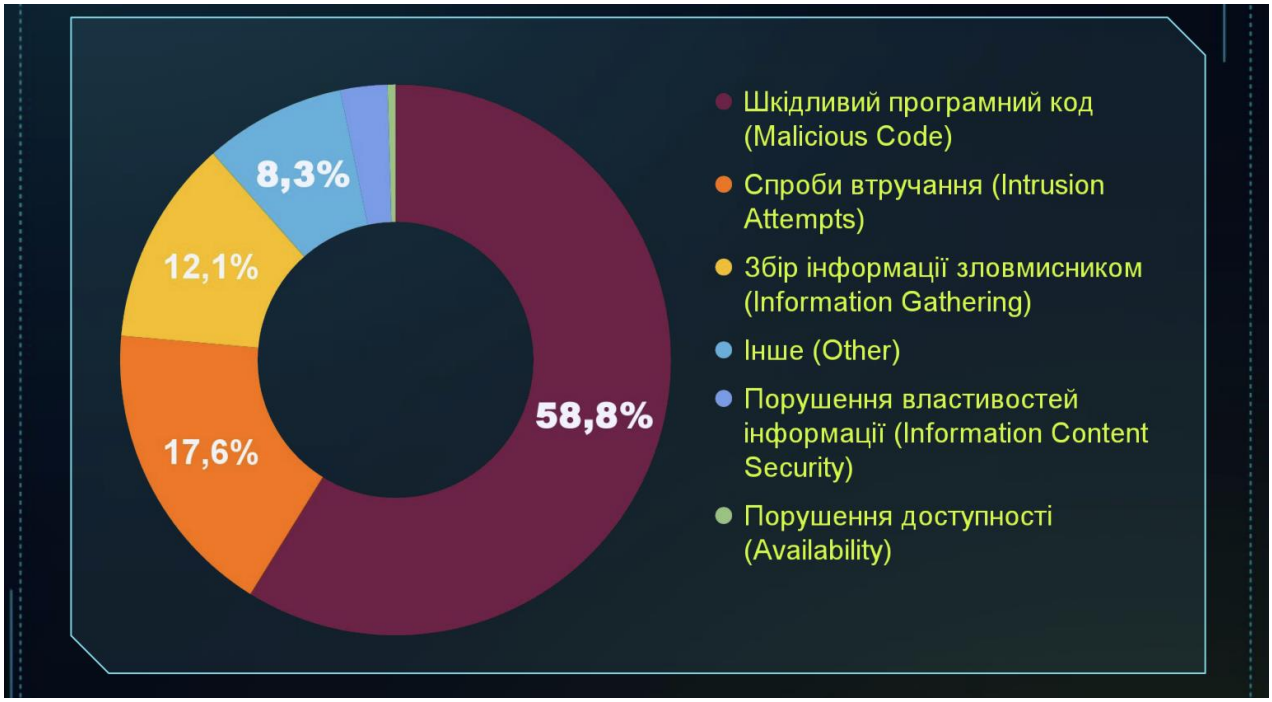
Перелік
категорій кіберінцидентів Держспецзв'язку[81]

Код	Категорія інциденту	Назва інциденту	Назва інциденту в MISP
01.	Шкідливий (образливий) вміст (Abusive content)	Спам	Spam
		Образливий контент	Harmful Speech[1]
		Шкідливий контент	Child/Sexual/Violence/...
02.	Шкідливий програмний код (Malicious Code)	Вірус	Virus
		Хробак	Worm
		Троян	Trojan
		Шпигунське програмне забезпечення	Spyware
		Діалер	Dialer
		Руткіт	Rootkit
		Шкідливе програмне забезпечення	Malware
		Управління ботами	Botnet drone
		Програма-здирник	Ransomware
		Конфігурація шкідливого програмного забезпечення	Malware configuration
		Командно-контрольний центр	C&C
03.	Збір інформації зловмисником (Information Gathering)	Сканування	Scanning
		Перехоплення і аналіз мережевого трафіку	Sniffing
		Соціальна інженерія	Social Engineering
04.	Спроби втручання (Intrusion Attempts)	Експлуатація відомих вразливостей	Exploiting of known Vulnerabilities
		Спроби авторизації	Login attempts
		Експлуатація раніше невідомих вразливостей	New attack signature (exploit)

