НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

КОЛЕСНИК ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ

УДК 342.9:004.056

ДИСЕРТАЦІЯ

КІБЕРБЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: ПРАВОВІ ВИКЛИКИ ГІБРИДНОЇ ВІЙНИ ТА МІЖНАРОДНИЙ ДОСВІД

Спеціальність – 081 «Право»
Галузь знань – 08 «Право»

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____О. О. Колесник

Науковий керівник **Сорока Лариса Володимирівна,** доктор юридичних наук, професор

Київ – 2025

АНОТАЦІЯ

Колесник О. О. Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід. – *Кваліфікаційна наукова праця на правах рукопису*.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». – Науково-дослідний інститут публічного права, Київ, 2025.

Дисертаційна робота присвячена комплексному дослідженню кібербезпеки як системоутворювального елемента національної безпеки України в умовах гібридної війни та з урахуванням міжнародно-правового досвіду провідних держав і міжнародних організацій. З огляду на стратегічний курс України на інтеграцію до Європейського Союзу та НАТО, розбудову цифрової держави й підвищення кіберстійкості критичної інфраструктури, проблема формування ефективної, правово визначеної та інституційно узгодженої системи кібербезпеки набуває особливої актуальності.

Кіберзагрози, що супроводжують збройну агресію Російської Федерації, продемонстрували, що кіберпростір став не лише технічним, а й правовим, політичним і безпековим виміром сучасних конфліктів, у межах якого захист даних, функціонування державного управління та гарантування прав людини потребують оновлених нормативних і управлінських підходів.

У цьому контексті показовим є міжнародний досвід Європейського Союзу, НАТО та Сполучених Штатів Америки. Європейський Союз сформував цілісну нормативну екосистему кіберзахисту, що ґрунтується на узгодженому пакеті актів (NIS2, CER, DORA, CRA, Cyber Solidarity Act) і методичній ролі ENISA. Сполучені Штати розвинули інституційно зрілу модель державно-приватного партнерства у сфері кібербезпеки, що спирається на діяльність CISA, рамку NIST CSF 2.0 та ініціативу JCDC. НАТО, своєю чергою, реалізує механізми колективної кібероборони та взаємодопомоги між державами-членами. Їх порівняльний аналіз дав змогу

визначити найефективніші інструменти нормативного, організаційного та технічного забезпечення кіберстійкості й адаптувати їх до українського правового та інституційного середовища.

Український досвід протидії кіберагресії 2014–2024 років розглянуто як унікальний приклад ведення оборони у цифровому вимірі та як емпіричну основу для виявлення закономірностей і тенденцій правового забезпечення кібербезпеки в умовах гібридної війни.

Методологічну основу дослідження становлять теоретико-правовий, порівняльно-інституційний і емпіричний методи, що забезпечують комплексне розкриття ролі міжнародного права у сфері кіберзахисту, ідентифікацію інституційних вразливостей національної системи та розроблення практичних рекомендацій щодо вдосконалення правового регулювання державно-приватної взаємодії, гармонізації законодавства з acquis ЄС і впровадження принципів shared responsibility та security by design у державну політику управління кіберризиками.

У першому розділі здійснено теоретико-методологічний аналіз еволюції поняття «кібербезпека» та розкрито його зміст у сучасному науковому дискурсі. Показано, що кібербезпека сформувалася як міждисциплінарне явище, яке інтегрує технічні, правові, управлінські, соціальні та етичні виміри, утворюючи цілісну соціотехнічну систему, спрямовану на забезпечення стійкого функціонування цифрового середовища.

Виявлено дефінітивну невизначеність і фрагментарність термінології, пов’язаної з поняттями «інформаційна безпека», «кібербезпека», «кіберзахист» і «кіберстійкість». Аргументовано, що відсутність уніфікованих дефініцій зумовлює методологічну та нормативну неузгодженість, яка ускладнює формування цілісної й узгодженої системи правового регулювання у сфері кібербезпеки.

Систематизовано основні наукові підходи до розуміння кібербезпеки – технократичний, правовий, організаційно-управлінський та

соціогуманітарний –і доведено, що лише їх інтеграція в межах системного підходу забезпечує комплексне осмислення кібербезпеки як динамічного процесу управління ризиками, довірою та стійкістю цифрових систем. Простежено трансформацію наукової парадигми – від традиційної концепції «захисту систем» до сучасної моделі кіберстійкості (cyber resilience), у межах якої безпека трактується не лише як здатність системи протидіяти загрозам, а й як її спроможність адаптуватися, відновлюватися та навчатися на основі отриманого досвіду.

Запропоновано авторське визначення поняття «кібербезпека», яке трактується як стан і водночас безперервний процес забезпечення стійкого, правомірного та етично врегульованого функціонування цифрового середовища. Запропоноване визначення інтегрує технічні, правові, організаційні та етичні компоненти у єдину системно-комплексну модель кіберстійкості, що відповідає сучасним тенденціям розвитку міжнародного кіберправа та практики глобального кіберзахисту.

Розкрито місце міжнародного права в архітектурі глобальної та національної кібербезпеки. Показано, що воно виконує подвійну функцію – універсального регулятора цифрових відносин і водночас засобу легітимації державної політики у сфері кіберзахисту. Проаналізовано основні напрями формування міжнародно-правового режиму кібербезпеки, зокрема діяльність ООН, ОБСЄ, Ради Європи та ЄС, а також позиції держав щодо застосування базових принципів міжнародного права до кібероперацій. Доведено, що поєднання норм «твердого» і «м’якого» права, інструментів довіри, прозорості та публічності формує поліцентричну, але внутрішньо узгоджену систему міжнародного кіберврядування.

Узагальнено зміст і значення базових принципів міжнародного права, релевантних цифровому середовищу, – суверенітету, невтручання, заборони сили, належної обачності та поваги до прав людини. Підкреслено, що саме вони становлять нормативне ядро міжнародно-правового режиму

кіберзахисту та забезпечують фундамент відповідальної поведінки держав у кіберпросторі.

Проведено комплексний аналіз міжнародно-правових механізмів протидії кіберзлочинності та кіберзагрозам. Встановлено, що глобальна система кіберзахисту функціонує як поліцентричний режим, який поєднує кримінально-правові, політико-правові та дипломатичні інструменти. Визначено провідну роль Будапештської конвенції про кіберзлочинність, Другого додаткового протоколу, санкційних механізмів ЄС та заходів довіри ОБСЄ. Наголошено, що «м'якоправові» інструменти, зокрема Талліннський посібник, сприяють уніфікації державної практики та зміцненню нормативної єдності міжнародного режиму кіберзахисту.

Систематизовано міжнародно-правові механізми відповідальності держав за шкідливу діяльність у кіберпросторі. Розкрито зміст норм, що регулюють атрибуцію, контрзаходи та пропорційність державної реакції, узагальнено доктринальні підходи до доказування й публічних звинувачень. Висвітлено практику ЄС, ООН і ОБСЄ щодо колективної превенції та забезпечення міжнародної відповідальності за дії у кіберпросторі.

Узагальнено доктринальні та інституційні засади міжнародно-правового режиму кіберзахисту. Розкрито значення Талліннських посібників як авторитетного тлумачення норм міжнародного права щодо кібероперацій і визначено їхню роль у формуванні єдиних підходів до правомірності дій держав у цифровому середовищі. Узагальнено підходи до визначення порогів застосування сили, права на самооборону та міжнародної відповідальності держав, а також проаналізовано діяльність ООН і ОБСЄ щодо розроблення норм відповідальної поведінки держав і заходів довіри у сфері кібербезпеки.

Визначено базові принципи державної політики у сфері кіберзахисту – верховенство права, законність, пропорційність, підзвітність і ризик-орієнтованість, які забезпечують її стабільність, ефективність і легітимність.

Систематизовано стратегічну архітектуру державної політики кібербезпеки, яка охоплює рамкові, секторальні та операційно-стратегічні

документи, що забезпечують цілісність і послідовність державної політики. Підкреслено роль механізмів стратегічного планування, міжвідомчої координації та розвитку оборонного кіберкомпонента, а також координаційну функцію Національного координаційного центру кібербезпеки, який забезпечує стабільність та результативність реалізації державних рішень у цій сфері.

Проаналізовано оновлення правової бази за 2022–2025 роки, спрямоване на підвищення компетенцій суб'єктів безпеки та адаптацію національного законодавства до стандартів ЄС. Водночас наголошено на потребі подальшої уніфікації термінології, процедур координації та імплементації європейських стандартів кіберстійкості.

У другому розділі системно проаналізовано феномен кіберагресії проти України як комплексне явище, що поєднує правові, технологічні та організаційні виміри. Сформовано типологію кіберагресії за трьома взаємопов'язаними осями – «цілі – інструменти – очікувані ефекти», яка дозволяє уніфікувати класифікацію інцидентів і поєднати технічні характеристики з правовими режимами реагування. Визначено, що сучасна практика кіберконфліктів утворює низку «сірих зон» у міжнародному праві, зокрема щодо порогів суверенітету, критеріїв атрибуції та правового режиму цифрових доказів, які часто перебувають у розпорядженні приватного сектору. Обґрунтовано потребу уніфікації доктринальних підходів до кваліфікації кібератак і створення механізмів публічно-приватної взаємодії, здатних забезпечити баланс між державними повноваженнями та технологічними ресурсами недержавних акторів.

Розкрито еволюцію російської кіберагресії проти України у 2014–2024 роках, що пройшла три фази з відмінною технологічною, організаційною та правовою специфікою – від атак на енергетичну інфраструктуру (BlackEnergy, Industroyer) до багатовекторних операцій періоду повномасштабної війни (NotPetya, wiper, DDoS, ураження супутникових мереж). Доведено, що ці дії мають спільні ознаки державного походження,

високого рівня координації та стратегічної спрямованості на підрив стійкості критичної інфраструктури, легітимності державних інститутів і суспільних комунікацій.

Систематизовано структурні вразливості національної кіберстійкості у трьох вимірах – інституційному, технічному та соціально-комунікаційному – і на основі емпіричних даних розроблено аналітичну матрицю «вразливість – прояви – напрями вдосконалення». Обґрунтовано потребу гармонізації національних підходів із європейськими стандартами (ENISA RICT, NIS2), створення механізмів оперативного обміну інформацією між державними та відомчими CSIRT/SOC і правового оформлення типових угод про рівень надання послуг (SLA) для критичних цифрових сервісів.

Підкреслено роль соціально-комунікаційних чинників – людського фактора, дезінформації та волонтерських кіберініціатив – як системоутворювальних елементів кіберстійкості. Відзначено, що відсутність уніфікованих протоколів кризової комунікації, нерівномірна підготовка кадрів і неформалізована взаємодія з волонтерськими спільнотами знижують ефективність реагування на інциденти. Запропоновано унормувати співпрацю між державними та недержавними акторами в межах публічно-приватного партнерства, а також розширити програми підготовки з кібергігієни та протидії соціальній інженерії.

Сформульовано концептуальні орієнтири переходу України до проактивної моделі кіберзахисту, заснованої на стандартизованих процедурах обміну інформацією, узгоджених технічних вимогах і розвитку довіри як стратегічного ресурсу цифрової безпеки. Показано, що зміцнення національної кіберстійкості потребує інституційного оформлення та нормативного закріплення публічно-приватного партнерства як ключового елементу державної політики у сфері кібербезпеки.

Узагальнено, що кіберагресія проти України має системний, багаторівневий і скоординований характер, а її наслідки за масштабом і впливом співмірні з традиційними воєнними діями, що свідчить про

трансформацію кіберпростору у сферу стратегічного протиборства. Доведено, що чинна модель реагування залишається переважно реактивною, зорієнтованою на постфактум-виявлення та локалізацію наслідків, що обмежує ефективність превенції, атрибуції й довгострокового стримування кіберзагроз. На цій підставі обґрунтовано необхідність переходу до інтегрованої системи кіберстійкості, яка поєднує інституційні, технічні та соціальні ресурси держави, бізнесу й громадянського суспільства.

У третьому розділі досліджено євроатлантичні моделі кіберзахисту та визначено напрями їх адаптації до української правової системи. Розділ ґрунтується на комплексному порівняльно-правовому аналізі європейського, американського та натівського підходів до формування архітектури кіберстійкості, що охоплює правові, інституційні, технічні та партнерські механізми управління кіберризиками.

Розкрито сутність європейської моделі кіберзахисту як нормативно зобов'язувальної екосистеми, що базується на взаємодії директив і регламентів NIS2, CER, DORA, CRA, DSA, Cyber Solidarity Act та Cybersecurity Act і координується Європейським агентством з кібербезпеки (ENISA). Показано, що ця модель еволюціонувала від декларативних положень до циклу «політика – виконання – контроль – реагування», у межах якого поєднано наднаціональну уніфікацію стандартів і національну відповідальність за їх імплементацію. Проаналізовано практики держав ЄС (Німеччини, Франції, Швеції, Естонії), які демонструють ефективне поєднання правового регулювання з операційною координацією та розвитком мереж CSIRT і механізмів сертифікації.

Визначено особливості американської моделі кіберзахисту, що спирається на стратегічне планування, стандартизацію, адміністративне регулювання та тісну співпрацю держави з приватним сектором. Простежено еволюцію від добровільних механізмів до системи нормативно визначених вимог, закріплених у Національній стратегії кібербезпеки (2023), Плані її реалізації (2023–2024), виконавчих актах (EO 14028, CIRCIA) і стандартах

NIST CSF 2.0 та NICE Framework. Підкреслено практичну спрямованість, гнучкість та високу адаптивність цієї моделі, що забезпечує збалансовану взаємодію державних, корпоративних і суспільних акторів у забезпеченні кіберстійкості.

Розглянуто політику кібероборони НАТО, у межах якої кіберпростір офіційно визнано сферою колективної оборони. Проаналізовано ключові документи й рішення Альянсу, які визначають принципи взаємодопомоги, стійкості та партнерства, а також роль Кооперативного центру кібероборони (CCDCOE, Таллінн) як провідного аналітичного й навчального осередку. Показано, що політика НАТО має переважно координаційний характер і спрямована на формування стандартів сумісності, обмін інформацією та підвищення готовності союзників до кіберзагроз, залишаючи кожній державі автономну відповідальність за власний кіберзахист.

На тлі цих моделей проаналізовано процес інтеграції України до міжнародного безпекового простору ЄС і НАТО. Встановлено поступову гармонізацію національної нормативно-правової бази з європейським правом (NIS2, CER, DORA, CRA, Cybersecurity Act) та посилення міжвідомчої координації між РНБО, НКЦК, ДССЗЗІ й CERT-UA. Окреслено дипломатичний вимір інтеграції – участь України у кібердіалозі з ЄС, співпрацю з ENISA, долучення до ініціатив Tallinn Mechanism і підготовку до приєднання до EU Cybersecurity Reserve, що забезпечує інституційну сумісність та підвищує довіру міжнародних партнерів.

Окремий підрозділ присвячено аналізу державно-приватного партнерства (ДПП) у сфері кібербезпеки як ключового інструменту колективної стійкості. Узагальнено досвід США (моделі JCDC, ISACs, ISAOs, підкріплені актами EO 14028, CIRCIA та стандартами NIST CSF 2.0) і ЄС (мережа CSIRTs, директиви NIS2, CER, DORA, CRA, Cyber Solidarity Act, координаційна роль ENISA). Досліджено національні практики Німеччини, Великої Британії та Естонії, що демонструють поєднання правових гарантій, технічних стандартів і відкритих протоколів взаємодії.

Доведено, що євроатлантична модель ДПП у кібербезпеці характеризується нормативною зрілістю, інституційною сталістю та високим рівнем взаємної довіри, ґрунтуючись на принципах правової визначеності, спільної відповідальності та технологічної прозорості. На цій основі сформульовано напрями адаптації євроатлантичних підходів до українського контексту:

– кодифікаційний напрям – доопрацювання та ухвалення спеціального закону «Про державно-приватну взаємодію у сфері кібербезпеки» (законопроєкт №14150), який встановлює статус, права, обов'язки та відповідальність учасників;

– гармонізаційний напрям – узгодження законопроєкту з нормами NIS2, CER, DORA та CRA, запровадження процедур інцидент-репортингу, обробки даних і спільних команд реагування;

– інституційний напрям – створення єдиного національного координатора (Single Point of Contact), секторальних ISAC-платформ, консультативних рад і публічної системи моніторингу;

– концептуально-принциповий напрям – закріплення у національній кіберполітиці євроатлантичних принципів «shared responsibility» та «security by design» як основи довіри, безпеки та сталого розвитку цифрового середовища.

Ключові слова: національна безпека; інформаційна безпека; цифрова безпека; кібербезпека; кіберстійкість; кіберагресія; гібридна війна; критична інфраструктура; управління кіберризиками; суверенітет у кіберпросторі; державна політика кіберзахисту; штучний інтелект; цифрові загрози; цифрові інновації та технології; інформаційні технології; правове регулювання; правий захист.

SUMMARY

Kolesnyk O. O. Cybersecurity in the System of National Security of Ukraine: Legal Challenges of Hybrid Warfare and International Experience. – *Qualification scientific work on the rights of the manuscript.*

The thesis for obtaining a scientific degree of Doctor of Philosophy in speciality 081 «Law» – Scientific Institute of Public Law, Kyiv, 2025.

The thesis is devoted to a comprehensive study of cybersecurity within the system of Ukraine's national security under the conditions of hybrid warfare and in light of the international experience of leading states and international organisations. Given Ukraine's strategic course towards integration with the European Union and NATO, the development of a digital state, and the strengthening of the cyber resilience of critical infrastructure, the formation of an effective, legally defined, and institutionally coherent cybersecurity system has become a matter of exceptional importance.

Cyber threats accompanying the armed aggression of the Russian Federation have demonstrated that cyberspace has become not only a technical but also a legal and security dimension of modern conflicts, where issues of data protection, public governance, and human rights require new regulatory approaches.

In this context, the international experience of the European Union, NATO, and the United States of America is particularly illustrative for Ukraine. The EU has developed a comprehensive regulatory ecosystem of cyber protection (NIS2, CER, DORA, CRA, Cyber Solidarity Act); the USA has established an institutionally mature model of public–private partnership in cybersecurity (CISA, NIST CSF 2.0, JCDC); and NATO has elaborated mechanisms of collective cyber defence and mutual assistance among its member states. Their comparative analysis enables the identification of the most effective normative, organisational, and technical instruments for ensuring cyber resilience and the adaptation of such instruments to Ukrainian realities.

Accordingly, Ukraine's experience in countering cyber aggression during 2014–2024 constitutes not only a unique case of defence in the digital domain but

also a representative basis for revealing the regularities of legal regulation of cybersecurity under hybrid warfare conditions. The dissertation combines theoretical–legal, comparative–institutional, and empirical analysis aimed at elucidating the role of international law in the field of cyber defence, identifying institutional vulnerabilities of the national system, and formulating proposals for improving the legal framework of public–private cooperation, harmonising legislation with the EU acquis, and implementing the principles of shared responsibility and security by design in public policy.

The first chapter presents a theoretical and methodological analysis of the evolution of the concept of "cybersecurity" and explores its meaning in contemporary academic discourse. It is shown that cybersecurity has emerged as an interdisciplinary phenomenon integrating technical, legal, managerial, social, and ethical dimensions, forming a holistic socio-technical system aimed at ensuring the sustainable functioning of the digital environment. The study reveals definitional uncertainty and terminological fragmentation in the use of related notions such as information security, cybersecurity, cyber defence, and cyber resilience. It is argued that the absence of unified definitions leads to methodological and normative inconsistency, which complicates the formation of a coherent system of legal regulation in the field of cybersecurity.

The principal scholarly approaches to understanding cybersecurity – technocratic, legal, organisational-managerial, and socio-humanitarian – have been systematised. It has been demonstrated that only their integration within a systemic approach ensures a comprehensive understanding of cybersecurity as a dynamic process of managing risks, trust, and the resilience of digital systems. The evolution of the scientific paradigm has been traced – from the traditional model of «system protection» towards the concept of cyber resilience, within which security is interpreted as the capability of a system not merely to resist threats but also to recover and to learn from experience.

An author's definition of «cybersecurity» is proposed. It is interpreted as both a state and a continuous process of ensuring the stable, lawful, and ethically

regulated functioning of the digital environment. This state is achieved through the coordinated interaction of technological, managerial, legal, and behavioural mechanisms aimed at protecting data, infrastructures, and public functions of the state from destructive influences and ensuring their recoverability. The proposed definition integrates technical, legal, managerial, and ethical components into a single systemic and comprehensive model of cyber resilience, corresponding to contemporary developments in cyber law and international practice in cyber defence.

The role of international law in the architecture of global and national cybersecurity is examined. It is shown that international law performs a dual function – that of a universal regulator of digital relations and, simultaneously, a means of legitimising state policy in the field of cyber defence. The dissertation analyses the principal directions in the formation of the international legal regime of cybersecurity, including the activities of the United Nations, the OSCE, the Council of Europe, and the European Union, as well as the positions of states regarding the applicability of fundamental principles of international law to cyber operations. It is substantiated that the combination of «hard law» and «soft law» norms, together with instruments of trust, transparency, and publicity, forms a polycentric yet internally coherent system of international cyber governance.

The content and significance of the fundamental principles of international law relevant to the digital environment – sovereignty, non-intervention, prohibition of the use of force, due diligence, and respect for human rights – have been generalised. It is emphasised that these principles constitute the normative core of the international-legal regime of cyber defence and provide the foundation for responsible state behaviour in cyberspace.

A comprehensive analysis of international legal mechanisms for countering cybercrime and cyber threats has been carried out. It has been established that the global system of cyber defence functions as a polycentric regime combining criminal law, politico-legal, and diplomatic instruments. The leading role of the Budapest Convention on Cybercrime, its Second Additional Protocol, the EU’s

sanctions mechanisms, and the OSCE confidence-building measures has been identified. It is stressed that soft-law instruments, such as the Tallinn Manuals, contribute to the unification of state practice and the strengthening of normative coherence within the international regime of cyber defence.

The international legal mechanisms of state responsibility for malicious activities in cyberspace have been systematised. The dissertation elaborates on the content of norms regulating attribution, countermeasures, and the proportionality of state responses, and summarises doctrinal approaches to evidence and public attribution. It further highlights the practice of the EU, UN, and OSCE regarding collective prevention and the enforcement of international responsibility for actions in cyberspace.

The doctrinal and institutional foundations of the international legal regime of cyber defence have been generalised. The significance of the Tallinn Manuals as an authoritative interpretation of the norms of international law applicable to cyber operations has been elucidated, as well as their role in shaping uniform approaches to the lawfulness of state conduct in the digital domain. The dissertation also explores the humanitarian law aspects of cyber conflicts, including the application of international humanitarian law to cyber operations during armed conflicts. It consolidates various doctrinal approaches to defining thresholds for the use of force, the right of self-defence, and state responsibility, and analyses the activities of the UN and the OSCE in developing norms of responsible state behaviour and confidence-building measures in the field of cybersecurity.

The legal foundations for the formation of Ukraine’s national cybersecurity system have been systematically examined as a multi-level socio-technical construct combining legal, organisational, technological, and managerial elements. The basic principles of state policy in the field of cyber defence have been identified, namely, the rule of law, legality, proportionality, accountability, and risk-orientation – which ensure its stability, effectiveness, and legitimacy.

The constitutional and legal foundations of the functioning of the cybersecurity system have been explored, defining the hierarchy of legal sources, the legitimacy, and the limits of public-law intervention.

The strategic architecture of state cybersecurity policy has been systematised; it encompasses framework, sectoral, and operational-strategic documents that ensure the integrity and internal consistency of governmental policy. Emphasis is placed on the role of strategic planning mechanisms, inter-agency coordination, and the development of the defence cyber component, as well as on the coordinating function of the National Cybersecurity Coordination Centre, which guarantees the stability and effectiveness of the implementation of state decisions in this domain.

The legislative framework of Ukraine's cybersecurity system has been analysed as a hierarchical structure of framework, special, and procedural acts defining the legal regimes of information protection, the resilience of critical infrastructure, and liability for cybercrime. The renewal of the legal base during 2022–2025, aimed at enhancing the competence of security actors and aligning national legislation with EU standards, has been examined. At the same time, attention is drawn to the continued need for further unification of terminology, coordination procedures, and implementation of European cyber-resilience standards.

The second chapter presents a systemic analysis of the phenomenon of cyber aggression against Ukraine as a complex occurrence combining legal, technological, and organisational dimensions. A typology of cyber aggression has been developed along three interrelated axes: «targets – instruments – expected effects» which makes it possible to standardise the classification of incidents and to correlate technical characteristics with the relevant legal regimes of response. It is established that the contemporary practice of cyber conflicts generates several «grey zones» in the international law, in particular with respect to thresholds of sovereignty, criteria of attribution, and the legal status of digital evidence, which is often held by private-sector entities. The dissertation substantiates the need to

harmonise doctrinal approaches to the qualification of cyberattacks and to develop mechanisms of public–private interaction capable of balancing state authority with the technological resources of non-state actors.

The evolution of Russian cyber aggression against Ukraine (2014–2024) has been elucidated as comprising three phases characterised by distinct technological, organisational, and legal features – from attacks on the energy infrastructure (BlackEnergy, Industroyer) to multi-vector operations during the full-scale war (NotPetya, wiper, DDoS, and attacks on satellite networks**). It has been demonstrated that these actions share the hallmarks of state origin, a high degree of coordination, and a strategic intent to undermine the resilience of critical infrastructure, the legitimacy of state institutions, and public communications. The key cases have been given legal qualification through the prism of the principles of sovereignty, non-intervention, due diligence, and the provisions of international humanitarian law concerning the protection of civilian objects.

The structural vulnerabilities of national cyber resilience have been systematised across three dimensions – institutional, technical, and socio-communicative – and, based on empirical data, an analytical matrix “vulnerability – manifestations – directions for improvement” has been developed. It has been established that institutional weaknesses stem from fragmentation of competences among cybersecurity actors, the absence of a unified taxonomy of incidents, and the insufficient development of public–private partnerships. The dissertation substantiates the necessity of harmonising national approaches with European standards (in particular, ENISA RICT, NIS2), of establishing mechanisms for rapid information exchange among governmental and departmental CSIRT/SOC units, and of legally formalising standardised Service Level Agreements (SLA) for critical digital services.

The role of socio-communicative factors – the human element, disinformation, and volunteer cyber initiatives – has been emphasised as system-forming components of cyber resilience. It is noted that the absence of unified crisis communication protocols, uneven professional training, and the informal

nature of cooperation with volunteer communities diminish the effectiveness of incident response. It is proposed to formalise cooperation between state and non-state actors within the framework of public–private partnership, as well as to expand training programmes on cyber hygiene and countering social engineering.

Conceptual guidelines have been formulated for Ukraine's transition to a proactive model of cyber defence, founded on standardised procedures for information exchange, harmonised technical requirements, and the development of trust as a strategic resource of digital security. It is demonstrated that strengthening national cyber resilience requires the institutionalisation and normative consolidation of public–private partnership as a key element of state policy in the field of cybersecurity.

It is summarised that cyber aggression against Ukraine is of a systemic, multi-level, and coordinated nature, and that its consequences – in both scale and impact – are comparable to traditional military actions, indicating the transformation of cyberspace into a domain of strategic confrontation. It has been proven that the existing response model remains predominantly reactive, focused on post-factum detection and mitigation, which limits the effectiveness of prevention, attribution, and long-term deterrence of cyber threats. On this basis, the dissertation substantiates the need to transition towards an integrated system of cyber resilience, combining the institutional, technical, and social resources of the state, the private sector, and civil society.

The third chapter examines Euro-Atlantic models of cyber defence and identifies directions for their adaptation to the Ukrainian legal system. This chapter is based on a comprehensive comparative-legal analysis of the European, American, and NATO approaches to constructing the architecture of cyber resilience, encompassing legal, institutional, technical, and partnership mechanisms of cyber risk governance.

The essence of the European model of cyber defence is revealed as a normatively binding ecosystem, grounded in the interaction of directives and regulations – NIS2, CER, DORA, CRA, DSA, the Cyber Solidarity Act, and the

Cybersecurity Act – and coordinated by the European Union Agency for Cybersecurity (ENISA). It is shown that this model has evolved from declaratory provisions towards a «policy–implementation–oversight–response» cycle, within which supranational standardisation is combined with national responsibility for implementation. The practices of EU Member States, notably Germany, France, Sweden, and Estonia, are analysed as examples of the effective integration of legal regulation with operational coordination and the development of CSIRT networks and certification mechanisms.

The distinctive features of the United States model of cyber defence have been identified as resting upon strategic planning, standardisation, administrative regulation, and close cooperation between the state and the private sector. The evolution of this model is traced from voluntary mechanisms to a system of normatively defined requirements, consolidated in the National Cybersecurity Strategy (2023), its Implementation Plan (2023–2024), relevant Executive Orders (EO 14028, CIRCIA), and the NIST Cybersecurity Framework 2.0 and NICE Framework. Emphasis is placed on the pragmatic orientation, flexibility, and high adaptability of this model, which ensures a balanced interaction among governmental, corporate, and societal actors in sustaining cyber resilience.

The NATO cyber defence policy is examined, within which cyberspace has been formally recognised as a domain of collective defence. The key policy documents and decisions of the Alliance have been analysed – those which establish the principles of mutual assistance, resilience, and partnership, as well as the role of the Cooperative Cyber Defence Centre of Excellence (CCDCOE, Tallinn) as a leading analytical and training institution. It is shown that NATO’s policy is primarily coordinative in nature, aimed at fostering interoperability standards, information exchange, and enhancing the preparedness of allies to confront cyber threats, while preserving each member state’s autonomous responsibility for its own cyber defence.

Against the background of these models, the process of Ukraine’s integration into the international security space of the EU and NATO has been

analysed. The research establishes a gradual harmonisation of the national regulatory and legal framework with European law (notably NIS2, CER, DORA, CRA, Cybersecurity Act) and a strengthening of inter-agency coordination among the National Security and Defence Council (NSDC), the National Cybersecurity Coordination Centre (NCCC), the State Service of Special Communications and Information Protection (SSSCIP), and CERT-UA. The diplomatic dimension of this integration has also been outlined, including Ukraine's participation in the EU–Ukraine Cyber Dialogue, cooperation with ENISA, involvement in the Tallinn Mechanism initiative, and preparation for accession to the EU Cybersecurity Reserve, all of which enhance institutional interoperability and reinforce international trust in Ukraine's cyber governance system.

A separate subsection is devoted to the analysis of public–private partnership (PPP) in the field of cybersecurity as a key instrument of collective resilience. The dissertation summarises the experience of the United States, including the JCDC, ISACs, and ISAOs models, supported by EO 14028, CIRCIA, and the NIST CSF 2.0 standards, and that of the European Union, represented by the CSIRTs Network, Directives NIS2, CER, DORA, CRA, the Cyber Solidarity Act, and the coordinating role of ENISA. National practices in Germany, the United Kingdom, and Estonia are highlighted as exemplifying the integration of legal safeguards, technical standards, and open protocols of cooperation, ensuring the resilience and accountability of public–private collaboration in cybersecurity governance.

It has been generalised that the Euro-Atlantic model of public–private partnership (PPP) in cybersecurity is characterised by normative maturity, institutional stability, and a high level of mutual trust, being grounded in the principles of legal certainty, shared responsibility, and technological transparency.

On this basis, the thesis formulates directions for the adaptation of Euro-Atlantic approaches to the Ukrainian context:

– Codification dimension – the refinement and adoption of a dedicated Law «On Public–Private Interaction in the Field of Cybersecurity» (draft law No. 14150), which defines the status, rights, duties, and liability of the participants;

– Harmonisation dimension – alignment of the draft law with the provisions of NIS2, CER, DORA, and CRA, including the introduction of incident-reporting procedures, data-handling protocols, and joint response teams;

– Institutional dimension – establishment of a single national coordinator (Single Point of Contact), creation of sectoral ISAC platforms, advisory councils, and a public monitoring system;

– Conceptual–principled dimension – incorporation into national cyber policy of the Euro-Atlantic principles of «shared responsibility» and «security by design» as the foundation of trust, security, and sustainable digital development.

It is further concluded that the Euro-Atlantic model of cyber defence integrates regulatory clarity, technological innovation, and advanced cross-sectoral cooperation, forming a polycentric yet coherent system of collective cyber resilience. Ukraine is gradually integrating into this architecture by developing its own model of public–private partnership, aligned with European standards of risk management, trust, and strategic cooperation in the sphere of digital security.

Keywords: national security; information security; digital security; cybersecurity; cyber resilience; cyber aggression; hybrid warfare; critical infrastructure; cyber risk management; sovereignty in cyberspace; attribution of cyber attacks; state cyber defense policy; artificial intelligence; digital threats; digital innovations and technologies; information technologies; legal regulation; legal protection.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Колесник О.О. Теоретико-правові засади формування та еволюції поняття кібербезпеки. Юридичний науковий електронний журнал. 2024. № 7. С. 636–641. DOI: https://doi.org/10.32782/2524-0374/2024-7/154

2. Колесник О.О. Нормативно-інституційні засади формування національної системи кібербезпеки України. *Право та державне управління*. 2025. № 1. С. 437–445. DOI: https://doi.org/10.32782/pdu.2025.1.61

3. Колесник О.О. Міжнародні стандарти та українська практика кіберзахисту: уроки війни. *Правові новели*. 2025. № 25. С. 375–382. DOI: https://doi.org/10.32782/ln.2025.25.48

4. Сорока Л.В., ***Колесник О.О.*** Міжнародно-правові принципи регулювання кіберпростору: суверенітет, невтручання та Due Diligence. *Держава та регіони*. Серія: Право. 2025. № 1. С. 246–253. DOI: https://doi.org/10.32782/1813-338X-2025.1.35

які засвідчують апробацію матеріалів дисертації:

5. Колесник О.О. Принципи міжнародного права в системі глобальної кібербезпеки. *Проблемні питання юридичної науки в контексті реформування правової системи України:* матеріали міжнародної науково-практичної конференції (Київ, 19–20 жовт. 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 121–123.

6. Колесник О.О. Формування поняття «кібербезпека» в сучасній правовій науці: теоретичні орієнтири та методологічні виклики. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність:* матеріали міжнародної науково-практичної конференції (Київ, 4–5 черв. 2024 р.). Київ: Науково-дослідний інститут публічного права, 2024. С. 98–100.

7. Колесник О.О. Кібербезпека як елемент національної безпеки України в умовах війни. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі:* матеріали міжнародної науково-практичної конференції

(Київ, 18–19 лют. 2025 р.). Київ: Науково-дослідний інститут публічного права, 2025. С. 71–73.

8. Колесник О.О. Сучасний стан і тенденції розвитку правового регулювання національної системи кібербезпеки України. *Актуальні питання науки і практики та шляхи їх вирішення:* матеріали другої міжнародної науково-практичної конференції (Київ, 4–5 черв. 2025 р.). Київ: Науково-дослідний інститут публічного права, 2025. С. 140–143.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Повномасштабна збройна агресія Російської Федерації проти України та перехід гібридного протиборства у затяжну фазу істотно трансформували архітектоніку національної безпеки, актуалізувавши проблему забезпечення кібербезпеки держави. У сучасних умовах кіберпростір набув статусу самостійного виміру стратегічного протиборства, у межах якого кібератаки за масштабом, інтенсивністю та наслідками співвідносяться з традиційними формами воєнних дій. Відтак кібербезпека набула значення ключового системоутворювального компонента національної безпеки, що забезпечує стабільне функціонування державних інститутів, безперервність роботи критичної інфраструктури, захист інформаційних ресурсів і підтримання суспільної довіри до публічної влади.

Разом із тим, за зовнішньою адаптивністю національної системи кібербезпеки простежуються глибинні інституційні та нормативно-правові вразливості, що знижують рівень її цілісності та ефективності. Вони проявляються у фрагментарності правового регулювання, розпорошеності повноважень між суб’єктами сектору безпеки й оборони, відсутності єдиного координуючого центру, а також у дефінітивній невизначеності ключових понять – «кібербезпека», «кіберзахист», «кіберстійкість». Наявність таких диспропорцій унеможливлює формування узгодженої системи державного управління у сфері кібербезпеки, знижує рівень правової визначеності та перешкоджає створенню сталої моделі колективної кіберстійкості, побудованої на принципах підзвітності, спільної відповідальності та технологічної прозорості.

Особливої уваги потребує нормативне закріплення механізмів державно-приватної взаємодії, які у провідних державах світу становлять основу ефективного кіберзахисту. Недостатня правова деталізація таких механізмів в Україні ускладнює координацію дій між державними та

недержавними суб’єктами, створює прогалини у розмежуванні повноважень і відповідальності, а також гальмує процес інституціоналізації партнерських форматів типу ISAC/CSIRT. Це, у свою чергу, негативно позначається на своєчасності виявлення та атрибуції кібератак, обмежує можливості доказування у справах, пов’язаних із кіберзлочинами, і створює ризики порушення принципу належної обачності (due diligence) у транскордонних інцидентах.

Не менш важливим викликом залишається необхідність забезпечення належного балансу між безпековими інтересами держави та дотриманням прав і свобод людини у цифровому середовищі. Цей баланс визначає легітимність державної кіберполітики та її відповідність міжнародно-правовим стандартам, що формують основу поліцентричного режиму глобальної кібербезпеки, у межах якого Україна виступає не лише об’єктом, а й активним суб’єктом нормотворення, партнерства та колективного реагування.

Геополітичний курс України на інтеграцію до Європейського Союзу та Північноатлантичного альянсу зумовлює необхідність глибокої гармонізації національної системи кібербезпеки з acquis ЄС і нормативно-організаційними стандартами євроатлантичної спільноти. У цьому контексті особливої актуальності набуває узгодження правової, інституційної та технічної бази з положеннями директив і регламентів NIS2, DORA, CRA, а також впровадження принципів ризик-орієнтованого управління, інцидент-репортингу, сертифікації та спільних процедур реагування. Водночас відсутність єдиного координаційного центру та чітко визначених механізмів державно-приватного партнерства обмежує ефективність реагування на кіберзагрози, знижує потенціал превенції та ускладнює формування довгострокової, інституційно узгодженої системи кіберстійкості.

Зазначені обставини обумовлюють потребу у комплексному науковому осмисленні кібербезпеки як системоутворювального елемента національної безпеки України, що інтегрує правові, інституційні, технологічні та

управлінські виміри. Особливої наукової ваги набуває розроблення концептуально-правових засад функціонування національної системи кіберзахисту, ідентифікація її інституційних вразливостей, адаптація євроатлантичних моделей до українського контексту, а також формування правових механізмів державно-приватної взаємодії у сфері кібербезпеки.

Таким чином, обрана тема дисертаційного дослідження має подвійний вимір значущості: теоретичний – як внесок у розвиток національної доктрини кіберправа та формування методологічної бази публічно-правового регулювання цифрової безпеки; та практичний – як інструмент удосконалення державної політики у сфері кіберзахисту, підвищення кіберстійкості критичної інфраструктури й забезпечення реалізації національних інтересів України в умовах гібридної війни та глобальної цифрової взаємозалежності.

Зв'язок теми дисертації із сучасними дослідженнями. Питання кібербезпеки у структурі національної безпеки України поступово набувають системного наукового висвітлення, однак потребують подальшого міждисциплінарного узагальнення. У межах вітчизняної правової науки вони розглядаються переважно у зв'язку з інформаційною безпекою, цифровим врядуванням чи протидією кіберзлочинності, що зумовлює потребу в комплексному підході до правового, інституційного та міжнародного виміру кібербезпеки.

Серед вітчизняних дослідників понятійно-категоріальні, теоретико-правові та організаційні засади забезпечення кібербезпеки розкрито у працях О. Баранова, І. Діордіци, В. Ліпкана, А. Тарасюка, Л. Веселової, С. Мельника, Є. Кубанова, Г. Гончаренка, Л. Арсенович, С. Горліченка, В. Фурашева, В. Бурячка та інших учених. Важливе методологічне підґрунтя для осмислення кібербезпеки як складного соціотехнічного явища, що поєднує правові, управлінські та технологічні компоненти, формують також монографічні дослідження О. Логінової, І. Кравчука, В. Котуха, В. Веселової.

Істотний внесок у дослідження міжнародно-правових аспектів кіберпростору зробили М. Камчатний, Б. Кормич, О. Довгань, А. Тарасюк, які аналізували застосовність принципів суверенітету, невтручання та належної обачності (due diligence) до кібероперацій. Зарубіжна доктрина представлена працями M. N. Schmitt, R. Buchan, N. Tsagourias, K. Mačák, M. Finnemore, D. Hollis, O. Hathaway, R. Hurwitz, R. Egloff, J. Kosseff, що заклали основи сучасного тлумачення міжнародного права у сфері кібербезпеки.

Окремі дослідження присвячені адміністративно-правовим і організаційним аспектам державної політики у сфері кібербезпеки. У цьому напрямі працювали В. Бурячок, Н. Ткачук, М. Гаврильців, Д. Гнатченко, М. Сироватченко, О. Крет, А. Лисеюк, С. Вдовенко, І. Логінова, О. Марущак. До цього ж напряму належать роботи К. Куркової, яка аналізує вплив інформаційних технологій, публічно-інформаційної політики та умов воєнного стану на стан національної безпеки й трансформацію системи публічного адміністрування.

Вітчизняний науковий дискурс активно залучає дослідження зарубіжних моделей державно-приватної взаємодії у сфері кіберзахисту. Значний доробок у цьому напрямі належить Д. Дубову, С. Гнатюку, Ю. Заскокі, С. Петрову, Б. Панасюку, О. Дідичу, В. Григоренку. До авторів, які аналізують окремі аспекти партнерства держави та бізнесу, цифрового врядування та адміністративно-правових механізмів у цифровому середовищі, належать також Л. Сорока, І. Костенко, В. Оксінь, Д. Левченко та А. Даниленко. Узагальнений аналіз зазначених підходів подано в аналітичній доповіді НІСД «Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України» (2018), а також у парламентських дослідженнях 2025 року, що розкривають нові форми й інструменти взаємодії держави та приватного сектору в умовах цифрової трансформації та збройної агресії.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження узгоджується з основними державними та

міждержавними програмами України у сфері національної безпеки, кіберзахисту й цифрового розвитку, а також із ключовими стратегічними документами, що визначають напрями реалізації євроінтеграційної політики держави.