05.	Втручання (Intrusion)	Компрометація привілейованого облікового запису	Privileged Account Compromise
		Компрометація непривілейованого облікового запису	Unprivileged account compromise
		Компрометація застосунку	Application compromise
		Бот	Bot
		Дефейс	Defacement
		Компрометація системи	Compromised
		Бекдор	Backdoor
06.	Порушення доступності (Availability)	Атака на відмову в обслуговуванні	DoS
		Розподілена атака на відмову в обслуговуванні	DDoS
		Саботаж, диверсія	Sabotage
		Збій без участі зловмисника	Outage, no malice
07.	Порушення властивостей інформації (Information Content Security)	Несанкціонований доступ до інформації	Unauthorised access to information
		Несанкціоноване внесення змін до інформації	Unauthorised modification of information
		Сервер з публічними правами на запис	Dropzone
08.	Шахрайство (Fraud)	Несанкціоноване використання ресурсів	Unauthorized use of resources
		Порушення авторських прав	Copyright
		Маскарадинг	Masquerade
		Фішинг	Phishing
09.	Відома вразливість (Vulnerable)	Вразливості, відкриті для експлуатації	Open for abuse
10.	Інше (Other)	Чорний список	Blacklist
		Недостатньо даних	Unknown
		Інше	Other

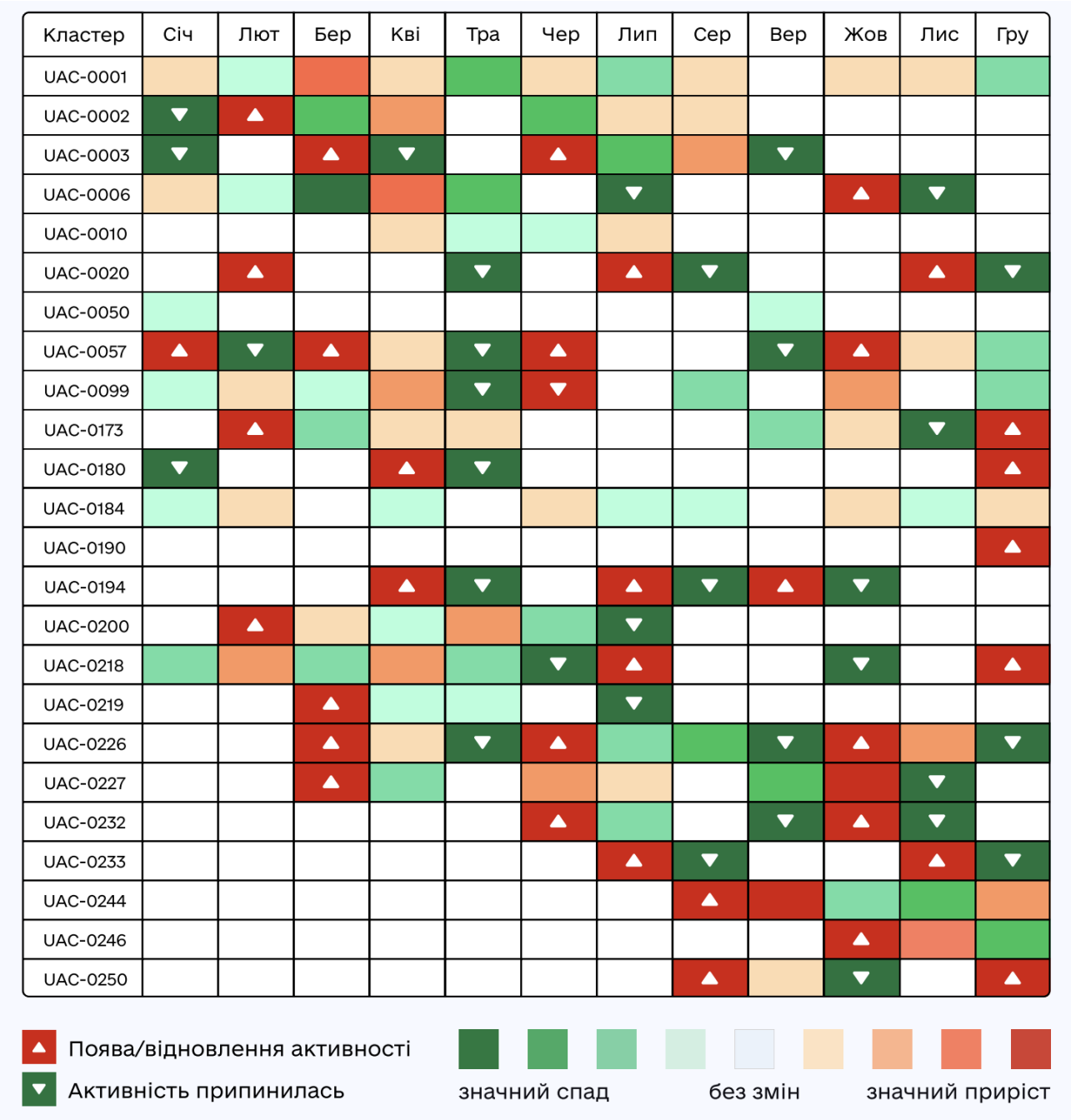
Додаток Д

Статистика моніторингу виявлення вразливостей згідно з Переліком категорій кіберінцидентів за 2024 рік



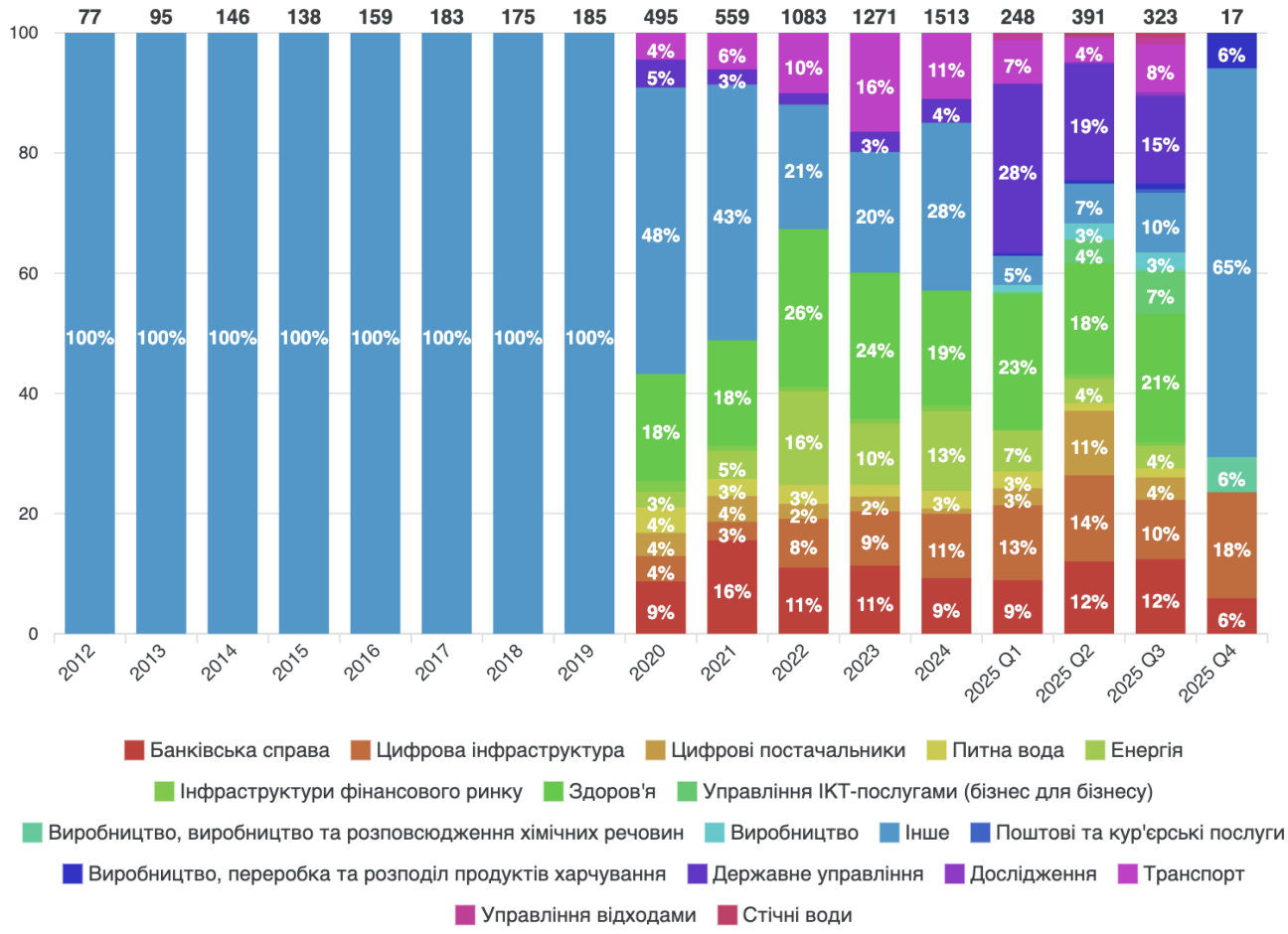
Додаток Е

Теплова карта,
що демонструє динаміку кіберінцидентів, атрибутованих до цих кластерів,
у розрізі місяців 2025 року[49, с. 13]