Робота співвідноситься з положеннями Угоди про асоціацію між Україною та Європейським Союзом, ратифікованої Законом України від 16 вересня 2014 року № 1678-VII, і Планом заходів з її виконання, затвердженим постановою Кабінету Міністрів України від 25 жовтня 2017 року № 1106. Тематика дослідження пов’язана з виконанням Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392/2020, та Стратегії кібербезпеки України, схваленої рішенням Ради національної безпеки і оборони України від 14 травня 2021 року і введеної в дію Указом Президента України від 26 серпня 2021 року № 447/2021. Розроблення теми здійснюється у руслі завдань, визначених Планом реалізації Стратегії кібербезпеки України (Указ Президента України від 1 лютого 2022 р. № 37/2022) та Планом заходів на 2025 рік з її виконання (розпорядження Кабінету Міністрів України від 7 березня 2025 р. № 204-р).

Дослідження враховує положення попередніх стратегічних актів – Стратегії кібербезпеки України 2016 р. (Указ Президента України від 15 березня 2016 р. № 96/2016) і рішення Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (Указ Президента України від 13 лютого 2017 року № 32/2017), які визначили базові підходи до формування системи державного реагування на кіберінциденти.

Окреме значення для теми має Концепція розвитку сектору безпеки і оборони України (Указ Президента України від 14 березня 2016 року № 92/2016), що передбачає інтеграцію кіберкомпонента у загальну систему національної безпеки, а також Концепція створення державної системи захисту критичної інфраструктури (розпорядження Кабінету Міністрів

України від 6 грудня 2017 року № 1009-р), у якій закладено інституційні основи захисту критичних об’єктів у цифровому середовищі.

Дослідження узгоджується з положеннями Стратегії розвитку сфери електронних комунікацій України на період до 2030 року (розпорядження Кабінету Міністрів України від 4 червня 2025 р. № 546-р), яка визначає цілі формування безпечного цифрового простору та впровадження сучасних механізмів кіберзахисту, а також зі Стратегією боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16 вересня 2020 року № 1126-р), що включає заходи з протидії кіберзлочинності.

Таким чином, тематика дисертаційного дослідження органічно вписується у стратегічні пріоритети державної політики України, спрямовані на зміцнення національної безпеки, розвиток цифрової інфраструктури, підвищення кіберстійкості та виконання євроінтеграційних зобов’язань у сфері кібербезпеки.

Дисертацію підготовлено у межах та на виконання плану науково-дослідних робіт Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб’єктів публічно-правових відносин» (номер державної реєстрації 0120U105390). Тему дисертації затверджено рішенням Вченої ради Науково-дослідного інституту публічного права від 21 листопада 2022 року (протокол № 15).

Мета і завдання дослідження. *Мета* роботи полягає у всебічному теоретико-правовому аналізі системи кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки, визначенні закономірностей її розвитку в умовах гібридної агресії проти України, виявленні ключових інституційно-правових вразливостей і напрямів підвищення кіберстійкості держави, а також у розробленні науково обґрунтованих пропозицій щодо вдосконалення національної моделі правового регулювання та інституційного забезпечення кіберзахисту з урахуванням євроатлантичних підходів.

Для досягнення поставленої мети в дисертації потрібно виконати такі *завдання*:

– розкрити теоретико-правові засади сутності кібербезпеки, з’ясувати її міждисциплінарну природу та співвідношення з суміжними категоріями – інформаційна безпека, кіберзахист, кіберстійкість;

– дослідити міжнародно-правові основи забезпечення кіберзахисту, виявити роль і вплив універсальних та регіональних актів (ООН, ОБСЄ, Ради Європи, ЄС) у формуванні глобальної системи норм та принципів;

– розкрити структуру національної системи кібербезпеки України, її законодавчі засади, інституційну архітектуру, повноваження суб’єктів і механізми взаємодії державного та приватного секторів;

– розкрити еволюцію форм та правову природу кібероперацій як інструмента сучасних воєн і конфліктів, зокрема в контексті російської гібридної агресії.

– провести аналіз основних кібератак проти України у 2014–2024 роках, визначити їхні цілі, масштаби, наслідки та отримані уроки для формування оновленої державної політики безпеки;

– визначити основні інституційно-правові вразливості критичної інфраструктури в умовах воєнного стану у правовому, інституційному та процедурному вимірах, запропонувати напрями їх мінімізації;

– визначити сучасні проблеми протидії кіберзлочинності та кіберагресії, зокрема ефективність нормативно-правових і оперативно-технічних механізмів реагування;

– здійснити порівняльно-правовий аналіз стратегій кіберзахисту США, НАТО та ЄС, визначити їх нормативні, організаційні та технологічні моделі;

– дослідити механізми інтеграції України у міжнародно-правову систему кібербезпеки, зокрема у форматах ЄС, НАТО та Ради Європи, та визначити шляхи гармонізації законодавства України;

– обґрунтувати можливості застосування євроатлантичних практик державно-приватного партнерства як інструменту підвищення кіберстійкості України, сформулювати пропозиції щодо удосконалення правових засад і процедур такої взаємодії.

Об'єктом дослідження є суспільні відносини, що виникають у процесі забезпечення кібербезпеки держави, суспільства та особи в умовах цифрової трансформації та гібридної агресії.

Предмет дослідження – кібербезпека як елемент системи національної безпеки України з урахуванням правових викликів гібридної війни та міжнародного досвіду.

Методи дослідження. Під час виконання цього дослідження застосовано комплекс загальнонаукових і спеціально-юридичних методів, кожен із яких мав визначальне значення для досягнення поставленої мети, розв'язання дослідницьких завдань і формування науково обґрунтованих висновків. Зокрема, *діалектичний* метод сприяв розкриттю сутності кібербезпеки як динамічного соціотехнічного явища, що формується на перетині правових, технологічних та політичних чинників, і дав змогу виявити внутрішні суперечності її розвитку в умовах гібридної агресії проти України (підрозділ 1.1). Методи *аналізу та синтезу* використано для виокремлення структурних елементів системи кібербезпеки, зокрема її нормативної, інституційної, технологічної та організаційної складових, а також для інтеграції їх у цілісну модель забезпечення національної кіберстійкості (підрозділи 1.2, 1.3). Застосування *формально-юридичного* методу дало змогу здійснити системний аналіз законодавчої бази України у сфері кібербезпеки, включно із законами «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України» та іншими актами, а також оцінити узгодженість національних норм із міжнародно-правовими стандартами поведінки держав у кіберпросторі (розділи 1–2). На основі *системно-структурного* методу визначено інституційну архітектуру кіберзахисту, ідентифіковано суб'єктів публічного управління у сфері

кібербезпеки, розкрито взаємозв'язки між ними та механізми реалізації їхніх повноважень (підрозділи 2.1, 2.2). Використання *порівняльно-правового* методу забезпечило можливість дослідити євроатлантичну нормативну екосистему кіберзахисту, виокремити її ключові риси та визначити напрями адаптації цих підходів до українського контексту (розділ 3). За допомогою *функціонального* методу проаналізовано механізми реалізації державної політики у сфері кібербезпеки, процедури реагування на кіберінциденти та взаємодію суб'єктів сектору безпеки й оборони в умовах гібридних загроз (підрозділи 2.3, 2.4). Використання *логіко-семантичного* методу дозволило уточнити понятійно-категоріальний апарат дослідження, розмежувавши такі поняття, як «інформаційна безпека», «кібербезпека», «кіберзахист», «кіберстійкість», «кібератака», «кіберзагроза», що забезпечило термінологічну чіткість і внутрішню послідовність роботи (підрозділ 1.1). Застосування *історико-правового* методу дало можливість простежити еволюцію становлення національної системи кібербезпеки, виокремити етапи її інституційного оформлення та виявити зовнішньополітичні й технологічні чинники, що вплинули на її розвиток (підрозділ 1.2). На основі методу *правового прогнозування* сформульовано пропозиції щодо вдосконалення національної моделі правового регулювання кібербезпеки, розбудови системи державно-приватної взаємодії та підвищення кіберстійкості критичної інфраструктури (розділ 3). Водночас методи *систематизації, індукції, дедукції, теоретичного узагальнення* та *аксіоматичний* метод використовувалися на всіх етапах дослідження для побудови логічно цілісної концепції кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки, а також для формулювання авторських положень і висновків.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших комплексних досліджень, присвячених системному теоретико-правовому аналізу феномену кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки

України. У роботі розкрито міждисциплінарну природу кібербезпеки, обґрунтовано її концептуальні засади, механізми правового регулювання та напрями гармонізації з євроатлантичними стандартами. За результатами дослідження сформульовано низку нових наукових положень, висновків і пропозицій, запропонованих особисто здобувачем. Основні з них такі:

вперше:

– сформульовано авторське інтегральне визначення поняття «кібербезпека» як стану й безперервного процесу забезпечення стійкого, правомірного та етично врегульованого функціонування цифрового середовища. Його досягнення забезпечується узгодженою взаємодією технологічних засобів, управлінських процедур, правових механізмів і поведінкових норм, спрямованих на захист даних, цифрових сервісів, інфраструктур, соціальних відносин та публічних функцій держави з гарантією їх відновлюваності у разі порушень. Запропоноване визначення інтегрує технічний, управлінський, правовий та етичний виміри у єдину комплексну модель кіберстійкості, що виходить за межі вузько технократичного трактування безпеки;

– розроблено інтегровану методологічну модель кібербезпеки, яка поєднує ієрархічну структуру референтних об’єктів захисту (дані – сервіси – інфраструктури – соціальні відносини – публічні функції держави) та аналітичну типологію кіберагресії за моделлю «цілі – інструменти – очікувані ефекти». У сукупності ці складники формують єдину систему оцінювання взаємозв’язку між об’єктами кіберзахисту, характером кібервпливів та відповідними правовими режимами реагування, забезпечуючи методологічну цілісність аналізу кібероперацій;

– запропоновано системну модель адаптації євроатлантичних підходів до української правової системи у сфері кібербезпеки, вибудувану за чотирма взаємопов’язаними напрямами – кодифікаційним, гармонізаційним, інституційним і концептуально-принциповим. Модель визначає послідовність правових, організаційних та методологічних кроків для

імплементації європейських стандартів управління кіберризиками та забезпечує узгодженість національної системи кібербезпеки з євроатлантичними принципами спільної відповідальності, прозорості та стійкості.

удосконалено:

– теоретико-методичний апарат осмислення феномену кібербезпеки шляхом систематизації типології наукових підходів – технократичних, організаційно-управлінських, правових, соціогуманітарних та освітньо-термінологічних – і обґрунтування необхідності їх інтеграції у межах системного підходу. Такий підхід дозволив розглядати кібербезпеку не як сукупність ізольованих напрямів, а як цілісний процес управління ризиками, довірою та стійкістю у цифровому просторі, що забезпечує комплексність і міждисциплінарність її наукового пізнання;

– концептуалізацію парадигми кіберстійкості як динамічного циклу передбачення, реагування, відновлення та навчання системи, у якому визначено ключову роль людського фактора й етики інформації як внутрішнього регулятора цифрової поведінки. Етика інформації трактується як фундаментальний елемент культури довіри, прозорості та підзвітності у цифровому середовищі, що забезпечує узгодженість між технологічними, правовими та соціальними аспектами функціонування системи кібербезпеки;

– підхід до правової кваліфікації кібероперацій у контексті міжнародного гуманітарного та звичаєвого права. На основі аналізу реальних кейсів кіберагресії проти України обґрунтовано застосовність принципів суверенітету, невтручання, належної обачності (due diligence) до цифрового середовища, що дозволило конкретизувати межі відповідальності держав за шкідливу діяльність у кіберпросторі. Уточнено критерії порогу «застосування сили», розмежування між воєнними та невоєнними кібердіями, а також визначено роль публічної атрибуції як ефективного інструмента формування практики державної відповідальності у сфері міжнародного кіберправа;

– методологію аналізу національної кіберстійкості шляхом розроблення аналітичної матриці «вразливість – прояви – напрями вдосконалення», яка відображає взаємозалежність інституційних, технічних і соціально-комунікаційних чинників безпеки. Така матриця поглиблює ризик-орієнтований підхід до управління кіберзагрозами, забезпечує системну ідентифікацію критичних вразливостей і дозволяє пріоритизувати напрями реформ, підвищуючи ефективність аудитів та стратегічного планування у сфері кіберстійкості;

– методологію порівняльно-правового аналізу євроатлантичних моделей державно-приватного партнерства у сфері кібербезпеки, у межах якої систематизовано ключові принципи (довіра, прозорість, розподіл відповідальності, обмін у реальному часі) та інституційні механізми (CSIRTs Network, ISACs, публічно-приватні платформи). Удосконалено підхід до визначення ролі держави як фасилітатора партнерства, що забезпечує баланс між регуляцією, саморегулюванням і технологічною автономією приватного сектору.

отримали подальший розвиток:

– наукове розуміння феномену кіберагресії як складової гібридної війни, у межах якої кібероперації розглядаються не як ізольовані технічні дії, а як інтегрований компонент воєнних, інформаційно-психологічних та логістичних кампаній. На основі проведеної періодизації кіберагресії РФ проти України (2014–2024 рр.) обґрунтовано її системний, багаторівневий і скоординований характер, що свідчить про трансформацію кіберпростору у повноцінну сферу стратегічного протиборства та формує методологічну основу для подальшого удосконалення міжнародно-правових і національних механізмів реагування;

– комплексне розуміння про чинники уразливості національної критичної інфраструктури, систематизовані у трьох взаємопов’язаних вимірах –інституційному, технічному та соціально-комунікаційному. На цій основі сформульовано концептуальні орієнтири переходу від реактивної до

проактивної моделі кіберзахисту, заснованої на стандартизованому обміні інформацією, взаємній довірі між секторами та інтегрованих механізмах моніторингу, превенції й реагування на кіберзагрози;

– концептуальні засади еволюції української моделі кібербезпеки у напрямі європейського типу врядування, у межах яких деталізовано потребу завершення розмежування повноважень між органами влади, інституціоналізації державно-приватного партнерства, розвитку кадрового потенціалу та забезпечення інтеграції у європейські механізми кризового реагування та кіберстійкості.

Особистий внесок здобувача. Наукові положення та узагальнення, які не мають посилання на джерела інформації розроблено автором особисто. Усі положення наукової новизни та висновки дисертаційного дослідження сформовані автором самостійно. У співавторстві з Сорокою Л. підготовлено статтю «Міжнародно-правові принципи регулювання кіберпростору: суверенітет, невтручання та Due Diligence», в якій автором здійснено системне порівняння підходів до поняття суверенітету в кіберпросторі, а також сформовано загальні висновки. Усі інші публікації є результатом самостійної роботи автора.

Практичне значення отриманих результатів полягає в тому, що сформульовані та обґрунтовані в дисертаційному дослідженні висновки, наукові положення й конкретні пропозиції мають прикладне значення для вдосконалення системи правового, організаційного та інституційного забезпечення кібербезпеки України, а також для гармонізації національної політики з євроатлантичними стандартами. Результати дослідження вже використовуються та можуть бути використані у:

– *науково-дослідній сфері* – як теоретико-методологічна основа для подальших досліджень питань правового регулювання цифрової безпеки, міжнародного кіберправа та публічного управління у сфері кіберзахисту (акт впровадження Науково-дослідного інституту публічного права);

– *правотворчій діяльності* – під час доопрацювання законопроєкту №14150 «Про державно-приватну взаємодію у сфері кібербезпеки», підготовки змін до законів України «Про основні засади забезпечення кібербезпеки України» та «Про критичну інфраструктуру», а також у процесі розроблення підзаконних актів щодо координації дій суб'єктів кіберзахисту;

– *правозастосовній діяльності* – для підвищення ефективності управління кіберризиками, розвитку публічно-приватного партнерства, створення механізмів обміну інформацією між державними та приватними структурами, а також оптимізації процедур реагування на кіберінциденти;

– *освітньому процесі* – під час викладання навчальних дисциплін «Інформаційні технології у науково-правових дослідженнях», «Проблеми публічно-правового регулювання системи правоохоронних органів в Україні» (акт впровадження Науково-дослідного інституту публічного права), а також при підготовці навчально-методичних матеріалів для програм підвищення кваліфікації державних службовців і фахівців з цифрової та національної безпеки.

Апробація матеріалів дисертації. Основні положення, результати та висновки дисертаційного дослідження були апробовані на науково-практичних конференціях: «Проблемні питання юридичної науки в контексті реформування правової системи України» (м. Київ, 19–20 жовтня 2022 р.), «Актуальні проблеми імплементації наукових досягнень у практичну діяльність» (м. Київ, 4–5 червня 2024 р.), «Перспективні напрямки розвитку юридичної науки у 21-му сторіччі» (м. Київ, 18–19 лютого 2025 р.), «Актуальні питання науки і практики та шляхи їх вирішення» (м. Київ, 4–5 червня 2025 р.).

Публікації. Основні результати дисертації, висновки та пропозиції знайшли своє відображення у восьми наукових публікаціях, з яких три одноосібних статті та одна у співавторстві (з Сорокою Л.) – у наукових виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, чотири – тези доповідей і повідомлень на міжнародних

науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що включають десять підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 312 сторінок. Робота містить список використаних джерел із 355 найменувань на 45 сторінках.

РОЗДІЛ 1
КІБЕРБЕЗПЕКА ЯК СКЛАДОВА СУЧАСНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ БЕЗПЕКИ

1.1. Теоретико-правові засади та еволюція поняття кібербезпеки

Поняття «кібербезпека» є одним із ключових у сучасному науковому та практичному дискурсі, проте його зміст залишається варіативним, контекстно зумовленим і недостатньо уніфікованим. Як зазначають дослідники, теоретико-методологічні підходи до визначення кібербезпеки все ще тяжіють до технократичного бачення, тоді як реальні загрози та виклики мають комплексний характер і охоплюють технічні, організаційні, правові, соціальні та етичні виміри [5; 192; 354; 234].

Відсутність узгодженого визначення ускладнює формування ефективної державної політики у сфері кіберзахисту, створення стандартів освітньої підготовки та забезпечення інтероперабельності суб'єктів національної й міжнародної безпеки [10; 15; 3; 192].

Крім того, термінологічна неоднорідність стає перешкодою для взаємодії в межах багатонаціональних структур безпеки, зокрема в середовищі НАТО [263].

Фрагментарність юридичних підходів до регулювання цифрового середовища зумовлює актуальність формування концепції «права кібербезпеки» як системи взаємопов'язаних правових режимів, що забезпечують захист прав, інтересів і ресурсів у кіберпросторі [269]. На думку Дж. Коссеффа, подальший розвиток цієї галузі потребує переходу від реактивної моделі регулювання, орієнтованої на реагування на інциденти, до системи превентивних правових обов'язків і стандартів належної цифрової поведінки [270].

Огляд наукової літератури з проблематики кібербезпеки охоплює праці з комп'ютерних наук, інженерії, державного управління, права, соціології,

психології, безпекознавства та освіти. Найбільш представлений масив становлять технічні та інженерні дослідження, проте вагоме місце займають також правничі, управлінські й освітні підходи [19; 72; 192; 248; 315; 323; 355].

Українська наукова традиція значну увагу приділяє аналізу терміносистеми та освітнім наслідкам термінологічних розбіжностей [3; 15; 55; 65; 66; 79], а також дослідженню адміністративно-правових механізмів забезпечення кібербезпеки [10; 28 - 35; 44; 76; 153]. Для уточнення семантики базових понять і їх нормативної кореляції використано лексикографічні джерела, що дозволяє порівняти наукові й правові вживання ключових категорій.

Перші спроби осмислення феномену кібербезпеки в українській доктрині здійснювалися крізь призму інформаційної безпеки. Це знайшло відображення у працях, присвячених розмежуванню понять «інформаційний» і «кіберпростір» та відповідних режимів їх захисту [60; 62; 154], з'ясуванню співвідношення категорій «інформаційна» і «кібернетична» безпека [78; 140] та порівняльно-правовому аналізу цих концептів [140]. Лише після 2010 р. термін *«кібербезпека»* виокремлюється як самостійний об'єкт теоретико-правового дослідження, що фіксується у загальнотеоретичних і спеціалізованих публікаціях [5; 61; 137; 143; 154].

У сучасній правовій доктрині дефінітивна проблема та міждисциплінарний характер явища чітко артикульовані у працях [5; 50; 55; 143], де наголошено на необхідності уніфікації юридичної мови та виділено базові атрибути стану захищеності – цілісність, доступність і достовірність (правомірний контроль). Павленко [76] розглядає кібербезпеку як правову гарантію стабільності інформаційного середовища держави, тоді як Веселова [10] визначає її як адміністративно-правовий режим, покликаний забезпечувати баланс інтересів особи, суспільства й держави. У сфері публічного управління акцент робиться на процесуальності, організаційній спроможності та управлінні ризиками [3; 55; 56; 57; 141]. Теоретико-правові

аспекти формулювання і практичної операціоналізації дефініцій уточнено у працях Скрипника та Стеця [137; 143]. Для побудови цілісних державницьких рамок дефініцій важливим є також довідково-понятійний апарат із безпекознавства [19; 60] та міжнародно-політичний вимір дослідження загроз у кіберпросторі [39; 40; 62].

Освітній і термінотворчий вектори послідовно розкривають: категоріально-понятійний апарат і компетентнісний профіль спеціальностей ІБ/КБ [3; 15; 55], етапи формування терміносистеми у вітчизняних університетських дослідженнях [65; 66], динамічну систему термінів як інтеграцію технічних, управлінських і правових компетенцій [79], актуальні вимоги до понятійного апарату підготовки фахівців [55; 66] і практичні аспекти впровадження в освіті [79].

Соціальний та етичний виміри, що коригують надмірну технократичність дискурсу, представлено аналізом людського чинника та поведінкових детермінант у забезпеченні кібербезпеки [192; 248], а також концепцією інформаційної етики як рамки належного врядування даними та цифровими взаємодіями [315]. Додатково, на рівні систем безпеки та оборони, увагу до уніфікації понятійного поля й інституційної чіткості дефініцій фіксує сучасний огляд [355]. У цьому контексті слушним є підхід Hansen і Nissenbaum, які, спираючись на концепцію сек’юритизації Копенгагенської школи, розглядають кібербезпеку як політичний акт перетворення технологічної проблеми на загрозу життєво важливим цінностям, що потребує владного втручання. Такий підхід дає змогу осмислити феномен кібербезпеки не лише як технічний чи правовий, а як соціальний процес формування довіри та відповідальності у цифровому середовищі [246].

У міжнародній науковій доктрині спостерігається така сама варіативність підходів до визначення сутності кібербезпеки. Наприклад, Кеммерер (2003) трактує кібербезпеку переважно як сукупність оборонних методів і процедур, спрямованих на виявлення та нейтралізацію потенційних

вторгнень у комп'ютерні системи [267]. Льюїс (2006) визначає її як захист комп'ютерних мереж і інформації, яку вони містять, від несанкціонованого проникнення, пошкодження чи зловмисних дій [275]. Аморозо (2006) підкреслює, що кібербезпека полягає у зменшенні ризику зловмисних атак на програмне забезпечення, комп'ютери та мережі й охоплює широкий спектр технічних інструментів –від антивірусного захисту до шифрування і контролю доступу [159]. Канонгія та Мандаріно (2014) розглядають кібербезпеку як мистецтво забезпечення життєздатності та безперервності інформаційного суспільства, спрямоване на охорону інформації, ресурсів і критичної інфраструктури держави у кіберпросторі [176].

Своєю чергою, Oxford University Press [303] у словниковій інтерпретації визначає її як стан або процес захищеності електронних даних від несанкціонованого використання чи злочинного втручання [192]. АКрейген, Д.-Т. та Перс [192] у міждисциплінарній рамці визначають кібербезпеку як синтез технічних, організаційних, людських і соціальних факторів, що забезпечують цілісне функціонування цифрового простору.

Поступово в наукових публікаціях відбувається перехід від вузько технічних до міждисциплінарних, соціально орієнтованих підходів. Так, Von Solms & Van Niekerk [354] відмежовують *information security* від *cyber security*, визначаючи останню як комплексну соціотехнічну систему, що поєднує людей, процеси та технології.

Schatz, Bashroush & Wall [315] наголошують на потребі формування «репрезентативного» визначення, яке інтегрує технічні, організаційні та поведінкові чинники.

Kosseff [269] вводить поняття *cybersecurity law* як цілісної системи правових режимів, що регулюють безпеку цифрового середовища, а Kello [266] критикує тенденцію «кібер-легалізму» – редукцію складних цифрових явищ до суто юридичних конструкцій.

Henrico & Putter [248], здійснивши систематичний огляд понад ста наукових робіт, доводять, що більшість наявних дефініцій залишаються дисциплінарно фрагментарними та не охоплюють людський вимір.

Floridi [234] розвиває концепцію «етики інформації» як універсальної рамки відповідальної поведінки у цифровому середовищі, наголошуючи, що моральна регуляція є невід'ємною складовою безпеки.

Tarhan [323] простежує історичну еволюцію досліджень кібербезпеки у контексті безпекових студій, а Tzavara & Vassiliadis [329] фіксують зміщення акцентів від моделі «захисту» до концепції *cyber resilience* – здатності до відновлення, адаптації та навчання після кіберінцидентів.

Schiliro [316] узагальнює сучасні тенденції до розуміння кібербезпеки як соціотехнічної системи, що перебуває у стані постійної динаміки.

Крім того, Janczewski, Pilarski & Marczyk [263] наголошують, що термінологічні розбіжності залишаються суттєвим бар'єром для міжсоюзної інтероперабельності у кібероперація НАТО. Цей висновок також корелює з українським досвідом розбудови уніфікованого понятійного апарату для органів сектору безпеки і оборони [3; 55; 65; 66; 79].

Сукупність проаналізованих джерел демонструє поступову еволюцію від технократичного до соціо-правового та управлінського розуміння кібербезпеки, у якому центральне місце посідає людина як носій компетентностей, цінностей і відповідальності. Узгодження термінів та уніфікація категоріального апарату стають необхідними передумовами для формування цілісної системи політик, освіти й міжнародної взаємодії у сфері кібербезпеки.

Семантика та еволюція пов'язаних понять. Етимологічні та тлумачні джерела фіксують глибинну семантику складників *«кібер-/кібернетичний»* і *«безпека»*, що визначають смислові межі терміна *«кібербезпека»*. Так, у «Великому тлумачному словнику сучасної української мови» за редакцією В. Бусла [9] префікс *«кібер-»* визначається як такий, що позначає належність до сфери кібернетики – науки про керування, зв'язок і

перероблення інформації у складних системах. Тобто первинно компонент *«кібер-»* апелює до процесів управління, контролю та комунікації, закладаючи технічний і системний виміри поняття.

Водночас лексема *«безпека»* у цьому ж джерелі трактується як *«стан, за якого кому-, чому-небудь ніщо не загрожує; захищеність від небезпеки, шкоди, посягання»* [9], що закріплює у слові базову ідею стабільності, убезпечення та збереження функціонування системи в умовах потенційної загрози.

Поняття «кібернетика» у сучасному академічному дискурсі розглядається як наука про загальні закономірності одержання, передавання, зберігання й оброблення інформації, а також управління в технічних, біологічних і соціальних системах, що концептуально відображено у працях В. М. Фурашева [154]. Цей контекст підкреслює універсальний – технічний, біологічний і соціальний – характер «кібернетичного» як системи регуляції, що оперує потоками інформації. У поєднанні з лексемою «безпека» формується змістовне поле «кібербезпеки» як стану упорядкованого, контрольованого функціонування інформаційних процесів, захищених від деструктивних впливів.

Таким чином, лексикографічні джерела засвідчують, що поняття *«кібербезпека»* поєднує у собі ідеї керованості та захищеності, а семантична структура терміна від самого початку передбачає системність, регуляцію й охорону інформаційних процесів.

Українські наукові дослідження послідовно розмежовують поняття «кіберпростір» та «інформаційний простір», а також уточнюють співвідношення між «кібербезпекою» та «інформаційною безпекою». У праці В. М. Фурашева визначено сутність і ключові відмінності цих просторів та відповідних режимів їх захисту [154]; І. М. Сопілко здійснює порівняльно-правовий аналіз категорій інформаційної та кібербезпеки [140]; А. В. Тарасюк конкретизує межі та перетини суміжних понять у правовому полі

[147]; а В. Ю. Лук'янчикова розглядає кіберпростір у міжнародно-політичному вимірі як середовище ризиків і загроз [62].

Важливим методологічним поворотом стало поступове зміщення фокуса від information security до ширшої cyber security як *соціотехнічної надсистеми*, що інтегрує технічні засоби, процеси, людей та інституції. Цю траєкторію концептуально обґрунтовано в працях Von Solms & Van Niekerk [354] та підсилено вимогою до «репрезентативного» визначення, здатного поєднати технічні, організаційні й поведінкові чинники [315].

Типологія наявних підходів до визначення. Аналіз вітчизняних і зарубіжних джерел дає підстави виділити кілька репрезентативних груп підходів до визначення сутності кібербезпеки, що відображають різні етапи еволюції наукової думки – від інженерно-технічних до соціо-правових і етичних. Така типологізація дає змогу простежити, як у процесі розвитку знань поняття «кібербезпека» поступово виходило за межі технічного дискурсу, набуваючи міждисциплінарного змісту.

Технократичні (інженерно-операційні). Ці підходи тяжіють до технічних наук і зосереджуються на питаннях захисту активів, протидії атакам, виявлення інцидентів та забезпечення конфіденційності, цілісності й доступності. Вони охоплюють кібербезпеку як сукупність інструментів, технологій і процедур реагування [159; 192; 260; 267; 315]. В українській науковій традиції цього напряму також дотримується Л. В. Скрипник [137].

Критична оцінка: технократична перспектива забезпечує точність операційних рішень, але обмежена у поясненні соціальних, правових і поведінкових аспектів безпеки.

Організаційно-управлінські. Розглядають кібербезпеку як процес управління ризиками, формування політик і побудови процедур, що інтегрують суб'єктів публічного управління та приватного сектору [55; 151; 76; 30; 29]. Цей підхід переносить акцент із технологій на управлінську спроможність і комунікацію між рівнями системи.

Критична оцінка: управлінський фокус забезпечує сталість процесів, проте схильний редукувати соціальні чинники до інституційних механізмів, залишаючи поза увагою етичні та поведінкові аспекти.

Правові. Описують кібербезпеку через систему норм, інститутів і меж відповідальності. Такі дослідження формують основу для виокремлення права кібербезпеки як комплексної галузі [5; 10; 269]. Lucas Kello (2021) застерігає від небезпеки «кіберлегалізму» – зведення складних соціотехнічних процесів до вузьких юридичних конструкцій, що спотворює сутність феномену [266].

Критична оцінка: правові підходи закріплюють інституційні рамки, проте недостатньо відображають динаміку технологічних і соціальних змін.

Соціогуманітарні та етичні. Фокусуються на поведінкових, ціннісних і моральних чинниках. Floridi (2014) пропонує концепцію етики інформації як підґрунтя для регулювання цифрової взаємодії [234]. Українські автори [147; 3; 15] розглядають людський чинник як системоутворюючий елемент ефективності кіберзахисту.

Критична оцінка: гуманітарна перспектива вносить необхідний баланс у технократичний дискурс, однак іноді страждає від браку операціональності.

Освітньо-термінологічні. Зосереджені на формуванні понятійно-категоріального апарату, стандартизації термінів і розробленні компетентнісних моделей підготовки фахівців [65; 79; 15]. Освітній компонент забезпечує трансфер знань і практик між секторами безпеки.

Критична оцінка: попри важливість, ці підходи часто залишаються прикладними й не формують цілісної теорії кібербезпеки.

Загальний консенсус полягає у визнанні багатовимірності феномену кібербезпеки, тоді як розбіжності спостерігаються:

– у визначенні її ядра (технічна складова чи соціально-інституційна);
– у співвідношенні понять *«кібербезпека»* та *«інформаційна безпека»*;
– у ступені нормативізації термінів у національних правових системах [354; 323; 269].

Для наочності порівняння підходів результати типологізації подано у вигляді систематизованої схеми (табл. 1). У ній відображено основні групи наукових трактувань поняття «кібербезпека», їх ключові характеристики, методологічні акценти та репрезентативних авторів. Такий формат дозволяє зіставити різні наукові школи – від технократичної до соціо-етичної – та простежити еволюцію змісту терміна у міждисциплінарному вимірі.

	Підхід	**Ключові характеристики**	**Репрезентативні автори / джерела**
	Технократичні (інженерно-операційні)	Захист активів і систем, процеси виявлення, протидії, забезпечення конфіденційності, цілісності, доступності (CIA-triad).	Craigen – [192] Schiliro – [316] Скрипник – [137]
	Організаційно-управлінські	Кібербезпека як процес управління ризиками, побудова політик, стратегій і процедур у межах публічного управління або корпоративного менеджменту.	Кубанов – [55] Тарасюк – [151] Павленко – [76] Діордіца – [29]
	Правові	Норми, інститути, компетенції, юридична відповідальність; формування права кібербезпеки; критика «кіберлегалізму».	Баранов – [5] Веселова – [10] Kosseff – [269] Kello – [266]
	Соціогуманітарні та етичні	Людський чинник, інформаційна етика, поведінкові аспекти, цінності цифрового суспільства.	Floridi – [234] Тарасюк –

			[147] Арсенович – [3] Горліченко – [15]
	Освітньо-термінологічні	Формування понятійно-категоріального апарату, стандартизація термінів, компетентнісний підхід до підготовки фахівців.	Мельник – [79] Пашорін – [65] Горліченко – [15]

Таблиця 1. Типологія наявних підходів до визначення поняття «кібербезпека»

Типологічна систематизація засвідчує поступове зміщення акцентів від технічного контролю та реагування до управління ризиками, етики, комунікації й соціальної відповідальності. Це свідчить, що кібербезпека еволюціонує від функціональної моделі «захисту систем» до соціотехнічного процесу підтримання довіри, стійкості та законності у цифровому середовищі. Подальший аналітичний синтез спрямований на виявлення змістових елементів і домінантних тем, які у взаємодії формують цілісну структуру поняття кібербезпеки як системи.

Домінантні теми й відмінні риси сучасного дискурсу кібербезпеки.

Узагальнення вітчизняних і зарубіжних досліджень дає змогу виокремити п’ять домінантних тематичних блоків, що відображають структурну багатовимірність феномену кібербезпеки – за аналогією до міждисциплінарної моделі, запропонованої Craigen, Diakun-Thibault & Purse [192]. Ці блоки характеризують не способи визначення поняття, а складові елементи, через які розкривається його сутність як комплексного соціотехнічного явища.

Систематизація тематичних площин сучасного наукового дискурсу дозволяє розглядати кібербезпеку як багаторівневу систему, у межах якої

технічні, організаційні, правові, соціальні та ціннісно-етичні компоненти функціонують у взаємозалежності та взаємодії.

Для наочності домінантні напрями подано у вигляді типологічної схеми (табл. 2), що узагальнює основні змістові акценти та ключові напрями наукового осмислення феномену кібербезпеки.

	Тематичний блок	**Змістовний акцент**	**Приклади досліджень**
	Технологічні рішення	Технічні інструменти захисту, стандарти, виявлення й запобігання атакам.	Баранов [5] Скрипник [137]
	Події та інциденти	Юридичне осмислення кіберінцидентів як фактів порушення правового режиму.	Павленко [76]
	Процеси й стратегії	Управлінські процеси, ризик-менеджмент, планування та відновлення.	Кубанов [55] Тарасюк [146] Діордіца [29]
	Людський фактор	Роль освіти, компетентностей, культури безпечної поведінки.	Арсенович [3] Горліченко [15]
	Референтні об’єкти	Розширення об’єктів захисту: від даних –до інфраструктури, сервісів, соціальних відносин.	Craigen [192]

Таблиця 2. Домінантні теми та відмінні риси сучасного дискурсу кібербезпеки

Представлена у таблиці 2 типологія тематичних напрямів відображає не лише багатовимірність феномену кібербезпеки, а й те, що різні дослідницькі школи інтерпретують його зміст із різних епістемологічних позицій – від інженерно-технологічних до соціо-етичних. У межах цього підрозділу здійснюється розгорнутий аналіз кожного з виділених блоків з урахуванням їхніх сильних і слабких сторін, а також запропоновано авторське узагальнення, спрямоване на інтеграцію різних підходів у єдину системно-комплексну рамку. Такий підхід дозволяє виявити внутрішні

взаємозалежності між окремими вимірами кібербезпеки та сформувати підґрунтя для власного визначення цього явища як цілісної соціотехнічної системи.

1) Технологічні рішення. У науковій і практичній літературі український дискурс традиційно тяжіє до технократичного підходу, орієнтованого на захист активів, системний моніторинг і реагування на інциденти [159; 192; 260; 267; 315; 137]. Цей напрям справедливо забезпечує високий рівень точності та ефективності операційних рішень і формує основу нормативних стандартів безпеки. Водночас надмірна зосередженість на технологічних аспектах призводить до редукції кібербезпеки до набору контрзаходів і технічних протоколів, залишаючи поза увагою управлінські, інституційні та етичні виміри. Подібну критику технократичності обґрунтовують міждисциплінарні підходи Craigen et al. (2014), які підкреслюють, що без людського, організаційного та соціального компонентів система не може вважатися цілісною [192].

Спираючись на етичну рамку інформаційного гуманізму Floridi (2014) [234] та концепцію кіберстійкості як здатності до адаптації і відновлення [329], у цій роботі запропоновано нову інтерпретацію технологічного виміру кібербезпеки – як підсистеми управління, підпорядкованої цілям стійкості, відповідальності та моральної легітимності дій у цифровому середовищі.

У такій парадигмі технології постають не самодостатнім «центром» системи, а функцією управлінських процесів, правових механізмів і ціннісних орієнтирів, що забезпечують баланс між ефективністю, прозорістю та відповідальністю. Цей підхід дає змогу перейти від технократичної до системно-інтегративної моделі, у якій технологічна безпека стає не лише інструментом захисту, а й складовою управління ризиками та підтримання довіри в цифровому суспільстві.

2) Події та інциденти. У правничій доктрині В.С. Павленка кіберінцидент визначається як юридичний факт, що змінює правовідносини у цифровому середовищі, створюючи підстави для виникнення

відповідальності та державного втручання [76]. Сильним боком цього підходу є нормативна чіткість і визначеність процедур реагування, однак він здебільшого орієнтований на реактивне трактування події – як завершеного порушення, що вимагає санкційного відгуку. Подібна тенденція спостерігається і в міжнародних роботах Kosseff [269] та Kello [266], де фокус зосереджено переважно на правових наслідках, а не на системній динаміці управління ризиками.

Спираючись на концепції Є. В. Кубанова [55] та А. В. Тарасюка [151], у роботі запропоновано подієво-процесуальну модель, у якій інцидент розглядається не лише як факт порушення, а як елемент циклу навчання та адаптації системи. Кожна подія тлумачиться як інформаційний зворотний зв'язок, що дає змогу вдосконалювати політики, підвищувати компетентність суб'єктів і коригувати технічні конфігурації. У такий спосіб інцидент трансформується із «юридичного факту» у механізм самооновлення системи кібербезпеки, який забезпечує її гнучкість, адаптивність і стійкість у динамічному середовищі цифрових загроз.

3) Процеси й стратегії. Ризик-менеджмент і стратегічне планування становлять основу управлінської інституалізації кібербезпеки, визначаючи її як безперервний цикл прогнозування, реагування, відновлення та вдосконалення [151; 55; 76]. Перевагою такого підходу є створення процедурної стабільності та чіткої системи відповідальності, однак надмірна орієнтація на формалізовані процедури іноді призводить до втрати гнучкості й аналітичного виміру ефективності.

З метою подолання цього обмеження у роботі запропоновано операціоналізацію процесів через показники кіберстійкості (resilience metrics), які дають змогу оцінювати не лише факт реагування, а й якість відновлення та здатність системи до навчання після інцидентів. Додатково сформульовано модель зворотного циклу "інцидент → корекція політик і компетентностей → технічна реконфігурація", що забезпечує взаємодію управлінського, технічного та освітнього рівнів. Такий підхід формує

адаптивну систему управління ризиками, узгоджену із сучасною парадигмою кіберстійкості та орієнтовану на безперервне вдосконалення [329].

4) Людський фактор. У більшості попередніх досліджень людина розглядалася переважно як «вразлива ланка» системи, що потребує контролю чи навчання. Однак сучасний український науковий дискурс демонструє еволюцію цього підходу – від реактивної до проактивної позиції, у межах якої людина постає активним суб'єктом кібербезпеки, носієм компетентностей і цінностей [3; 15; 147]. Така інтерпретація узгоджується з позицією Floridi (2014), де моральна поведінка і цифрова відповідальність розглядаються як основа довіри в кіберпросторі [234].

На підставі цих концепцій вводиться поняття "інтегрованого професійно-етичного профілю", який корелює з процесуальними вимогами управління ризиками [151] та правовими механізмами реагування на інциденти [76; 269].

5) Референтні об'єкти. Міжнародний дискурс засвідчує поступове розширення переліку референтних об'єктів кібербезпеки: від захисту даних і інформаційних систем – до критичної інфраструктури, цифрових сервісів, соціальних відносин та державних функцій [354; 316; 323].