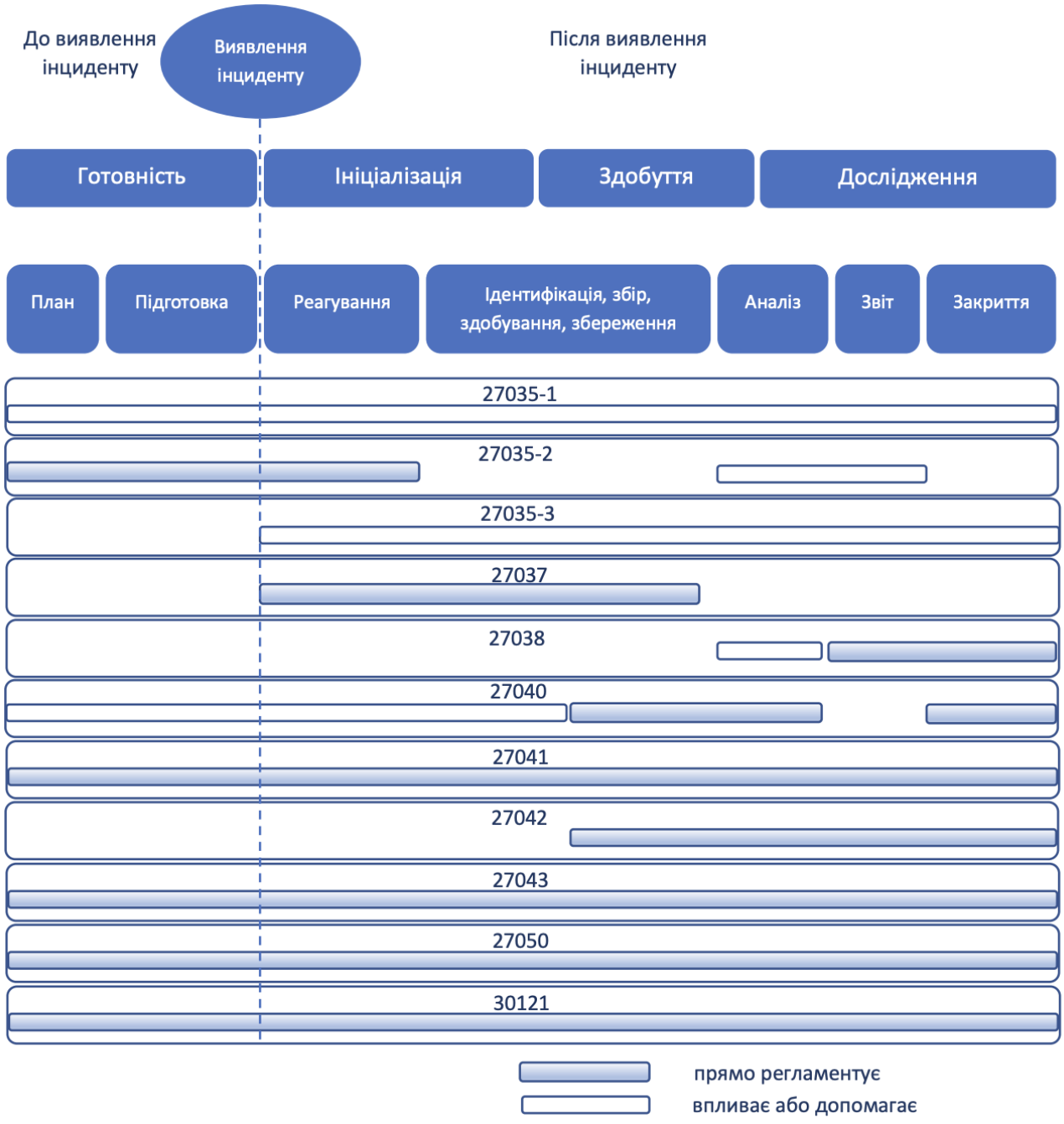
Додаток Ж

Інформація щодо секторіальність кіберзагроз в ЄС



Додаток И

Стандарти ISO/IEC,
які або безпосередньо регламентують управління інцидентами інформаційної безпеки або впливають на цю діяльність



Додаток К

Типологічні моделі обходу санкційних обмежень із використанням криптоактивів[162, с. 127; 217; 178;]

Типологія	Опис	Основний актив	Масштаб / Джерело
Державна стейблкоїн-інфраструктура	Токени, прив'язані до рубля/фіату, випущені квазідержавними структурами для трансакцій поза SWIFT. Приклад: A7A5.	A7A5 (рублевий)	$93,3 млрд за 10 міс.
КВІР-орієнтована інфраструктура	UK-зареєстровані біржі (Zedcex, Zedxion), пов'язані з КВІР, — обробка USDT-потоків для Ірану. Позначені OFAC у січні 2026 р.	USDT	~$1 млрд (TRM Labs, 2026b)
Вкладена VASP-експлуатація	Підсанкційні біржі (Garantex, Nobitex) як вузли ліквідності; маршрутизація через субрахунки у сумісних VASP. Garantex→Grinex.	USDT, BTC	$100 млрд+ (весь строк Garantex)
IT-схеми КНДР	Північнокорейські IT-фахівці у легальних компаніях за підробленими особами; зарплата конвертується у крипто та репатріюється через ETH/USDT/BTC.	USDT, ETH, BTC	$800 млн лише в 2024 р.
Мікшер / Тумблер + крос-чейн	Послідовне розщеплення через Tornado Cash-подібні протоколи та крос-ланцюгові містки. Містки зросли до $2,01 млрд у 2025 р.	BTC, ETH, USDC	$2,01 млрд містки (2025)
Платформи-гаранти типу Huione	Інфраструктура «під ключ» для шахрайства, відмивання та розрахунків. Huione Group позначена FinCEN у жовтні 2025 р.	USDT	$98 млрд+ надходжень (2021–2025)
DeFi-шарування	Багатохопова маршрутизація через децентралізоване кредитування, своп та пули ліквідності; комбінується з крос-чейн містками.	ETH, USDC, DAI	Перша санкція DeFi-протоколу OFAC — ян. 2025

Додаток Л

Відібрані кейси Департаменту кіберполіції НПУ у сфері крипто-злочинності (2024-2026 р.р.)[23; 24; 197; 209; 162, с. 131]

Кейс	Типологія злочину	Масштаб / Збиток	Оперативні дії	Партнери / Результат
Міжнародна хакерська група (Quantum→Royal→BlackSuit→Chaos), лют. 2025	Ransomware-as-a-Service; вимога викупу в крипто	Заявлені вимоги >$500 млн; збиток >3 млрд грн; атаки на Францію, Норвегію, Німеччину, Нідерланди, Канаду, США	Обшуки в Україні; ідентифікація ймовірного організатора-громадянина РФ; ймовірний зв'язок з Conti	ВКА (Німеччина), Швейцарія, Нідерланди, UK, Europol; організатор — в міжнародному розшуку
Екстрадиція хакера до ФБР, червень 2025	Шифрувальне ПЗ (ransomware); вимога викупу в крипто	Збиток понад 3 млрд грн (еквівалент); атаки на Францію, Норвегію та інші	Ідентифікація, процесуальні дії, екстрадиційна перевірка	Передача ФБР 18 червня 2025; до 7 років ув'язнення
Псевдоінвестиційна мережа (Латвія/ЄС), квітень 2025	Фіктивні брокерські платформи; крипто-шахрайство	Мільйони доларів збитку іноземцям; 30+ обшуків у кількох регіонах	Вилучення крипто-гаманців, серверів, автомобілів; арешт активів судом	Латвія, Europol, Євроюст; ОЗГ нейтралізовано; підозра оголошена
Любовний кол-центр + фейкові крипто-біржі (Дніпро), квітень 2026	Pig-butchering ('романтичне' шахрайство) + фіктивна торговельна платформа	100 000 дол. готівкою; 10 елітних авто; 40+ обшуки (Україна+Казахстан)	Спільна слідча група Україна–Казахстан; вилучення зброї та техніки	8 підозрюваних; клопотання про варту
Псевдотрейдингова фінансова біржа (Харків), листопад 2025	Фальшиві торговельні платформи; крипто та ЦП	Кол-центр на 20 місць; міжнародний масштаб	ГСУ НП, Управління кіберполіції Харківщини, УСБУ	3 підозрюваних (до 12 років в'язниці); ОГП; справа ЄС
Транснаціональна хакерська група, 2022–2025 (кейс 2026)	Кібератаки на компанії та органи влади ЄС; вимагання в крипто	Сотні організацій; «сотні мільйонів євро» збитку	Обшуки у Харкові та Харківській обл.; ідентифікація 2 учасників	ВКА, Швейцарія, Нідерланди, UK; Europol; позначення організатора; провадження триває
Відмивання крипто через Garantex-мережу (контекст)	Використання підсанкційної інфраструктури РФ; кримінальні доходи	Garantex: $96 млрд транзакцій; >$1,3 млрд — злочинна діяльність	Аналітичний моніторинг ДКП; взаємодія з Global Ledger, Chainalysis	Внесок до бази даних для міжнародних позначень; підтримка OFAC/ЄС

Додаток М

Модель Аналітичного Життєвого Циклу Крипто-Санкцій (АЖЦКС), адаптована для правозастосовчого контексту України

[178; 191; 217; 162, с. 132]

Етап	Діяльність	Інструменти / Методи	Регуляторна прив'язка 2026	Результат
1. Виявлення	Ідентифікація аномальних патернів у блокчейні; крос-чейн та мульти-актив потоки	Автом. KYT, Crystal/GL скоринг, реальний час	MiCA ст. 86; TFR Travel Rule; ЗУ «Про ВА»	Сигнал підозрілої активності; SAR-тригер
2. Атрибуція	Зв'язок псевдоанонімних адрес з реальними суб'єктами через OSINT + дані VASP + Egmont	CIOH, Signals (Chainalysis), GL 700M атрибуцій, запити до VASP/Tether	FATF R.15; MiCA CASP; GENIUS Act BSA	Аналітичний звіт з судово-допустимими доказами
3. Пакет розвідки	Підготовка аналітичних меморандумів для позначення (OFAC/OFSI/Рада ЄС/ДКП)	Блокчейн-форензика, SDN-готові адресні списки (TRM/Chainalysis)	Процес SDN; Reg. ЄС 269/2014; OFSI UK	Пакет розвідки для позначення
4. Правозастосовча дія	Заморозка активів, вилучення домену, підозра, МЛАТ, запит до Tether/Circle	Судові ухвали, ДКП обшуки, Egmont, Tether API	IEEPA (США); Reg. ЄС; SAIII 2018; КПК України	Санкційне позначення, арешт, вилучення
5. Пост-моніторинг	Відстеження наступників, нової інфраструктури, міграції користувачів (Grinex, MKAN)	Crystal VASP Check, GL містковий моніторинг, OSINT	MiCA дідус-ліценз. закінчення (1.07.2026); CARF 2026 дані	Оцінка стійкості виконання; пакет позначення наступника