В українській науковій традиції цей процес лише набуває системності: Баранов (2014) підкреслює потребу у визначенні ознак захищеності [5], Павленко (2021) – у забезпеченні стабільності інформаційного середовища держави [76], Гончаренко (2024) – у дефініційній точності для сектору безпеки й оборони [18].

Розвиваючи ці положення, у роботі запропоновано ієрархічну модель референтних об'єктів, що відображає послідовність рівнів захисту: *дані - сервіси - інфраструктури - соціальні відносини - публічні функції держави.*

Така модель забезпечує зв'язок між технічними контролями, управлінськими процедурами та нормативно-правовими механізмами. Вона сприяє підвищенню інтероперабельності у багатонаціональних форматах

[263] і створює підґрунтя для нормативного закріплення узгоджених понять у вітчизняному правовому полі [5; 76]. Це дозволяє розглядати систему кібербезпеки не як сукупність розрізнених сфер, а як ієрархічно впорядковану структуру захисту суспільних відносин і державних функцій у цифровому просторі.

Синтез п’яти тематичних блоків засвідчує, що ефективна система кібербезпеки формується не як механічна сума окремих підсистем, а як динамічна архітектура взаємопов’язаних технологічних, організаційних, правових і етичних компонентів, які забезпечують цілісність і стійкість цифрового середовища. Кожен вимір компенсує обмеження інших: технології без процесів і етики не формують довіри; етика без операціоналізації залишається декларативною; а право без інтероперабельності не гарантує ефективної стійкості системи.

У межах цієї логіки концептуальний внесок дослідження полягає у таких положеннях:

зміщення домінанти з реактивної моделі “захисту систем” до парадигми управління стійкістю, реалізованої через подієво-процесуальну петлю, що поєднує реагування, навчання та адаптацію системи [151; 55; 329];

інтеграція етики інформації у практики управління, освіти й професійної діяльності як операційного елементу, а не факультативного доповнення, що забезпечує моральну легітимність рішень у сфері кібербезпеки [234; 147; 15];

формалізація ієрархії референтних об’єктів, яка створює методологічну основу для узгодження політик, компетентностей і технічних заходів на всіх рівнях системи [354; 5; 76; 18];

уніфікація термінологічного поля для підвищення міжвідомчої та міжнародної інтероперабельності, із одночасним збереженням опори на вітчизняну правничу школу [263; 5; 10; 76].

Таке бачення переводить дослідження кібербезпеки у площину системно-інтегративного підходу, у межах якого технології, право,

управління й етика функціонують як взаємодоповнюючі складові єдиної парадигми кіберстійкості.

Саме ця методологічна рамка створює підґрунтя для переходу від описово-класифікаційного рівня аналізу до поняттєво-синтетичного, у межах якого формується інтегральне визначення кібербезпеки як комплексного соціотехнічного феномену.

Авторське визначення поняття кібербезпеки. Здійснений міждисциплінарний аналіз підтвердив, що жоден із наявних підходів – технократичний, управлінський, правовий чи соціоетичний – не забезпечує повного та системного розуміння кібербезпеки як комплексного явища.

Існуючі дефініції, представлені у науковій, правовій та нормативно-стратегічній літературі, демонструють суттєві розбіжності за аналітичною глибиною, методологічними акцентами й об’єктами фокусування.

Так, технічні школи визначають кібербезпеку як систему захисту даних, мереж і програмного забезпечення від зовнішніх втручань, що концентрується на засобах і технологічних контрзаходах [267; 159; 260].

Юридичні підходи підкреслюють регулятивний характер безпеки – як механізму встановлення правових режимів, меж відповідальності та процедур легітимного втручання [269; 266].

Управлінські моделі інтерпретують кібербезпеку через ризик-менеджмент, стратегії, політики та процеси реагування [151; 55; 76], а соціогуманітарні концепції – через призму етики, довіри та відповідальної поведінки у цифровому середовищі [234; 147; 15].

Така система не лише протидіє загрозам, але й створює умови для правомірного, передбачуваного та етично врегульованого розвитку цифрової взаємодії у межах держави й міжнародної спільноти.

Кібербезпека *– це стан і безперервний процес забезпечення стійкого, правомірного та етично врегульованого функціонування цифрового середовища, який досягається через узгоджену взаємодію технологічних засобів, управлінських процедур, правових механізмів і поведінкових норм,*

спрямованих на захист даних, інфраструктур, соціальних відносин і публічних функцій держави від деструктивних впливів і забезпечення їх відновлюваності у разі порушень[1].

Пояснення концептуальних відмінностей та відхід від технократизму. На відміну від класичних міжнародних підходів [267; 159; 260], у яких кібербезпека редукується до технічного захисту мереж, даних та інформаційних систем, запропоноване визначення виходить за межі техноцентризму, інтегруючи організаційні, правові й етичні виміри. Таке бачення ґрунтується на концепції соціотехнічної цілісності [192] та інформаційного гуманізму [234], у межах яких безпека трактується як функція довіри, відповідальності та регулятивної збалансованості між людиною і технологією.

Процесуальність і динамічність. Кібербезпека розглядається не як статичний стан захищеності, а як динамічний процес передбачення, реагування, відновлення та навчання системи. Такий підхід відображає перехід від концепції «захисту систем» до парадигми керування стійкістю, що фокусується на адаптивності, відновлюваності та здатності до самонавчання [329]. У цьому контексті безпека набуває характеру неперервного циклу, у якому кожен інцидент стає джерелом удосконалення політик і практик.

Ієрархія референтних об’єктів. У межах авторського визначення конкретизовано розширене коло об’єктів захисту – дані, сервіси, інфраструктури, соціальні відносини та публічні функції держави. Така ієрархія формує багаторівневу систему пріоритетів, що забезпечує методологічну узгодженість між національними, міжвідомчими та міжнародними рівнями управління безпекою. Вона створює підґрунтя для

---

[1] Запропоноване визначення сформоване на основі узагальнення положень міжнародної (Craigen et al., 2014; Floridi, 2014; Tzavara & Vassiliadis, 2024) та вітчизняної (Баранов, 2014; Павленко, 2021; Веселова, 2019) доктрини.

інтеграції вітчизняної системи кіберзахисту у глобальні стандарти інтероперабельності [263].

Інтеграція етики інформації. Етичні засади, розвинуті у концепції Floridi [234], інтерпретуються не як зовнішнє нормативне обмеження, а як внутрішній регулятивний механізм функціонування цифрового середовища. У такий спосіб етика перетворюється на системоутворюючий чинник кібербезпеки, що забезпечує баланс між технологічною ефективністю, правомірністю дій суб'єктів та моральною відповідальністю у сфері цифрової взаємодії.

Вітчизняна специфіка. Авторське визначення спирається на напрацювання української правничої доктрини [5; 10; 76; 55; 151; 3; 29] та враховує національний контекст становлення системи кібербезпеки як складової державної стійкості. У центрі уваги – необхідність термінологічної уніфікації, міжвідомчої координації та гармонізації національних підходів із міжнародними стандартами, що відповідає стратегічним орієнтирам кіберполітики України [263].

Запропоноване визначення виконує інтегративну та методологічну функцію, поєднуючи технічні, управлінські, правові та соціоетичні аспекти у єдиній системі наукового й практичного осмислення кібербезпеки [192; 234; 329]. Воно може бути використане як теоретичне підґрунтя для:

– формування уніфікованої терміносистеми у науковій, освітній та нормативно-правовій практиці [55; 5; 10];

– розроблення критеріїв і показників кіберстійкості для оцінювання ефективності державних політик і стратегій [329];

– створення комплексних освітніх програм підготовки фахівців, що поєднують технічні, правові, управлінські та етичні компетентності [15; 147; 79];

– удосконалення механізмів інституційної координації між державними, приватними та міжнародними суб'єктами у сфері захисту цифрового простору [151; 76; 263].

У межах запропонованої концепції кібербезпека постає як проактивна, ціннісно збалансована система управління ризиками у цифровому середовищі, у якій технології, право, управління та етика функціонують у взаємозалежній парадигмі стійкості, довіри та відповідальної цифрової взаємодії [192; 234]. Такий підхід забезпечує перехід від фрагментарного до інтегрального розуміння кібербезпеки, що відповідає вимогам сучасної державної політики та міжнародних стандартів у сфері безпеки [263].

1.2. Міжнародно-правові основи забезпечення кіберзахисту

Роль міжнародного права у формуванні сучасної системи кіберзахисту визначається подвійною природою кіберпростору. З одного боку, він охоплює сфери суверенної юрисдикції держав, які здійснюють контроль над власною інформаційно-комунікаційною інфраструктурою. З іншого боку, кіберпростір має глобальний, технічно інтегрований характер, унаслідок чого будь-які транскордонні дії здатні впливати на міжнародну стабільність і безпеку. Така подвійність зумовлює потребу у виробленні нормативних механізмів, що поєднують універсальні принципи міжнародного права із технологічною специфікою цифрового середовища, забезпечуючи водночас узгодженість юрисдикцій та уникнення правових колізій [327; 312; 345].

Сучасна доктрина міжнародного права послідовно підкреслює, що у сфері кібербезпеки не йдеться про створення «нового» права, відірваного від традиційних засад міжнародного правопорядку. Йдеться про уточнення та конкретизацію вже наявних норм – принципів суверенітету, невтручання, заборони сили, належної обачності (due diligence), а також дотримання прав і свобод людини в інформаційному середовищі [247; 312; 250; 327; 345]. Поряд із цим формується корпус норм і практик «відповідальної поведінки держав», покликаний сприяти зміцненню довіри та передбачуваності у взаємодії держав у кіберпросторі [341; 342; 343; 347; 301; 302].

У науковій думці все більшого поширення набуває концепція «режимного комплексу» (regime complex), що розкриває децентралізований характер глобального управління кібербезпекою [299; 307; 308]. Вона виходить із того, що норми й стандарти в цій сфері формуються різними міжнародними інституціями – ООН, ОБСЄ, Радою Європи, Європейським Союзом та іншими організаціями, які діють у взаємопов'язаному, але не ієрархічному порядку [187; 189; 220; 223; 227; 300; 301]. Саме тому для держав, зокрема для України, стратегічного значення набуває послідовна інтеграція національних пріоритетів у систему міжнародних механізмів і документів, а також гармонізація внутрішнього законодавства з усталеними міжнародними стандартами – у питаннях атрибуції кіберінцидентів, боротьби з кіберзлочинністю та забезпечення прав людини у цифровому середовищі [211; 328; 187; 189; 250; 256].

Ключову роль у кодифікації універсальних норм міжнародного права, що застосовуються до кіберпростору, відіграють ініціативи Організації Об'єднаних Націй. У звітах Групи урядових експертів (GGE) 2010, 2013, 2015 та 2021 років, а також у підсумковому звіті Відкритої робочої групи (OEWG) 2019–2021 і в подальших доповідях про прогрес, представлених у 2024 році, послідовно підтверджено чинність загальних норм міжнародного права у цифровій сфері [339; 340; 343; 342; 341; 344; 347; 348]. У цих документах визначено каталог добровільних норм «відповідальної поведінки держав», наголошено на важливості заходів зміцнення довіри (confidence-building measures) та розвитку потенціалу держав у сфері кібербезпеки [341; 342; 343; 347; 301; 302]. Їхня логіка ґрунтується на трьох взаємопов'язаних засадах:

а) визнання застосовності чинних міжнародно-правових принципів до кіберпростору;

б) вироблення «м'яких» стандартів поведінки, що конкретизують зміст правових норм;

в) заохочення прозорості, обміну інформацією та формування каналів комунікації для зниження ризиків ескалації кіберконфліктів [341; 342; 343; 347; 348; 301; 302].

Саме такий багатовекторний підхід – поєднання інструментів «твердого» та «м'якого» права – відповідає динаміці технологічного розвитку і характеру загроз сучасного цифрового середовища [165; 232; 342].

Ідея «відповідальної поведінки держав» у кіберпросторі набуває дедалі більшої ваги як своєрідний міст між традиційною догматикою міжнародного права та практичними потребами безпеки. Вона спирається на основоположні принципи – суверенітет, невтручання, заборону застосування сили, повагу до прав людини, – і водночас трансформується у комплекс очікувань та стандартів, дотримання яких є добровільним, але має значний превентивний ефект. Саме завдяки цим стандартам держави прагнуть зменшити ризики непорозумінь, випадкових ескалацій чи прихованих агресивних дій, що можуть маскуватися під законні кібероперації [165; 232; 233].

У цьому контексті дедалі більшого значення набуває публічна атрибуція кіберінцидентів, яка розглядається як інструмент підтримання міжнародного правопорядку. Обґрунтоване публічне визначення джерела кібератаки може виступати елементом колективного реагування та запобігання новим порушенням, хоча сама процедура атрибуції залишається складним методологічним і політичним викликом [211; 233; 328].

Паралельно з універсальним треком ООН вагому роль у формуванні міжнародного режиму кібербезпеки відіграє Організація з безпеки і співробітництва в Європі (ОБСЄ). У межах цієї організації створено систему заходів зміцнення довіри (Confidence-Building Measures, CBMs) у сфері інформаційно-комунікаційних технологій, головна мета яких полягає у зниженні ризиків конфліктів, підвищенні передбачуваності дій держав і зміцненні взаємної прозорості [301].

Рішення Постійної ради ОБСЄ № 1202 від 10 березня 2016 р. закріпило та розширило існуючий перелік таких заходів, утвердивши механізми

регулярного обміну інформацією щодо національних доктрин, каналів комунікації та процедур реагування на кіберінциденти [302]. Станом на 2023 рік каталог ОБСЄ налічує 16 заходів CBMs, серед яких – створення контактних пунктів, повідомлення про значні інциденти, обмін національними позиціями щодо міжнародного права в кіберпросторі та підготовка кадрів для кризових комунікацій [302].

Для України, яка протистоїть гібридній агресії, цей процедурний інструментарій має особливе значення як механізм міжнародного інформування, пояснення національних правових позицій і запобігання неконтрольованій ескалації в суміжних сферах безпеки [42].

На рівні доктринальних і методичних орієнтирів важливим напрямом розвитку є формування державами власних позицій щодо застосування міжнародного права у кіберпросторі. Протягом останніх років низка держав – Франція (2019), Нідерланди (2019), Німеччина (2021), Канада (2022), Японія (2021), Велика Британія (2022), Італія (2021), Нова Зеландія (2025) – оприлюднили офіційні позиційні документи, у яких конкретизовано бачення застосовності принципів суверенітету, невтручання, належної обачності (due diligence), а також порогів «застосування сили», «збройного нападу», атрибуції та контрзаходів [175; 238; 240; 242; 259; 264; 297; 337]. Такі заяви мають значення opinio juris, тобто формують практику держав, яка поступово кристалізує звичаєві норми міжнародного права. Водночас вони демонструють не лише тенденції зближення позицій провідних країн, а й існування доктринальних розбіжностей щодо обсягу та змісту окремих принципів, зокрема суверенітету та due diligence [278; 327].

Важливим етапом практичної інституціоналізації цих підходів стало оприлюднення Handbook on Developing a National Position on International Law and Cyber Activities [178], який пропонує методику вироблення та публікації національних позицій. У цьому документі надано структуровану рамку для аналізу міжнародно-правових питань кібероперацій, формулювання офіційної правової позиції держави та забезпечення її

узгодженості з практикою партнерів [175; 178; 240–242; 259]. Таким чином, поступове поширення таких орієнтирів сприяє нормативній визначеності, підвищує рівень транспарентності та створює умови для кодифікаційного розвитку міжнародного права у сфері кібербезпеки [179; 287; 301; 302; 317; 318].

Поряд із безпеково-політичним аспектом, у системі міжнародного права важливе місце посідає правозахисний вимір. Резолюція Ради з прав людини ООН 20/8 від 16 липня 2012 р. закріпила принцип рівнозначності захисту прав людини в онлайн- та офлайн-середовищах, наголосивши, що держави зобов'язані дотримуватися критеріїв законності, необхідності та пропорційності втручання навіть під час здійснення заходів кіберзахисту [250]. Для України, яка водночас забезпечує оборону від збройної агресії та утверджує демократичні стандарти управління, баланс між безпекою й свободою вираження поглядів і приватністю є визначальною умовою легітимності державної політики у сфері кібербезпеки та її відповідності міжнародним зобов'язанням [56–58; 146; 355].

В українській правовій доктрині вже накопичено певний досвід синтезу універсальних норм міжнародного права з національними потребами безпеки. Узагальнення нормативних актів і міжнародно-правових рамок, здійснене українськими дослідниками, свідчить про необхідність послідовної імплементації міжнародних стандартів у внутрішнє законодавство, гармонізації термінології та процедур взаємодії з іноземними юрисдикціями у сферах протидії кіберзлочинності, атрибуції кіберінцидентів і надання міжнародної правової допомоги [42; 53; 58; 74; 268; 281; 320].

Розвиток зазначених підходів продовжено у вітчизняних дослідженнях, зокрема в роботі *«Міжнародно-правові принципи регулювання кіберпростору: суверенітет, невтручання та due diligence»*, де уточнено зміст і взаємозв'язок відповідних принципів міжнародного права у цифровому середовищі. У цій публікації обґрунтовано функціональне розуміння суверенітету як поєднання правомочності держави контролювати

власну кіберінфраструктуру з позитивним обов'язком запобігати використанню її території для шкідливих кібероперацій; принцип невтручання проаналізовано крізь призму критерію примусу, а принцип належної обачності (*due diligence*) – як стандарт належної державної поведінки у транскордонному цифровому просторі [142; 271; 272]. Такий підхід відповідає тенденціям розвитку сучасної міжнародно-правової доктрини та практиці провідних держав світу, що підтверджує актуальність досліджуваної проблематики для української правової науки.

З огляду на зазначене, міжнародне право для України постає не лише зовнішнім регулятором діяльності у сфері кібербезпеки, а й внутрішнім джерелом легітимації державної політики у галузі кіберзахисту. Воно забезпечує узгодженість національних рішень із глобальними нормами, підвищує рівень довіри з боку міжнародних партнерів і зміцнює позиції України як суб'єкта сучасного міжнародного правопорядку в цифрову добу [42; 142; 232].

У глобальному вимірі особливого значення набуває інституційна взаємодія та координація між основними міжнародними форумами, що формують норми і стандарти поведінки держав у кіберпросторі. Дискусії щодо співвідношення універсальних і регіональних майданчиків (ООН, ОБСЄ, Рада Європи, Європейський Союз) та різних форм правових документів – від звичаєвих норм і резолюцій до позиційних заяв держав і тлумачних керівництв – засвідчують, що ефективність міжнародно-правового режиму кіберзахисту значною мірою залежить від узгодженості цих компонентів і від здатності держав формувати власні позиції з урахуванням як універсальних принципів, так і регіональних зобов'язань [299; 165; 245].

Аналітична література підкреслює ризики так званої «стратегічної неоднозначності», коли відсутність спільної інтерпретації окремих норм (зокрема щодо порогів «застосування сили» або кваліфікації актів втручання в інформаційні системи) підвищує рівень невизначеності й створює потенційний простір для зловживань [165; 233; 232; 319]. Водночас

оприлюднення державами національних позицій щодо застосовності міжнародного права у кіберпросторі та розвиток заходів зміцнення довіри (CBMs) в межах ОБСЄ істотно знижують транзакційні витрати взаємного тлумачення, підвищують прозорість і сприяють зближенню очікувань щодо правомірної та неправомірної поведінки [301; 302; 175; 238; 240; 242; 264; 337; 297].

Для України наслідки цієї міжнародно-правової еволюції мають безпосередній прикладний характер. По-перше, наявність визнаного корпусу універсальних норм і добровільних стандартів відповідальної поведінки держав підвищує легітимність міжнародної підтримки України у протидії кіберагресії, зокрема у сфері координації публічних заяв, атрибуції та запровадження спільних заходів реагування в межах правових режимів партнерів [187; 189; 220; 207; 227; 229; 230; 231; 257; 258; 300; 186; 191; 190; 222; 333; 335; 342]. По-друге, узгодженість національної практики з рекомендаціями Групи урядових експертів (GGE) та Відкритої робочої групи (OEWG) ООН, а також з мерами довіри ОБСЄ забезпечує кращу інтероперабельність органів сектору безпеки й оборони України з відповідними структурами інших держав – у межах процедур повідомлення, обміну технічною інформацією та реагування на інциденти [342; 347; 348; 302; 301]. По-третє, правозахисний вимір, закріплений у резолюції Ради з прав людини ООН 20/8 (2012), формує внутрішній стандарт для законодавства й практики у сфері кіберзахисту, зокрема щодо балансу між безпекою, свободою вираження та правом на приватність, що має безпосереднє значення для демократичної легітимності державних рішень [250; 146].

Методологічно міжнародне право в кіберпросторі постає як багаторівневий каркас, який поєднує універсальні принципи, норми м’якого права та державні позиції у єдиний, динамічний, проте узгоджуваний режим [232; 246; 323; 329]. Для даного дисертаційного дослідження це означає, що аналіз національної системи кібербезпеки (підрозділ 1.3) має спиратися на

зазначену нормативну рамку як на критерій відповідності – оцінюючи, наскільки національні норми та інституції реалізують міжнародні зобов'язання України, узгоджуються зі стандартами відповідальної поведінки та забезпечують баланс між безпекою і правами людини [45–51; 53; 56–58; 74; 141; 268; 271; 272; 281; 320; 355]. У наступних розділах (2 і 3) ця нормативна основа слугуватиме методологічною матрицею для аналізу практичних викликів гібридної війни та релевантного міжнародного досвіду [299; 165; 232; 342; 344; 347; 348; 301; 302; 42; 146; 148; 142].

Базові принципи міжнародного права, релевантні забезпеченню кіберзахисту. Нормативна архітектоніка кіберзахисту вибудовується через застосування базових принципів і норм міжнародного права до цифрового середовища. Насамперед ідеться про суверенітет, невтручання, заборону застосування сили та пов'язані пороги use of force/armed attack, обов'язок належної обачності (due diligence), а також права людини в Інтернеті. Їхній зміст конкретизується в доктринальних працях і в офіційних позиційних заявах держав, що разом формують *opinio juris* щодо допустимих і недопустимих дій у кіберпросторі [169; 247; 238; 240; 242; 259; 264; 175; 337; 297; 327; 178; 42; 148; 149; 142].

1) Суверенітет у цифровому середовищі. Принцип суверенітету охоплює територіальну цілісність та правомочність держави здійснювати владу щодо об'єктів і процесів у межах її юрисдикції, включно з ІКТ-інфраструктурою. Офіційні документи окремих держав прямо підтверджують застосовність суверенітету до кібероперацій. Так, Франція розглядає суверенітет як самостійну норму, порушення якої можливе у разі спричинення ефектів на території іншої держави (зокрема впливу на мережі та системи) [240]. Нідерланди виходять з того, що дії, які спричиняють наслідки на території іншої держави або здійснюються у владній сфері без її згоди, можуть становити порушення суверенітету [242]. Німеччина підтверджує застосовність принципу суверенітету до кіберпростору, пов'язуючи оцінку з характером і масштабом втручання в державні функції

чи інфраструктуру [238]. Канада у Заяві 2022 р. також виходить із юридичної релевантності суверенітету для кібердіяльності [175]. Водночас у позиції Великої Британії (Chatham House, 2022) обережно оцінюється питання самостійної «правильності» правила суверенітету як підстави відповідальності, за акценту на застосовності інших норм (невтручання, заборона сили тощо) [337]. Сучасна доктрина узагальнює ці підходи, виходячи з того, що кіберпростір не є правовим вакуумом, а суверенітет має як «негативний» захисний, так і «функціональний» вимір позитивних обов'язків держави [327; 161; 42; 142].

2) Принцип невтручання. Невтручання забороняє примусовий вплив на сфери, що належать до резервованої компетенції держави (вибори, внутрішня політика, основні безпекові функції). У кіберконтексті правова оцінка прив'язується до критерію примусу та націленості дій на обмеження свободи суверенного вибору іншої держави. Доктрина і державні позиції погоджуються, що операції, які примушують державу змінити поведінку у її виключних сферах (наприклад, шляхом зламу та маніпулювання критичними урядовими системами, примусового блокування ресурсів, втручання у виборчі процеси), можуть становити заборонене невтручання [169; 240; 242; 238; 337]. Українські автори наголошують на потребі чіткого розмежування політико-правового впливу (допустимого) та примусових дій, що порушують міжнародно-правову рівновагу [42; 148].

3) Заборона застосування сили; пороги *use of force* та *armed attack*. Питання про те, коли кібероперації перетинають поріг «застосування сили» у розумінні Статуту ООН і/або поріг «збройного нападу», який відкриває право на самооборону, вирішується здебільшого у наслідково-орієнтованій парадигмі. У доктрині наголошується, що про «застосування сили» може свідчити масштаб і інтенсивність ефектів, еквівалентних традиційному збройному застосуванню сили (фізична деструкція, жертви серед населення, суттєве порушення функціонування критичної інфраструктури) [247; 312]. R.Buchan пропонує розрізняти «незаконне застосування сили» та

«заборонене невтручання», підкреслюючи різні пороги та правові наслідки цих кваліфікацій [169]. Офіційні позиції держав здебільшого уникають фіксації універсальної «метрики», однак визнають релевантність наслідків, контексту та наміру для визначення порога [240; 238; 242; 175; 264; 297].

4) Обов'язок належної обачності (*due diligence*). *Due diligence* трактується як позитивний стандарт належної державної поведінки, який вимагає вживання розумних заходів для запобігання використанню території чи інфраструктури держави для шкідливих кібероперацій проти прав інших держав. У позиційних документах Нідерландів, Німеччини та Канади, а також у сучасній доктрині, підкреслюється, що обов'язок оцінюється з огляду на можливості, знання та контроль держави у конкретних умовах; він не є абсолютним і передбачає належну обачність добросовісного державного управління [242; 238; 175; 327]. Вітчизняний дискурс розглядає *due diligence* як елемент «цифрової належної обачності» держави, що поєднує внутрішні спроможності кіберзахисту з міжнародними зобов'язаннями попереджувати та припиняти транскордонну шкідливу активність [42; 148]. У публікації автора дисертації запропоновано функціональне тлумачення суверенітету у зв'язку з *due diligence*: контроль над інфраструктурою поєднується з позитивним обов'язком держави діяти з належною обачністю щодо діяльності, яка походить з її території [48].

5) Права людини в Інтернеті. Резолюція Ради з прав людини ООН 20/8 (2012) закріпила принцип еквівалентності захисту прав людини онлайн та офлайн. Звідси випливає, що державні заходи кіберзахисту мають відповідати критеріям законності, необхідності та пропорційності, уникаючи надмірного втручання у свободу вираження поглядів, приватність і захист персональних даних [235; 250; 300]. Українська наукова література підкреслює, що правозахисний вимір є структурним обмеженням будь-якої безпекової політики в цифровій сфері та умовою її легітимності й міжнародної довіри [42; 57; 58; 140; 146; 148; 355].

6) *Opinio juris* і кристалізація норм: роль державних позицій і методичних орієнтирів. Позиційні документи Франції, Нідерландів, Німеччини, Італії, Японії, Канади, Великої Британії та Нової Зеландії виконують подвійну функцію: по-перше, підтверджують застосовність базових принципів до кібероперацій і деталізують підходи до суверенітету, невтручання, заборони сили, атрибуції та контрзаходів [175; 238; 240; 242; 259; 264; 297; 337]; по-друге, формують масив *opinio juris*, у межах якого поступово кристалізуються звичаєві норми й окреслюються зони консенсусу та вузли розбіжностей (зокрема щодо правової природи «правила суверенітету» чи змісту *due diligence*) [165; 232; 278; 287; 317; 319; 327; 342; 347; 348]. Для системного вироблення та публічної артикуляції таких підходів придатною є методична рамка CCDCOE – *Handbook on Developing a National Position on International Law and Cyber Activities* (2025), яка пропонує процедуру аналізу правових питань кібероперацій і принципи послідовного, узгодженого представлення державної позиції [178]. У вітчизняному дискурсі ці підходи корелюють із спробами концептуалізувати міжнародно-правові принципи регулювання кіберпростору – суверенітет, невтручання та due diligence – в українському контексті [142; 45–47; 50; 51].

7) Проблеми ідентифікації суб’єктності, атрибуції дій та встановлення відповідальності у кіберпросторі. Хоча міжнародне право насамперед адресоване державам, у кіберсфері значну частину операцій здійснюють або опосередковують недержавні суб’єкти, що ускладнює технічну та правову атрибуцію. У доктрині звертається увага на розрив між технічними стандартами доказування і порогами, необхідними для юридичної кваліфікації (від простого «пов’язаності» до «ефективного» чи «загального контролю») [327]. Це безпосередньо впливає на класифікацію дій за принципами невтручання і заборони сили та на можливість правомірного застосування контрзаходів [169; 240; 242; 238]. Поряд із цим, виваженість публічних звинувачень і обґрунтованість атрибуції є критично важливими для підтримання легітимності правового режиму і запобігання ескалації [271;

272; 281; 320; 268], що підкреслюють і сучасні міжнародно-правові дослідження [165; 287].

Архітектура багаторівневих механізмів: «режимний комплекс» та інституційна комплементарність. Сучасна система протидії кіберзагрозам сформована як «режимний комплекс» – сукупність частково перекривних норм і інституцій глобального, регіонального та секторального рівнів, що взаємодіють між собою й забезпечують кумулятивний регулятивний ефект. У цій моделі поєднуються кримінально-правові інструменти (конвенційне співробітництво та електронні докази), політико-правові контрзаходи (санкції), запобіжна дипломатія та доктринально-експертні орієнтири (soft law) [175; 271; 272; 281; 320]. Така децентралізована конструкція створює як переваги (гнучкість, швидкість реагування, багатоакторність), так і виклики (фрагментація, ризик колізій), що потребують механізмів «налагодження» узгодженості між режимами та практиками держав [287; 319; 327; 53; 56; 57; 58].

Кіберкримінальне співробітництво Ради Європи: Будапештська конвенція та Другий додатковий протокол. Конвенційні стандарти криміналізації та процесуальні інструменти. Конвенція про кіберзлочинність (ETS № 185) встановлює мінімальні стандарти щодо криміналізації незаконного доступу, перехоплення, втручання в дані/системи та зловживання пристроями (ст. 2–6), а також містить процесуальні інструменти для збирання електронних доказів (збереження, видача, обшук/вилучення, перехоплення), доповнені механізмами міжнародної взаємодопомоги [187]. Пояснювальна доповідь наголошує, що ці склади злочинів спрямовані на захист конфіденційності, цілісності та доступності систем і даних, і не повинні криміналізувати легітимні технічні та комерційні практики [188]. Разом з тим, гармонізація здійснюється на рівні «мінімуму», що об’єктивно залишає простір для розбіжностей між національними правопорядками [184].

Швидкі транскордонні докази. Другий додатковий протокол спрямований на прискорення доступу до електронних доказів у транскордонних провадженнях. Ключові новели включають: (а) прямі запити компетентних органів до провайдерів іншої держави-учасниці щодо абонентської інформації (Art. 7); (б) екстрені процедури взаємодопомоги у випадках загрози життю або безпеці; (в) стандартизовані канали комунікації та розширення мережі контактних пунктів 24/7. Аналітичні матеріали Євроюст підкреслюють комплементарність цього інструмента до MLA-процедур і його практичну цінність в умовах швидкоплинності цифрових слідів [189].

Межі гармонізації та операційні виклики. Попри оновлення доказових механізмів, розбіжності в процесуальних стандартах (тести необхідності/пропорційності, строки зберігання даних, правила автентичності) і застереження держав впливають на практичну швидкість і передбачуваність транскордонної взаємодії. Ці виклики системно описано в літературі щодо «нерівномірної» імплементації Конвенції [184].

Універсальний трек ООН: проєкт глобальної конвенції проти кіберзлочинності. Робота Ad Hoc Committee при ООН спрямована на вироблення проєкту Конвенції ООН проти кіберзлочинності. Пояснювальні примітки UNODC (03.09.2024) фіксують логіку змін і компромісів щодо складів злочинів, процесуальних інструментів, взаємної допомоги та гарантій прав людини/верховенства права. Документ підкреслює мету посилення спроможності держав розслідувати технологічно складні правопорушення і зміцнювати міжнародну співпрацю, залишаючи відкритими питання узгодженості з наявними договірними режимами (зокрема з ETS № 185), що потребуватиме подальшої координації в межах «режимного комплексу» [346; 299].

Політико-правові контрзаходи ЄС: режим адресних кіберсанкцій. ЄС у 2019 р. створив правову рамку адресних обмежувальних заходів щодо осіб/суб’єктів, відповідальних за кібернапади чи їх спроби, що становлять

зовнішню загрозу для Союзу або його держав-членів: Рішення (CFSP) 2019/797 та Регламент (ЄС) 2019/796. Рамка охоплює кібернапади з «істотним ефектом», включно із замахами з потенційно істотним ефектом (ст. 1), та передбачає замороження активів і заборону на поїздки не лише для безпосередніх виконавців, а й для тих, хто надає фінансову, технічну чи матеріальну підтримку або бере участь у підготовці/співучасті [186; 191]. У доктрині EUISS Brief розглядає цей режим як елемент «Cyber Diplomacy Toolbox», що забезпечує ескалаційну «сходинку» правових реакцій – від дипломатичних демаршів і публічної атрибуції до адресних санкцій [285; 58; 142].

Запобіжна дипломатія та деескалація: міри довіри (CBMs) ОБСЄ. Для зниження ризиків конфліктної ескалації, пов'язаних із застосуванням ІКТ у міждержавних відносинах, ОБСЄ ухвалила Рішення Постійної ради № 1202 (10.03.2016) про міри довіри (CBMs), що включають обмін контактами на випадок інцидентів, прозорість доктрин і політик, добровільний обмін інформацією про загрози/уразливості та взаємодію з приватним сектором [302]. Брошура 2023 р. систематизує 16 CBMs, наголошуючи на їх практичному характері та комплементарності до зусиль ООН у сфері відповідальної поведінки держав [301; 281; 320; 141].

Доктринально-експертна опора: «Талліннський процес» як soft law. Попри відсутність обов'язкової юридичної сили, Tallinn Manual виконує роль доктринального орієнтира («рестейтменту») міжнародного права у кіберпросторі, що використовується державними радниками, судами й академічною спільнотою [317; 318]. Проєктна сторінка CCDCOE (2021–2025) підтверджує триваюче оновлення («3.0 update») з урахуванням публічних державних позицій щодо суверенітету, due diligence, атрибуції тощо [179]. Це *soft law* джерело допомагає узгоджувати практики у межах режимного комплексу та слугує методичною надбудовою до конвенційних, санкційних і CBMs-інструментів [299; 308; 142; 45; 50].

Загальна рамка відповідальності держав: структура ARSIWA та її релевантність для кібероперацій. Норми міжнародної відповідальності, кодифіковані в Проєкті статей про відповідальність держав за міжнародно-протиправні діяння 2001 р. (Draft Articles on Responsibility of States for Internationally Wrongful Acts, далі - ARSIWA), закріплюють базові принципи притягнення держав до відповідальності за порушення міжнародного права. Відповідно до ст. 1–2, кожне міжнародно-протиправне діяння держави тягне її міжнародну відповідальність, якщо поведінка (дія чи бездіяльність) є атрибутованою державі і становить порушення її міжнародного зобов'язання. Подальші норми визначають критерії такої атрибуції: ст. 4 – дії будь-яких органів держави; ст. 5 – осіб чи організацій, наділених елементами державної влади; ст. 6–7 – органів, наданих іншою державою, або перевищення повноважень; ст. 8 – приватних осіб, що діють за інструкціями, під керівництвом чи контролем держави. Окрім того, ст. 16–18 визначають відповідальність держави за допомогу, напрям чи примус іншої держави при вчиненні міжнародно-протиправного діяння, а ст. 11 передбачає можливість подальшого «усиновлення» поведінки, коли держава визнає та приймає її як власну. У частині наслідків ст. 30–31 покладають на державу обов'язки припинення порушення, надання гарантій неповторення та повного відшкодування шкоди, що охоплює матеріальні й моральні збитки. Водночас, у межах ст. 49–54, допускається застосування контрзаходів виключно для спонукання держави-порушниці до виконання зобов'язань, за умови дотримання принципів необхідності, пропорційності та, як правило, попереднього повідомлення, крім випадків крайньої терміновості. Ці положення становлять вторинну систему норм, яка забезпечує універсальну матрицю оцінки державної поведінки у кіберпросторі та визначає межі правомірної реакції на шкідливі дії цифрового характеру [345].

Атрибуція у кіберпросторі: технічні та юридичні виміри, стандарти доказування. Складність атрибуції у кіберсправах зумовлена багаторівневістю технічних візерунків (ланцюжки проксі, повторне

використання інструментарію, навмисні «false-flag»), що ускладнює перехід від форензичної ідентифікації виконавців до юридичної атрибуції конкретній державі. У міжнародно-правовій площині атрибуція спирається на розділ II ARSIWA (ст. 4–11): дії органів держави (ст. 4), приватних осіб/організацій, наділених елементами державної влади (ст. 5), органів, наданих іншою державою (ст. 6), навіть у разі перевищення повноважень (ст. 7), а також поведінку осіб або груп, що діють за інструкціями, під керівництвом чи контролем держави (ст. 8), і випадки визнання та прийняття поведінки як власної (ст. 11). До цього блоку належать і зв'язки між державами у вчиненні порушення: допомога/сприяння (ст. 16), напрям і контроль (ст. 17) та примус (ст. 18) [345]. У доктрині показано, що стандарт доказування у державній практиці варіює залежно від форуму, типу запланованої реакції та політичного контексту; ключове – переконливо продемонструвати юридично релевантний зв'язок між встановленими технічними індикаторами та підставою атрибуції, передбаченою ARSIWA. Отже, сам по собі висновок про інструментарій/інфраструктуру не автоматично конвертується у правову атрибуцію без доказів «інструкції/керівництва/контролю» або іншої підстави, зазначеної у статтях 4–11, 16–18 ARSIWA [327; 345].

Публічна атрибуція та звинувачення: політика доказів і правові наслідки. Публічна атрибуція дедалі частіше використовується як інструмент політичної стратегії для створення стримувального ефекту, консолідації партнерів та формування міжнародного наративу, але її нормативна результативність не є гарантованою: адресати нерідко заперечують, і «соціальне соромлення» не настає [287]. Тому практики потребують правового осмислення з огляду на стандарти доказування, коректність підстав атрибуції за ARSIWA та легітимність обраної відповіді. Адже перехід до правових контрзаходів вимагає дотримання умов гл. II Частини третьої ARSIWA, і недостатньо обґрунтовані публічні звинувачення можуть створювати ризик ескалації та контрнаративів [165; 53; 56; 57; 58].

Відповідь на міжнародно-протиправні кібердіяння: контрзаходи, реторсії та санкційні режими ЄС. Підхід, сформульований у Проєкті статей про відповідальність держав за міжнародно-протиправні діяння (ARSIWA, 2001), чітко розрізняє реторсії – недружні, але правомірні дії (дипломатичні або економічні заходи у межах міжнародного права), та контрзаходи, які передбачають тимчасове невиконання міжнародного зобов'язання з метою спонукання держави-порушниці до припинення протиправного діяння і відновлення належного правопорядку. Відповідно до ст. 49–54 ARSIWA, такі заходи мають бути пропорційними, тимчасовими й процедурно обґрунтованими: перед їх застосуванням держава має повідомити порушника, надати можливість для переговорів і вжити контрзаходів лише тією мірою, яка необхідна для відновлення порушеного права [345; 45; 47; 51].

У межах Європейського Союзу цей підхід знайшов практичне втілення через запровадження адресних обмежувальних заходів проти суб'єктів, причетних до кібероперацій, що становлять загрозу безпеці Союзу або його держав-членів. Правову основу становлять Рішення Ради (CFSP) 2019/797 і Регламент (ЄС) 2019/796, ухвалені 17 травня 2019 р. Відповідно до ст. 1 обох актів, санкційний режим поширюється на кібернапади із «значним ефектом» (включно зі спробами) і на осіб, які надають фінансову, технічну або матеріальну підтримку чи беруть участь у підготовці та співучасті в таких діях [186; 191]. Ці заходи – обмежувальні дії в межах Спільної зовнішньої та безпекової політики (СЗБП), юридична легітимність яких оцінюється крізь призму пропорційності, обґрунтованості атрибуції та дотримання процесуальних гарантій [141; 142].

У доктрині ЄС санкційний механізм інтерпретується як складова «EU Cyber Diplomacy Toolbox», що доповнює інші інструменти – публічну атрибуцію, дипломатичні демарші, попереджувальні заяви, політичні заходи та класичні контрзаходи держав [285; 272; 281; 320]. Таким чином, режим кіберсанкцій ЄС відображає інституціоналізацію контрзаходів у

наддержавній системі, надаючи їм узгодженості з міжнародно-правовими принципами відповідальності, закріпленими у ARSIWA, і водночас створюючи практичний прецедент правового реагування на шкідливі кібердії у багаторівневій системі міжнародного управління.

Колективна превенція та деескалація: норми ООН і заходи довіри ОБСЄ. Нормативна діяльність ООН у сфері безпеки інформаційно-комунікаційних технологій сформувала рамку відповідальної поведінки держав у кіберпросторі. У доповідях Групи урядових експертів 2015 р. (A/70/174) та 2021 р. (A/76/135) підкреслено застосовність міжнародного права до кібероперацій і визначено перелік добровільних, але політично зобов'язуючих норм, які охоплюють недопущення дій проти критичної інфраструктури, гарантування безпеки ланцюгів постачання, обмін інформацією про вразливості та взаємну допомогу у реагуванні на інциденти [340; 341; 339]. Зазначені документи заклали нормативну основу колективної превенції та підтвердили, що держави мають обов'язок діяти відповідально і прозоро у сфері кібербезпеки [53; 56; 57; 58; 142].

Подальший розвиток цієї лінії забезпечила Відкрито-складова робоча група (Open-ended Working Group, OEWG), утворена за резолюцією ГА 75/240. У Підсумковому звіті (A/75/816, 2021) та Третьому щорічному звіті про прогрес (A/79/214, 2024) запропоновано конкретні механізми практичної реалізації норм – зокрема, створення каналів прямого зв'язку «точка-до-точки» (Points of Contact) між державами, уніфікованих шаблонів обміну технічною інформацією, а також процедур кризової комунікації та взаємного попередження про інциденти [342; 343; 320; 271; 272].

На регіональному рівні ОБСЄ доповнила цей процес власним набором заходів довіри у сфері ІКТ. Рішення Постійної ради № 1202 (10.03.2016) започаткувало перший комплекс із 16 CBMs, що систематизовані у брошурі 2023 р. і мають на меті зниження ризиків непорозуміння, запобігання інцидентам і зміцнення транспарентності. Ці заходи передбачають обмін контактами компетентних органів, повідомлення про національні доктрини

кібербезпеки, добровільний обмін інформацією про кіберзагрози, сповіщення про вразливості та сприяння участі приватного сектору [302; 301; 141].

Сукупно норми ООН та заходи ОБСЄ формують механізм колективної превенції та деескалації у кіберпросторі, який поєднує поведінкові стандарти, інституційні канали комунікації та інформаційну транспарентність. Такий підхід сприяє зменшенню правової невизначеності у випадках кіберінцидентів, запобігає помилковій атрибуції та забезпечує основу для подальшої кодифікації норм відповідальної поведінки держав у цифровому середовищі [45; 46; 47; 50; 51].

Операціоналізація норм відповідальності у державній політиці: практичні орієнтири CCDCOE. Документ “Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States” сформулював системний підхід до розроблення офіційних національних позицій держав щодо застосування міжнародного права у кіберпросторі. У ньому узагальнено результати консультацій із 46 державами та запропоновано структуровану методику, що охоплює визначення мотивацій, процедурні кроки, змістовне наповнення та способи представлення таких позицій. Посібник рекомендує державам формувати національні концепції з основних міжнародно-правових питань – суверенітету, due diligence, атрибуції, контрзаходів, міжнародного гуманітарного права – з урахуванням власних інтересів і практики інших країн [178; 142; 271; 272; 281; 320].

У прикладному вимірі *Handbook* окреслює три взаємопов’язані етапи політики державного реагування на шкідливу кібердіяльність. Перший етап – аналітичний, який передбачає форензичне розслідування та юридичну атрибуцію згідно зі статтями 4–11 і 16–18 *Проєкту статей про відповідальність держав за міжнародно-протиправні діяння* [345]. Другий етап – нормативно-оцінювальний: визначення правових умов застосування контрзаходів, виходячи з принципів пропорційності, необхідності та процедурності (ст. 49–54 ARSIWA) [345; 45; 47; 50]. Третій етап –

комунікаційний, що включає підготовку офіційних заяв, дипломатичних нот і доказової бази для публічної та міжнародної презентації позиції держави, а також координацію з партнерами, союзниками та приватними провайдерами.

Застосування цієї методики сприяє послідовності державної політики, підвищує прозорість і знижує ризики виникнення спорів щодо достовірності доказів або пропорційності дій. У такий спосіб *Handbook CCDCOE* перетворює норми міжнародної відповідальності на практичний інструмент стратегічного управління, що поєднує правовий аналіз, міжвідомчу координацію та публічну дипломатію – у повній відповідності до сучасних вимог міжнародної правосуб'єктності держав у цифрову епоху [178].

Узгодження відповідальності, атрибуції та «інструментів тиску». Проблематика узгодження атрибуції, юридичної відповідальності та інструментів реагування (реторсії, контрзаходи, санкційні режими) набуває особливої ваги в умовах поліцентричної структури кіберпростору. Як підкреслює доктрина, публічні звинувачення без належного юридичного обґрунтування мають обмежений нормативний ефект і можуть провокувати контрнаративи або політичну ескалацію, знижуючи довіру до самого механізму міжнародної відповідальності [165; 53; 56; 57; 58]. Відтак формалізація національних позицій, підкріплена процедурними нормами ARSIWA та міждержавними рамками ООН і ОБСЄ, створює більш стійкий та легітимний механізм реагування [345; 341; 301; 142].

Зокрема, доповідь Групи урядових експертів ООН 2021 р. (A/76/135) наголошує на важливості використання правових механізмів і взаємоповаги до суверенітету при державних кібердіях, а також на потребі підвищення транспарентності у публічній атрибуції [341]. У цьому контексті заходи довіри ОБСЄ (CBMs, 2023) виступають інституційною платформою для обміну інформацією, підтвердження атрибуції та деескалації конфліктних інцидентів [301].

Синтез цих елементів – ARSIWA, механізмів ООН/ОБСЄ та методичних орієнтирів CCDCOE (2025) – формує цілісний правовий ланцюг:

від фіксації порушення та доведення його атрибуції до прийняття правомірної, пропорційної та комунікативно вивіреної реакції. Саме така комплексна модель узгоджує технічну, політичну й юридичну складові державної поведінки у кіберпросторі, забезпечуючи баланс між національними інтересами, колективною безпекою та загальними принципами міжнародного права [178; 341; 301; 142].

Доктринальні та інституційні орієнтири формування міжнародно-правового режиму кіберзахисту. Талліннський підхід, викладений у працях Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) та Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017), став основним доктринальним орієнтиром для держав, міжнародних організацій і наукової спільноти щодо застосування норм міжнародного права до діяльності у кіберпросторі [318; 317]. Якщо перший посібник зосереджувався переважно на правовому регулюванні кібероперацій у контексті збройних конфліктів – на рівні jus ad bellum та jus in bello, то Tallinn Manual 2.0 розширив аналітичну рамку до ширшого спектра кібероперацій у мирний час. У ньому комплексно розглянуто питання суверенітету, невтручання, належної обачності (due diligence), міжнародної відповідальності держав, захисту прав людини в онлайновому середовищі та безпеки критичної інфраструктури [317; 345].

У 2021 році Кооперaційний центр кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE) оголосив про започаткування п’ятирічного проєкту Tallinn Manual 3.0, спрямованого на перегляд і оновлення змісту попередніх редакцій з урахуванням зростання державної практики, появи публічних національних позицій і розвитку технологічних реалій [179; 178]. Цінність Талліннського підходу полягає не у створенні нових норм міжнародного права, а у систематизації правозастосовної практики. Посібники пропонують узгоджене тлумачення чинних положень Статуту ООН, норм гуманітарного права, принципів відповідальності держав та стандартів доказування у кіберпросторі [317; 318;

345]. Саме тому Tallinn Manual виконує функцію доктринального «містка» між позитивним правом і практичними потребами його застосування у цифровому середовищі, формуючи базу для подальшої кодифікації норм поведінки держав у кіберсфері [317; 179; 345].

Гуманітарно-правовий вимір. Міжнародний комітет Червоного Хреста у своєму Позиційному документі (2019 р.) офіційно підтвердив застосовність норм міжнародного гуманітарного права (МГП) до кібероперацій, що здійснюються у контексті збройних конфліктів [253; 306]. У документі наголошується, що держави, які ведуть або підтримують кібероперації в умовах війни, зобов'язані неухильно дотримуватися основоположних принципів МГП – розрізнення, пропорційності та запобіжних заходів. Підкреслюється, що навіть некінетичні дії у кіберпросторі можуть спричиняти кумулятивний негативний вплив на цивільне населення через порушення функціонування критичних цивільних об'єктів – енергетичних систем, мереж охорони здоров'я, водопостачання чи комунікаційної інфраструктури. МКЧХ застерігає, що такі наслідки здатні завдати гуманітарної шкоди, співмірної з ефектами традиційних засобів ведення війни, а відтак підпадають під дію чинних заборон та обмежень міжнародного гуманітарного права [253; 306].

Подальша аналітична робота МКЧХ, узагальнена у *Executive Summary: Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, акцентує на практичних аспектах впровадження норм IHL у кіберпросторі [255]. У документі розглянуто методи оцінювання ризиків для цивільних, процедури інтеграції аналізу кіберзагроз у планування військових операцій, заходи з координації між підрозділами кіберзахисту та гуманітарними структурами. Ці положення не створюють нових норм міжнародного права, проте деталізують і конкретизують стандарти належної поведінки держав і збройних сил у межах чинного IHL, надаючи методичні орієнтири для адаптації гуманітарних принципів до сучасного цифрового середовища [253; 255; 306].

Правовий статус кібероперацій. Проблема визначення правового статусу кібероперацій – зокрема моменту, коли вони досягають порогу «застосування сили» відповідно до статті 2(4) Статуту ООН або переростають у «збройний напад» у розумінні статті 51, – є центральною в сучасній доктрині міжнародного права. Як показує Roscini M. , кваліфікація кібердій залежить не від форми чи технологічного засобу, а від їхніх субстантивних характеристик: масштабу, тривалості, інтенсивності, природи цілей і фактичних наслідків для життєво важливих об'єктів держави [312]. Учений обґрунтовує, що кібероперації, які спричиняють фізичні руйнування, жертви або серйозні перебої у функціонуванні критичної інфраструктури, можуть за певних умов досягати порогу «застосування сили», а у випадку крайньої інтенсивності наслідків – кваліфікуватися як «збройний напад», що активує право держави на самооборону. Водночас переважна більшість кіберінцидентів залишається нижче цих порогів і розглядається у площині міжнародної відповідальності держави та правомірних контрзаходів, передбачених вторинним правом відповідальності.

Такий підхід концептуально узгоджується з положеннями *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, у якому експертна група розробила детальну шкалу критеріїв оцінювання масштабу й наслідків кібероперацій, пов'язаних із застосуванням сили. У документі наголошується, що правова оцінка кіберінцидентів має враховувати не лише фізичні результати, а й системні наслідки для державних функцій, фінансових систем і безпеки населення. Таким чином, *Tallinn Manual 2.0* фіксує поступову конкретизацію критеріїв jus ad bellum у кіберпросторі без зміни текстуальних положень Статуту ООН, відображаючи еволюцію доктрини від абстрактного тлумачення до практичного застосування норм у контексті нових технологічних викликів [312; 317].

Еволюція «кіберномр»: між стратегічною амбівалентністю й правилами. Після 2015 року процес формування «норм відповідальної поведінки держав у кіберпросторі» (non-binding norms) супроводжується

інтенсивною доктринальною дискусією щодо їхньої ефективності та правової природи. У праці *The End of Cyber Norms* Grigsby A. застерігає від інфляції поняття «норма» у ситуації, коли відсутні механізми юридичного закріплення й виконання. На його думку, «кінець норм» настає тоді, коли політичні декларації не переростають у стабільну практику правозастосування, що знижує їхню регулятивну дієвість і девальвує саму ідею нормативного управління кіберпростором [245].

На противагу цьому, Mačák K обґрунтовує необхідність повернення держав до активної правотворчої ролі. Учений підкреслює, що лише «перехід від норм до правил», тобто від декларативного *soft law* до конкретизованих правових приписів, може забезпечити стабільність міжнародного режиму кібербезпеки. На його переконання, технічна динаміка та еволюція кіберзагроз вимагають від держав формулювання чітких, взаємно визнаних стандартів поведінки у критичних сферах – від захисту інфраструктури до запобігання деструктивним інформаційним операціям [278].

У ширшій аналітичній перспективі ці підходи корелюють із висновками Hurwitz R, який описує взаємодію держав у кіберпросторі як «гру стратегічної невизначеності». Він зазначає, що така амбівалентність дозволяє урядам уникати жорстких зобов'язань, зберігаючи простір для політичного маневру, проте водночас перешкоджає інституційному закріпленню спільних правил і стабільних режимів безпеки [251].

Таким чином, сучасна еволюція «кібернорм» характеризується пошуком балансу між нормативною гнучкістю та потребою у правовій визначеності. Для міжнародно-правового режиму кіберзахисту це означає необхідність гармонійного поєднання двох взаємодоповнюючих підходів: по-перше, формування чітких і обов'язкових правових приписів у найбільш чутливих сферах – захисту критичної інфраструктури, безпеки ланцюгів постачання, виборчих процесів та інформаційного простору; по-друге, збереження адаптивних форматів співпраці у напрямах, де універсальна кодифікація поки що є неможливою [245; 278; 251].

Інституційні вектори кодифікації та імплементації: ООН і ОБСЄ. На універсальному рівні Організація Об’єднаних Націй сформувала цілісну «рамку відповідальної поведінки держав» у сфері інформаційно-комунікаційних технологій, яка охоплює чотири взаємопов’язані компоненти: (1) застосовність міжнародного права; (2) добровільні норми поведінки; (3) заходи довіри; (4) розвиток національного потенціалу. Ця структура вперше була відображена у Доповіді Групи урядових експертів 2015 року (A/70/174), схваленій Генеральною Асамблеєю, та закріплена в Резолюції 70/237, що підтвердила застосовність чинного міжнародного права до кіберпростору [343; 341].

Подальший розвиток цих положень відбувся у Доповіді Групи урядових експертів 2021 року (A/76/135), де наголошено на необхідності операціоналізації вироблених норм через створення механізмів кризової комунікації, мережі контактних пунктів (*points of contact*) та стандартизованих процедур обміну технічною інформацією [342]. Звіт також закріпив бачення міжнародного співробітництва у сфері кібербезпеки як інклюзивного процесу, що базується на поєднанні обов’язкових та політично зобов’язуючих норм.

Відкрито-складова робоча група (OEWG) 2021–2025 років у своєму Третьому щорічному звіті (A/79/214, 2024) підтвердила консенсус щодо розроблення нових заходів довіри, уніфікованих шаблонів обміну даними та зміцнення інституційних каналів міждержавної взаємодії. Документ фіксує погоджене оновлення термінології щодо кіберзагроз і початкові переліки глобальних CBMs, затверджені консенсусом держав-членів [348].

На регіональному рівні Організація з безпеки і співробітництва в Європі (ОБСЄ) стала піонером інституційного впровадження заходів довіри у сфері ІКТ-безпеки. Рішення Постійної ради № 1202 від 10 березня 2016 року започаткувало ініціативу зі створення 16 базових заходів довіри, які включають обмін контактними даними компетентних органів, підвищення

транспарентності національних доктрин, обмін інформацією про вразливості та взаємодію з приватним сектором [302].

У сукупності діяльність ООН та ОБСЄ формує інституційний каркас міжнародно-правового режиму кіберзахисту – від універсальних рамкових норм поведінки до конкретних процедурних каналів координації, що дають змогу державам мінімізувати ризики хибної атрибуції, непорозумінь і небажаної ескалації у кіберпросторі [342; 348; 302].

1.3. Національна система кібербезпеки України: законодавство та інституційна структура

Загальні правові засади формування національної системи кібербезпеки. Національна система кібербезпеки України вибудовується як цілісна публічно-правова конструкція, що поєднує норми матеріального та процесуального права з організаційно-управлінськими механізмами, технічними стандартами та інструментами нагляду і контролю. У доктрині підкреслюється соціотехнічна природа кібербезпеки: правове регулювання має узгоджувати технологічні засоби захисту з належними процедурами прийняття рішень, відповідальністю суб’єктів та гарантіями прав людини [6; 10]. У цьому контексті загальні правові засади охоплюють, по-перше, принцип верховенства права (як методологічний імператив законності, необхідності та пропорційності втручань); по-друге, адміністративно-правову визначеність повноважень і підзвітності органів публічної влади; по-третє, системність та ризик-орієнтованість державної політики у сфері захисту цифрових процесів і інформаційних ресурсів [3; 7; 11; 12].

Доктринально система кібербезпеки трактується як сукупність норм і інститутів, які забезпечують досягнення стану захищеності життєво важливих інтересів особи, суспільства і держави в цифровому середовищі. Її ключовими елементами визнаються: 1) суб’єкти публічної влади з чітко

окресленою компетенцією; 2) механізми координації та взаємодії; 3) стандартизовані процедури запобігання, виявлення, реагування і відновлення; 4) інструменти контрольно-наглядової діяльності; 5) належний режим відповідальності [28; 29; 7]. Концептуальні положення щодо інституційної структури та нормативно-правових механізмів функціонування національної системи кібербезпеки викладено у науковій статті Нормативно-інституційні засади формування національної системи кібербезпеки України [47]. У працях із державного управління наголошено, що ефективність такої системи зумовлюється не лише репресивними заходами, а насамперед превенцією, безперервним управлінням ризиками, розвитком інституційних спроможностей та якісною регуляторною оцінкою [12; 17; 18].

Окремим методологічним вузлом виступає правове забезпечення захисту об’єктів критичної інформаційної інфраструктури (КІІ). Для нього визначальними є: належна ідентифікація й категоризація КІІ, впровадження організаційно-технічних моделей захисту (включно з SOC/CSIRT), формалізовані процедури взаємообміну даними про інциденти та аудит стану безпеки. Вітчизняні дослідження пропонують узгоджений понятійний апарат і підкреслюють потребу уніфікації критеріїв критичності, що забезпечує правову передбачуваність для регуляторів і операторів [2]. Паралельно в роботах з безпекознавства апелюється до принципів системності, безперервності й відмовостійкості, які мають бути відтворені у правових нормах та процедурах публічної адміністрації [6].

Адміністративно-правовий вимір цих засад полягає у чіткому нормативному розмежуванні функцій формування політики, її координації та правозастосування; визначенні порядку взаємодії між органами безпеки, оборони, правоохоронними органами й цивільними регуляторами; закріпленні режимів доступу до інформації, інцидент-респонсу та перевірок. У центрі –гарантії підзвітності, внутрішнього і зовнішнього контролю, а також процесуальні запобіжники від зловживань (включно з судовим контролем і засобами оскарження) [7; 17]. Важливу роль відіграють і загальні

підходи до визначення публічного інтересу у сфері інформаційної безпеки та його співвідношення з приватною автономією, що окреслюють рамки допустимих обмежень і вимоги до якості закону [11].

Змістовним підґрунтям для загальних засад є також безпекознавчі та політологічні студії, які концептуалізують кіберпростір як автономний, але взаємопов'язаний вимір національної безпеки. Вони акцентують на необхідності інституційної цілісності, міжвідомчої взаємодії та участі недержавних стейкхолдерів (операторів, провайдерів, науково-освітнього середовища) у виконанні публічних завдань у сфері кіберзахисту [32; 33; 35; 54; 71; 273; 320]. У цій парадигмі кібербезпека розглядається як один із пріоритетів національної політики, що вимагає системного планування, ресурсного забезпечення та професійної підготовки кадрів [19; 26; 78; 143; 153].

Узагальнюючи, загальні правові засади у пп. 1.3 можна звести до таких груп: (1) принципові вимоги верховенства права, законності, необхідності та пропорційності втручань; (2) структурні вимоги адміністративно-правової визначеності суб'єктів і процедур, підзвітності та контролю; (3) функціональні вимоги ризик-орієнтованості, превенції, безперервності та відновлюваності; (4) організаційні вимоги до координації, взаємодії та участі приватного сектору; (5) епістемні вимоги доказовості рішень і відповідності правових інструментів реальній технічній архітектурі цифрового середовища [6; 7; 17; 21; 35; 61; 273].

Конституційні засади. Вихідним рівнем формування національної системи кібербезпеки є конституційно-правові приписи, які задають ієрархію джерел, окреслюють межі дискреції публічної влади та встановлюють баланс між безпековою функцією держави і гарантіями прав людини. У межах цих приписів доктрина наполягає на поєднанні соціотехнічної природи кіберзагроз із вимогами верховенства права, адміністративно-правової визначеності та підзвітності суб'єктів владних повноважень [6; 7; 11; 12; 17; 61].

Стаття 8 закріплює принцип верховенства права, найвищу юридичну силу Конституції та пряму дію її норм, що гарантує можливість судового захисту прав і свобод безпосередньо на конституційній основі [52]. Для сфери кібербезпеки це означає, що будь-які режими моніторингу, обміну інформацією, реагування на інциденти, а також кримінально-правові та адміністративно-процесуальні інструменти повинні відповідати критеріям законності, легітимної мети, необхідності та пропорційності втручань у приватну сферу (у т.ч. у комунікаційну та інформаційну недоторканність) [4; 11; 76; 135; 140]. Наукові підходи підкреслюють, що верховенство права функціонує як методологічний фільтр «соціотехнічних» рішень: технічні засоби безпеки та організаційні процедури легітимні лише остільки, оскільки узгоджені з матеріальними і процесуальними гарантіями прав людини та підлягають ефективному судовому контролю [4; 6; 11; 17; 76; 135].

Стаття 17 фіксує, що захист суверенітету і територіальної цілісності України та забезпечення її економічної й інформаційної безпеки є найважливішими функціями держави і «справою всього Українського народу» [52]. У доктрині ця норма розглядається як джерело позитивних зобов’язань держави створити ефективну організаційно-правову систему кіберзахисту, здатну протидіяти загрозам як внутрішнього, так і зовнішнього походження [28; 29; 32; 33; 61]. Звідси випливають вимоги до визначеності суб’єктного складу, координації, процедур взаємодії та належного режиму відповідальності [7; 17; 32; 33]. У площині захисту критичної інформаційної інфраструктури ця конституційна рамка конкретизується через ідентифікацію та категоризацію КІІ, організаційно-технічні моделі (SOC/CSIRT), стандартизований обмін інформацією про інциденти та аудит безпеки [2; 22; 23; 24; 44; 69; 75; 95; 98; 101; 102; 106]. Безпосередній зв’язок з оборонним компонентом – предметом спеціальної доктрини кібероборони – також витікає зі ст. 17 і обґрунтовує потребу в системному поєднанні військових, технічних та правових інструментів [8; 19; 71; 282; 350].

Стаття 18 встановлює, що зовнішньополітична діяльність України спрямована на забезпечення національних інтересів і безпеки з дотриманням загальновизнаних принципів і норм міжнародного права [52]. Для кібербезпеки це є конституційною підставою імплементації міжнародних та європейських стандартів, доктринальних настанов і найкращих практик – від конвенційних підходів до секторальних вимог до мережевої та інформаційної безпеки [33; 45; 46; 47; 48; 49; 50; 51; 273]. У політико-правовій площині це забезпечує узгодженість внутрішньої моделі кіберзахисту з міжнародним правопорядком та системою партнерств у сфері кібербезпеки [21; 32; 53; 54; 139; 141; 281; 320].

Стаття 92 визначає, що питання національної безпеки і оборони, а також організація та діяльність органів, покликаних їх забезпечувати, встановлюються виключно законами України [52]. Це закладає ієрархію джерел у сфері кібербезпеки: базові елементи системи (суб’єкти, повноваження, координація, процедури реагування, контроль і нагляд, засади відповідальності) мають бути врегульовані на рівні закону, тоді як підзаконні акти покликані деталізувати й імплементувати законодавчі приписи [4; 7; 10; 17]. Адміністративно-правовий підхід акцентує на потребі нормативної визначеності компетенцій і процесуальних гарантій при здійсненні контролю, доступу до інформації та розслідувань у кіберсфері [20; 56; 57; 141; 147].

Сукупно статті 8, 17, 18 і 92 формують «конституційну матрицю» національної системи кібербезпеки, яка репрезентує:

–принципові вимоги верховенства права, прямої дії конституційних норм і судового контролю (легальність, необхідність, пропорційність) [11; 60];

–безпекову місію держави, що охоплює інформаційну безпеку як конституційно значущий елемент, та відповідні позитивні зобов’язання зі створення інституційної архітектури кіберзахисту [28; 29; 30; 61; 153];

–міжнародний вимір політики кібербезпеки, який детермінує гармонізацію внутрішнього регулювання зі світовими підходами та стандартами [21; 33; 54; 139; 142; 173; 207; 220];

–ієрархічну будову правового регулювання, де закон визначає засадничі елементи системи, а підзаконні та відомчі акти – техніко-процедурні інструменти реалізації [4; 7; 10; 17].

З огляду на наведене, конституційний рівень не лише легітимує публічно-правову активність у сфері кібербезпеки, а й встановлює методологічні обмеження для правозастосування: будь-які технологічні та організаційні рішення мають бути вмонтовані у процедури належного врядування, підзвітності та судового контролю, забезпечуючи співмірність між захистом публічних інтересів і охороною приватної автономії у цифровому середовищі [6; 17; 53; 56; 57; 58; 141].

Стратегічні основи. Сучасна архітектура державної політики України у сфері кібербезпеки має системний, ієрархічно впорядкований характер, що ґрунтується на послідовності «рамкова стратегія – доменна стратегія – інструменти імплементації – інституційно-технічні засоби». Її концептуальну вершину становить Стратегія національної безпеки України, затверджена рішенням Ради національної безпеки і оборони України та введена в дію Указом Президента № 392/2020. У цьому документі кібербезпеку визначено серед ключових пріоритетів державної політики у сфері національної безпеки, що охоплює розвиток національної системи кіберзахисту, підвищення кіберстійкості критичної інфраструктури, створення ефективної системи управління ризиками в кіберпросторі, а також розбудову партнерських механізмів взаємодії між державним і приватним секторами [107; 119].

Доменний рівень стратегічного планування конкретизується Стратегією кібербезпеки України, схваленою рішенням РНБО від 14 травня 2021 року та введеною в дію Указом Президента № 447/2021. Документ визначає мету, принципи, пріоритетні напрями та завдання державної

політики у сфері кібербезпеки, а також закріплює центральну координаційну роль Національного координаційного центру кібербезпеки при РНБО України (НКЦК). Стратегія спрямована на забезпечення стійкого функціонування цифрового середовища, зміцнення здатності держави до запобігання, виявлення, реагування та відновлення після кіберінцидентів, а також на формування національної культури кібергігієни й підвищення рівня довіри в інформаційному просторі [97; 111; 117; 121].

Інструментальну площину реалізації цієї політики становить План реалізації Стратегії кібербезпеки України, затверджений рішенням РНБО від 30 грудня 2021 року та введений у дію Указом Президента № 37/2022. У ньому деталізовано механізми виконання стратегічних завдань, визначено відповідальних виконавців, строки, очікувані результати та показники ефективності. Документ заклав основу системного підходу до моніторингу, координації та звітності у сфері кібербезпеки, забезпечивши узгодженість дій усіх суб'єктів національної системи кіберзахисту [118].

Подальша операціоналізація стратегічних цілей здійснюється через щорічні урядові плани заходів, серед яких актуальним є План на 2025 рік, затверджений розпорядженням Кабінету Міністрів України № 204-р від 7 березня 2025 року. У документі визначено конкретні етапи реалізації завдань, розподіл компетенцій між органами виконавчої влади, строки виконання та індикатори результативності. Таким чином, запроваджено практику поетапного, вимірюваного впровадження положень Стратегії кібербезпеки, що забезпечує її безперервність, адаптивність і підзвітність у межах загальної системи національної безпеки [121].

Операційно-стратегічний вимір державної політики у сфері кібербезпеки формується через рішення Ради національної безпеки і оборони України, уведені в дію указами Президента, які визначають конкретні механізми реалізації стратегічних орієнтирів та уточнюють компетенційні зв'язки між суб'єктами національної системи кіберзахисту.

Історично ключовим каталізатором розвитку нормативного середовища став Указ Президента № 32/2017 «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». Цим актом уперше на рівні найвищого органу сектору безпеки було окреслено системний перелік актуальних кіберзагроз, визначено необхідність формування єдиної державної політики у сфері кіберзахисту, створення міжвідомчих механізмів реагування та забезпечення оперативного обміну інформацією між компетентними органами [97]. Саме цей документ став основою для подальшої деталізації стратегічних завдань у Стратегіях кібербезпеки 2016 і 2021 років, а також для формування інституційного контуру, який нині забезпечує функціонування НКЦК [111; 117].

Важливе місце в системі операційно-стратегічного управління належить механізмам застосування спеціальних економічних та інших обмежувальних заходів (санкцій) як інструменту державного реагування на кіберагресію. Указ Президента № 749/2025 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» конкретизує підходи до використання санкційної політики щодо фізичних і юридичних осіб, причетних до кібератак, деструктивних інформаційних операцій або підтримки агресії у кіберпросторі. Така політика корелює з положеннями Стратегії національної безпеки України 2020 року, у якій кіберзагрози державного походження визначено як один із ключових викликів для суверенітету й стабільності держави [119; 107].

На перетині оборонної та кібернетичної політик функціонує Концепція розвитку сектору безпеки і оборони України, уведена в дію Указом Президента № 92/2016, що заклала підвалини інтеграції кіберспроможностей до системи стратегічного оборонного планування. У документі визначено необхідність створення сучасної системи управління кібероборони, розвитку спеціалізованих структур у Збройних Силах України та координації їхньої діяльності з іншими суб’єктами сектору безпеки [95].

Ключову координаційну роль у реалізації державної кіберполітики відіграє Національний координаційний центр кібербезпеки при РНБО України (НКЦК), правовий статус і повноваження якого закріплено в Указі Президента № 242/2016 «Про Положення про Національний координаційний центр кібербезпеки» та оновлено Указом № 547/2025. В останньому уточнено функціональні компетенції Центру з урахуванням сучасних викликів – розширено повноваження з моніторингу кіберзагроз, координації реагування та забезпечення міжвідомчої взаємодії, що відображає перехід від дорадчої до оперативно-управлінської моделі діяльності [96; 122].

Таким чином, комплекс операційно-стратегічних актів Президента України та рішень РНБО забезпечує інституційне наповнення стратегічної рамки кібербезпеки, поєднуючи механізми раннього попередження, нейтралізації загроз, санкційного стримування та міжвідомчої координації [117-122]. У сукупності ці документи формують основу функціональної взаємодії між секторами безпеки, оборони та інформаційної політики, що забезпечує сталість і керованість державної системи кіберзахисту в умовах гібридних викликів [107; 111; 106].

Горизонтальні стратегічні документи формують інфраструктурне та інституційне «підґрунтя» кіберполітики, забезпечуючи її узгодженість із суміжними публічними політиками. Насамперед Стратегія розвитку сфери електронних комунікацій до 2030 року разом з операційним планом на 2025–2027 рр. визначає цільову модель мережевої інфраструктури, принципи її розвитку й управління та очікувані результати на середньострокову перспективу, що безпосередньо корелює з вимогами до кіберстійкості електронних комунікаційних мереж і послуг [128]. Важливим елементом міжсекторальної узгодженості є Стратегія боротьби з організованою злочинністю, у якій протидію кіберзлочинності інтегровано як структурну складову державної політики безпеки та правопорядку [127].

Технологічний вимір підтримується Концепцією розвитку штучного інтелекту, що встановлює етичні та безпекові орієнтири використання систем

ІІ у публічному та приватному секторах; такі орієнтири є релевантними для управління ризиками, сумісності та довіри до цифрових сервісів, у тому числі критичних [125]. Ризик-орієнтовану основу для захисту об’єктів життєзабезпечення закладено Концепцією створення державної системи захисту критичної інфраструктури, яка визначає засади ідентифікації, категоризації, координації та взаємодії учасників, що прямо підживлює кіберкомпонент безпеки КІ/КІІ [126].

Міжнародно-правовий вектор гармонізації забезпечує План заходів з виконання Угоди про асоціацію, який слугує процедурною рамкою адаптації національного регулювання у дотичних до кібербезпеки сегментах (електронні комунікації, захист даних, мережеві та інформаційні системи тощо) [96]. Нарешті, організаційна стійкість державного ІТ-сектору підсилюється змінами до Концепції ІТ-централізації у системі управління державними фінансами, що стандартизують підходи до ІТ-управління, сумісності та контролю, створюючи передумови для уніфікованого впровадження вимог кіберзахисту в публічних інформаційних системах [84].

Таким чином, зазначені горизонтальні акти не лише «підпирають» стратегічні цілі кібербезпеки інфраструктурно та процедурно, а й забезпечують узгодженість державної політики у сферах комунікацій, правопорядку, критичної інфраструктури, технологічного розвитку та європейської інтеграції [128; 127; 125; 126; 96; 84].

Горизонтальні стратегічні документи становлять важливий елемент системи національної кібербезпеки, забезпечуючи її міжгалузеву узгодженість і функціональну взаємодію з іншими напрямами державної політики. Зокрема, Стратегія розвитку сфери електронних комунікацій України до 2030 року, схвалена розпорядженням Кабінету Міністрів України від 4 червня 2025 р. № 546-р, разом з операційним планом на 2025–2027 рр. визначає цільову модель розвитку національної мережевої інфраструктури, її управління та стандарти технічної сумісності, що створює основу для підвищення кіберстійкості електронних комунікаційних систем [128].

У межах протидії злочинності вагоме місце посідає Стратегія боротьби з організованою злочинністю, затверджена розпорядженням КМУ від 16 вересня 2020 р. № 1126-р, яка вперше інтегрувала кіберкомпонент у систему заходів кримінально-правового реагування, підкресливши потребу у взаємодії силових органів, судових інституцій і приватного сектору у сфері кіберзлочинності [127].

Технологічний аспект підтримується Концепцією розвитку штучного інтелекту в Україні (розпорядження КМУ від 2 грудня 2020 р. № 1556-р), яка встановлює етичні, правові та безпекові принципи застосування ІІ, релевантні для розвитку національної кіберстійкості, довіри до цифрових сервісів і мінімізації ризиків автоматизованого втручання [125].

Основу для системного управління ризиками у сфері критичної інфраструктури формує Концепція створення державної системи захисту критичної інфраструктури (розпорядження КМУ від 6 грудня 2017 р. № 1009-р), яка визначає засади ідентифікації, категоризації та координації суб’єктів безпеки, поєднуючи фізичну й кіберкомпоненти захисту [126].

У міжнародному контексті План заходів з виконання Угоди про асоціацію між Україною та ЄС (постанова КМУ від 25 жовтня 2017 р. № 1106) забезпечує рамкову гармонізацію законодавства у сферах електронних комунікацій, захисту персональних даних і мережевої безпеки відповідно до європейських стандартів [126].

Водночас організаційну стійкість публічного сектору підсилює оновлена Концепція ІТ-централізації у системі управління державними фінансами (розпорядження КМУ від 3 березня 2020 р. № 215-р), що стандартизує підходи до управління інформаційними системами, їхньої сумісності та контролю, створюючи передумови для інтегрованого впровадження вимог кіберзахисту у державному секторі [84].

Узагальнюючи, слід зазначити, що ці стратегічні документи забезпечують нормативну, організаційну та технологічну підтримку реалізації державної кіберполітики, формуючи єдину логіку розвитку

цифрової інфраструктури, управління ризиками та забезпечення національної кіберстійкості [128; 127; 125; 126; 96; 84; 107; 111].

Перспективний оборонний вимір полягає у формуванні окремої компоненти кібероборони. Парламентське рішення про прийняття за основу законопроєкту щодо створення Кіберсил Збройних Сил України (постанова Верховної Ради № 4628-IX; законопроєкт від 03.09.2025) фіксує політичну волю інституціоналізувати військовий елемент національних кіберспроможностей [115; 131]. Дотично, у законопроєкті № 8087, який включено до порядку денного законом № 4586-IX від 03.09.2025, окреслено невідкладні кроки з посилення кіберзахисту державних інформаційних ресурсів та об’єктів критичної інфраструктури, що має підсилити практичну складову реалізації державної кіберполітики [82; 81].

Наукові оцінки підтверджують логіку багаторівневої конструкції «стратегія –планування –виконання –моніторинг». Зокрема, наголошується на системному зв’язку між актами РНБО/Президента (рамкова й доменна стратегії), планувальними документами (Указ № 37/2022) та щорічними урядовими планами, а також на потребі формалізації показників ефективності, ресурсної стабілізації й міжвідомчої координації із врахуванням суміжних стратегій (електронні комунікації, критична інфраструктура, оборона) [64; 17; 29; 151]. Раніше ідентифіковані проблеми імплементації Стратегії-2016 –фрагментарність підзаконної бази, нечіткий розподіл повноважень, кадрово-бюджетні обмеження та відсутність узгоджених планів реалізації і моніторингу – пояснюють акцент 2021–2025 рр. на процедуризації та координації виконання [43; 64; 153]. Комплексний огляд правової бази також підтверджує, що «ядро» чинної політики становлять Стратегія національної безпеки (2020) і Стратегія кібербезпеки (2021) у парі з Планом реалізації (2022) та щорічними урядовими планами (зокрема на 2025 р.), тоді як ключовими викликами залишаються сталість фінансування, роль НКЦК у координації, належний нагляд/аудит і

повноцінна інтеграція з режимом захисту критичної інфраструктури [256; 119; 117; 121; 97; 106; 112; 87].

Узагальнюючи, стратегічна рамка (Указ № 392/2020; Указ № 447/2021) у поєднанні з вмонтованими механізмами виконання (Указ № 37/2022; розпорядження КМУ № 204-р/2025) та підтримувальними секторальними політиками формує цілісну систему, в якій координація НКЦК, регулювання у сфері КІ/КІІ, організаційно-технічна модель кіберзахисту і державний аудит спроможностей утворюють «інфраструктуру виконання» [119; 117; 121; 97; 112; 87; 106; 95; 23; 24; 98; 101]. Подальший поступ прямо залежить від інституційної узгодженості та фінансової передбачуваності, на чому послідовно наголошують як академічні, так і прикладні джерела [64; 17; 29; 256].

Законодавчий рівень. Законодавчий рівень національної системи кібербезпеки становить ієрархічно впорядковану сукупність актів прямої дії (закони та кодифіковані закони), яка: (1) визначає засади державної політики, коло суб'єктів та механізми координації у сфері кібербезпеки; (2) установлює спеціальні правові режими захисту критичної інфраструктури та інформації; (3) регламентує електронну ідентифікацію, довірчі послуги, електронний документообіг і комунікації; (4) криміналізує суспільно небезпечні посягання у кіберпросторі та забезпечує процесуальні інструменти їх виявлення і розслідування. У такій конструкції «законодавче ядро» виконує інтегруючу функцію між технічними, організаційно-управлінськими та правозастосовними компонентами, задаючи нормативну рамку для підзаконних стандартів і стратегічних актів, що забезпечують реалізацію та розвиток відповідних приписів [17; 29; 151; 61].

Рамкові акти. Базовим законодавчим актом, який визначає системні засади державної політики у сфері кібербезпеки, є Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 р. Цей Закон встановлює основні принципи функціонування національної системи кібербезпеки, визначає суб'єктів сектору (зокрема

Службу безпеки України, Національний координаційний центр кібербезпеки при РНБО, Державну службу спеціального зв'язку та захисту інформації, Національну поліцію, Національний банк України тощо) та закріплює механізми взаємодії, координації і реагування на кіберінциденти [111; 89; 124; 112]. Системно пов'язаний із ним Закон України «Про критичну інфраструктуру» № 1882-IX від 16 листопада 2021 р., який уперше на нормативному рівні визначив категорії об'єктів критичної інфраструктури, критерії їх ідентифікації, принципи управління ризиками, а також базові вимоги до стійкості, безпеки та кіберзахисту критично важливих послуг [106; 23; 24; 95].

Функцію «техно-юридичного мосту» між зазначеними актами виконує Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР від 5 липня 1994 р., який заклав понятійно-категоріальний апарат, визначив загальні вимоги до комплексної системи захисту інформації та моделі забезпечення конфіденційності, цілісності й доступності (КЦД) інформації [103; 114; 113; 2].

Водночас загальнодержавні нормативні орієнтири визначають Закони України «Про національну безпеку України» № 2469-VIII від 21 червня 2018 р. та «Про інформацію» № 2657-XII від 2 жовтня 1992 р., які встановлюють системні принципи національної безпекової політики, визначають інформаційну безпеку як її складову та закріплюють правовий статус інформації як об'єкта правовідносин, що підлягає багаторівневому правовому захисту [107; 105; 90; 104].

Як справедливо підкреслює І. Діордіца, саме узгоджене функціонування цих рамкових актів забезпечує системність правового регулювання у сфері кібербезпеки та створює необхідні умови для реалізації міжвідомчої координації і належного балансу повноважень суб'єктів безпеки [29; 30; 61].

Ідентифікація, довіра, документообіг. Правову інфраструктуру електронної взаємодії в межах кібербезпекового простору України формують

низка спеціальних законів. Центральне місце серед них посідає Закон України «Про електронні довірчі послуги» № 2155-VIII від 5 жовтня 2017 р., який імплементує європейську модель eIDAS, встановлюючи правові засади функціонування кваліфікованих електронних підписів, печаток, сертифікаційних центрів та механізмів взаємного визнання електронних ідентифікацій [92; 86]. Йому кореспондують Закон України «Про електронні документи та електронний документообіг» № 851-IV від 22 травня 2003 р. і Закон України «Про хмарні послуги» № 2075-IX від 17 лютого 2022 р., який закріплює нормативний режим використання хмарних технологій у публічному секторі, включно з вимогами до захисту інформації в об’єктах критичної інфраструктури [93; 130; 94; 81].

У практичному вимірі зазначені інститути тісно пов’язані з режимами захисту державної таємниці й забезпечення доступу до публічної інформації (Закони № 3855-XII від 21.01.1994 р. і № 2939-VI від 13.01.2011 р.), а також з нормами, що регулюють оперативно-розшукову діяльність та протидію організованій злочинності (Закони № 2135-XII від 18.02.1992 р. і № 3341-XII від 30.06.1993 р.). Їх взаємодія забезпечує необхідний баланс між реалізацією прав людини у сфері доступу до інформації, потребами правоохоронних органів у розслідуванні кіберінцидентів та гарантіями національної безпеки [90; 91; 109; 110; 256]. Як відзначається в аналітичних дослідженнях, саме на перетині цих правових режимів формується сучасна модель «довірчої кіберінфраструктури», у якій правові, організаційні та технічні компоненти з’єднані в єдину систему забезпечення кіберстійкості держави [256; 35; 61].