Додаток Н

Порівняння сумісних термінів: «інтероперабельність у кібербезпеці», «сумісність», «координація» та «стандартизація» [157, с. 110]

Критерій порівняння	«інтероперабельність у кібербезпеці»	«сумісність»	«координація»	«стандартизація»
Сутність	Системна властивість, що забезпечує узгоджену взаємодію технічних, організаційних і правових компонентів кібербезпекового середовища	Технічна здатність різних систем або компонентів працювати спільно без конфліктів	Організаційна узгодженість дій між суб'єктами з метою спільного реагування на кіберзагрози	Процес розроблення та впровадження спільних норм, вимог і протоколів
Рівень прояву	Системний (охоплює технічний, процедурний, правовий, організаційний рівні)	Технічний (апаратний або програмний)	Організаційні, управлінський	Нормативно-технічний
Цільове призначення	Забезпечення безперервного, безпечного й достовірного обміну інформацією між суб'єктами	Уникнення технічних конфліктів і забезпечення працездатності компонентів	Узгодження дій між структурами в межах спільних завдань	Уніфікація параметрів, процесів і вимог для підвищення сумісності
Ключовий механізм реалізації	Використання спільних протоколів, стандартів (STIX, TAXII, ISO/IEC 27001, NIS2), організаційних процедур і правових угод	Технічна інтеграція, драйвери, API, формат даних	Управлінські рішення, накази, координаційні ради, взаємні домовленості	Розробка стандартів, технічних регламентів, інструкцій
Результат	Узгоджене функціонування різнорідних систем у межах єдиного простору кіберзахисту	Сумісна робота продуктів або технологій	Синхронізація діяльності суб'єктів	Упорядкована нормативна база, що задає параметри взаємодії
Приклад у сфері кібербезпеки	Взаємодія CERT-UA з ENISA через спільні протоколи обміну даними про кіберінциденти	Можливість запуску антивірусного ПЗ різних виробників на одному сервері	Координація дій між НКЦК, ДКП НПУ та Держспецзв'язку під час реагування на кібератаки	Впровадження стандартів ISO/IEC 27001 або ENISA Best Practices
Тип взаємозв'язку з іншими поняттями	Інтеграційне поняття, що ґрунтується на сумісності, координації та стандартизації	Є складовою технічної основи інтероперабельності	Є організаційною передумовою інтероперабельності	Є нормативною базою, що забезпечує інтероперабельність
Кінцева мета	Створення єдиного, узгодженого кібербезпекового простору	Технічна працездатність компонентів	Злагоджені дії учасників системи	Єдність вимог і процедур

Додаток О

Нормативні стандарти
у сфері інформаційної безпеки та цифрової криміналістики

Назва документа	Коротка характеристика	Релевантність для НПУ
ДСТУ ISO/IEC 27035-1:2024 [33]	Визначає основні принципи, структуру та етапи керування інцидентами інформаційної безпеки. Регламентує процеси виявлення, реєстрації, оцінювання, реагування та відновлення після інцидентів	Є методичною основою для формування внутрішніх процедур реагування на кіберінциденти в діяльності НПУ
ДСТУ ISO/IEC 27035-2:2024	Містить настанови щодо планування та підготовки до реагування на інциденти, включаючи розподіл ролей, ресурсне забезпечення, створення команд реагування та розроблення планів дій	Важливий для організації системної підготовки підрозділів НПУ до реагування на інциденти та для координації
ДСТУ EN ISO/IEC 27043:2022 [31]	Установлює принципи та процеси розслідування інцидентів інформаційної безпеки. Охоплює підходи до планування розслідування, збирання матеріалів, аналізу подій та документування результатів	Має значення для кримінального аналізу, службових перевірок і цифрової криміналістики у справах, пов’язаних із кіберправопорушеннями
ДСТУ EN ISO/IEC 27037:2022 [29]	Надає настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Основна увага приділяється забезпеченню цілісності, автентичності та простежуваності доказової інформації	Важливий для забезпечення допустимості цифрових доказів у провадженні та для правильної первинної роботи з електронними носіями
ДСТУ EN ISO/IEC 27042:2022 [30]	Регламентує підходи до аналізу та інтерпретації цифрових доказів, їх змісту, логічних зв’язків та доказового значення, забезпечує обґрунтованість і відтворюваність	Використовується під час експертного аналізу цифрової інформації, OSINT-опрацювання матеріалів та підготовки аналітичних висновків
ДСТУ ISO/IEC 27041:2016 [34]	Визначає вимоги до забезпечення прийнятності та адекватності методів розслідування. Передбачає оцінювання придатності інструментів, процедур і методик, які застосовуються у цифровій криміналістиці	Сприяє використанню валідних та процесуально обґрунтованих методів дослідження цифрових слідів

Продовження Додатку О

Міжнародні стандарти у сфері штучного інтелекту та інформаційної безпеки

ISO/IEC 27001	Установлює вимоги до системи управління інформаційною безпекою в організації. Орієнтований на захист конфіденційності, цілісності та доступності інформації через ризик-орієнтований підхід	Є базовим стандартом для побудови захищених інформаційних систем і процесів роботи з оперативною, аналітичною та службовою інформацією.
ISO/IEC 31700	Закріплює підхід «privacy by design» і «privacy by default», за яких захист приватності має бути інтегрований у розроблення та функціонування цифрових систем із самого початку	Допомагає враховувати вимоги захисту персональних даних під час збору та обробки інформації
ISO/IEC 5338	Пропонує рамку управління життєвим циклом систем штучного інтелекту, включаючи етапи планування, розроблення, експлуатації, моніторингу й удосконалення	Актуальний для впровадження ШІ-рішень у кримінальний аналіз, прогнозування ризиків та підтримку управлінських рішень НПУ
ISO/IEC 42001	Перший міжнародний стандарт для системи управління штучним інтелектом. Визначає підходи до впровадження, підтримки та вдосконалення управління ШІ з урахуванням ризиків, етики та відповідальності	Дає нормативну основу для безпечного й контрольованого використання ШІ в правоохоронній діяльності, зокрема в аналітичних і моніторингових системах
ISO/IEC TS 6254	Містить огляд технологій створення синтетичного мультимедійного контенту, а також методів і показників його виявлення. Особливо актуальний для аналізу deepfake-контенту	Має практичне значення для протидії дезінформації, виявлення маніпулятивних матеріалів та підтримки інформаційної безпеки в умовах гібридних загроз
ISO/IEC TS 5259-1	Формує підхід до забезпечення якості даних і простежуваності їх походження протягом усього життєвого циклу. Спрямований на підвищення надійності та прозорості даних	Важливий для перевірки джерел інформації, забезпечення достовірності OSINT-матеріалів і підвищення якості аналітичної продукції

Додаток П

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Шаронов А.П. Трудові функції оперуповноваженого в парадигмі ILP: нормативно-практичні ориси та кіберкомпонент. *Юридичний бюлетень.* № 37. 2025. С. 97-106. DOI: https://doi.org/10.32850/LB2414-4207.2025.37.13

2. Шаронов А.П. Інтероперабельність у кібербезпеці: виклики, підходи та перспективи. *Морська безпека та оборона.* № 2 (6). 2025. С. 106-115. DOI: https://doi.org/10.32782/msd/2025.2/13

3. 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. DOI: https://doi.org/10.32782/2408-9257-2025-6-18

4. Шаронов А.П. Протидія кіберзагрозам Національною поліцією України: нормативно-правові засади та процесуальна допустимість AI-даних. *Юридичний бюлетень.* № 39. 2025. С. 147-155. DOI: https://doi.org/10.32850/LB2414-4207.2025.39.17

5. Шаронов А.П., Самойлов С.В., Крайнічук (Шелепало) Г.В. Організаційно-правовий аспект використання відбитку браузера для заходів кіберзахисту. *Наше право*. № 1. 2026. С. 42-52. DOI: https://doi.org/10.71404/NP.2026.1.6

6. 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.* № 41. 2026. С. 120-136. DOI: https://doi.org/10.32850/LB2414-4207.2026.41.15

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. 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.

2. 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.

3. 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.