Секторні та інституційні акти. Інституційний вимір національної системи кібербезпеки визначається сукупністю спеціальних законів, які встановлюють правовий статус, компетенцію та функціональні повноваження органів публічної влади у відповідній сфері. Ключове місце у цій структурі займає Закон України «Про Державну службу спеціального зв’язку та захисту інформації України» № 3475-IV від 23 лютого 2006 р., що закріплює повноваження служби у сферах технічного й криптографічного

захисту інформації, організації реагування на кіберінциденти, забезпечення функціонування державних інформаційних ресурсів, а також здійснення державного нагляду (контролю) у зазначеній галузі [89; 69; 70; 75].

Вагоме значення у системі кібербезпеки має також контррозвідувальна складова, нормативно визначена Законом України «Про Службу безпеки України» № 2229-XII від 25 березня 1992 р., який покладає на СБУ функції щодо виявлення, запобігання та нейтралізації кіберзагроз, спрямованих проти суверенітету, конституційного ладу й обороноздатності держави [124; 8; 32; 33]. Водночас стратегічний напрям цифрової трансформації держави інституційно підкріплюється Законом України «Про національну програму інформатизації» № 74/98-ВР від 4 лютого 1998 р., який визначає цілі, напрями та інструменти державної політики у сфері інформатизації, формує правові засади розвитку цифрових сервісів, телекомунікаційної та інформаційної інфраструктури, у тому числі з урахуванням безпекового компоненту [108; 60; 32].

Для об’єктів критичної інфраструктури особливої ваги набувають положення Закону України «Про захист персональних даних» № 2297-VI від 1 червня 2010 р., а також суміжні стандарти приватності та інформаційної безпеки, що формують нормативну основу для побудови систем управління інформаційною безпекою (СУІБ) [104; 44; 4]. Як слушно зауважує М. Ковалів, правовий режим обробки персональних даних у контексті КІ є елементом цілісної політики кіберзахисту, а не лише інструментом захисту приватності [44].

Кримінально-правові та процесуальні норми. Кримінально-правове забезпечення кібербезпеки в Україні становить окремий нормативний блок, інтегрований до Кримінального кодексу України (розд. XVI), де передбачено відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних систем (ст. 361), створення та розповсюдження шкідливих програмних чи технічних засобів (ст. 361-1), несанкціоновані дії з інформацією, яка обробляється в таких системах (ст. 362–363-1) [37; 134;

256]. Ці норми відображають еволюцію підходів до криміналізації кіберзлочинів та узгоджуються з положеннями Конвенції про кіберзлочинність [116; 184; 187; 188].

З метою підвищення ефективності реагування на кіберінциденти у 2022 р. було прийнято Закон України № 2137-IX, який вніс зміни до Кримінального процесуального кодексу та Закону «Про електронні комунікації», запровадивши механізми проведення слідчих дій «за гарячими слідами» і фіксації цифрових доказів [85; 94].

Подальший розвиток процесуально-правових інструментів забезпечено двома системними актами 2025 р. – Законом № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів і об’єктів критичної інформаційної інфраструктури», який унормував нові режими кіберзахисту, узгодив вимоги до комплексних систем захисту інформації (КСЗІ) та систем управління інформаційною безпекою (СУІБ); і Законом № 4542-IX «Про внесення змін до деяких законів України щодо удосконалення окремих питань діяльності Служби безпеки України», що уточнив компетенції СБУ у сфері кіберрозвідки та реагування на кібератаки [81; 83; 89; 103; 106; 111; 95; 98; 101].

Як відзначає С. Мазепа, зазначені новели відображають тенденцію до поступового поєднання адміністративних і кримінально-правових інструментів кіберзахисту, що свідчить про формування комплексного правового режиму протидії кіберзлочинності [63; 37].

Електронні комунікації та спадщина телекомунікаційного регулювання. Закон України «Про телекомунікації» № 1280-IV від 18 листопада 2003 р. історично відіграв визначальну роль у становленні правових основ національного телекомунікаційного сектору, проте із набуттям чинності Закону «Про електронні комунікації» (№ 1089-IX від 16 грудня 2020 р.) більшість його положень втратила актуальність. Новий закон увів сучасну концепцію електронних комунікаційних послуг, гармонізовану з

правом ЄС, визначив правила надання, регулювання та захисту комунікацій у цифровому середовищі, що має безпосередній зв'язок із забезпеченням кібербезпеки [129; 94; 136; 54].

У контексті національної системи кібербезпеки норми про електронні комунікації формують технічну основу для реалізації функцій з виявлення, моніторингу та запобігання кіберінцидентам. Як зазначає Д. Гнатченко, саме ефективна взаємодія між суб'єктами комунікаційного сектору та державними органами забезпечує належний рівень інформаційної безпеки в державі [12; 32; 33]. Водночас, як слушно зауважують О. Крет та Р. Крет, правове регулювання електронних комунікацій має узгоджуватися із базовими актами у сфері кібербезпеки для уникнення дублювання повноважень і колізій правозастосування [54; 136].

Законодавчі новели у сфері кібербезпеки 2022–2025 рр. Упродовж 2022–2025 рр. законодавство України у сфері кібербезпеки зазнало суттєвої модернізації, спрямованої на підвищення оперативності реагування держави на кіберзагрози та узгодження національних режимів із сучасними технологічними практиками. Важливим етапом стало ухвалення Закону України № 2137-IX від 15 березня 2022 р. «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам», яким закріплено процесуальні механізми оперативного реагування на кіберінциденти, визначено порядок фіксації цифрових доказів і розширено компетенції органів досудового розслідування у сфері кіберзлочинності [85; 94; 37; 134].

Подальше вдосконалення базових інститутів кібербезпеки забезпечив Закон України № 4336-IX від 27 березня 2025 р. «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури». Цим актом унесено комплексні поправки до Закону №

80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах», Закону № 2163-VIII «Про основні засади забезпечення кібербезпеки України» та Закону № 1882-IX «Про критичну інфраструктуру». Визначено єдині вимоги до кіберзахисту державних інформаційних ресурсів і критичної інфраструктури, унормовано підходи до функціонування комплексних систем захисту інформації (КСЗІ) та систем управління інформаційною безпекою (СУІБ), а також закладено організаційні основи національної системи реагування на кіберінциденти [81; 103; 111; 106; 95; 98; 101; 256].

Подальшу інституційну консолідацію у сфері кібербезпеки забезпечив Закон України № 4542-IX від 16 липня 2025 р. «Про внесення змін до деяких законів України щодо удосконалення окремих питань діяльності Служби безпеки України та підвищення її ефективності у зв'язку з участю у відсічі і стримуванні збройної агресії проти України». У межах цього закону конкретизовано кіберкомпетенції Служби безпеки України – насамперед у сферах контррозвідувальної діяльності в кіберпросторі, оперативного обміну інформацією та міжвідомчої координації у разі кібератак [83].

Таким чином, оновлення 2022–2025 рр. сформували багаторівневу структуру регулювання – від процесуальних механізмів до організаційної інтеграції суб'єктів безпеки. У цьому контексті особливої актуальності набуває питання узгодження нових законодавчих норм із підзаконною та методичною базою. У науковій літературі підкреслюється, що ефективність реалізації Стратегії кібербезпеки України безпосередньо залежить від синхронізації законодавчих оновлень із процедурним забезпеченням та діяльністю уповноважених органів; інакше норми залишаються декларативними [64; 256]. Аналогічну позицію висловлено в аналітичному звіті Міжнародної фундації виборчих систем «Правова база української кібербезпеки: загальний огляд і аналіз», де наголошено на необхідності усунення нормативної фрагментарності, чіткого розмежування компетенцій між суб'єктами та запровадження системного моніторингу імплементації стратегічних документів [256].

Отже, законодавчі новели 2022–2025 рр. істотно розширили нормативне поле кібербезпеки, створивши передумови для інтегрованої моделі державного реагування на кібератаки й інциденти. Водночас наукова доктрина підкреслює, що подальший поступ у цій сфері має супроводжуватися методичною уніфікацією, оновленням підзаконної бази та забезпеченням реальної, а не формальної стійкості кіберпростору [29; 30; 17; 61].

Рівень підзаконних актів і нормативно-технічних документів. Підзаконний і нормативно-технічний рівень правового регулювання кібербезпеки забезпечує імплементацію положень базових законів і стратегічних документів у конкретні процедури, стандарти та регламенти, що безпосередньо застосовуються суб'єктами системи кіберзахисту. Як зазначає І. В. Діордіца, цей рівень утворює «функціональну інфраструктуру» кібербезпеки, де загальні приписи законодавства набувають форми практичних вимог, протоколів і технічних норм [29; 30]. На думку Ю. А. Гульванської, підзаконні акти становлять «операційну основу реалізації» державної політики у сфері кіберзахисту, визначаючи інституційні зв'язки, технологічні стандарти та механізми координації [17].

Ключову групу становлять акти, що регламентують захист критичної інформаційної інфраструктури (КІІ). Постанова Кабінету Міністрів України від 19.06.2019 р. № 518 затвердила Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, які визначають мінімальні організаційні та технічні критерії, обов'язок проведення аудитів і сертифікації комплексних систем захисту інформації [95]. Їй відповідає постанова КМУ від 09.10.2020 р. № 943, що встановлює Порядок ідентифікації та категоризації об'єктів критичної інформаційної інфраструктури, порядок ведення реєстру та визначення критеріїв критичності [23]. Комплементарно постанова КМУ від 09.10.2020 р. № 1109 врегульовує деякі питання об'єктів критичної інфраструктури, уточнюючи організаційні засади формування переліків КІ та взаємодії відповідальних органів [24]. Завершує цей процедурний ланцюг

постанова КМУ від 11.11.2020 р. № 1176, яка затвердила Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації з вимогою щодо захисту [101]. У науковій літературі підкреслено, що зазначені документи вперше створили чітку адміністративно-процедурну систему для реалізації Закону «Про критичну інфраструктуру», наближену до стандартів NIS/NIS 2 Directive [2; 106; 207; 224].

Систему державного моніторингу та реагування на інциденти визначає постанова КМУ від 23.12.2020 р. № 1295 *«Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»*, якою створено централізовану мережу сенсорів, регламентовано обмін інформацією та взаємодію суб'єктів системи [22]. Подальший розвиток цього напряму закріплено постановою КМУ від 29.12.2021 р. № 1426, що затвердила *Положення про організаційно-технічну модель кіберзахисту*, визначивши структуру, механізми моніторингу, повідомлення про інциденти й розподіл повноважень між державними органами та приватними операторами [98]. Її офіційний Науково-практичний коментар ДССЗЗІ роз'яснює правові та технічні аспекти впровадження цієї моделі, підкреслюючи гармонізацію з міжнародними стандартами ISO/IEC 27001 [69; 257]. За слушним зауваженням В. В. Бухарєва, наявність узгоджених процедур реагування є необхідною умовою дієвості національної системи кіберзахисту [7].

Технічний блок підзаконного рівня становлять нормативи у сфері криптографічного й технічного захисту інформації. Постанова КМУ від 21.10.2020 р. № 991 затвердила *Технічний регламент засобів криптографічного захисту інформації*, що встановлює вимоги до сертифікації, маркування та державного нагляду за засобами КЗІ [102]. Регламент конкретизує положення Указу Президента № 505/98 *«Про порядок здійснення криптографічного захисту інформації в Україні»* [113] та Указу № 1229/99 *«Про технічний захист інформації в Україні»* [114]. Як зазначає

В. Л. Бурячок, ці документи створюють основу нормативно-технічної узгодженості між державними стандартами, вимогами безпеки та функціонуванням систем захисту інформації [6].

Організаційно-комунікаційна складова кіберзахисту врегульована постановами, що забезпечують міжвідомчу взаємодію і конфіденційний зв'язок. Постанова КМУ від 16.11.2002 р. № 1772 визначає *порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних і телекомунікаційних системах* [99]. Постанова КМУ від 14.05.2015 р. № 303 унормовує *організацію міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку (НСКЗ)* [25], а постанова КМУ від 11.10.2002 р. № 1519 встановлює *порядок надання послуг конфіденційного зв'язку органам державної влади, підприємствам та установам* [100]. Як слушно підкреслює Л. А. Веселова, практична дієвість національної системи кібербезпеки безпосередньо залежить від ефективності таких процедур захищеної міжвідомчої комунікації [10].

Важливим елементом інтеграції кіберзахисту в інфраструктуру електронного урядування є постанова КМУ від 16.09.2020 р. № 827, якою внесено зміни до *Положення про інтегровану систему електронної ідентифікації*, що ув'язує безпечний доступ до державних ресурсів із процедурою автентифікації користувачів [86]. Її реалізація, як підкреслюють М. Кравчук та В. Кравчук, сприяє створенню національної довірчої інфраструктури – необхідного елементу кіберстійкої держави [273]. Завершує підзаконний блок розпорядження КМУ від 07.03.2025 р. № 204-р, яким затверджено *План заходів на 2025 рік з реалізації Стратегії кібербезпеки України* – документ, що конкретизує терміни та виконавців упровадження ухвалених нормативних рішень [97].

Отже, підзаконні та нормативно-технічні акти деталізують положення законів і стратегій у практичні адміністративні процедури, стандарти й технічні вимоги. Вони визначають правила ідентифікації критичних об'єктів, критерії їхнього кіберзахисту, порядок державного контролю, організацію

моніторингу та реагування, вимоги до технічних засобів, захищеного зв'язку й електронної ідентифікації. Як підкреслює В. Л. Бурячок, саме така «інфраструктура виконання» забезпечує практичну реалізацію принципів кіберстійкості та підзвітності в державному секторі [6; 256].

Висновки до Розділу 1

1. Проаналізовано теоретичні підходи до визначення сутності поняття «кібербезпека». Встановлено, що воно сформувалося як міждисциплінарне явище, що поєднує технічні, правові, управлінські, соціальні та етичні виміри. Простежено еволюцію від вузької концепції інформаційної безпеки до комплексного розуміння кібербезпеки як соціотехнічної системи, спрямованої на забезпечення стійкого функціонування цифрового середовища.

2. З'ясовано дефінітивну невизначеність і фрагментарність термінології, пов'язаної з поняттями «інформаційна безпека», «кібербезпека», «кіберзахист» і «кіберстійкість». Обґрунтовано, що відсутність уніфікованих дефініцій зумовлює методологічну та нормативну неузгодженість. Підкреслено потребу гармонізації термінологічного апарату у науковій, освітній та правозастосовній практиці, що має забезпечити єдність мови кіберправа.

3. Систематизовано типологію підходів до визначення кібербезпеки – технократичні, організаційно-управлінські, правові, соціогуманітарні та освітньо-термінологічні. Встановлено, що кожен із них відображає окремий аспект феномену, однак лише їх інтеграція у межах системного підходу забезпечує цілісне уявлення про кібербезпеку як процес управління ризиками, довірою та стійкістю у цифровому просторі.

4. Обґрунтовано ключову роль людського фактора й етики інформації у структурі сучасної кібербезпеки. Людина розглядається як центральний

елемент соціотехнічної системи, носій компетентностей і цінностей, від яких залежить ефективність технічних і правових механізмів. Етика інформації визначається внутрішнім регулятором цифрової поведінки, що формує культуру довіри, прозорості й відповідальності у кіберпросторі.

5. Сформовано ієрархію референтних об’єктів захисту, яка відображає сучасне розширення предметного поля кібербезпеки: від даних і цифрових сервісів до критичної інфраструктури, соціальних відносин і публічних функцій держави. Такий підхід створює теоретичне підґрунтя для уніфікації категоріального апарату, підвищення міжвідомчої інтероперабельності та гармонізації національної системи кіберзахисту з міжнародними стандартами.

6. Запропоновано авторське визначення поняття «кібербезпека», відповідно до якого кібербезпека – це стан і безперервний процес забезпечення стійкого, правомірного та етично врегульованого функціонування цифрового середовища, що досягається через узгоджену взаємодію технологічних засобів, управлінських процедур, правових механізмів і поведінкових норм, спрямованих на захист даних, інфраструктур, соціальних відносин і публічних функцій держави від деструктивних впливів і забезпечення їх відновлюваності у разі порушень. Це визначення інтегрує технічні, правові, управлінські й етичні компоненти в єдину системно-комплексну модель кіберстійкості.

7. Досліджено та системно проаналізовано місце міжнародного права в системі глобальної та національної кібербезпеки, розкрито його роль як універсального регулятора цифрових відносин і водночас як інструмента легітимації державної політики у сфері кіберзахисту. Систематизовано основні напрями формування міжнародно-правового режиму кібербезпеки, зокрема діяльність ООН, ОБСЄ, Ради Європи та ЄС, а також позиції окремих держав щодо застосовності базових принципів міжнародного права до кібероперацій. Показано, що поєднання норм “твердого” та “м’якого” права,

механізмів довіри й публікації національних позицій формує динамічний, але узгоджуваний режим міжнародного кіберврядування.

8. З’ясовано та систематизовано зміст основних принципів міжнародного права, що мають безпосереднє значення для забезпечення кіберзахисту. Обґрунтовано їхню застосовність до цифрового середовища й показано, що суверенітет, невтручання, заборона сили, належна обачність та права людини утворюють нормативне підґрунтя сучасного міжнародно-правового режиму кібербезпеки.

9. Проведено комплексний аналіз міжнародно-правових механізмів протидії кіберзагрозам і кіберзлочинності. Встановлено, що сучасна система глобального кіберзахисту має поліцентричний характер і функціонує як цілісний «режимний комплекс», у межах якого поєднуються кримінально-правові, політико-правові та превентивно-дипломатичні інструменти. Визначено провідну роль Будапештської конвенції про кіберзлочинність і Другого додаткового протоколу як основи міжнародного співробітництва у сфері протидії кіберкриміналу, а також окреслено значення проєкту Конвенції ООН проти кіберзлочинності, санкційних механізмів Європейського Союзу та міждержавних заходів довіри ОБСЄ як взаємодоповнюючих елементів глобальної архітектури кібербезпеки.

10. Систематизовано міжнародно-правові механізми притягнення держав до відповідальності за шкідливу діяльність у кіберпросторі та доведено їх визначальне значення у формуванні глобального режиму кібербезпеки. Розкрито зміст і взаємозв’язок норм міжнародного права, що визначають підстави атрибуції, форми правових наслідків і межі правомірних контрзаходів. Узагальнено доктринальні підходи до проблеми атрибуції кібероперацій і публічних звинувачень, обґрунтовано критерії допустимого доказування та пропорційності державної реакції. Проаналізовано функціонування санкційних механізмів Європейського Союзу, діяльність ООН і ОБСЄ у сфері колективної превенції та деескалації, а також практичні

орієнтири міжнародних інституцій у забезпеченні операційного застосування норм відповідальності в національній політиці держав.

11. Системно проаналізовано загальні правові засади формування національної системи кібербезпеки України як багаторівневої соціотехнічної конструкції, що поєднує правові, організаційні, технологічні та управлінські компоненти. Визначено методологічні принципи – верховенство права, законність, пропорційність, підзвітність і ризик-орієнтованість – як основоположні для функціонування державної політики у сфері кіберзахисту. Обґрунтовано системність та адміністративно-правову визначеність суб'єктів публічного управління, їхню взаємодію та координацію з приватним сектором і громадянським суспільством. Доведено, що сучасна модель кібербезпеки формується на засадах структурно-ієрархічного підходу, у якому поєднуються правові норми, стандартизовані процедури реагування, організаційні механізми контролю і технічні інструменти забезпечення стійкості цифрового середовища.

12. Систематизовано стратегічну архітектуру державної політики України у сфері кібербезпеки як багаторівневу систему, що включає рамкові, доменні та операційно-стратегічні документи. Встановлено, що вона забезпечує послідовність цілей, інструментів реалізації та механізмів координації, утворюючи цілісну модель стратегічного управління у сфері кібербезпеки. Обґрунтовано, що ключовими її елементами є стратегічне планування, секторальна інтеграція, міжвідомча взаємодія та розвиток оборонного кіберкомпонента, а ефективність функціонування визначається інституційною узгодженістю, стабільністю ресурсного забезпечення та провідною координаційною роллю Національного координаційного центру кібербезпеки.

13. Проаналізовано законодавчі зміни 2022–2025 років, що спрямовані на оновлення режимів кіберзахисту державних інформаційних ресурсів і вдосконалення компетенцій суб'єктів безпеки. Узагальнено, що попри поступову гармонізацію нормативної бази, зберігається потреба у подальшій

уніфікації термінології, процедур та механізмів координації для підвищення ефективності національної системи кібербезпеки.

16. Проведено системний аналіз законодавчої бази національної системи кібербезпеки України. Визначено її структуру як багаторівневу систему нормативних актів, що регулюють ідентифікацію критичної інфраструктури, реагування на інциденти, сертифікацію засобів захисту та міжвідомчу взаємодію. Доведено, що подальший розвиток має орієнтуватися на стандарти ризик-менеджменту та кіберстійкості ЄС.

РОЗДІЛ 2
КІБЕРЗАГРОЗИ В УМОВАХ ГІБРИДНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

2.1. Кібероперації як інструмент сучасних воєн і конфліктів: еволюція форм та правова природа

У попередньому розділі було доведено, що національна система кібербезпеки України формується як складова публічно-правового механізму забезпечення національної безпеки, у межах якого правові, організаційні та технологічні елементи взаємодіють у єдиному стратегічному просторі [47; 49; 50; 59; 61; 151; 320; 355]. Проте така модель потребує перевірки на стійкість в умовах зовнішньої агресії, коли цифровий простір перетворюється на самостійний театр дій, здатний безпосередньо впливати на результати традиційних військових операцій. Логічним продовженням попередніх теоретико-правових висновків є звернення до практичного виміру – аналізу проявів кіберагресії в умовах сучасної гібридної війни.

Сучасні конфлікти розгортаються у багатовимірному середовищі, де класичні військові інструменти поєднуються з інформаційними, економічними та технологічними засобами впливу [246; 299; 321; 323]. Як слушно зазначають окремі західні дослідники, кіберпростір перетворився на арену стратегічної конкуренції, у якій межі між війною та миром, між діями державних і приватних суб’єктів дедалі частіше розмиваються [176; 299; 321]. У цьому контексті кібероперації постають не ізольованим явищем, а складовою ширшої системи політичного, інформаційного та військового впливу [232; 245]. Л. Келло справедливо підкреслює, що вони створюють «сірий простір» між дипломатією та війною, у якому технологічні інструменти виступають засобом демонстрації сили без формального оголошення збройного конфлікту [266; 278; 319].

Як зазначає І. Костенко, використання супутникових технологій у російсько-українській війні підтвердило тенденцію до мілітаризації кіберпростору: космічні платформи зв’язку, навігації та спостереження стали невід’ємним елементом цифрового поля бою, поєднавши кібернетичні та інформаційно-технічні інструменти у єдиному воєнному середовищі [271; 272; 274]. Український досвід останніх років переконливо свідчить, що кібератаки можуть набувати системного характеру, виконуючи розвідувальні, підривні або дестабілізаційні функції у загальній архітектурі воєнних дій [71; 75; 133; 195; 222; 268; 282]. Як показують вітчизняні дослідження, цифрові удари по об’єктах енергетики, телекомунікацій та державного управління стали складником комплексної агресії, спрямованої на підрив функціонування державних інститутів і деморалізацію суспільства [71; 133; 195; 206; 268; 273]. Подібні висновки підтверджуються й міжнародними джерелами, зокрема описами операцій NotPetya та Sandworm, які розглядаються як приклади скоординованого застосування шкідливих програм у поєднанні з інформаційно-психологічними кампаніями [243; 244; 289; 305].

Еволюцію сприйняття кіберкомпонента війни докладно проаналізовано в аналітичному звіті Національного інституту стратегічних досліджень [71; 166; 177; 222; 353]. На початковому етапі повномасштабного вторгнення фахівці та урядові структури різних країн відзначали, що очікуваної масштабної хвилі російських кібератак не відбулося, попри окремі інциденти у сферах енергетики, зв’язку й державного управління [166; 177; 261; 277; 279; 283]. Лише після квітневих повідомлень про спробу APT-атаки угруповання Sandworm (UAC-0082) із використанням Industroyer2 та знищувальних програм типу wiper для ураження систем управління енергомережами ситуація почала оцінюватися як етапна ескалація кіберконфлікту [182; 218; 219; 236; 305]. Відтоді міжнародні огляди та провідні ЗМІ дедалі частіше характеризують російську активність у цифровому просторі як кібервійну, що супроводжує конвенційні бойові дії

[166; 177; 195; 222; 353]. У цьому контексті аналітики НІСД підкреслюють: кіберпростір став самостійним виміром війни, перебуваючи у фокусі урядів, міжнародних організацій і провідних експертних центрів [71; 190; 292; 321].

Виходячи з цього, подальший виклад у межах Розділу 2 спрямований на виявлення закономірностей і правових наслідків кіберактивності, а також на з'ясування її внутрішньої логіки – від постановки політичних цілей до добору інструментів і засобів впливу [45; 46; 48; 51; 53; 56; 57; 58; 74; 141; 142; 281]. Підрозділ 2.1 присвячено уточненню базових понять і правових меж кібероперацій, що дозволяє розмежувати кіберагресію як форму державної дії від звичайної кіберзлочинності, яка підпадає під юрисдикцію кримінального права [142; 169; 184; 187; 247; 319; 327; 328; 345].

Підрозділ 2.2 ґрунтуватиметься на верифікованих емпіричних даних про наймасштабніші кібератаки, спрямовані проти України у 2014–2024 роках. Особливу увагу буде приділено їхній хронології, масштабам і технічним характеристикам, зафіксованим у міжнародних звітах та аналітичних оглядах [71; 75; 195; 215; 219; 222; 256]. Аналіз цих даних дозволить простежити еволюцію кібероперацій – від ураження енергетичних систем до атак на урядові ресурси й супутникові мережі – та визначити типові цілі, засоби й ефекти таких дій. Отримані результати слугуватимуть підґрунтям для подальшого дослідження вразливостей критичної інфраструктури та соціально-економічних систем у підрозділі 2.3, а також для аналізу правових аспектів протидії кіберагресії у підрозділі 2.4 [2; 44; 142; 268; 271; 272; 281; 320; 355].

Таким чином, Розділ 2 виконує роль логічного містка між доктринально-правовим осмисленням феномену кібербезпеки (Розділ 1) та розробленням практичних механізмів зміцнення кіберстійкості й міжнародної координації дій України (Розділ 3) [29; 30; 45–51; 59; 61; 63; 64; 71; 141; 256; 320]. У його межах не лише розкривається фактологічна основа воєнних кібероперацій, а й формулюється методологічна рамка для оцінки їхніх правових наслідків –через призму суверенітету, міжнародної

відповідальності та співвідношення між державними і приватними суб'єктами у кіберпросторі [*142; 213; 232; 233; 287*].

Для подальшого аналізу необхідно окреслити понятійні межі трьох споріднених, але різних феноменів – кіберагресії, кібероперації та кіберзлочинності. Їх розмежування має принципове значення як для визначення природи сучасних кіберконфліктів, так і для побудови адекватних механізмів правового реагування [55; 60; 65].

Кіберагресія розуміється як дії держави або осіб, що діють від її імені чи за її дорученням, спрямовані на досягнення політичних або військових цілей шляхом використання кіберпростору як середовища стратегічного впливу. Вони можуть охоплювати як прямі атаки на інформаційні системи, так і опосередковані форми тиску – дестабілізацію інформаційних ресурсів, підрив критичних інфраструктур, вплив на комунікаційні мережі чи публічну думку. Правова оцінка таких дій здійснюється в межах міжнародного публічного права – через принципи суверенітету, невтручання, заборони сили, реторсій і контрзаходів [48; 142; 169; 247; 317; 327; 339–343; 345]. Як зазначає М. Шмітт, саме у сфері кібероперацій проступають *«сірі зони»* міжмирного і воєнного станів, коли втручання не досягає порогу збройного нападу, але має значні політичні наслідки [319].

Кібероперація є ширшим техніко-організаційним поняттям – це спланована дія у кіберпросторі, спрямована на досягнення воєнних, розвідувальних чи операційно-тактичних цілей. Вона може бути як елементом кіберагресії, так і складовою оборонних або контррозвідувальних заходів. Л. Келло наголошує, що кібероперації створюють *«сіру зону»* між дипломатією та війною, виступаючи інструментом демонстрації сили без формального оголошення конфлікту [266].

Кіберзлочинність, натомість, охоплює кримінально протиправні дії окремих осіб або груп, що не мають ознак державної участі й підлягають переслідуванню за нормами національного кримінального законодавства. Її міжнародна координація забезпечується через механізми взаємної правової

допомоги і мережу контактних пунктів 24/7, закріплену Будапештською конвенцією Ради Європи 2001 року [116; 187–189]. Як відзначає Дж. Клаф, основна цінність Конвенції полягає у створенні «спільної мови криміналізації» та гармонізації процедур розслідування у цифровому середовищі [184].

На практиці ці правові режими можуть перетинатися. Одна й та сама подія нерідко має *«державний»* і *«кримінальний»* виміри – наприклад, коли державні структури використовують приватні хакерські групи як *proxy*-акторів або коли кримінальні інструменти застосовуються для виконання політичних завдань. Як підкреслює К. Айхензер, у таких випадках відповідальність розподіляється між індивідуальними виконавцями і державою, що їх контролює або підтримує, а реагування повинно здійснюватися у двох паралельних площинах: міжнародно-правовій (через санкції, реторсії, політичні заяви) та кримінально-правовій (через притягнення конкретних осіб і правову допомогу між державами) [212; 213; 319].

В українському контексті така подвійна система реагування реалізується через механізми національної системи кібербезпеки, побудованої за принципом багаторівневої координації суб’єктів безпеки і оборони [29; 30; 45–51; 59; 61; 63; 64; 71; 141; 256; 320]. Як слушно зазначають В. Ліпкан та І. Діордіца, ця система інтегрує організаційно-правові, оперативні та технічні компоненти, забезпечуючи єдність управління й реагування у кіберпросторі [29; 30; 61]. А. Тарасюк конкретизує її суб’єктний склад, визначаючи провідну координаційну роль Ради національної безпеки і оборони, Служби безпеки України та Державної служби спеціального зв’язку і захисту інформації [150; 151]. Водночас, як підкреслюють А. Лисеюк і Т. Свінцицька, умови воєнного стану потребують підвищеної оперативності, спільного моніторингу інцидентів і тісної взаємодії між урядовими структурами, приватним сектором та волонтерськими ініціативами [59].

Отже, дефінітивне й інституційне розмежування кіберагресії, кібероперацій і кіберзлочинності створює методологічну основу для подальшого аналізу у підрозділі 2.2, який спрямований на верифікацію конкретних випадків кібератак проти України [45; 142; 169; 212]. Такий підхід дозволяє не лише уточнити правові межі відповідальності, а й визначити характер сучасних кіберконфліктів – за цілями, засобами, ефектами й суб'єктною структурою.

Комплементарність кібердій у структурі гібридної агресії. Досвід сучасних воєн і конфліктів засвідчує, що кіберпростір перестав бути лише технічним середовищем комунікації – він перетворився на окремий, але не самодостатній вимір збройного протиборства. Кібероперації не створюють ізольованого «фронту» з миттєвим ефектом ураження, а функціонують у взаємозв'язку з іншими доменами – розвідувальним, інформаційно-психологічним, логістичним і кінетичним. Їхня динаміка підпорядковується загальній логіці гібридного конфлікту, у якому технічний вплив поєднується з політичними та соціальними інструментами тиску. Послідовність дій зазвичай включає етапи спостереження та збору розвідданих, впливу на інформаційні ресурси й сервіси, формування інформаційно-психологічного ефекту, підтримку управління і комунікацій, а також синхронізацію з наземними операціями [45; 46; 56; 57;142].

Як слушно зазначає Л. Келло, кібердії постають особливим різновидом «сірих операцій» – формою демонстрації сили та політичного тиску без формального переходу до стану війни [266]. На його думку, вони утворюють поле стратегічної конкуренції, у якому держава, приватний сектор і недержавні актори взаємодіють одночасно, часто поза межами усталених правових режимів [266]. Таким чином, кіберінструменти не замінюють традиційні засоби ведення війни, а посилюють їхню ефективність, забезпечуючи інформаційне прикриття, підтримку зв'язку, розвідку й вплив на морально-психологічний стан противника.

Особливістю українського досвіду протидії кіберагресії стало утвердження публічно-приватної моделі кіберстійкості. У сучасних умовах значна частина критичних сервісів і технологічних ресурсів перебуває у розпорядженні приватного сектору, що зумовлює необхідність партнерства між державними інституціями та технологічними компаніями. Саме приватні оператори стали активними учасниками кібероборони, забезпечуючи телеметрію, технічне укріплення інфраструктури, виявлення й нейтралізацію шкідливих програм типу *wiper*, а також безпосередню взаємодію з національними центрами реагування CERT-UA і CSIRT [141; 320; 355]. Водночас комерційні супутникові системи зв'язку, зокрема *Starlink*, стали ключовим елементом забезпечення безперервності комунікацій і логістики під час активних фаз агресії [268; 271; 272; 274].

Варто відзначити також феномен «горизонтальної» самоорганізації кіберспільноти, яка мобілізувалася на підтримку державних зусиль у вигляді волонтерських OSINT-проєктів, DDoS-кампаній та інформаційного протистояння. Ця активність істотно посилила національний потенціал кіберстримування, проте водночас створила низку правових і етичних дилем: проблеми атрибуції, ризики ескалації, порушення юрисдикційних меж і принципу пропорційності. З огляду на це, міжнародна й українська доктрина наголошують на необхідності державної координації таких ініціатив і вироблення прозорих правил взаємодії з офіційними структурами [180; 352; 213].

Українські науковці послідовно підкреслюють, що кіберстійкість держави має соціотехнічну природу: правові, організаційні, кадрові й етичні чинники є не менш важливими, ніж технічні рішення. Зокрема О. Романова обґрунтовує необхідність удосконалення механізмів координації міждержавних і міжсекторальних дій у сфері кібероборони [133].

Отже, кібердії у структурі гібридної агресії виступають не ізольованим видом воєнної активності, а інтегрувальним інструментом багатодоменного впливу, що забезпечує підтримку, синхронізацію та підсилення інших форм

протиборства. Їхня результативність полягає у здатності поєднувати технологічні, правові та організаційні механізми у єдину систему стратегічного реагування. Такий підхід визначає методологічне підґрунтя для подальшого аналізу конкретних кібератак проти України у 2014–2024 роках, який здійснюється у підрозділі 2.2.

Робоча типологія «цілі - інструменти - очікувані ефекти». З огляду на потребу належної доктринальної систематизації кіберагресії доцільно перейти від опису поодиноких інцидентів до аналітичної моделі, що фіксує сталі кореляції між політичними цілями, застосованими технічними засобами та їхніми реальними чи очікуваними наслідками. Така модель забезпечує порівнюваність кейсів, коректне співвіднесення операційних і правових параметрів та створює підґрунтя для подальшого розгляду у підрозділах 2.2–2.4 [2; 35; 44; 71; 194; 206; 215; 223; 224; 276].

1) Цільовий вимір кібероперацій

Спираючись на верифіковані публікації та звітні матеріали, виокремлюємо три домінантні напрями спрямування кібератак проти України у 2014–2024 роках.

1. Критична інфраструктура (СКІ) – енергетика, електронні комунікації, транспорт, фінансовий сектор, державні послуги. Домінуюча мета –порушення безперервності надання послуг, примус до ручних режимів, збільшення часу відновлення. Репрезентативним є зафіксовані у 2022 р. спроби втручання в енергосистему, які у публічній аналітиці пов’язувалися з діяльністю *Sandworm* [166; 195; 243; 282; 305]. Уразливість СКІ та потребу в превентивному управлінні ризиками послідовно підкреслено у вітчизняній літературі [3; 35; 44; 71; 95; 98; 101; 194].

2. Інформаційна довіра та дані – державні реєстри, урядові портали, системи моніторингу та телеметрії. Ціль полягає у спотворенні або знищенні даних і девальвації достовірності офіційних комунікацій. Міжнародні огляди початкової фази повномасштабної агресії фіксують реагування за участю приватних корпорацій (екстрений харднінг, телеметрія, анти-wiper заходи),

спрямоване на підтримання функціонування та довіри до цифрових сервісів [19; 71; 75; 215; 217; 223; 224].

3. Керованість, логістика і зв'язок – насамперед супутниковий сегмент як опора стійкого зв'язку у воєнний час. Йдеться про створення «сліпих зон» для командування, розриви у взаємодії військових і цивільних структур, деградацію каналів передавання даних. На початку 2022 р. повідомлялося про інциденти у секторі супутникових комунікацій, що негативно позначилися на мережевій зв'язності та логістиці [172; 196; 262; 335]. Паралельно фіксується критична залежність оборонних та гуманітарних операцій від систем супутникового доступу до Інтернету, передусім на базі платформ типу Starlink [271; 274]. Узгоджено з цим, українські звітні матеріали фіксують зростання навантаження на канали урядового зв'язку, інтенсивну міграцію сервісів у хмарне середовище та об'єктивну потребу у багаторівневому резервуванні [70; 71; 75; 130; 256].

Підсумовуючи, цільовий вимір демонструє не орієнтацію на разовий «руйнівний ефект», а послідовну ерозію функціональної стійкості державних і суспільних підсистем шляхом синхронізованого ураження критичних сервісів, довіри до даних і каналів керованості [44; 71; 195; 206; 215; 217].

2) Інструментальний вимір

У структурі кіберагресії засоби реалізації мають різну глибину впливу, рівень технічної складності та ступінь інтегрованості з іншими доменами сучасної війни. Аналіз верифікованих джерел дозволяє окреслити низку типових інструментів, що системно застосовуються проти України у 2014–2024 роках.

1. Руйнівні програми типу *wiper* (зокрема, *CaddyWiper*) – призначені для швидкого знищення даних і виведення з ладу інформаційних систем. Подібні інциденти неодноразово фіксувалися в українських мережах у 2022 році та мали на меті не лише технічну дестабілізацію, а й психологічний тиск на користувачів [236].

2. ICS/OT-операції – цільові втручання у промислові системи управління, що забезпечують функціонування енергетики, транспорту чи об’єктів критичної інфраструктури. Такі атаки характеризуються високим потенціалом деструктивності, оскільки навіть короткочасне порушення технологічного циклу може спричинити масштабні наслідки. Репрезентативним прикладом є спроби знеструмлення української енергосистеми у 2022 році, атрибуційно пов’язані з діяльністю угруповання *Sandworm* [243].

3. Компрометація ланцюгів постачання (*supply-chain attacks*) – один із найнебезпечніших напрямів, що полягає у поширенні шкідливого програмного забезпечення через довірені канали оновлень, партнерські зв’язки або постачальницькі мережі. Класичним прикладом стала атака *NotPetya* (2017), наслідки якої вийшли далеко за межі України, завдавши мільярдних збитків міжнародним компаніям. Подібна логіка була реалізована і у випадку інциденту *SolarWinds* (2020), який виявив глибинні ризики глобальної цифрової взаємозалежності [244; 214].

4. Порушення супутникових і комунікаційних систем (satcom-disruption) – форма цілеспрямованого впливу на інфраструктуру супутникового зв’язку, що забезпечує комунікаційну стійкість у воєнний час. Зокрема, на початку 2022 року було зафіксовано кібератаку на систему Viasat, наслідком якої стало часткове відключення користувачів та ускладнення логістичних процесів у зоні бойових дій [172; 262].

Окрім супутникового сегмента, потужний удар було завдано і по наземних телекомунікаційних мережах. Так, за повідомленням Reuters, 28 березня 2022 р. державний оператор Ukrtelecom зазнав масштабної кібератаки, що спричинила тимчасове порушення інтернет-з’єднання в масштабах усієї країни. Як зазначив голова Держспецзв’язку Ю. Щиголь, атаку було відбито, однак відновлення послуг потребувало додаткових ресурсів і часу [163].

Такі інциденти підтверджують багаторівневий характер кіберагресії, яка охоплює як супутникові, так і наземні елементи зв'язку, ускладнюючи керованість і координацію дій у критичні фази бойових операцій.

5. DDoS, фішинг, дефейсинг, соціальна інженерія – допоміжні, але постійно застосовувані засоби, що посилюють інформаційно-психологічний ефект основних операцій. Вони спрямовані на перевантаження каналів зв'язку, компрометацію облікових записів, дискредитацію офіційних ресурсів і створення хаосу в інформаційному середовищі. У деяких випадках такі дії здійснювалися із залученням волонтерських і проксі-груп, що ускладнює процес атрибуції [180].

Комплексний характер зазначених інструментів полягає у їх здатності взаємодоповнювати одне одного, утворюючи багаторівневу систему технічного, організаційного й інформаційного впливу. Як засвідчують офіційні матеріали Державної служби спеціального зв'язку, ефективність таких атак визначається не лише технологічною складністю, а й узгодженістю дій у межах загальної гібридної стратегії противника [75].

3) Ефектологічний вимір

У структурі кіберагресії наслідки мають багаторівневий характер, що охоплює технічні, організаційні, комунікаційно-психологічні та стратегічні площини впливу. Комплексне розуміння цих ефектів є необхідною умовою для оцінки реальної потужності кібероперацій та визначення пріоритетів державної політики кіберстійкості.

Технічні ефекти виражаються у порушенні працездатності інформаційних систем, деградації мережевої інфраструктури, збільшенні часу виявлення та відновлення після інцидентів (*MTTD/MTTR*), а також у втраті інтегрованості між окремими сегментами технологічних процесів. Зниження ефективності роботи критичних сервісів у більшості випадків є першим сигналом успішної атаки, що вимагає негайного реагування на рівні державних і корпоративних центрів кіберзахисту [206].

Організаційні ефекти проявляються у перевантаженні оперативних центрів реагування (*SOC/CSIRT*), переході на ручні або резервні процедури керування, зниженні швидкості комунікації між суб'єктами національної системи кібербезпеки, а також у необхідності залучення зовнішньої технічної допомоги. У національних звітах зазначається, що подібні обставини суттєво впливають на якість управлінських рішень і потребують сталих механізмів внутрішньої координації [2].

Комунікаційно-психологічні ефекти охоплюють девальвацію суспільної довіри до офіційних джерел інформації, дезорієнтацію населення та формування атмосфери невизначеності. Такі наслідки часто є цілеспрямованими: кібератаки супроводжуються інформаційно-психологічними кампаніями, спрямованими на послаблення морального стану населення та дискредитацію інституцій влади.

Стратегічні ефекти полягають в уповільненні процесів прийняття рішень, розсіюванні управлінської уваги, ускладненні логістичних і комунікаційних ланцюгів. У підсумку кібероперації здатні опосередковано впливати на воєнно-політичну динаміку, зменшуючи ефективність державного управління і підриваючи здатність до оперативної реакції в умовах воєнного стану [206; 2].

Узагальнюючи викладене, можна констатувати, що ефекти кіберагресії не обмежуються технологічними збоями – вони формують системну дестабілізацію, яка охоплює інституційну, комунікаційну та стратегічну сфери. Саме тому взаємозв'язок між цілями, інструментами та наслідками кібератак доцільно репрезентувати у вигляді зведеної типологічної моделі, що забезпечує уніфіковану основу для подальшого аналізу конкретних кейсів у підрозділах 2.2–2.4.

Цілі (що уражається)	**Типові інструменти та репрезентативні сюжети**	**Очікувані/спостережені ефекти**	**Відповідні правові режими реагування**

Критична інфраструктура (енергетика, зв'язок, транспорт, фінанси, держпослуги)	ICS/OT-операції; wiper-атаки; supply-chain компрометації (*NotPetya*). Приклад: спроби blackout, що пов'язують із *Sandworm* [243; 244; 75]	Технічні (безперервність, деградація); організаційні (перевантаження SOC/CSIRT, ручні процедури).	Міжнародне публічне право (суверенітет, невтручання); право нацбезпеки України; профільні закони.
Дані та довіра (реєстри, урядові портали, телеметрія, медіа)	wiper; дефейсинг; фішинг/соцінженерія; інфокампанії. Приклад: захист і відновлення урядових сервісів з участю корпорацій [313; 206].	Комунікаційні (підрив довіри); технічні (втрата цілісності/доступності даних).	Інформаційне та кримінальне право; стандарти співпраці за Будапештською конвенцією.
Керованість, логістика і зв'язок (у т.ч. супутниковий сегмент)	satcom-disruption; DDoS на комунікаційні вузли; порушення ланцюгів командування. Приклад: інциденти у мережах супутникового зв'язку на поч. 2022 р. [262; 172].	Стратегічні (деградація зв'язності, ускладнення логістики); організаційні (перехід на резервні канали).	Міжнародне гуманітарне право (за умов воєнного конфлікту); правові режими воєнного стану; публічно-приватна взаємодія.
Підтримка операцій/відволікання уваги (психологічний домен)	масовані DDoS; координація «горизонтальних» кіберініціатив; інформаційно-психологічні кампанії [180; 206].	Комунікаційно-психологічні (дезорієнтація, деморалізація); соціальні (мобілізація приватних суб'єктів).	Публічно-правові механізми координації/деескалації; міжнародна взаємодія й атрибуція.

Таблиця 2.1. Типологічна модель кіберагресії в умовах гібридної війни проти України (розроблено автором на основі: [243; 75; 244; 236; 172; 313; 206; 2; 75; 214; 276]).

Як вбачається з наведеної моделі, домінантні вектори кіберагресії проти України фокусуються на порушенні безперервності СКІ, девальвації довіри до даних і зниженні керованості, причому інструментарій поєднує технічні та інформаційні засоби. Запропонована схема є «каркасом» для уніфікованого розгляду кейсів у п. 2.2; кожен епізод надалі

співвідноситиметься за трьома осями – ціль, інструмент, ефект – із підтвердженням за наведеними джерелами.

Запропонована типологічна модель виконує функції: (а) стандартизації опису інцидентів (параметри «ціль – інструмент – ефект»); (б) виявлення інтенсивності та послідовності взаємодії технічних і організаційних чинників; (в) підготовки до правової кваліфікації інцидентів у площині державної відповідальності/суверенітету та кримінального переслідування (див. підрозділи 2.2–2.4). У такий спосіб типологія поєднує операційний вимір кіберагресії з правовими механізмами її нейтралізації, логічно продовжуючи положення Розділу 1 і готуючи перехід до Розділу 3.

Правові «сірі зони» у контексті кіберагресії. Аналіз характеру сучасних кібероперацій засвідчує, що їх правова природа досі перебуває у полі невизначеності. На відміну від традиційних форм збройної агресії, дії у кіберпросторі рідко мають однозначно ідентифікованого суб’єкта, чітко встановлений причинно-наслідковий зв’язок або безпосередні матеріальні наслідки. Саме ці чинники створюють «сірі зони» у міжнародному праві, де важко визначити, чи певний кіберінцидент становить втручання у внутрішні справи держави, порушення її суверенітету, чи акт застосування сили. Як зазначає М. Шмітт, у кіберпросторі традиційні пороги суверенітету й невтручання «розмиваються», а більшість дій відбувається нижче рівня, який запускає класичні механізми колективної безпеки [319].

Цю тезу підтверджує і практика кібератак проти України. Значна частина з них мала комбінований характер – одночасно технічний, інформаційно-психологічний та політичний. Вони не супроводжувалися прямими руйнівними наслідками, однак порушували стабільність державного управління, функціонування критичної інфраструктури та довіру громадян до офіційних джерел інформації. Відповідно, виникає питання кваліфікації таких дій: чи можуть вони розглядатися як застосування сили у розумінні статті 2(4) Статуту ООН, чи лише як недружній акт або реторсія у межах права держави на відповідь.

Наукова дискусія також стосується атрибуції – встановлення фактичного джерела кібератаки. Складність полягає у тому, що держави часто діють через проксі-групи або напівавтономні хакерські спільноти, що унеможливлює пряме доведення контролю й наміру. Як зауважує К. Айхеншер, у випадку з Україною 2014–2024 рр. міжнародне право продемонструвало недостатню ефективність у встановленні відповідальності держави, оскільки доказова база у кіберпросторі ґрунтується переважно на технічних сигнатурах, а не на формалізованих юридичних критеріях [212].

Не менш дискусійним є й питання меж взаємодії держави з приватним сектором, який володіє критичною інфраструктурою, комунікаційними мережами та інформаційними ресурсами. У більшості випадків саме приватні корпорації мають первинні дані телеметрії, журнали подій та цифрові артефакти, необхідні для атрибуції й реагування. Це породжує потребу у формуванні механізмів публічно-приватного партнерства, де держава та приватні компанії спільно забезпечують стійкість кіберпростору. У цьому контексті слушною є позиція К. Eichensehr про необхідність «спільної відповідальності» публічних і приватних акторів у підтриманні кібербезпеки [212; 213].

Отже, правові «сірі зони» у сфері кібербезпеки охоплюють три ключові виміри: суверенітет і невтручання – відсутність єдиних критеріїв для визначення порогу втручання у кіберпросторі [142; 327]; атрибуція та відповідальність –проблеми доказування контролю й наміру держави [212; 328]; публічно-приватна взаємодія –відсутність чітких правових процедур доступу до цифрових доказів, що належать приватним суб’єктам [21; 53; 320].

Вирішення цих питань є центральним для формування ефективного міжнародно-правового режиму протидії кіберагресії. У подальшому дослідженні (див. підрозділ 2.4) буде деталізовано правові механізми атрибуції, координації суб’єктів та застосування контрзаходів у межах міжнародного й національного права.

2.2. Основні кібератаки проти України (2014–2024): правова оцінка та інституційні уроки

Для забезпечення достовірності аналітичних висновків підрозділ базується на принципі подвійної верифікації фактів, відповідно до якого кожен зафіксований кіберінцидент підтверджується щонайменше двома незалежними джерелами – офіційним та аналітичним. Такий підхід відповідає вимогам академічної доброчесності й забезпечує належний рівень доказовості реконструкції подій, що мають суспільно-правове значення.

Верифікаційний каркас утворюють перевірені масиви даних національного та міжнародного рівнів:

– річний звіт Оперативного центру реагування на кіберінциденти ДССЗЗІ України за 2024 р., що містить офіційні показники виявлених атак, векторів проникнення та заходів реагування [75] ;

– *CSO Online Timeline of Russian-linked Cyberattacks on Ukraine* (2022) [166], який подає послідовну хронологію ключових подій з 2014 р.;
– *European Parliamentary Research Service (EPRS) Briefing: Russia's War on Ukraine – Timeline of Cyberattacks* (2022) як еталон для перехресної перевірки та зіставлення фактів [222];

– трекер *CyberPeace Institute* [195], що фіксує атаки на об'єкти критичної інфраструктури та цивільні цілі з урахуванням галузевої та часової диференціації.

Для інтерпретації масштабів та інтенсивності атак використано також аналітичні публікації *Foreign Affairs, The Wall Street Journal, The Washington Post , The Hill* та *Politico*, у яких висвітлюється дискусія щодо очікуваної «великої кібервійни» та реального спектра російських дій у цифровому просторі [177; 353; 277; 279; 280; 265; 283]. Це дозволяє співвіднести офіційні показники з міжнародними оцінками наслідків і характеру кіберагресії.

На основі верифікованих джерел виокремлено три послідовні фази ескалації кібератак проти України у 2014–2024 роках.

Фаза I (2014–2016) охоплює період перших цілеспрямованих дій проти об’єктів критичної енергетичної інфраструктури. Атаки, здійснені угрупованням *Sandworm* із використанням шкідливих програм *BlackEnergy* та *Industroyer*, призвели до короткочасних відключень електропостачання та стали першим у Європі підтвердженим випадком ураження систем керування технологічними процесами (ICS/OT) [243; 305; 199; 206]. Ці події позначили початок перманентної кіберконфронтації у гібридному форматі, коли технічні засоби втручання поєднувалися з інформаційним тиском.

Фаза II (2017–2020) характеризується переходом від точкових атак до руйнівних кампаній у ланцюгах постачання (*supply chain*). Наймасштабнішою серед них стала атака *NotPetya*, реалізована через компрометацію українського бухгалтерського програмного забезпечення *M.E.Doc*. Цей інцидент набув глобального резонансу, уразивши понад 60 держав і великі транснаціональні корпорації, що засвідчило трансграничний характер сучасних кіберзагроз та їх потенційну здатність спричиняти економічні наслідки, співмірні з воєнними [244; 289; 206].

Фаза III (2021–2024) стала періодом найвищої інтенсивності кіберактивності, що супроводжувала повномасштабну збройну агресію Російської Федерації проти України. У цей час зафіксовано серії атак типу *wiper* (*HermeticWiper*, *CaddyWiper*, *Industroyer2*), масовані *DDoS*-атаки на фінансові установи та державні інформаційні ресурси, а також резонансні інциденти у сфері супутникового зв’язку (*KA-SAT, Viasat*) [218; 219; 236; 182; 198; 249; 172; 196; 262; 314; 333; 335; 282; 313; 195]. Ця фаза характеризується не лише підвищенням технічної складності атак, а й інституціоналізацією державно-приватного партнерства у сфері кіберзахисту: провідні ІТ-компанії (*Microsoft*, *Starlink*) були залучені до оперативного реагування та підтримки стійкості українських комунікаційних мереж [282; 313; 274; 352; 206].

Таким чином, еволюція кібератак проти України від 2014 до 2024 року демонструє перехід від експериментальних операцій до системних, багаторівневих дій із поєднанням технічних, інформаційних та організаційних засобів впливу.

Для систематизації отриманих даних розроблено таблицю-матрицю, що поєднує типологію кібератак, визначену у підрозділі 2.1.3, із фактичними інцидентами 2014–2024 років. Класифікаційна модель побудована з урахуванням міжнародних підходів до менеджменту кібербезпеки критичної інфраструктури [194; 276] і слугує базою для подальшого аналізу ключових кейсів (2.2.2) та узагальнення уроків десятиліття (2.2.3).

Тип атаки	Ключові інциденти та джерела підтвердження
ICS/OT-атаки на критичну інфраструктуру (Sandworm, BlackEnergy, Industroyer)	Цільові атаки на енергетичні компанії *«Прикарпаттяобленерго»* (грудень 2015) і *«Київобленерго»* (грудень 2016) призвели до відключень електропостачання. Це перші в Європі задокументовані ураження систем керування технологічними процесами (ICS/OT). [166; 222; 75; 243; 195].
Supply-chain атаки (ланцюги постачання) – NotPetya	Масштабна атака *NotPetya* (червень 2017) через компрометацію українського бухгалтерського ПЗ *M.E.Doc* уразила держустанови, банки, транспорт, ЗМІ, а також міжнародні компанії (Maersk, Merck, FedEx). Визнана найруйнівнішою кібератакою сучасності. [244; 166; 222; 195].
Wiper-атаки (руйнівне шкідливе ПЗ) – HermeticWiper, CaddyWiper, Industroyer2, IsaacWiper	Серії wiper-атак у лютому–квітні 2022 р. супроводжували початок повномасштабної агресії РФ. Уражено державні органи, фінансовий сектор і енергетику. *Industroyer2* (квітень 2022) – новий варіант шкідливого ПЗ для знищення систем управління енергомережами. [75; 166; 222; 195; 236].
DDoS-атаки на урядові та фінансові ресурси	Масовані DDoS-атаки на вебресурси *Міністерства оборони*, *Збройних Сил України*, *ПриватБанку*, *Ощадбанку* (лютий 2022), а також на *Ukrtelecom* (березень 2022), спрямовані на порушення стабільності фінансових і комунікаційних сервісів. Частина атак супроводжувалась фішингом та інформаційними вкидами. [166; 222; 75; 249; 163].
SatCom-атака на супутникові мережі – Viasat KA-SAT	24 лютого 2022 р. здійснено багаторівневу атаку на супутникову мережу *Viasat KA-SAT*, що призвела до збоїв зв'язку в Україні та країнах ЄС. У травні 2022 р. офіційно атрибутована США та ЄС до російського ГРУ [262; 314; 172; 222; 166].
Інформаційно-	Проведення інформаційно-психологічних операцій (*deepfake*-відео зі

психологічні операції та дезінформаційні кампанії (ІПО)	«зверненням» Президента України, березень 2022; кампанії *Ghostwriter* і *Gamaredon*; масові дезінформаційні дії в соцмережах). Встановлено синхронізацію таких кампаній із військовими подіями [222; 185; 177; 353; 265; 279].

Таблиця 2.1 – Матриця відповідності типів кібератак та інцидентів (2014–2024 рр.)

Таким чином, наведена таблиця-матриця відображає поступову трансформацію кіберагресії проти України – від цільових атак на промислові системи керування до багатовекторних кампаній, що поєднують технічні, інформаційно-психологічні та комунікаційні засоби впливу. Узагальнення цих даних дає змогу виявити закономірності еволюції кібератак у межах гібридної війни та визначити їх вплив на формування правових і організаційних засад національної кібероборони.

Виходячи з результатів проведеної систематизації, у наступному підрозділі розглядаються конкретні прецедентні кейси, які мали визначальний вплив на розвиток правових механізмів протидії кіберагресії та міжнародну практику реагування.

Подальший аналіз спирається на верифіковані у попередньому підрозділі дані та має на меті юридичне осмислення найбільш значущих кібератак проти України у 2014–2024 роках. Оцінювання здійснюється крізь призму норм міжнародного публічного права та міжнародного гуманітарного права, принципів атрибуції державної участі у кіберпросторі, а також стандартів захисту критичної інформаційної інфраструктури. Такий підхід дозволяє перейти від суто фактологічного опису до правової кваліфікації дій як складових гібридної агресії та, відповідно, виокремити узагальнені правові уроки для подальшого розвитку національної системи кібербезпеки.

Для кожного кейсу застосовується єдиний аналітичний шаблон: (а) Контекст і масштаб – часові рамки, об’єкти ураження, встановлені наслідки; (б) Технічна природа / вектор – ключові інструменти, уразливості, спосіб реалізації; (в) Правова кваліфікація – релевантні норми (суверенітет,

невтручання, відповідальність держав, IHL щодо цивільної інфраструктури); (г) Узагальнений правовий урок – висновок про правову природу інциденту та його значення для правозастосовної практики.

Енергетика / Sandworm: BlackEnergy - Industroyer / Industroyer2. У грудні 2015 року в Україні було зафіксовано масштабну цілеспрямовану кібератаку на об'єкти електроенергетики, наслідком якої стало тимчасове припинення електропостачання в окремих регіонах країни. Подібний інцидент повторився наприкінці 2016 року, що, як наголошується у дослідженні *European Parliamentary Research Service*, засвідчило системний характер дій, спрямованих на ураження індустріальних систем управління (ICS/SCADA) та стало одним із перших підтверджених випадків використання кіберзасобів проти критичної інфраструктури держави в Європі [222].

Згідно з аналітичними матеріалами Європейського парламенту, зазначені атаки були частиною тривалої кампанії угруповання *Sandworm*, що діяло під контролем російських державних структур, і стали початком персистентної кіберагресії проти України, яка тривала у 2014–2022 роках та характеризувалася послідовним ураженням секторів енергетики, телекомунікацій та державного управління [222]. Як зазначає *A. Greenberg* у виданні *WIRED*, у квітні 2022 року було зафіксовано спробу відновлення аналогічного сценарію – так званого «третього блекауту», здійсненого з використанням модернізованої версії шкідливого програмного забезпечення *Industroyer 2*, що уможливлює безпосередню взаємодію з протоколами енергетичних підстанцій [244]. Дослідники ототожнюють цю операцію з діяльністю угруповання *Sandworm*, вказуючи на її технологічну спадковість від атак 2015–2016 років [243; 305].

Таким чином, у сукупності наведені факти підтверджують, що атаки на енергетичну інфраструктуру України становлять послідовну ескалацію кіберактивності державного походження, спрямовану на ураження критично

важливих об’єктів, і розглядаються в європейських аналітичних джерелах як складова гібридної агресії проти України [243; 244; 222].

Технічна природа. Кібератаки 2015–2016 років були спрямовані безпосередньо на операційний (OT) рівень енергосистем України. Як засвідчує технічний аналіз компанії *Mandiant (Google Cloud)*, у цих інцидентах було застосовано інструменти родини *Industroyer*, здатні взаємодіяти з промисловими протоколами керування підстанціями, зокрема *IEC-104* та *IEC-61850*, що забезпечило можливість безпосереднього втручання в процеси розподілу електроенергії [305].

Подальший розвиток діяльності угруповання *Sandworm* у 2022 році засвідчив зміну тактичної моделі – від використання спеціально розробленого шкідливого програмного забезпечення до застосування прийомів типу *living-off-the-land*, які передбачають використання легітимних системних інструментів для здійснення шкідливих дій і приховування слідів атаки. У звіті *Mandiant* зазначено, що така еволюція методів свідчить про підвищення рівня операційної складності та адаптації кіберінструментарію до умов активного протиборства [305].

Правова кваліфікація. Кібератаки угруповання Sandworm, пов’язаного за відкритими урядовими та технічними звітами з підрозділом ГРУ РФ (GTsST, в/ч 74455) [243; 305], кваліфікуються як порушення суверенітету України. Відповідно до положень *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Rule 4), будь-яке несанкціоноване втручання в інформаційні чи технічні системи іншої держави, що спричиняє шкоду або перешкоджає здійсненню її суверенних функцій, становить порушення суверенітету [317; 318]. У даному випадку йдеться про цілеспрямоване втручання у промислові системи управління енергетичними підстанціями (ICS/SCADA), наслідком чого стало відключення енергопостачання, тобто пряме порушення функцій держави з підтримання життєво важливої інфраструктури [305; 222].

Такі дії також підпадають під кваліфікацію незаконного втручання у внутрішні справи держави. Як зазначено у *Tallinn Manual 2.0* (Rule 66), втручання має місце тоді, коли одна держава примушує іншу змінити поведінку у сфері її виключної компетенції – у даному разі в енергетичному секторі [317]. За умови встановлення державної атрибуції, діяльність угруповання Sandworm становить міжнародно-протиправний акт, який тягне міжнародну відповідальність відповідно до *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA, 2001) [345]. Такий висновок узгоджується з офіційними заявами Європейського Союзу, Сполучених Штатів та інших держав щодо атрибуції російської кіберактивності проти України [190], а також із технічними оцінками компанії *Mandiant (Google Cloud)* і аналітичними даними CERT-UA [305].

Кейс Sandworm засвідчує системний характер кіберзагроз, спрямованих проти операційного (OT) сегмента критичної інфраструктури, та виявляє потребу у посиленні правових механізмів атрибуції і документування кіберінцидентів як передумови реалізації міжнародної відповідальності держав. Він також демонструє, що межа між технічним фіксуванням події і правовою кваліфікацією має бути інституційно забезпечена – через розвиток національних процедур реагування, збереження цифрових доказів і співпрацю з міжнародними структурами (CERT-UA, CCDCOE, EU Cyber Rapid Response Teams) [243; 305].

Як слушно зауважує K. Eichensehr [212; 213], кібератаки проти критичної інфраструктури під час міжнародних збройних конфліктів «випробовують межі існуючих правил» і засвідчують нагальну потребу в подальшій кодифікації міжнародно-правових норм щодо деструктивних і гібридних кібероперацій. Цей висновок узгоджується з практикою України, яка продемонструвала, що навіть “обмежені” кібератаки можуть мати системно дестабілізуючий ефект, а отже потребують правового реагування на рівні міжнародних інституцій і державної атрибуції. Отже, основний урок полягає в тому, що ефективне реагування на кібератаки державного

походження потребує інтеграції технічного, доказового та правового виміру, а також міжнародного визнання актів атрибуції як елемента формування сталого кіберправопорядку [212; 213; 305].

NotPetya глобальна supply-chain атака. 27–28 червня 2017 року внаслідок компрометації системи оновлень українського бухгалтерського програмного забезпечення M.E.Doc відбулася одна з наймасштабніших кібератак сучасності – NotPetya (ExPetr). За даними *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, шкідливе програмне забезпечення поширювалося через централізоване оновлення M.E.Doc, що використовувалося більшістю українських підприємств і державних установ. Первинним вектором ураження стали організації публічного та приватного секторів України (понад 80% усіх інфікованих систем), проте згодом вірус вийшов за національні межі й уразив міжнародні компанії – Maersk, Merck, FedEx, Saint-Gobain та інші [289].

Як зазначається у звіті *European Parliamentary Research Service (EPRS)*, атака призвела до знищення близько 13 000 пристроїв в органах влади, банківських структурах, поштових службах і транспортній інфраструктурі України, а також спричинила зупинку системи радіаційного моніторингу на Чорнобильській АЕС. Вірус поширився щонайменше у 65 країнах, уразивши близько 50 000 систем, а сукупні економічні втрати перевищили 10 млрд доларів США [222].

Технічний вектор. Згідно з аналітичними матеріалами *CCDCOE* і технічними звітами *Microsoft*, NotPetya використовував експлойт EternalBlue, розроблений, ймовірно, Агентством національної безпеки США (NSA) і згодом оприлюднений хакерською групою *Shadow Brokers* [289; 282]. Після первинного зараження шкідник поширювався внутрішніми мережами, використовуючи вразливість протоколу SMB, а також інструменти для викрадення облікових даних (*Mimikatz*). Функціонально вірус імітував ransomware, вимагаючи викуп у біткоїнах, однак, як доведено у технічному розборі *Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating*

Cyberattack in History" [244], механізм дешифрування фактично був відсутній, що унеможливлювало відновлення даних. Отже, реальна мета атаки полягала не у фінансовій вигоді, а у нанесенні економічної шкоди українським установам шляхом безповоротного знищення інформації.

Правова оцінка. У міжнародно-правовому контексті кібератака NotPetya (2017) розглядається як показовий приклад складності визначення меж державної відповідальності за дії у кіберпросторі. Як підкреслює *Kristen E. Eichensehr* у статті *"Ukraine, Cyberattacks, and the Lessons for International Law"* [212], серія кібератак проти України, включно з NotPetya, поставила питання про застосування принципів суверенітету, невтручання та належної обачності (due diligence). Авторка зазначає, що держави по-різному інтерпретують, чи становлять такі дії порушення суверенітету, і що відсутність єдиного підходу свідчить про нормативну невизначеність у правовому режимі кібероперацій. Eichensehr не дає остаточної кваліфікації NotPetya, але наголошує, що саме такі інциденти актуалізують необхідність уточнення правових стандартів атрибуції та відповідальності держав у кіберпросторі.

З технічної та політичної перспективи, *Andy Greenberg* у статті *"The Untold Story of NotPetya, the Most Devastating Cyberattack in History"* характеризує NotPetya як операцію, що мала «руйнівний ефект, несумісний із мотивами здирництва» [244]. Автор наголошує, що шкідливий код був розроблений і запущений групою Sandworm, пов'язаною з Головним управлінням розвідки ЗС РФ (GRU), і став інструментом геополітичного впливу, спрямованим на дестабілізацію України, а не на економічний прибуток. У статті не використовується юридична кваліфікація нападу, але описується масштаб і свідомий державний характер дії, що створило передумови для подальших міжнародно-правових оцінок.

Аналітичний огляд *C. Brumfield* у матеріалі *"Russia-linked Cyber-Attacks on Ukraine: A Timeline"* [166] підтверджує, що NotPetya стала переломним моментом еволюції російських кібератак, демонструючи здатність державних

акторів застосовувати шкідливе ПЗ для масштабних деструктивних операцій проти критичної інфраструктури України. Автор описує її як «найруйнівнішу атаку в історії», що позначила зростання рівня організованості та стратегічного характеру російських кіберактивностей.

Отже, атака NotPetya показала, що компрометація ланцюгів постачання програмного забезпечення (software supply chain) створює системні правові виклики, які виходять за межі традиційних концепцій державної відповідальності. У таких інцидентах одночасно задіяні державні органи (як ініціатори або куратори) та приватні компанії (як носії вразливостей і жертви), що формує змішану модель відповідальності й ускладнює атрибуцію дій у міжнародному праві. NotPetya засвідчила, що навіть локальна атака, спрямована проти однієї держави, може спричинити транскордонну шкоду, порушуючи принципи належної обачності та створюючи підстави для перегляду підходів до кібербезпеки критичної інфраструктури у глобальному вимірі.

KA-SAT / Viasat – супутникові комунікації. 24 лютого 2022 р., у день початку повномасштабного вторгнення Російської Федерації в Україну, було зафіксовано масштабну кібератаку на супутникову мережу KA-SAT, оператором якої є компанія Viasat Inc.. За повідомленням *Wired* [172], атака порушила роботу супутникового широкосмугового доступу до Інтернету на території України та в низці європейських країн, вивівши з ладу «десятки тисяч модемів, що використовувалися як для військових, так і для цивільних потреб» і спричинивши значний spillover-ефект за межами України.

Як зазначає *Reuters* [262], зловмисники вивели з ладу модеми, які забезпечували з’єднання з супутником KA-SAT, що надавав доступ до Інтернету клієнтам у Європі, включно з українськими державними структурами, енергетичними операторами та комерційними користувачами. Унаслідок цього «частина абонентів залишалася без зв’язку протягом тижнів після нападу», а масштаб інциденту охопив кілька держав-членів ЄС.

Європейська парламентська дослідницька служба (EPRS) у своєму аналітичному звіті *Russia's War on Ukraine: Timeline of Cyber-Attacks* [222] віднесла інцидент Viasat до категорії транскордонних атак на цивільні комунікаційні мережі, підкресливши, що операція відбулася «за годину до початку вторгнення» і мала наслідки для розповсюдження гуманітарних та урядових даних у Європі, що створило ризики для безпеки цивільного сектору.

Згідно зі спеціальним звітом *Microsoft "Special Report: Ukraine – An Overview of Russia's Cyberattack Activity in Ukraine"* (2022) [282], атака на KA-SAT стала першим підтвердженим випадком застосування руйнівних дій проти супутникової інфраструктури у рамках російської агресії, спрямованих на порушення комунікацій між цивільними та військовими користувачами України. Microsoft підкреслює, що цей епізод відкрив новий етап ескалації кібероперацій, оскільки він поєднав елементи інформаційної війни та фізичної дестабілізації зв'язку.

Атрибуція. 10 травня 2022 р. Європейський Союз, Сполучені Штати Америки та Велика Британія публічно поклали відповідальність на Російську Федерацію за кібератаку на супутникову мережу Viasat KA-SAT, що відбулася 24 лютого 2022 р. у перші години повномасштабного вторгнення в Україну. У Декларації Ради ЄС від імені Високого представника Європейського Союзу із закордонних справ та безпекової політики (*Council of the European Union, 2022*), зазначено, що «Європейський Союз та його держави-члени вважають Російську Федерацію відповідальною за кібератаку проти мережі супутникового зв'язку KA-SAT, що належить компанії Viasat». У документі підкреслено, що ця атака «мала значний вплив на громадян, бізнес та державні установи по всій Європі» і стала частиною ширшої кампанії з дестабілізації України [190].

Уряд Великої Британії, через Національний центр кібербезпеки (*NCSC*), оприлюднив того ж дня узгоджену позицію:

“The UK Government assesses that the Russian military was behind the cyber-attack with Europe-wide impact on Viasat one hour before the invasion of Ukraine” [190]. У заяві наголошувалося, що це був свідомо спланований напад з метою «порушення українських військових комунікацій» і «впливу на європейських користувачів цивільних супутникових послуг».

Паралельно Державний департамент США (*U.S. Department of State, 2022*) офіційно підтвердив аналогічні висновки, підкресливши, що атака на SATCOM-інфраструктуру KA-SAT була частиною російської кампанії «спрямованої на підрив і дестабілізацію суверенітету України». Заява містила узгоджену атрибуцію, погоджену з партнерами з ЄС та Великої Британії, і назвала цей інцидент першим випадком колективної міждержавної реакції на російську кібератаку у 2022 р [333].

Аналітичні огляди, зокрема *CyberScoop*, відзначили, що координація публічних атрибуцій трьох провідних державних блоків – ЄС, США та Великої Британії – стала прецедентом спільного офіційного визнання кібератаки як дії, здійсненої державним суб’єктом, що демонструє посилення практики колективної атрибуції в міжнародному правопорядку [196].

Джерело *Wired* підтвердило технічні аспекти, описавши атаку як «масштабну операцію з виведення з ладу десятків тисяч модемів, що обслуговували цивільні й урядові структури в Україні та ЄС», яка стала «першою зафіксованою кібероперацією в день початку війни» [172].

Правова кваліфікація. Інцидент KA-SAT стосувався цивільних супутникових послуг і мав транскордонні наслідки: виведення з ладу тисяч модемів спричинило перебої зв’язку в Україні та низці держав ЄС. У брифінгу Європейського парламенту це віднесено до переліку кібератак із впливом на цивільні комунікації, що “могли поширитися на інші країни й спричинити системні ефекти”, із прямими згадками про ризики для доступу до базових послуг та загрозу безпеці громадян Європи. Це піднімає питання порушення суверенітету/невтручання і рамок міжнародної відповідальності

за транскордонну шкоду, завдану цивільному зв'язку під час збройного конфлікту [222].

Кейс-стаді CyberPeace Institute системно фіксує публічні атрибуції (ЄС, США, Велика Британія) й кваліфікує атаку як таку, що націлювалася на супутникові модеми KA-SAT та деактивувала їх через шкідливе ПЗ (AcidRain), із наслідками для десятків тисяч користувачів у Європі. У правовому вимірі це підкреслює, що цілеспрямоване ураження цивільної SATCOM-інфраструктури у воєнному контексті створює транскордонну шкоду приватним і публічним суб'єктам, ускладнюючи визначення обов'язків і меж відповідальності держав та приватних операторів [195].

Додатково література з міжнародного права акцентує на невизначеності стандартів застосовності суверенітету й невтручання до кібероперацій, що проявляється саме у випадках ударів по цивільних цифрових сервісах із ефектом spillover за межі території первинної цілі [212]. Як підкреслює І. Костенко, ураження цивільних супутникових систем у війні РФ проти України продемонструвало змішаний характер правового режиму dual-use технологій, де цивільні оператори стають об'єктами воєнних дій, а правові межі захисту таких систем залишаються недостатньо визначеними [271]. Це створює потребу у розробці спеціальних норм щодо відповідальності держав за використання або ураження супутникових комунікацій, що мають подвійне призначення.

Таким чином, кейс Viasat показує, що компрометація цивільних satcom-послуг у контексті міжнародного збройного конфлікту виходить за межі технічного інциденту – вона порушує питання міжнародної відповідальності, правового статусу приватних операторів і захисту транскордонної інфраструктури.

Узагальнений правовий урок. Атака на KA-SAT показала доктринальну вагу скоординованих публічних атрибуцій: 10 травня 2022 р. ЄС, США та Велика Британія синхронно поклали відповідальність на РФ за ураження мережі Viasat, що стало прецедентом колективної реакції на кібератаку з

транскордонними наслідками. Такі узгоджені заяви підсилюють доказову базу міжнародної відповідальності та задають практику взаємоузгодженого політико-правового реагування [261].

Фактичну «мультиюрисдикційність» шкоди підтверджують як журналістські й технічні описи spillover-ефекту (деактивація модемів поза Україною), так і оцінки інституцій ЄС щодо ризиків для громадян у Європі. Отже, ураження цивільної SATCOM-інфраструктури в умовах міжнародного збройного конфлікту створює багаторівневі наслідки (держави – оператори – користувачі) й потребує узгоджених правових підходів до атрибуції та відшкодування шкоди.

Серії «wiper»-атак 2022 р. (HermeticWiper, CaddyWiper, Industroyer2). У перші тижні повномасштабного вторгнення (з 24 лютого 2022 р.) у Україні було зафіксовано послідовні хвилі деструктивних кібератак, які супроводжувалися як атаками на інформаційні ресурси державних установ, так і на підприємства критичної інфраструктури та фінансові організації. У хронологічному огляді Європейської дослідницької служби (EPRS) прямо зазначається, що в період лютий–квітень 2022 р. спостерігалися інциденти, пов’язані з сімействами HermeticWiper, IsaacWiper, CaddyWiper та Industroyer2, а також наведено часову шкалу першої хвилі атак і приклади уражених секторів [222].

Компанія Microsoft у своєму спеціальному звіті зафіксувала широку сукупність операцій проти українських інформаційних систем і охарактеризувала «кіберний компонент» конфлікту як руйнівний і тривалий; у звіті наводиться опис численних операцій проти урядових, енергетичних і приватних мереж, а також спільна робота Microsoft з українськими CERT і приватними секторами задля виявлення й пом’якшення загроз [282].

Журналістський хронологічний огляд CSO Online надав додаткову послідовну хронологію подій перших тижнів кризового періоду з посиланнями на технічні розвідки (CERT-UA, ESET тощо) і відзначив, що

низка wiper-інцидентів була відразу ж ідентифікована й описана незалежними фахівцями-дослідниками [166].

Узагальнення фактів із цих джерел дозволяє констатувати таке (строго фактологічно): (1) деструктивні wiper-сімейства були ідентифіковані та пов’язані в часі з початком широкомасштабних бойових дій у лютому–квітні 2022 р.; (2) цілі атак включали державні інституції, фінансові установи й об’єкти критичної інфраструктури; (3) низка міжнародних технологічних і аналітичних організацій (Microsoft, Accenture) і оглядові хроніки (EPRS, CSO) документували ці інциденти та класифікували їх як «деструктивні» за способом дії (безповоротне стирання даних / порушення працездатності систем).

Технічний вектор атак (wiper-модулі, OT-націленість, Industroyer2). Упродовж перших місяців повномасштабного вторгнення Російської Федерації проти України було виявлено кілька технічно різнорідних, але функціонально споріднених сімейств шкідливого програмного забезпечення типу *wiper*, призначених для безповоротного знищення даних і виведення з ладу систем. Ці інструменти діяли у різних секторах – від державного управління до фінансових установ та енергетики – і свідчили про поєднання кіберактивності з воєнними діями у фізичному просторі.

Як зазначає Sergiu Gatlan у публікації *BleepingComputer* (2022), виявлене 14 березня 2022 р. шкідливе програмне забезпечення CaddyWiper призначалося для «затирання» вмісту жорстких дисків та видалення критичних системних структур, що робило відновлення операційних систем неможливим без резервних копій [236]. Дослідження компанії ESET, на яке посилається автор, підтвердило, що цей зразок було зафіксовано у мережах кількох українських організацій, зокрема у фінансовому секторі [218; 219]. Такий тип деструктивного ПЗ відрізнявся від попередніх wiper-кампаній (HermeticWiper, IsaacWiper) простішою архітектурою та спрямованістю на швидке знищення даних на великій кількості систем без вимоги викупу або спроби приховати сліди [218].

Окрему категорію становлять інструменти, орієнтовані на промислові системи управління (ICS/OT). У доповіді Wired викладено технічні характеристики варіанта Industroyer (Industroyer2), зокрема його здатність взаємодіяти з обладнанням підстанцій і логікою керування енергосистемою, що робить його потенційно придатним для ініціювання відключень електропостачання; Wired повідомляє, що використання Industroyer2 виявлялося як спроба викликати «чорний-аут» і що спроба була виявлена й локалізована силами CERT-UA та приватної компанії ESET у квітні 2022р. [243].

Офіційна аналітична довідка Cybersecurity and Infrastructure Security Agency (CISA) систематизує такі випадки у ширшому контексті російських державних і кримінальних кіберакторів. У документі підтверджується використання деструктивного ПЗ типу *wiper* та спрямованість операцій проти об’єктів критичної інфраструктури, включно з енергетичними мережами, транспортом та фінансовими установами. CISA наголосила на необхідності впровадження захисних заходів для запобігання впливу подібних шкідливих модулів, підкреслюючи, що вони мають безпосередній потенціал спричинити фізичні порушення функціонування систем ICS/OT [198] .

Таким чином, технічна складова wiper-кампаній 2022 р. демонструє подвійний характер кіберагресії: по-перше, її деструктивність і спрямованість на стирання інформаційних активів, а по-друге, розширення операцій до промислових систем керування, де кіберінструменти – такі як Industroyer2 –працюють безпосередньо на рівні OT-інфраструктури, створюючи потенційну загрозу безпеці фізичного середовища.

Сумарно, на підставі наведених джерел, можна узагальнити такі фактичні твердження: (1) у весняний період 2022 р. в Україні було виявлено кілька сімейств wiper-ПЗ (зокрема CaddyWiper), які реалізовували алгоритми безповоротного видалення даних; (2) одночасно спостерігалися спроби застосування спеціалізованих OT-інструментів (Industroyer2), що потенційно здатні були впливати на електричні підстанції; (3) технічні звіти приватних

компаній (ESET, Mandiant) і публічні попередження (CISA) конвергують у висновку про наявність у цих операцій як елементів «деструктивного» цифрового впливу, так і ознак спрямованості на критичну інфраструктуру [198; 236; 243].

Правова кваліфікація У контексті серій «wiper»-атак 2022 р. питання їхньої правової оцінки розглядається крізь призму норм міжнародного гуманітарного права (IHL) та принципів суверенітету й невтручання.

Відповідно до Додаткового протоколу I до Женевських конвенцій 1949 р. (ст. 48, 51, 52), сторони збройного конфлікту зобов'язані розрізняти цивільні й військові об'єкти [306]. Кібератаки, які вражають інформаційні системи державного управління, фінансових чи енергетичних структур, *можуть порушувати* цей принцип, якщо вони не мають безпосереднього воєнного призначення.

Як зазначає K. Eichensehr, досвід України свідчить, що норми IHL застосовні до кіберпростору, коли дії мають реальні наслідки для цивільної інфраструктури [116]. Водночас, за підходом M. Schmitt (*Yale J. Int. Law Online*, 2017), втручання у мережі іншої держави без її згоди може розглядатися як порушення суверенітету або принципу невтручання [319]. Аналітичні матеріали CISA підкреслюють ризики деструктивних кібератак для критичної інфраструктури й важливість дотримання міжнародних зобов'язань у цій сфері [319].

З огляду на наведене, серії «wiper»-атак 2022 р. *можуть розглядатися* як такі, що порушують принципи суверенітету, невтручання та захисту цивільних об'єктів, остаточна кваліфікація яких залежить від міжнародної правозастосовної практики [236; 218]

Узагальнений правовий урок подій 2022 року засвідчили, що ефективна правова оцінка кібератак можлива лише за умови своєчасного технічного документування інцидентів і належної координації між державними, міжнародними та приватними структурами. Практика CERT-UA, Microsoft, ESET та інших організацій показала значення оперативної фіксації технічних

ознак атак для подальшого їх аналізу з позицій міжнародного права [282; 166].

Водночас досвід «wiper»-кампаній підкреслює потребу уточнення міжнародних стандартів кваліфікації кібероперацій, зокрема меж застосування норм міжнародного гуманітарного права до цифрового середовища, критеріїв атрибуції та визначення порушення суверенітету в кіберпросторі [236].

Загалом, ці події підтвердили, що поєднання технічної експертизи й правової фіксації фактів є ключовою передумовою для встановлення відповідальності та формування сталої міжнародної практики реагування на деструктивні кібератаки.

Масові DDoS проти держресурсів/банків і інцидент у Ukrtelecom (лютий–березень 2022). У перші тижні повномасштабної агресії Російської Федерації проти України зафіксовано низку масштабних DDoS-кампаній, спрямованих проти державних вебресурсів та фінансових установ. Згідно з повідомленням Reuters від 18 лютого 2022 р., офіційні представники урядів США та Великої Британії публічно заявили про причетність російського Головного розвідувального управління (ГРУ) до кібератак, що вивели з ладу сайти українських банків і державних органів. Представники Білого дому охарактеризували ці події як елемент спланованої кампанії дестабілізації, спрямованої на підрив довіри до національних фінансових і публічних сервісів [249].

Хронологічний огляд, оприлюднений виданням CSO Online, підтверджує, що DDoS-атаки у лютому–березні 2022 р. супроводжувалися перевантаженням порталів Кабінету Міністрів, Міністерства оборони та декількох систем онлайн-банкінгу, внаслідок чого було тимчасово порушено доступність електронних сервісів. Ці інциденти стали першою хвилею кібератак у період вторгнення, що збігалася в часі з початком активних бойових дій [166].

Аналітичний документ Європейської дослідницької служби Європарламенту (EPRS) систематизував події лютого–квітня 2022 р., зазначивши, що DDoS-операції, атаки на урядові мережі та елементи критичної інфраструктури України розглядалися як складова багатовекторного кіберкомпонента війни, який супроводжував кінетичні дії РФ. У звіті EPRS наголошено, що атаки мали послідовний характер і значний вплив на публічні онлайн-послуги [222].

У цьому ж часовому періоді, 28 березня 2022 р., стався інцидент у мережі державного оператора «Ukrtelecom». Як повідомило агентство Reuters, компанія та Державна служба спеціального зв'язку та захисту інформації України підтвердили «потужну кібератаку» на IT-інфраструктуру оператора, унаслідок чого було тимчасово обмежено надання інтернет-послуг для користувачів. За офіційною позицією, для збереження цілісності мережі було прийнято рішення тимчасово обмежити трафік і провести технічну ізоляцію окремих сегментів системи, після чого поступово відновлено функціонування сервісів [163].

У доповіді Cybersecurity and Infrastructure Security Agency (CISA) «AA22-110A» зазначено, що атаки на українські інформаційні системи у цей період були складовою ширшої кампанії російських державних і кримінальних суб'єктів, спрямованої на порушення функціонування критичної інфраструктури держав, що підтримують Україну. CISA попередила про потенційну небезпеку аналогічних DDoS-операцій у транскордонному вимірі [198].

Корпорація Microsoft у спеціальному звіті *Special Report: Ukraine* (27 квітня 2022 р.) зафіксувала комплексну сукупність кібератак проти урядових, енергетичних і приватних мереж України, серед яких операції з порушення доступності державних онлайн-ресурсів і банківських систем. Компанія оцінила ці події як елемент тривалого деструктивного кіберкомпонента війни, що поєднував різні техніки – від DDoS до деструктивного шкідливого ПЗ [198; 282]. Отже, з огляду на наведені джерела, встановлено, що: у

лютому–березні 2022 р. зафіксовано серію масових DDoS-операцій проти державних і фінансових ресурсів України, підтверджену офіційними урядовими заявами та міжнародними аналітичними оглядами [249; 222; 198]; інцидент Ukrtelecom (28 березня 2022 р.) був частиною тієї ж хвилі кіберактивності, однак мав більш технічно складний характер, пов'язаний із безпосереднім втручанням у мережеву інфраструктуру оператора [163; 282]; міжнародні структури (CISA, Microsoft, Accenture, EPRS) розглядали ці дії як скоординовані кампанії з підриву функціонування публічних сервісів та інформаційних комунікацій [198; 282; 222].

Правова кваліфікація. Згідно з публічною заявою урядів США та Великої Британії від 18 лютого 2022 р., до DDoS-атак проти українських банків і державних вебресурсів безпосередньо причетні російські державні структури –зокрема, Головне розвідувальне управління (ГРУ). В офіційних коментарях підкреслено, що ці дії є навмисним втручанням у функціонування інформаційних систем і частиною ширшої кампанії з дестабілізації України перед початком воєнних дій [249; 333; 314].

Європейська дослідницька служба Європарламенту (EPRS) у своєму огляді (червень 2022 р.) кваліфікувала атаки лютого–березня 2022 р. як цілеспрямовані операції з порушення доступності державних і фінансових онлайн-сервісів, що мають транскордонний характер і потенційно зачіпають критичну інфраструктуру [222].

У звіті CISA (*Alert AA22-110A*, квітень 2022 р.) зазначено, що російські державні та кримінальні кіберугруповання здійснювали атаки проти інформаційних систем України та її партнерів, зокрема DDoS-операції проти державних установ і комерційних сервісів. Ці дії визнано частиною координованої кампанії, спрямованої на переривання функціонування критичних послуг [198].

Звіт корпорації Microsoft (Special Report: Ukraine, 27 квітня 2022 р.) зафіксував, що під час початкової фази війни було здійснено численні операції проти урядових і приватних мереж, включно з атаками на

доступність і деструктивними кампаніями, які мали на меті порушити нормальне функціонування державного управління та суспільних комунікацій [282].

У свою чергу, Reuters щодо інциденту *Ukrtelecom* (28 березня 2022 р.) зафіксував офіційні коментарі компанії та Держспецзв'язку про «потужну кібератаку» на IT-інфраструктуру, яка тимчасово вивела з ладу інтернет-послуги [163; 261]. Фактичні обставини цих подій підтверджують наявність несанкціонованого втручання в інформаційні системи державного та комерційного секторів, що призвело до порушення доступності послуг.

Таким чином, відповідно до змісту наведених офіційних звітів і повідомлень, ці події кваліфікуються як цілеспрямовані кібероперації з порушення функціонування інформаційних систем і тимчасового обмеження публічних сервісів, здійснені російськими державними або пов'язаними з ними структурами. У жодному з проаналізованих джерел не вказано на фізичні руйнування чи втрати, тому зафіксовані інциденти віднесено до кібератак, що порушують доступність (availability), без ознак застосування сили в матеріальному сенсі [247; 312; 212].

Узагальнений правовий урок. Масові DDoS-атаки проти державних і фінансових ресурсів України, а також інцидент у мережі «Ukrtelecom» у лютому–березні 2022 р., демонструють, що навіть технічно «нематеріальні» форми кібервпливу можуть мати стратегічний характер і кваліфікуватися як порушення суверенітету та принципу невтручання у внутрішні справи держави. Встановлена публічна атрибуція цих дій російським державним структурам підтверджує наявність ознак міжнародно-протиправних діянь та актуалізує питання державної відповідальності у кіберпросторі [249; 333; 166; 222; 317].

З правової точки зору, подібні операції не досягають порогу «застосування сили» у розумінні статті 2(4) Статуту ООН, проте порушують засадничі норми міжнародного права – поваги до суверенітету, належної обачності (due diligence) та невтручання у функціонування органів влади й

критичних сервісів. Вони можуть розглядатися як «недружні дії», що створюють міжнародно-правову напруженість та формують прецеденти для подальшої кодифікації практики реагування [247; 312; 319; 317; 212].

Таким чином, масові й цілеспрямовані кібероперації проти України у 2014–2024 роках засвідчили становлення системного кіберкомпонента гібридної агресії Російської Федерації – від точкових атак на енергетичні об’єкти до комплексних кампаній, спрямованих на дестабілізацію комунікаційного, фінансового та інформаційного середовищ [243; 244; 172; 282; 195]. Досвід цих інцидентів виявив глибинні вразливості національної критичної інфраструктури, фрагментарність нормативно-правових механізмів і залежність державних та приватних секторів від зовнішніх технологічних рішень. Саме ці чинники обумовлюють потребу у подальшому дослідженні природи вразливостей критичної інфраструктури та суспільства, що стали підґрунтям успішності кібератак, – питання, якому присвячено наступний підрозділ.

2.3. Інституційно-правові вразливості критичної інфраструктури України

Розглянуті у попередньому підрозділі кейси –енергетичні атаки Sandworm (2015–2016, 2022), NotPetya (2017), інцидент у супутниковій мережі KA-SAT/Viasat (2022), серії wiper-операцій (2022) та масові DDoS-атаки (зокрема проти «Ukrtelecom») – відображають еволюцію російської кіберагресії від окремих деструктивних дій до системно скоординованих, багаторівневих кампаній, у межах яких поєднуються технічні, інформаційно-психологічні та організаційні засоби впливу [305; 289; 236; 218; 163].

Якщо початкові операції були спрямовані переважно на порушення функціонування промислових систем управління (ICS/SCADA) чи обмежене виведення з ладу телекомунікаційних вузлів, то згодом вони переросли у

комплексні гібридні операції, що поєднують ОТ-саботаж, порушення ланцюгів постачання цифрових ресурсів, деструкцію каналів цивільного зв'язку та інформаційно-психологічний тиск на державні інституції та громадян [198; 282; 206; 177; 292].

Досвід України засвідчує, що навіть кібератаки без безпосереднього фізичного ураження здатні призводити до глибокої дестабілізації функціонування державних органів та критичних сервісів, порушення міжсекторальних комунікаційних ланцюгів, а також зниження суспільної довіри до спроможності держави забезпечувати стабільність і безперервність управлінських процесів. У такий спосіб кібероперації перетворюються з допоміжного засобу ведення бойових дій на самостійний інструмент стратегічного впливу, співмірний за масштабом і наслідками з традиційними формами воєнних дій у політичному та економічному вимірах [215; 223; 300; 252; 275].

У правовому аспекті така трансформація кіберагресії свідчить про системне порушення принципів суверенітету та невтручання у внутрішні справи держави, що підтверджується офіційними атрибуціями, здійсненими державами – членами ЄС, НАТО, США та Великої Британії. Разом із тим, зазначені події висвітлили структурні прогалини міжнародно-правового регулювання у сфері кібероперацій, зокрема відсутність чітких критеріїв відмежування між протиправним втручанням і застосуванням сили у розумінні статті 2(4) Статуту ООН. Внаслідок цього виникає нормативна «сіра зона», у межах якої навіть деструктивні кібероперації можуть залишатися поза сферою ефективної міжнародно-правової відповідальності, незважаючи на їхню стратегічну мету та суспільно небезпечні наслідки [190; 212; 317; 319; 333].

Невизначеність правового статусу деструктивних, але нефізичних кібероперацій сприяє розмиванню меж між кіберзасобами і традиційними збройними діями, особливо коли об'єктом ураження стають цивільні інфраструктурні системи подвійного (dual-use) призначення –

телекомунікації, енергетика, фінанси. Це, у свою чергу, загострює потребу у кодифікації міжнародно-правових критеріїв кваліфікації кібероперацій, які здатні завдавати шкоди цивільним об’єктам без застосування кінетичної сили, але з аналогічними наслідками для національної безпеки, стабільності управління та громадської безпеки [222; 166; 163; 243].

Отже, узагальнення наведених кейсів дозволяє перейти від аналізу зовнішніх форм кіберагресії до оцінки внутрішніх чинників її ефективності. Вразливість державних систем виявилася не лише наслідком технічних дій противника, а й результатом інституційних, правових та організаційних прогалин у забезпеченні кіберзахисту. Подальший аналіз спрямовано на з’ясування цих структурних вразливостей критичної інфраструктури та їхнього впливу на рівень національної кіберстійкості.

Доказова база та атрибуція. Розслідування більшості кібератак проти України спираються на поєднання офіційних урядових заяв та технічної аналітики приватних компаній і дослідницьких структур [190; 333; 335; 282; 198]. Такий підхід підвищує доказову переконливість висновків, проте водночас формує залежність від корпоративних методологій, обмежених рамками доступу до телеметрії, закритістю вихідних даних і зобов’язаннями конфіденційності (NDA) [282]. У результаті достовірність атрибуції набуває змішаного характеру – політичного за формою та техніко-аналітичного за змістом [190; 333; 282]. Це підкреслює потребу у державному нормативному врегулюванні процесу збору, збереження й оприлюднення цифрових доказів, зокрема через запровадження уніфікованих протоколів chain of custody та незалежних механізмів верифікації атрибуції третіми сторонами [212].

Нормативна невизначеність. Наявна міжнародна практика підтверджує застосовність до кібероперацій базових принципів суверенітету та невтручання, а також окремих положень міжнародного гуманітарного права. Водночас відсутні усталені порогові критерії для кваліфікації дій як «застосування сили» у випадках, коли кібератака не спричиняє фізичних руйнувань, але має масштабні наслідки для функціонування держави (як у

випадку NotPetya або KA-SAT/Viasat). Така невизначеність породжує нормативну «сіру зону», у межах якої кібератаки залишаються поза сферою чіткої міжнародно-правової відповідальності, незважаючи на їхню стратегічну мету та деструктивний ефект [212; 247; 312; 317; 319].

Цивільно-військовий та приватно-публічний інтерфейс. Інциденти з мережами KA-SAT та NotPetya наочно демонструють правову колізію у зоні подвійного (dual-use) використання технологій. Приватні оператори зв'язку, постачальники програмного забезпечення та елементи цифрових ланцюгів постачання фактично опиняються серед об'єктів кібероперацій, що мають воєнний характер. Це створює прогалину у розподілі відповідальності між державами та приватним сектором щодо запобігання, виявлення та усунення наслідків таких інцидентів. Відповідно, потребує розвитку правова модель публічно-приватної взаємодії у сфері кібербезпеки, заснована на чітких обов'язках сторін щодо обміну інформацією, реагування та відшкодування шкоди [244; 289; 172; 195; 196].

Гібридна інтеграція OT/IT. Еволюція діяльності угруповання Sandworm, зокрема застосування Industroyer2 і техніки *living-off-the-land*, засвідчує системну вразливість на стику операційних (OT) і інформаційних (IT) систем. Промислові мережі, інтегровані у цифрову інфраструктуру, часто не мають достатніх механізмів контролю безпеки: обмежена ідентифікація активів, недостатня сегментація, відсутність захищених каналів оновлення та неефективний моніторинг промислових протоколів (IEC, Modbus тощо). У підсумку технічна вразливість OT-компонентів стає юридично значущим фактором – як доказ недотримання державою або оператором критичної інфраструктури стандартів належної обачності (*due diligence*) [243; 305; 182; 183; 199].

Операційна стійкість vs. юридичне реагування. Практика доводить, що навіть за наявності політико-правової позиції, вирішальним чинником мінімізації шкоди від кібератак є рівень операційної кіберстійкості держави. Успішні приклади діяльності CERT-UA, приватних CSIRT, а також своєчасні

технічні ізоляційні заходи (зокрема під час інциденту «Ukrtelecom») показали ефективність скоординованих дій. Водночас, для забезпечення сталого захисту необхідно нормативно закріпити вимоги до планів безперервності діяльності (BCP/DRP), журналювання OT-подій, стандарти збереження цифрових артефактів та строки інцидент-репортингу. Це дозволить поєднати технічні критерії стійкості з юридичною валідністю доказової бази та забезпечити реалізацію принципу міжнародної відповідальності держав у кіберпросторі [163; 75; 223; 215; 206].

Український досвід переконливо свідчить, що: (i) системні кібероперації державного походження, спрямовані проти критичної інфраструктури, надійно підпадають під заборону втручання та становлять порушення суверенітету держави; (ii) колективні публічні атрибуції, здійснені ЄС, США, Великою Британією та іншими партнерами, формують новий прецедент міжнародної практики, який поступово набуває ознак звичаєвої норми у сфері фіксації державної відповідальності за кібероперації; (iii) для цифрових інцидентів, що не спричиняють фізичних руйнувань, необхідно виробити чіткі порогові тести (за масштабом, тривалістю та наслідками) та процедурні стандарти доказування, які забезпечували б їх однозначну правову кваліфікацію; (iv) ефективність юридичної реакції безпосередньо залежить від операційної спроможності держави швидко документувати технічні факти –що потребує закріплення у вигляді національних стандартів обліку та збереження технічних журналів подій, збереження цифрових артефактів і аудиту ланцюгів постачання [169; 247; 312; 211; 190; 333; 328; 223].

Узагальнення проведеного аналізу свідчить, що розглянуті кібератаки виявили комплекс взаємопов’язаних вразливостей – *інституційно-правових, техніко-організаційних і соціально-комунікаційних.* Їх сукупний вплив формує підвищену нестійкість окремих сегментів національної критичної інфраструктури перед сучасними гібридними загрозами та окреслює пріоритети подальшого вдосконалення механізмів кіберзахисту (управління

ризиками, інцидент-репортинг, стандартизація взаємодії держави й приватного сектору, підготовка персоналу) [71; 206; 223; 226; 273; 300; 331].

Для належної правової оцінки та вироблення регуляторних рішень необхідно систематизувати виявлені слабкі місця за їхнім походженням і впливом на рівень державної кіберстійкості. Від констатації окремих інцидентів і їхніх правових наслідків логічно перейти до виявлення структурних чинників уразливості, що лежать «під поверхнею» подій та зумовлюють повторюваність і каскадність наслідків. Саме така структурна перспектива дозволяє поєднати емпіричні факти з вимогами публічного права та секторального регулювання, визначивши точки інституційного й технологічного посилення системи [71; 273].

Аналіз емпіричних даних 2022–2024 рр. та профільних міжнародних і національних оглядів свідчить, що російські кібероперації проти України мають багаторівневий і скоординований характер, поєднуючи технічні, організаційні та інформаційно-психологічні впливи. Вони спрямовані на порушення безперервності функціонування критичних секторів, створення дестабілізаційних «каскадних» ефектів та підрив довіри до державних і суспільних інститутів [222; 282; 215]

Публічно підтверджені інциденти, зокрема кібератака на Ukrtelecom (березень 2022 р.) та саботаж у супутниковій мережі KA-SAT/Viasat напередодні широкомасштабного вторгнення РФ (лютий 2022 р.), продемонстрували високу взаємозалежність секторів, транскордонність кіберзагроз і чутливість національної інфраструктури до порушення цифрових комунікацій [163; 196].

Сукупність цих подій засвідчила, що вразливості українського кіберпростору не обмежуються технічними дефектами окремих систем, а мають комплексний, структурний характер, який охоплює інституційно-правові, техніко-організаційні та соціально-комунікаційні чинники. У цьому підрозділі систематизовано зазначені групи вразливостей, виявлені внаслідок

кібератак 2014–2024 рр., і здійснено їх правову та організаційну оцінку з огляду на вплив на рівень національної кіберстійкості.

1) Інституційні вразливості. Система національної кібербезпеки України, закріплена у профільному законодавстві, охоплює широкий спектр суб'єктів – державні органи, військові структури, регуляторів, операторів критичної інфраструктури та приватний сектор. Її нормативна основа створює формальну рамку для взаємодії між ними, однак у кризових ситуаціях, зокрема в умовах воєнного стану, проявляються істотні розриви координації. Як зазначають Ліпкан і Діордіца, така багаторівнева модель поки що не забезпечує належного рівня оперативності та цілісності управлінських рішень, а розподіл компетенцій між суб'єктами системи залишається надмірно фрагментованим [61]. Подібного висновку доходить і Тарасюк, наголошуючи, що координаційна структура системи кібербезпеки має бути більш централізованою та уніфікованою, особливо щодо реагування на загрози, які стосуються критичної інфраструктури [150]. Під час воєнного стану ці проблеми загострюються: як підкреслюють Тіщенко та Логвиненко, неузгодженість дій між органами безпеки, регуляторами та операторами створює ситуації, коли управлінські рішення ухвалюються ситуативно, без урахування єдиної процедури кризового реагування [152].

На рівні правового регулювання дослідники відзначають брак цілісних стандартів управління ризиками та відповідальності у сфері кіберзахисту. Алексеєва обґрунтовує, що вітчизняний правовий режим кібербезпеки критичної інфраструктури потребує не лише фрагментарних змін, а й перегляду підходів до обов'язковості стандартів безпеки для суб'єктів, які виконують функції життєзабезпечення держави [2]. Подібну позицію поділяють Лисеюк і Свінцицька, зазначаючи, що лише уніфікована модель управління ризиками, яка встановлює чіткі процедури моніторингу, звітності та відповідальності, може забезпечити належну безперервність роботи критичних систем [59]. Додатково Ніконенко та Халіна звертають увагу на недостатність інтегрованого підходу до організаційно-правового

забезпечення кібербезпеки соціально-економічних систем, підкреслюючи важливість запровадження обов'язкових правил реагування на інциденти [73]. Аналізуючи динаміку інцидентів у державному секторі, щорічний звіт Державної служби спеціального зв'язку та захисту інформації України за 2024 рік підтверджує зростання кількості зареєстрованих кібератак і водночас акцентує на необхідності стандартизації процесів виявлення та реагування в межах державної екосистеми кіберзахисту [75].

Значним викликом для інституційної стійкості є питання інцидент-репортингу та таксономії кіберподій. Міжнародна практика демонструє, що своєчасна звітність і уніфікована класифікація інцидентів є ключовими передумовами ефективної координації між державними й приватними структурами. Американські рекомендації CISA (Alert AA22-110A) встановлюють вимогу негайного повідомлення про кіберінциденти, що становлять потенційну загрозу критичній інфраструктурі [198]. Європейські підходи, закріплені у довіднику ENISA *Reference Incident Classification Taxonomy* [216], передбачають стандартизовану систему категоризації подій, яка дозволяє інтегрувати національні CSIRT у спільний інформаційний простір реагування. Як зазначається у щорічному звіті ENISA *Threat Landscape 2023* [215], застосування цих підходів дає змогу скоротити часовий лаг між виявленням і нейтралізацією загроз та підвищити взаємодію між секторальними центрами реагування.

Питання публічно-приватної взаємодії посідає центральне місце у сучасній архітектурі кібербезпеки. Події 2022 року продемонстрували, що саме приватні постачальники цифрових сервісів – телекомунікаційні оператори, хмарні провайдери, компанії супутникового зв'язку – відіграють критичну роль у забезпеченні безперервності державних комунікацій. Під час широкомасштабного вторгнення РФ компанії Microsoft і Viasat здійснювали оперативну технічну підтримку українських користувачів, сприяючи відновленню цифрових сервісів і захисту від атак [313; 282]. Разом з тим, як слушно зауважує Eichensehr, відносини між державою та приватним

сектором у сфері кібербезпеки залишаються юридично вразливими через відсутність прозорих договірних рамок, чітких зобов'язань щодо звітності та обмеження, пов'язані з юрисдикційними межами надання послуг [213; 214]. Це зумовлює необхідність запровадження типових угод про рівень надання послуг (SLA) та процедур екстреної взаємодії, що узгоджують технічні стандарти із нормами публічного права.

Інституційним чинником зміцнення кіберстійкості України є також поступова інтеграція до міжнародних структур. Приєднання України до НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE) у статусі *contributing participant* у 2022 році створило нові можливості для обміну знаннями, участі в спільних навчаннях та адаптації найкращих практик у сфері кібероборони [291]. Додатково, такі аналітичні ресурси, як таймлайни кібератак, підготовлені European Parliamentary Research Service [222] і CyberPeace Institute [195], забезпечують емпіричну основу для оцінки тенденцій і структури загрозового середовища, слугуючи підґрунтям для корекції національних політик кіберзахисту.

Узагальнюючи викладене, можна стверджувати, що інституційні вразливості системи кібербезпеки України мають характер незавершеного інституційного циклу управління ризиками. Відсутність уніфікованої таксономії інцидентів, недостатня формалізація процесів звітності та брак нормативно визначених процедур публічно-приватної взаємодії зумовлюють ситуативний характер координації між суб'єктами системи. Як наслідок, державна система реагування часто діє реактивно, а не превентивно, що знижує рівень національної кіберстійкості. Подолання цих вразливостей вимагає гармонізації національного правового режиму з європейськими стандартами ENISA та практиками CISA, а також запровадження системного моніторингу ефективності інституційних механізмів кіберзахисту [2; 73; 215].

2) Технічні вразливості. Технічний вимір національної кіберстійкості у 2015–2024 рр. засвідчив наявність системних уразливостей на стику

операційних технологій (OT/ICS), ланцюгів постачання, зовнішніх цифрових сервісів та організаційних практик суб'єктів критичної інфраструктури. Узагальнення емпіричних даних і профільних аналітичних звітів за 2022–2024 рр. дозволяє виділити чотири ключові групи технічних вразливостей: (1) уразливості OT/ICS і межі IT/OT; (2) залежності ланцюгів постачання; (3) комбіновані тактики із застосуванням деструктивного ПЗ; (4) нерівномірність базових контролів у бізнес-секторі, кожна з яких має власні технічні та нормативно-організаційні наслідки [75].

По-перше, найбільш критичним напрямом залишаються вразливості операційних технологій (OT/ICS), які зумовлені недостатньою сегментацією мереж, відсутністю ефективного контролю віддалених доступів і можливістю експлуатації промислових протоколів. Інциденти, пов'язані з діяльністю угруповання *Sandworm* (зокрема *Industroyer* та *Industroyer2*), підтвердили потенціал деструктивного впливу на технологічні процеси енергетичних підприємств шляхом проникнення через IT-сегмент до OT-мереж [243; 305]. Спільні рекомендаційні документи CISA та NSA(AA22-265A, AA22-103A) визначають мінімальні вимоги до безпеки OT/ICS – інвентаризацію активів, сегментацію, принцип найменших привілеїв, контроль привілейованих облікових записів, моніторинг аномалій [183; 199; 203]. Рамка Shields Up деталізує організаційні кроки підвищення кіберпильності операторів критичної інфраструктури, включаючи перевірку резервних каналів, багатофакторну автентифікацію та тестування процедур відновлення [183; 199; 203]. Як випливає з наведених джерел, в українській практиці такі вимоги переважно мають рекомендаційний характер, що потребує їх нормативної імплементації як обов'язкових технічних стандартів для операторів критичної інфраструктури.

По-друге, залежності ланцюгів постачання створюють додаткові ризики для безперервності функціонування критичних секторів. Компрометація окремої ланки в системі постачання, як показав приклад кібератаки на супутникову мережу KA-SAT/Viasat (лютий–березень 2022 р.),

призвела до масштабних перебоїв у роботі комунікаційних сервісів в Україні та інших державах Європи, що засвідчило транскордонний характер сучасних кіберзагроз [172; 196; 271; 333; 335]. Аналогічно, кібератака на Ukrtelecom 28 березня 2022 р. підтвердила вразливість базових телекомунікаційних послуг та відсутність уніфікованих механізмів швидкого відновлення критичних сервісів [163; 195; 222]. Ці факти підкреслюють потребу в нормативному закріпленні процедур обов'язкової оцінки постачальників, вимог до резервування та геодиверсифікації каналів і сервісів, а також у встановленні типових умов рівня надання послуг (SLA) для суб'єктів критичної інфраструктури [95; 106; 207; 229; 230].

По-третє, характерною тенденцією стало поширення комбінованих тактик кібератак, що поєднують використання деструктивного програмного забезпечення з іншими методами впливу. Упродовж 2022 р. в Україні зафіксовано застосування кількох родин *wiper*-шкідників (зокрема *CaddyWiper*), які використовувалися у зв'язці з фішинговими кампаніями, викраденням облікових даних і DDoS-атаками, що створювало каскадний ефект і ускладнювало реагування [75; 195; 206; 218; 219; 236; 282]. Згідно з оглядами ENISA, зафіксовано зростання кількості атак на ланцюги постачання та активності «проксі-акторів», включно з феноменом hacktivism-as-a-service, який ускладнює атрибуцію й подовжує часовий проміжок між виявленням і нейтралізацією загроз [215; 217; 226]. У контексті національної практики це обґрунтовує необхідність законодавчого встановлення мінімального переліку технічних контролів для суб'єктів критичної інфраструктури – обов'язкової телеметрії, журналювання подій і централізованого обміну індикаторами компрометації [69; 75; 95; 97; 98; 117].

По-четверте, у бізнес-секторі, особливо серед малих і середніх підприємств, зберігається нерівномірність упровадження базових заходів кіберзахисту, таких як багатофакторна автентифікація, резервне копіювання, журналювання, сегментація мережі та підготовка персоналу. Практичні

рекомендації для бізнесу та правові дослідження підтверджують, що відсутність системного підходу до цих елементів у воєнний період масштабувалася до рівня системних ризиків через міжсекторальні залежності, зокрема внаслідок використання спільних провайдерів і підрядників [68; 70; 72; 75; 206; 215; 252]. Такий стан речей обґрунтовує доцільність нормативного закріплення мінімальних вимог до кіберзахисту постачальників, які беруть участь у забезпеченні суспільно значущих функцій [95; 106; 207; 229; 230].

Узагальнюючи наведене, можна констатувати, що технічні вразливості національної кіберінфраструктури мають системний і взаємопов'язаний характер, формуючи комплекс ризиків на стику технологічних, організаційних і правових чинників. Їхнє виникнення обумовлене структурними дисбалансами між рівнем технологічної зрілості, нормативним забезпеченням і практиками управління безпекою [59; 95; 98; 106; 194; 206; 258; 273; 275; 300]. Ключовими проявами є нестабільність на межі IT/OT-середовищ, залежність від зовнішніх постачальників цифрових сервісів, а також нерівномірність застосування базових кіберконтролів у різних секторах. Сукупно це засвідчує перехід українського кіберпростору від етапу фрагментарної адаптації технічних рішень до потреби комплексної інтеграції стандартів безпеки у систему державного та корпоративного управління [59; 95; 98; 117; 121; 206].

3) Соціально-комунікаційні вразливості. У структурі сучасних кіберзагроз соціально-комунікаційний вимір залишається одним із найменш керованих і водночас найуразливіших елементів національної кіберстійкості. Аналіз актуальних звітів, емпіричних досліджень та профільних публікацій свідчить, що ключові ризики зосереджуються навколо трьох взаємопов'язаних компонентів – людського фактора, інформаційно-психологічних впливів та волонтерських ініціатив у кіберпросторі, які часто діють поза рамками державного регулювання [71; 180; 185; 206; 212; 215; 352].

Людський фактор і соціальна інженерія. Упродовж 2022–2024 рр. стійко фіксується тенденція до використання соціальної інженерії як первинного інструмента компрометації інформаційних систем. Українські дослідження вказують на нерівномірність рівня підготовки користувачів у державному секторі та серед малих і середніх підприємств, що зумовлює відмінності у здатності виявляти фішингові атаки та дотримуватися базових стандартів кібергігієни [54; 59; 71; 72; 75; 133; 155; 158]. Окремі практичні огляди, зокрема матеріали аналітичного порталу Мінфін, акцентують на необхідності формування корпоративних політик безпечної поведінки в цифровому середовищі та впровадження постійних навчальних програм для працівників [68; 252]. У європейському вимірі звіти ENISA підтверджують підвищення питомої ваги атак, орієнтованих на користувача, які дедалі частіше поєднуються з технічними кампаніями зловмисників [215; 217; 223; 224]. Додатково, аналітичні спостереження компанії Microsoft засвідчують, що соціальна інженерія залишається одним із ключових елементів багаторівневих кібероперацій, зокрема через фішинг і компрометацію облікових даних [252; 282].

Інформаційно-психологічні операції та «мультиефект». В умовах війни проти України значно активізувався взаємозв’язок між технічними атаками й дезінформаційними кампаніями. Дослідження Chatham House відзначає, що технічні інциденти часто виступають тригером для поширення хвиль дезінформації, спрямованих на підрив довіри до державних інституцій і створення панічних настроїв серед населення [337]. Європейський парламентський дослідницький сервіс (EPRS) у своєму таймлайні також фіксує паралельність кібератак і інформаційних впливів, що засвідчує формування «каскадного ефекту» у просторі суспільних комунікацій [222]. Український звіт Державної служби спеціального зв’язку та захисту інформації (ДССЗЗІ) підкреслює важливість створення єдиних процедур кризової комунікації, оперативного оприлюднення перевірених технічних даних та узгодження позицій між відомствами для запобігання спотворенню

інформації [75]. Аналогічні положення викладено у монографічному виданні *Digital Security in Wartime*, де узагальнено український та міжнародний досвід протидії дезінформаційним впливам у період воєнних дій. Авторський колектив обґрунтовує, що підвищення рівня суспільної довіри можливе лише за умови фактологічної прозорості комунікацій і забезпечення доступу до достовірної інформації, що виступає фундаментальною передумовою цифрової стійкості держави [206]. У цьому контексті слушною є позиція О. М. Романової, яка підкреслює, що інформаційна комунікація становить невід'ємний елемент правового механізму забезпечення кібербезпеки в умовах воєнного стану, оскільки впливає як на громадське сприйняття безпеки, так і на легітимацію рішень органів публічної влади [133].

У період повномасштабної збройної агресії Російської Федерації проти України суттєво активізувалася діяльність неформальних волонтерських спільнот, орієнтованих на здійснення контркібероперацій проти ворожих цифрових ресурсів. Зазначені об'єднання беруть участь у розповсюдженні індикаторів компрометації, технічному аналізі шкідливого програмного забезпечення, ідентифікації бот-мереж та протидії інформаційно-психологічним операціям. За даними аналітичних та журналістських джерел, їхня діяльність стала важливим елементом підвищення кіберстійкості національного інформаційного простору, сприяючи оперативному виявленню загроз і посиленню оборонних спроможностей держави у цифровій сфері [352; 185; 180].

Водночас відсутність єдиного центру координації між державними органами та волонтерськими об'єднаннями зумовлює низку потенційних ризиків. Як слушно зауважують журналісти *The New York Times* [185], децентралізований характер дій таких груп створює передумови для операційних конфліктів, юрисдикційних порушень та колатеральних наслідків для третіх сторін. Це свідчить про об'єктивну потребу у формуванні нормативно врегульованих механізмів взаємодії між державними і недержавними суб'єктами у сфері кібербезпеки.

На доктринальному рівні зазначене положення узгоджується з концепцією K. Eichensehr, яка обґрунтовує необхідність правової інституціоналізації публічно-приватного партнерства у сфері кіберзахисту [213]. Дослідниця доводить, що ефективне забезпечення кібербезпеки неможливе без нормативного закріплення ролі приватних суб'єктів, визначення меж їхньої участі в операціях реагування та встановлення прозорих процедур відповідальності й нагляду.

Узагальнюючи, слід зазначити, що соціально-комунікаційні вразливості становлять системоутворювальний чинник, який безпосередньо впливає на результативність технічних, організаційних і правових механізмів кіберзахисту. Відсутність уніфікованих протоколів кризової комунікації, нерівномірність програм підготовки з основ кібергігієни та неформалізований характер взаємодії між державними, приватними і волонтерськими структурами суттєво обмежують здатність суспільства до колективного реагування на кібератаки та мінімізації їхніх наслідків. Як свідчать результати національних і міжнародних досліджень, підвищення рівня кіберстійкості можливе лише за умови системного розвитку людського капіталу, нормативного врегулювання комунікаційних процесів і впровадження стандартизованих механізмів публічно-приватної взаємодії [68; 75; 282]. З огляду на аналітику провідних міжнародних інституцій та доктринальні підходи K. Eichensehr [213], інформаційна відкритість, узгодженість дій і суспільна довіра виступають не лише етичними чи комунікаційними, а й безпековими категоріями, що визначають здатність держави протистояти комплексним кіберзагрозам у сучасному безпековому середовищі.

Комплексний аналіз інституційних, технічних і соціально-комунікаційних вразливостей свідчить про їх взаємопов'язаність та інтегрований вплив на рівень національної кіберстійкості. Сформована система ризиків має багатовимірний характер і відображає необхідність поєднання технологічних, управлінських і нормативних заходів. Її

вдосконалення передбачає інституціоналізацію управління ризиками, гармонізацію регуляторних процедур реагування та розвиток культури колективної безпеки на засадах довіри й відповідальності.

Інституційний рівень. Потребує вдосконалення система класифікації та звітності про кіберінциденти, зокрема шляхом узгодження національних підходів із *ENISA Reference Incident Classification Taxonomy* [126]. Доцільним видається подальше вдосконалення механізмів оперативного інформаційного обміну між державними та відомчими центрами реагування на інциденти (CSIRT/SOC), що забезпечуватиме мінімізацію часових затримок у виявленні кіберзагроз і підвищення узгодженості дій суб'єктів національної системи кібербезпек [198; 75]. У цьому контексті актуалізується потреба у правовій формалізації публічно-приватної взаємодії, зокрема шляхом розроблення типових угод про рівень надання послуг (SLA) для критичних цифрових сервісів, що відповідає доктринальним підходам до інституціоналізації публічно-приватного партнерства у сфері кіберзахисту [214].

Технічний рівень. Подальшого вдосконалення потребує впровадження базових технічних стандартів безпеки для операторів об'єктів критичної інфраструктури з урахуванням положень міжнародних рекомендацій *CISA/NSA* та рамкових настанов *Shields Up* [203]. Оптимізація відповідних процесів має охоплювати системну інвентаризацію активів, сегментацію технологічних мереж, управління доступом і привілеями користувачів, постійний моніторинг аномальної активності, а також резервування та геодиверсифікацію каналів зв'язку й постачальників цифрових сервісів. Урахування досвіду інцидентів, пов'язаних із діяльністю угруповання *Sandworm* (зокрема випадків *Industroyer* та *Industroyer2*) [243; 305], свідчить про доцільність інституціоналізації практики регулярних перевірок типу «червоні команди» у технологічних мережах як елемента управління операційними ризиками. Зазначені заходи корелюють із висновками звіту *ENISA Threat Landscape 2023* [215], у якому наголошено на важливості

інтеграції превентивних технічних контролів у загальну систему управління кібербезпекою та забезпечення сталості критичних цифрових процесів.

Соціально-комунікаційний рівень. У сфері комунікацій та людського чинника вдосконалення потребують протоколи кризового інформування й публічних комунікацій, що забезпечують достовірність і своєчасність офіційних повідомлень під час кіберінцидентів [75; 222]. Необхідним є розширення практики навчання з кібергігієни та протидії соціальній інженерії для працівників державного сектору та представників малого і середнього бізнесу, що узгоджується з рекомендаціями *ENISA* (2023) [215] та аналітичними матеріалами *Microsoft* [282]. Окремої уваги потребує нормативне врегулювання взаємодії між державними структурами та волонтерськими кіберспільнотами в межах публічно-приватного партнерства, що відповідає міжнародній практиці та висновкам дослідників і журналістських розслідувань [352; 180].

Сформульовані підходи узгоджуються зі змістом проаналізованих джерел і відтворюють їхні ключові положення: емпіричні кейси (Ukrtelecom, KA-SAT/Viasat, OT-ланцюжки) підтверджують наявність системної взаємозалежності між критичними секторами та актуалізують необхідність підвищення рівня їхньої технологічної і організаційної захищеності [163]; офіційні рекомендації CISA/NSA та ENISA конкретизують базові вимоги до технічної, організаційної та комунікаційної безпеки, визначаючи орієнтири для адаптації національних стандартів кіберзахисту до міжнародної практики [198; 183; 305]; українська правова доктрина та звітність компетентних органів відображають потребу в уніфікації управлінських процедур і посиленні правових механізмів відповідальності у сфері кібербезпеки, що є необхідною умовою розвитку ефективної національної системи кіберстійкості [2; 59; 75].

Для систематизації отриманих результатів і подальшого аналітичного узагальнення доцільним є представлення виявлених структурних вразливостей та відповідних напрямів їх мінімізації у вигляді аналітичної

матриці, яка інтегрує основні висновки дослідження. Така форма подання сприяє цілісному відображенню взаємозв'язків між видами вразливостей, їхніми емпіричними проявами та потенційними заходами вдосконалення, що базуються на положеннях міжнародних і національних стандартів кібербезпеки.

Група вразливостей	**Основні прояви**	**Напрями вдосконалення та мінімізації ризиків**
Інституційні	Фрагментація повноважень між суб'єктами системи кібербезпеки; відсутність уніфікованої таксономії інцидентів; недостатня формалізація ППП.	Гармонізація національних підходів з ENISA RICT; розвиток механізмів оперативного обміну між CSIRT/SOC; правове оформлення SLA для критичних цифрових сервісів.
Технічні	Уразливість OT/ICS через недостатню сегментацію; залежність ланцюгів постачання; комбіновані атаки (wiper, DDoS, фішинг).	Гармонізація технічних вимог із рекомендаціями CISA/NSA (Shields Up, OT-Advisories); удосконалення резервування та геодиверсифікації; регулярні «red team exercises» для перевірки ICS/SCADA; законодавче закріплення базових технічних контролів.
Соціально-комунікаційні	Використання соціальної інженерії; поєднання технічних атак із дезінформаційними кампаніями; неформалізованість волонтерських кіберініціатив.	Розвиток навчання з кібергігієни; удосконалення кризових протоколів комунікації; нормативне врегулювання ППП із волонтерськими спільнотами.

Таблиця 2.3. Аналітична матриця структурних вразливостей і напрямів їх мінімізації [2]

[2] Таблицю сформовано на основі офіційних звітів і попереджень Cybersecurity and Infrastructure Security Agency (CISA) – Alerts AA22-110A, AA22-265A, AA22-103A (2022–2023); National Security Agency (NSA) – Joint Cybersecurity Advisories on OT/ICS security (2022–2023); European Union Agency for Cybersecurity (ENISA) – Threat Landscape 2022–2023, Reference Incident Classification Taxonomy (RICT); NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) – Cyber Defence Analysis on Ukraine (2022); European Parliamentary Research Service (EPRS) – Cyberattacks in the Context of Russia's War Against Ukraine (2022); аналітичних звітів Microsoft (Special Report: Ukraine Conflict, 2022–2023) та Accenture (Global Incident Report: Russia–Ukraine Crisis, 2022); публікацій Chatham House (Cyber Operations and Information Warfare in Ukraine, 2023); наукових і практичних праць О. А. Алексеєвої, В. М. Ліпкана, І. В. Тарасюка, Н. В. Тіщенка, А. С. Логвиненка, К. Eichensehr, S. Shackelford, а також щорічних звітів Державної служби спеціального зв'язку та захисту інформації України (2022–2024).

Як показано в таблиці, всі три групи вразливостей взаємопов'язані та формують багаторівневу систему ризиків, у якій технічні дефекти посилюються інституційною фрагментацією та комунікаційною неузгодженістю. Представлена матриця відображає системний підхід до оцінювання стану кіберстійкості України й окреслює базові орієнтири для подальшого вдосконалення державної політики у сфері кібербезпеки.

Структурні вразливості системи національної кіберстійкості мають комплексний, багаторівневий характер і проявляються у поєднанні управлінських, технічних та соціально-комунікаційних дефіцитів. Їх наявність знижує ефективність реагування на кіберінциденти та створює умови для каскадного поширення загроз у суміжних секторах. Подолання таких вразливостей вимагає переходу до проактивної моделі кіберзахисту, заснованої на стандартизованих процедурах обміну інформацією, уніфікованих технічних контролях та формуванні довіри як стратегічної складової національної безпеки. Зміцнення кіберстійкості України можливе за умови синхронізації інституційних реформ, імплементації міжнародних стандартів ENISA і CISA/NSA, а також розвитку нормативно врегульованого публічно-приватного партнерства, яке інтегрує ресурси держави, бізнесу та громадянського суспільства в єдину екосистему цифрової безпеки.

2.4. Актуальні проблеми протидії кіберзлочинності та кібератрегресії: правовий, інституційний та процедурний виміри

Аналіз, здійснений у попередніх підрозділах, окреслив складну багаторівневу структуру кібератрегресії проти України, її інструменти, динаміку та наслідки для системи національної безпеки. У підрозділі 2.1 простежено еволюцію кібероперацій як форми сучасного гібридного протиборства, визначено їх цільові настанови, технічні й інформаційні засоби, а також виявлено правові невизначеності, що стосуються меж застосування сили,

атрибуції та співвідношення державного і приватного секторів у забезпеченні кіберзахисту. На цьому тлі емпіричні матеріали підрозділу 2.2 продемонстрували поступовий перехід від поодиноких деструктивних дій до комплексних, скоординованих операцій, спрямованих на критичну інфраструктуру, державне управління та суспільні комунікації. Приклади атак – від енергетичних інцидентів Sandworm і кампанії NotPetya до втручань у мережі KA-SAT/Viasat та масових DDoS-операцій – засвідчили, що цифрові засоби дедалі частіше використовуються як самостійний інструмент стратегічного впливу, здатний спричиняти ефекти, співмірні з традиційними воєнними діями [166; 243; 244; 172; 196; 185; 249].

У подальшому аналізі (пп.2.3.) було встановлено, що ефективність таких атак зумовлена не лише їх технологічною складністю, а й внутрішніми чинниками державної кіберстійкості. Уразливість критичних секторів постає наслідком поєднання інституційно-правових, техніко-організаційних і соціально-комунікаційних дефіцитів. До найпомітніших належать фрагментарність повноважень між суб’єктами системи кібербезпеки, відсутність уніфікованих процедур інцидент-репортингу, недостатня стандартизація технічних контролів і залежність від зовнішніх постачальників цифрових сервісів, а також низький рівень узгодженості кризових комунікацій та підготовки персоналу [75; 223; 224; 288]. Своєрідною «точкою розриву» виявилася й неформалізована участь приватних і волонтерських структур у забезпеченні кіберзахисту, що водночас посилює адаптивність системи й підвищує ризики правової неврегульованості [185; 352; 213; 320].

Узагальнення результатів попереднього аналізу дає підстави розглядати сучасну модель реагування на кіберзагрози як переважно реактивну, зорієнтовану на постфактум-виявлення інцидентів і локальне усунення наслідків. Натомість масштаби та комплексність сучасних кібератак вимагають переходу до інтегрованої, проактивної системи протидії, у якій технічні, правові та організаційні засоби взаємодоповнюють один

одного [215; 217; 202; 203]. Відсутність сталих процедур атрибуції, процесуального закріплення цифрових доказів, єдиних стандартів звітності та координації дій між державними і приватними структурами, а також нерозвиненість позакримінальних механізмів реагування – санкцій, публічних атрибуцій, кібердипломатичних кроків – формують комплекс структурних проблем, що визначають ефективність національної відповіді на кіберагресію.

Подальший аналіз зосереджується на окресленні цих проблем у правовому, інституційному та процедурному вимірах, розкриваючи їхній взаємозв'язок із виявленими вразливостями критичної інфраструктури та суспільства. Такий підхід забезпечує логічний перехід від аналітичного розгляду загроз до вироблення системних орієнтирів удосконалення державної політики кібербезпеки, що надалі буде співвіднесено з міжнародними моделями управління кіберстійкістю, розглянутими у третьому розділі.

Сучасна система протидії кіберзлочинності та кіберагресії в Україні є переважно орієнтованою на реагування постфактум. Вона спирається насамперед на кримінально-правові інструменти, створені для «класичних» злочинів, тоді як гібридні кібероперації мають міждержавний і військово-політичний вимір [140; 76; 30]. За таких умов постають три взаємопов'язані групи проблем: *(1) атрибуція та доказування* (технічна і юридична ідентифікація суб'єкта атаки, процесуальний статус і придатність цифрових доказів) [211; 328; 214]; (*2) нормативно-правова невизначеність і фрагментація режимів* (розрив між кримінально-правовими процедурами та механізмами міжнародно-правової відповідальності держав, включно з санкційними інструментами й нормами МГП) [247; 312; 189; 306]; *(3) інституційно-організаційні спроможності* (координація органів, стандарти взаємодії з приватним сектором і міжнародними партнерами, оперативні протоколи запобігання та стійкості критичної інфраструктури) [75; 223; 226; 202].

Атрибуція та доказування. Атрибуція у кіберпросторі має подвійний –технічний і юридичний – вимір. Технічна атрибуція полягає у встановленні джерела або виконавця кібератаки на основі телеметричних даних, індикаторів компрометації (IoC) та типових тактик, технік і процедур (TTPs). Юридична атрибуція, натомість, передбачає віднесення встановленої поведінки до конкретної держави, що зумовлює настання міжнародно-правової відповідальності. Перехід від технічних артефактів до правових висновків становить одну з найскладніших проблем сучасного міжнародного права кіберпростору [328]. Це зумовлено децентралізованою архітектурою мережі, використанням «проксі»-акторів, ботнетів і автономних шкідливих програм, а також навмисними операціями з дезінформації, що ускладнюють ідентифікацію фактичного джерела атаки.

Як слушно зазначає M. Roscini, навіть точне визначення технічного походження кібератаки не гарантує доведення державного контролю над нею, оскільки традиційні критерії ефективного контролю, розроблені в межах Статей про відповідальність держав (ARSIWA), не завжди можуть бути застосовані до кіберсередовища [312; 345]. Подібну позицію висловлює M. Schmitt, наголошуючи, що технічні показники самі по собі рідко є достатніми для юридичної атрибуції, адже між технічними даними та міжнародно-правовими стандартами відповідальності існує «сіра зона» невизначеності [317; 319]. Tsagourias, Nicholas & Farrell, розвиваючи цю тезу, підкреслюють, що процес атрибуції у кіберпросторі має одночасно технічну й правову природу, а перехід між ними супроводжується доказовою та нормативно-правовою невизначеністю, спричиненою складністю підтвердження автентичності цифрових слідів і можливістю навмисного введення в оману шляхом «false flag operations» [328]. Унаслідок цього атрибуція набуває багаторівневого, міждисциплінарного характеру, що потребує поєднання технічної експертизи, процесуальних стандартів доказування та міждержавної співпраці у сфері кіберзахисту.

Міжнародно-правові критерії віднесення поведінки до держави у сфері кібероперацій визначаються *Проєктом статей про відповідальність держав за міжнародно-протиправні діяння* (ARSIWA): дії будь-якого органу держави, а також приватних осіб чи груп, що діють за «напрямом або контролем» держави, можуть бути атрибутовані їй із настанням міжнародно-правової відповідальності [345]. Застосовність загальних норм міжнародного права до кіберпростору неодноразово підтверджувалася в межах ООН: у звітах Групи урядових експертів (GGE) 2010 та 2013 рр. держави визнали чинність Статуту ООН та принципів суверенітету, невтручання і належної обачності щодо діяльності у кіберсфері [339; 340]. Звіт Групи урядових експертів ООН 2015 р. уточнив обов'язок держав не допускати використання власної території для міжнародно-протиправних дій із застосуванням ІКТ, що конкретизує принцип due diligence. Подальші документи підтвердили цю позицію: GGE 2021 р. наголосив на чинності міжнародного права в кіберпросторі та необхідності його добросовісного застосування [342], а Відкрита робоча група (OEWG) у 2021 р. акцентувала на прозорості, довірі та відповідальності у сфері ІКТ [344]. У прогрес-звіті OEWG 2024 р. підкреслено потребу спільних підходів до атрибуції кіберінцидентів і механізмів обміну інформацією для запобігання ескалації [348]. Зазначені положення узгоджуються із резолюцією ГА ООН 70/237 щодо відповідальної поведінки держав у кіберпросторі [341].

Окремі держави конкретизували ці принципи у національних позиційних документах. Франція у *Droit international appliqué aux opérations dans le cyberespace* підкреслює обов'язковий характер принципу суверенітету та можливість міжнародно-правової відповідальності за його порушення [240]. Німеччина у *Position Paper on International Law in Cyberspace* підтверджує застосовність норм про державну відповідальність (зокрема статей 4–8 ARSIWA) і визнає порушення суверенітету самостійним міжнародно-протиправним діянням [238]. Нідерланди у листі до парламенту також наголошують на чинності принципів суверенітету, невтручання та

належної обачності [242]. Схожі підходи демонструють Канада [175], Японія [264] та Нова Зеландія [297], які прямо пов’язують віднесення кібероперацій до держави з критеріями ARSIWA.

Водночас Велика Британія у промові Генерального прокурора застерігає, що не кожне посягання на суверенітет автоматично становить міжнародно-протиправне діяння [337].

У підсумку, нормативну рамку становить поєднання універсальних положень ARSIWA [345], напрацювань ООН (GGE/OEWG) [339; 340; 342; 348] та державних інтерпретацій; попри розбіжності в деталях, консенсус полягає у чинності міжнародного права в кіберпросторі та відповідальності держав за дії їхніх органів і підконтрольних суб’єктів.

Формат «публічної атрибуції» – узгоджені заяви урядів або міждержавних коаліцій – набув виразності у випадку кібератаки на супутникову мережу KA-SAT/Viasat у лютому 2022 р., коли ЄС, Велика Британія та США публічно заявили про причетність Російської Федерації, посилаючись на результати міжвідомчого аналізу розвідданих і технічних індикаторів компрометації [190; 196; 335].

Подібним чином, у лютому 2022 р. США та Велика Британія приписали відповідальність за серію DDoS-атак проти українських банків і державних онлайн-ресурсів російським державним структурам, зокрема підрозділам, пов’язаним із Головним управлінням Генерального штабу ЗС РФ (ГРУ), на підставі розвідданих і технічного аналізу, не розкриваючи повну доказову базу з міркувань безпеки [249; 333]. Такі заяви мають вагомий нормативно-політичний ефект, однак їхня доказова прозорість часто обмежена режимами секретності та договірними зобов’язаннями комерційних провайдерів, що впливає на подальше використання матеріалів у судових чи санкційних процедурах [211; 212]. Відтак для забезпечення відтворюваності та процесуальної стійкості висновків про атрибуцію необхідним є формування «кейс-файлів» зі структурованими індикаторами (IoC/TTPs), чіткою методологією збору та фіксацією *chain of custody* –

підходи, які підтримує і практичний посібник CCDCOE щодо вироблення державних позицій із міжнародного права у сфері кібердіяльності [178].

Технічна атрибуція ґрунтується на аналізі телеметричних даних, індикаторів компрометації (IoC) та типових тактик і процедур (TTPs), які фіксуються спеціалізованими командами реагування та приватними компаніями у сфері кібербезпеки [215; 216; 211; 328]. Для України релевантні приклади включають документування шкідливих програм типу wiper (зокрема CaddyWiper) у 2022 р. [218; 219; 236], зафіксовану атаку на Ukrtelecom [163; 195] та аналітику промислових інцидентів, пов'язаних із діяльністю групи Sandworm [243; 282; 305]. Ці джерела формують емпіричну основу технічного доказування, однак самі по собі не є достатніми для встановлення міжнародно-правової відповідальності без належної процесуальної верифікації [211; 328; 247; 312].

Водночас первинне виявлення більшості інцидентів здійснюється саме приватними структурами – постачальниками цифрових сервісів, провайдерами хмарних технологій і антивірусними вендорами. Це створює інформаційну асиметрію між державними та недержавними акторами й обмежує доступ до повних даних через умови конфіденційності. З огляду на це міжнародна практика, представлена у звітах ENISA та CCDCOE, наголошує на потребі публічно-приватного партнерства (ППП) у сфері кібердоказування – спільних стандартів збереження цифрових артефактів, фіксації ланцюга збереження (*chain of custody*) і незалежної експертизи [215;223;226;288].

Процесуальний аспект атрибуції безпосередньо пов'язаний із кримінально-правовими механізмами. Конвенція про кіберзлочинність (ETS 185) [187; 188] та Другий додатковий протокол (CETS 224) [189] забезпечують правову основу транскордонного доступу до електронних доказів і взаємодії компетентних органів [184; 256]. Проте ці інструменти стосуються індивідуальної відповідальності – для кваліфікації міждержавних дій застосовуються норми Проєкту статей про відповідальність держав

(ARSIWA) [345]. В українському контексті процесуальні реформи воєнного часу, зокрема спрощений порядок фіксації електронних доказів «за гарячими слідами», сприяли оперативності документування інцидентів [85; 81].

Особливу складність становить визначення порогів кваліфікації кібердій між «застосуванням сили» та «забороненим втручанням». Міжнародна доктрина вказує на «сіру зону» між цими категоріями, коли нефізичні ефекти –припинення послуг чи збої інфраструктури –можуть мати стратегічні наслідки, але не досягають рівня збройного нападу [169; 247; 312; 319; 266; 278]. У разі міжнародного збройного конфлікту застосовні норми міжнародного гуманітарного права, зокрема Додаткового протоколу I, що встановлює обов'язок захисту цивільних осіб і критичної інфраструктури [306; 253; 255].

На рівні міжнародної відповідальності Європейський Союз запровадив «кіберсанкційний» режим як частину EU Cyber Diplomacy Toolbox – інструмент реагування на атрибутовані кібератаки [186; 191; 285]. Його застосування вимагає достовірної фактологічної бази та узгоджених стандартів класифікації інцидентів, що підтримуються ENISA [215; 216; 223].

Узагальнення українського досвіду – від *DDoS*-кампаній до *wiper*-операцій – підтверджує необхідність розбудови повного циклу атрибуції: від технічної фіксації артефактів до процесуальної легітимації й міжнародного визнання. Лише інтеграція технічних, правових і організаційних механізмів дозволяє перетворити емпіричні дані на доказову базу, придатну для відповідальності як приватних осіб, так і держав-ініціаторів кібероперацій [45; 141; 142; 320].

Нормативно-правова невизначеність і фрагментація режимів. Нормативно-правова невизначеність і фрагментація режимів. Нормативно-правова невизначеність у сфері міжнародного регулювання кібердіяльності зумовлена відсутністю єдиного універсального міжнародного договору, який би комплексно визначав правила поведінки держав у кіберпросторі. На глобальному рівні сформувалася множинність правових режимів –

міжнародного публічного, гуманітарного, безпекового, кримінального права, а також регіональних інструментів боротьби з кіберзлочинністю (зокрема, Конвенції ETS 185 та Додаткового протоколу CETS 224) [48; 49; 116; 187; 189]. Зазначені режими лише частково перетинаються, проте не утворюють узгодженої системи регулювання, що посилює фрагментацію міжнародного правопорядку в кіберсфері [45; 49; 50; 142].

Унаслідок цього одна й та сама кібератака може одночасно підпадати під дію різних правових режимів – кримінально-правового, санкційного або міжнародно-політичного, – залежно від характеру суб'єкта, масштабів наслідків та політичного контексту [45; 46; 50]. Додатковим чинником нормативної невизначеності є відсутність усталених критеріїв кваліфікації кібердій за ступенем їх інтенсивності та наслідків. Як зазначають M. Schmitt та N. Tsagourias, сучасне міжнародне право не встановлює чіткої межі між поняттями «застосування сили», «збройний напад» і «заборонене втручання», що породжує так звану «сіру зону» між військовими та невійськовими кібероперaціями [317; 319; 327; 328]. Внаслідок цього держави по-різному тлумачать базові принципи міжнародного права – суверенітету, невтручання та належної обачності (due diligence), що ускладнює формування єдиних стандартів поведінки в кіберпросторі [142; 238; 240; 242].

У таких умовах позакримінальні засоби реагування – санкційні, дипломатичні та інформаційно-політичні – набувають особливого значення як практичний інструмент заповнення нормативних прогалин і узгодження національних підходів до атрибуції та міжнародно-правової відповідальності. Вони виконують функцію своєрідної *«міжрівневої ланки»* між технічним етапом встановлення джерела кібератаки, юридичними процедурами кваліфікації діяння та політико-дипломатичними формами міжнародної реакції [53; 141; 271; 272; 281; 320; 355].

Позакримінальні засоби реагування. Коли кіберінцидент має ознаки державної участі, традиційні кримінально-правові механізми виявляються недостатніми для забезпечення повної та ефективної відповідальності

суб'єкта. У таких випадках необхідним є застосування позакримінальних засобів реагування, які охоплюють міжнародно-правові, санкційні та політико-дипломатичні інструменти. Їхнє призначення полягає у встановленні факту протиправного втручання, формуванні доказової бази, консолідації міжнародного осуду та відновленні безпеки у кіберпросторі [285].

Європейський Союз сформував цілісну нормативно-політичну архітектуру таких заходів у межах EU Cyber Diplomacy Toolbox (2017), що передбачає багаторівневу систему реагування на зловмисну кібердіяльність – від дипломатичних демаршів і публічних заяв до запровадження обмежувальних заходів і санкційних рішень [220; 285]. Правовими підставами цього режиму є Рішення Ради (CFSP) 2019/797 та Регламент (EU) 2019/796, якими встановлено спеціальний порядок застосування обмежувальних заходів ЄС у відповідь на серйозні кібератаки [186; 191]. Цей режим передбачає замороження активів, заборону на в'їзд і інші санкції щодо фізичних та юридичних осіб, причетних до таких дій [186; 191].

Зазначений механізм було реалізовано 30 липня 2020 року, коли Європейський Союз ухвалив рішення про введення санкцій проти шести фізичних осіб і трьох організацій, залучених до масштабних кібератак NotPetya (2017), Cloud Hopper (2014–2017) та спроби зламу OPCW. До санкційного списку було внесено, зокрема, структурні підрозділи ГРУ та угруповання Sandworm, яке неодноразово здійснювало атаки проти критичної інфраструктури України [289; 243; 305].

У травні 2022 року Європейський Союз оприлюднив Декларацію про кібератаку на супутникову мережу KA-SAT/Viasat, у якій публічно приписав відповідальність Російській Федерації. Цей крок став важливим прецедентом застосування механізмів кібердипломатії без запровадження нових санкцій [190; 172; 196].

Публічна атрибуція у подібних випадках має не лише політичний, а й нормативний вимір. Вона виконує функцію «комунікації норм» –

підтверджує чинність міжнародно-правових стандартів поведінки держав у кіберпросторі та слугує засобом превентивного стримування подальших агресивних дій [232; 233]. Водночас прозорість доказової бази таких заяв є обмеженою через режим секретності, комерційні зобов'язання приватних провайдерів та відсутність уніфікованих процедур перевірки технічних артефактів. З огляду на це CCDCOE та ENISA підкреслюють необхідність формування відтворюваних *«кейс-файлів»*, які містять стандартизовані індикатори компрометації (IoC/TTPs), методики збору даних та фіксацію ланцюга збереження доказів (*chain of custody*) [178; 215; 216]. Запровадження таких підходів забезпечує процесуальну придатність результатів атрибуції для їх подальшого використання у міжнародно-правових і санкційних процедурах [328; 215].

В українському контексті аналіз практики реагування, здійснений EPRS (2022) та CCDCOE (2025), свідчить, що позакримінальні інструменти наразі застосовуються епізодично – переважно у формі публічних заяв про міжнародну солідарність або в межах спільних дипломатичних кроків [178; 222; 190; 335]. Відсутність налагодженого міжвідомчого механізму координації таких дій обмежує їхню результативність та міжнародну видимість [256; 273]. На цій підставі актуальним завданням постає формування національної моделі кібердипломатії, яка б інтегрувала діяльність Міністерства закордонних справ, Державної служби спеціального зв'язку та захисту інформації (CERT-UA), Служби безпеки України, Міністерства оборони та Міністерства цифрової трансформації, забезпечуючи узгоджене ініціювання санкційних і політико-дипломатичних заходів [64; 71; 111; 117].

Узагальнюючи, позакримінальні засоби реагування становлять невід'ємний елемент сучасної системи кіберстійкості, який поєднує технічний, правовий і політичний рівні державної відповіді на кібератаки. Їх інтеграція у національну практику створює передумови для переходу від реактивного до проактивного, стратегічно скоординованого формату

кіберзахисту, у межах якого юридичні, дипломатичні та санкційні інструменти забезпечують цілісний цикл державного реагування на кіберзагрози [64; 117; 223; 224; 225].

Інституційно-організаційні спроможності та кіберстійкість. Як засвідчено у підрозділі 2.3, структурні вразливості критичної інфраструктури України посилюються через фрагментарність механізмів виявлення й обміну інформацією про кіберінциденти [71; 75; 98]. На відміну від європейської практики, де сформовано цілісну систему обов'язкового повідомлення та міжсекторальної координації дій у разі кіберінцидентів [225; 227; 229; 231], в Україні такі процедури досі реалізуються переважно у відомчому форматі [75; 101; 111]. Як зазначено у звітах Європейської парламентської дослідницької служби (EPRS, 2022) та Агентства з кібербезпеки і безпеки інфраструктури США (CISA, 2022) [222; 182; 203], механізми реагування залишаються фрагментованими, а обмін інформацією між державними структурами, CERT-UA, приватним сектором і операторами критичної інфраструктури не має уніфікованої платформи чи сталих протоколів. Відсутність централізованої системи інцидент-репортингу ускладнює своєчасне виявлення атак, аналіз їхніх каскадних наслідків і формування доказової бази для національних та міжнародних органів реагування [75; 200; 201].

Європейський Союз виробив комплексну нормативну основу, яка визначає єдині стандарти повідомлення про інциденти, оцінки ризиків і перевірки готовності операторів критичних послуг [173; 181; 220; 227]. Директива (ЄС) 2022/2555 (NIS2) установлює обов'язкові процедури нотифікації для «суттєвих» і «важливих» суб'єктів, передбачаючи поетапну звітність: раннє попередження – протягом 24 годин, проміжне повідомлення – у межах 72 годин і фінальний звіт – протягом місяця після інциденту [173; 207].

Регламент (ЄС) 2024/2847 (Cyber Resilience Act, CRA) установлює горизонтальні вимоги до кіберстійкості «продуктів із цифровими

елементами» та покладає на виробників обов’язок повідомляти про активно експлуатовані вразливості й серйозні інциденти через єдину платформу звітності (ст. 14, 16). Згідно зі ст. 14, виробник має надіслати попереднє повідомлення протягом 24 годин, основне – упродовж 72 годин, а підсумковий звіт – не пізніше ніж через 14 днів / один місяць залежно від типу події. Відповідні вимоги до звітування почнуть діяти з 11 вересня 2026 р., а повна застосовність Регламенту – з 11 грудня 2027 р. [173; 230].

Регламент «Про кіберсолідарність» (Cyber Solidarity Act) запроваджує механізми спільної готовності та реагування, створення транскордонних центрів моніторингу (SOC) та резерву експертів для оперативної допомоги під час масштабних інцидентів. ENISA забезпечує методологічну підтримку цих інструментів, розробляючи уніфіковану таксономію інцидентів і рекомендації для обміну телеметрією між секторами [215; 216; 223; 224; 227; 231].

Національна система кіберзахисту України перебуває на етапі поступової гармонізації з європейськими підходами. Базові вимоги до захисту об’єктів критичної інформаційної інфраструктури закріплено у постановах Кабінету Міністрів № 518 від 19.06.2019 р. та № 1176 від 11.11.2020 р., які регламентують порядок огляду стану кіберзахисту державних інформаційних ресурсів [95; 101; 106]. Постанова № 1426 від 29.12.2021 р. визначає організаційно-технічну модель кіберзахисту та координаційні повноваження Державної служби спеціального зв’язку [69; 98; 111]. Розвиток механізмів виявлення уразливостей і реагування підтримано постановою № 1295 від 09.12.2020 р. [22; 75].

У 2025 р. ухвалено Закон № 4336-IX “Про внесення змін до деяких законів України щодо удосконалення системи захисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури” [81; 106; 111], який уточнює правові вимоги до захисту державних інформаційних ресурсів і критичної інфраструктури, а також

затверджено План реалізації Стратегії кібербезпеки на 2025 рік, спрямований на подальшу імплементацію норм ЄС [96; 97; 117; 121; 220].

Попри певний прогрес, система залишається переважно такою, що реагує постфактум: обмін інформацією між CERT-UA, правоохоронними органами та операторами КІ не є повністю інтегрованим, а процедури звітування про інциденти – неоднорідні [47, 61, 75]. Практичні приклади підтверджують, що відсутність стандартизованого інцидент-репортингу й єдиної бази індикаторів компрометації обмежує ефективність реагування [46, 216]. Документовані операції типу wiper, атака на Ukrtelecom та ланцюги ураження ICS/OT-систем, що приписуються угрупованню Sandworm/Industroyer2, демонструють потребу у формалізованих протоколах звітування та регулярних аудитах безпеки промислових мереж [163, 218, 268, 305]. Як слушно зазначається в авторській публікації [46], ефективна протидія гібридним кібератакам можлива лише за умови синергії технічних, організаційних і правових стандартів, що забезпечують єдину систему інцидент-репортингу та верифікацію цифрових доказів [46, 50, 51, 355]. Саме така взаємодія визначає сучасну модель кіберстійкості, яка формується в Україні у процесі гармонізації з європейськими нормами [47, 207, 230]. У звітах CISA та NSA аналогічно підкреслюється важливість регулярної перевірки архітектури безпеки, сегментації мереж і підтримки готовності персоналу [182, 183].

Узагальнюючи результати проведеного аналізу, можна констатувати, що національна система протидії кіберзагрозам в Україні перебуває на етапі інституційного становлення: попри нормативне зближення з європейськими стандартами, її функціонування все ще залишається переважно реактивним [45, 47, 49]. Виявлені структурні вразливості – фрагментарність координації, відсутність єдиних процедур інцидент-репортингу, нерозвиненість механізмів атрибуції та позакримінальних форм реагування – зумовлюють потребу у системному оновленні підходів до забезпечення кіберстійкості [61, 141, 142]. Подальший розгляд у розділі 3 спрямований на порівняльний

аналіз міжнародних стратегій кіберзахисту (США, НАТО, ЄС) та оцінку можливостей їх адаптації в Україні, зокрема через розвиток державно-приватного партнерства і гармонізацію національної моделі кібердипломатії з глобальними стандартами [16; 21; 27; 38; 53; 77; 88; 53, 320].

Висновки до Розділу 2

1. З'ясовано, що кіберагресія, кібероперації та кіберзлочинність становлять три взаємопов'язані, але самостійні правові феномени, кожен із яких має власну юрисдикційну природу, суб'єктний склад і механізми відповідальності. Уточнено, що для належного реагування необхідне поєднання двох взаємодоповнювальних режимів – міжнародно-правового, спрямованого на притягнення держав до відповідальності, та кримінально-правового, орієнтованого на переслідування індивідуальних виконавців.

2. Узагальнено, що кібердії у структурі гібридної агресії мають комплементарний характер і не виступають ізольованим видом збройної активності. Вони інтегруються в загальну систему воєнних дій, поєднуючи технічні, розвідувальні, інформаційно-психологічні та логістичні інструменти впливу. Показано, що ефективна протидія таким діям можлива лише за умови взаємодії державних, приватних і волонтерських структур у режимі оперативного публічно-приватного партнерства, яке забезпечує безперервність функціонування критичних сервісів і каналів комунікації.

3. Систематизовано робочу типологію кіберагресії за трьома взаємопов'язаними осями – «цілі – інструменти – очікувані ефекти». Доведено, що така модель забезпечує уніфікацію опису інцидентів, порівнюваність їхніх наслідків та можливість інтеграції технічних характеристик із правовими режимами реагування.

4. Визначено, що сучасна практика кіберконфліктів формує низку «сірих зон» у міжнародному праві, пов'язаних із визначенням порогів

суверенітету й невтручання, критеріями атрибуції дій держави та правовим режимом доступу до цифрових доказів, що перебувають у розпорядженні приватного сектору. Обґрунтовано потребу уніфікації доктринальних підходів до кваліфікації кібератак і створення механізмів публічно-приватної взаємодії, які б забезпечували баланс між державними повноваженнями та технологічними можливостями недержавних акторів.

5. Встановлено послідовну еволюцію російської кіберагресії проти України у 2014–2024 роках, що охоплює три фази з відмінною технологічною, організаційною та правовою специфікою. Перша фаза (2014–2016) позначена цілеспрямованими атаками на системи критичної енергетичної інфраструктури (Sandworm: BlackEnergy, Industroyer/Industroyer2), які вперше в Європі засвідчили можливість ураження промислових систем керування (ICS/OT) державним актором. Друга фаза (2017–2020) характеризується переходом від окремих цільових операцій до масштабних кампаній у ланцюгах постачання, кульмінацією яких стала атака NotPetya з транскордонними наслідками, що завдала збитків, співмірних із наслідками воєнних дій. Третя фаза (2021–2024) збігається з періодом повномасштабної агресії РФ та позначена багатовекторними деструктивними діями – від атак типу wiper до DDoS і ураження супутникових мереж зв’язку (KA-SAT/Viasat), що свідчить про інтеграцію кібер-, інформаційних і військових засобів у межах єдиного гібридного операційного середовища. Доведено, що зазначені операції мають спільні ознаки державного походження, високого рівня координації та стратегічної спрямованості на підрив стійкості критичної інфраструктури, легітимності публічної влади та суспільних комунікацій.

6. Розроблено аналітичну таблицю-матрицю відповідності «тип атаки – фактичні інциденти», що уніфіковано репрезентує структуру кіберагресії проти України за підходами менеджменту безпеки критичної інфраструктури. Матриця відобразила поступову трансформацію кіберзагроз – від локальних експериментальних операцій до системних, скоординованих

кампаній, у яких поєднано технічні, інформаційно-психологічні та організаційно-управлінські інструменти впливу.

7. Сформовано верифікаційний каркас аналізу на принципі подвійної перевірки та розроблено таблицю-матрицю відповідності «тип атаки – інциденти –джерела», що забезпечує відтворюваність і порівнюваність кейсів та слугує підґрунтям для подальшої правової оцінки

8. Проведено поглиблену правову кваліфікацію ключових кейсів крізь призму суверенітету, невтручання, due diligence та релевантних норм міжнародного гуманітарного права щодо цивільних об’єктів. Показано, що більшість операцій не досягають порогу «застосування сили», проте становлять міжнародно-протиправні втручання; встановлено, що колективні публічні атрибуції формують практику спільного визнання та фіксації державної відповідальності.

9. Здійснено аналітичне узагальнення ключових кейсів кіберагресії проти України і на його підставі ідентифіковано головні чинники уразливості національної критичної інфраструктури: інституційно-правові (фрагментарність повноважень, прогалини у стандартизованому зборі та верифікації цифрових доказів, нечіткість порогів між «невтручанням» і «застосуванням сили»); техніко-організаційні (залежність від ланцюгів постачання і зовнішніх сервісів); соціально-комунікаційні (людський фактор, дезінформація). Показано, що навіть нефізичні операції можуть мати стратегічні наслідки, що вимагає кодифікації критеріїв правової кваліфікації інцидентів та нормативного закріплення процедур доказування.

10. Систематизовано структурні вразливості системи національної кіберстійкості у трьох взаємопов’язаних вимірах – інституційному, технічному та соціально-комунікаційному, і на основі емпіричних кейсів розроблено аналітичну матрицю «вразливість – прояви – напрями вдосконалення». Матриця забезпечує цілісне відображення взаємозалежностей між типами загроз і відповідними інституційно-

правовими та технічними заходами й слугує практичним інструментом для пріоритизації реформ і планування аудитів кіберстійкості.

11. Встановлено, що інституційні вразливості мають характер незавершеного циклу управління ризиками, що проявляється у фрагментації повноважень між суб'єктами системи кібербезпеки, відсутності уніфікованої таксономії інцидентів та нерозвиненості механізмів публічно-приватного партнерства. Обґрунтовано необхідність гармонізації національних підходів з європейськими (ENISA RICT, NIS2), створення механізму оперативного обміну інформацією між державними та відомчими CSIRT/SOC, а також визначено доцільність правового оформлення типових угод про рівень надання послуг (SLA) для критичних цифрових сервісів.

12. Доведено, що технічні вразливості зосереджуються на стику IT/OT-середовищ, у ланцюгах постачання та при використанні зовнішніх хмарних і супутникових сервісів. На основі аналізу міжнародних рекомендацій CISA/NSA (Shields Up, OT-advisories) та звітів ENISA сформульовано напрями оптимізації технічної безпеки, які включають інвентаризацію активів, сегментацію мереж, контроль привілеїв, моніторинг аномалій, резервування й геодиверсифікацію каналів зв'язку. Запропоновано інституціоналізувати практику регулярних перевірок типу «червоні команди» як складову системи управління операційними ризиками.

13. Виявлено, що соціально-комунікаційні чинники – людський фактор, дезінформаційні кампанії та волонтерські кіберініціативи – виступають системоутворювальними елементами кіберстійкості. Показано, що відсутність уніфікованих протоколів кризової комунікації, нерівномірність підготовки кадрів і неформалізованість взаємодії з волонтерськими спільнотами знижують ефективність реагування на інциденти. Обґрунтовано доцільність унормування взаємодії між державними та недержавними акторами в межах публічно-приватного партнерства, а також розширення навчальних програм із кібергігієни та протидії соціальній інженерії.

14. Узагальнено результати аналізу інституційних, технічних та комунікаційних чинників, що впливають на рівень кіберстійкості України, і верифіковано їхній взаємозв'язок як системний комплекс управлінських, технологічних і соціальних вразливостей. На цій основі сформульовано концептуальні орієнтири переходу до проактивної моделі кіберзахисту, заснованої на стандартизованих процедурах обміну інформацією, узгоджених технічних вимогах і розвитку довіри як стратегічного ресурсу цифрової безпеки.

15. Доведено, що зміцнення національної кіберстійкості України потребує інституційного оформлення та нормативної стабілізації публічно-приватного партнерства як складової державної політики у сфері цифрової безпеки. Це передбачає синхронізацію реформ із міжнародними стандартами (ENISA, CISA/NSA, NIS2), розвиток національних процедур обміну інформацією та інтеграцію потенціалу держави, бізнесу й громадянського суспільства у єдину систему кіберстійкості.

16. Встановлено, що кіберагресія проти України у 2014–2024 рр. має багаторівневий, системний і скоординований характер, який охоплює дії проти критичної інфраструктури, державних сервісів і суспільних комунікацій. Її наслідки за масштабом і впливом співмірні з традиційними воєнними діями, що підтверджує трансформацію кіберпростору у сферу стратегічного протиборства. Доведено, що чинна модель реагування України залишається переважно реактивною, зорієнтованою на постфактум-виявлення та локалізацію наслідків, що обмежує ефективність превенції, атрибуції й системної протидії кіберзагрозам.

17. На основі аналізу української практики реагування на кібератаки систематизовано основні проблемні блоки, що зумовлюють обмежену ефективність національної відповіді: (а) атрибуція та доказування – наявність розриву між технічним та юридичним рівнями атрибуції, невизначеність процесуального статусу цифрових доказів; (б) нормативно-правова невизначеність і фрагментація режимів – відсутність універсального

міжнародного договору, різні інтерпретації принципів суверенітету, невтручання та належної обачності, а також розрив між кримінальними процедурами й механізмами міжнародної відповідальності держав; (в) інституційно-організаційні спроможності – фрагментарність повноважень суб'єктів системи кібербезпеки, відсутність уніфікованих процедур інцидент-репортингу, недостатня стандартизація технічних контролів та комунікаційна неузгодженість між секторами.

18. Доведено, що позакримінальні інструменти реагування – санкційні, дипломатичні та механізми публічної атрибуції – є необхідним доповненням до кримінально-правових засобів і слугують практичним механізмом подолання виявлених нормативних прогалин. Вони сприяють відтворенню міжнародно-правових норм через практику публічних реакцій і колективних санкційних дій, підсилюючи ефективність системи колективного стримування й превенції кіберагресії.

19. Запропоновано методологічні орієнтири підвищення процесуальної стійкості атрибуції кібератак: створення відтворюваних «кейс-файлів», що включають стандартизовані індикатори компрометації (IoC/TTPs), уніфіковані методики збору даних і фіксацію ланцюга збереження доказів (chain of custody), а також інституціалізацію публічно-приватного партнерства для подолання інформаційної асиметрії між державними структурами та провайдерами цифрових послуг.

РОЗДІЛ 3
МІЖНАРОДНО-ПРАВОВИЙ ДОСВІД СТРАТЕГІЙ КІБЕРЗАХИСТУ І ПЕРСПЕКТИВИ ЙОГО АДАПТАЦІЇ В УКРАЇНІ

Виявлені у попередніх розділах закономірності розвитку національної системи кіберзахисту показали, що її подальше вдосконалення потребує опори на міжнародно визнані стандарти регулювання. Зіставлення наявних правових інститутів і процедур з тими, що функціонують у провідних демократичних державах, є необхідною умовою формування цілісної моделі кіберстійкості. Таким чином, результати попереднього аналізу не лише окреслили проблемні зони українського правопорядку, а й визначили орієнтири для їх подолання через вивчення зарубіжних практик, де відповідні норми вже мають усталену правову форму та перевірену ефективність.

З огляду на це, Розділ 3 спрямовано на дослідження міжнародного досвіду правового забезпечення кібербезпеки та визначення його потенціалу для адаптації в Україні. У центрі уваги – три основні моделі: нормативно-зобов'язуюча модель Європейського Союзу [220], регуляторно-стандартна модель Сполучених Штатів Америки [324] та координаційно-політична модель Організації Північноатлантичного договору [292]. Їхнє вивчення дає змогу простежити, яким чином у різних правових системах поєднуються інструменти державного регулювання, ринкових стимулів і механізмів міжнародної взаємодії у сфері кіберстійкості.

Джерельну базу становлять офіційні документи Європейського Союзу –The EU's Cybersecurity Strategy for the Digital Decade [220], директиви NIS 2 [207], регламенти DORA [229], CRA [230], DSA [228], Cyber Solidarity Act [231], Cybersecurity Act [227] та методичні матеріали ENISA [223–226]; нормативно-стратегічні акти уряду США – National Cybersecurity Strategy 2023 [324], Executive Order 14028 [351], TSA Security Directive 2021-01D [326], NIST Cybersecurity Framework 2.0 [304]; а також політичні рішення і правові напрацювання НАТО та CCDCOE [292; 287–291]. Порівняльно-

правовий аналіз здійснюється за критеріями: (1) джерело й юридична сила норми; (2) суб'єкти та їх обов'язки; (3) механізми звітування та обміну інформацією; (4) нагляд і санкції; (5) стандартизація та сертифікація; (6) інституційна координація та колективне реагування.

Метою є з'ясування, які правові інструменти довели результативність у практиці ЄС, США та НАТО, та яким чином їх можна адаптувати до українського законодавства як основу для модернізації системи кібербезпеки відповідно до принципів acquis ЄС і глобальних стандартів.

3.1. Стратегії кіберзахисту США, НАТО та ЄС: порівняльно-правовий аналіз

Європейський Союз: «жорстке право» та інституційна екосистема. Європейський Союз упродовж останнього десятиліття сформував послідовну, багаторівневу систему правового регулювання кібербезпеки, що поєднує обов'язкові норми («жорстке право») та координаційно-інституційні механізми їх реалізації. Від початкових рамкових рекомендацій ЄС перейшов до нормативно зобов'язувальної моделі, у якій директиви та регламенти встановлюють прямі юридичні обов'язки для держав-членів і визначених суб'єктів як у публічному, так і в приватному секторах [220; 221].

Фундамент сучасної європейської системи кіберзахисту становить узгоджений пакет актів, що формує нормативну екосистему кіберстійкості. До нього входять: Директива (ЄС) 2022/2555 (NIS2) [207]; Директива (ЄС) 2022/2557 (CER) [207]; Регламент (ЄС) 2022/2554 (DORA) [229]; Регламент (ЄС) 2024/2847 (CRA) [230]; Регламент (ЄС) 2022/2065 (DSA) [228]; Регламент (ЄС) 2025/38 (Cyber Solidarity Act) [231]; Регламент (ЄС) 2019/881 (Cybersecurity Act) [227]. Практична імплементація цього комплексу забезпечується методичними документами та рекомендаціями Європейського

агентства з кібербезпеки (ENISA), які виконують функцію «м'якого права» (soft law), особливо у сферах кризового менеджменту, оцінки ризиків і розроблення національних стратегій кібербезпеки [223; 224; 225].

Директива (ЄС) 2022/2555 (NIS 2) є центральним елементом сучасного нормативного оновлення у сфері кібербезпеки Європейського Союзу, покликаним забезпечити високий спільний рівень кіберстійкості в межах Союзу. Вона замінила попередню Директиву 2016/1148, розширивши сферу регулювання та уточнивши обов'язки держав-членів і суб'єктів господарювання [207]. Основна мета директиви – гармонізація вимог щодо управління ризиками та реагування на кіберінциденти шляхом установлення обов'язкових мінімальних стандартів для організацій, діяльність яких є критично важливою для стабільності внутрішнього ринку ЄС.

Директива вводить поділ суб'єктів на «суттєві» (essential entities) та «важливі» (important entities) залежно від критичності сектору та потенційного впливу їхньої діяльності на безпеку Союзу. Для обох категорій визначено обов'язки щодо впровадження систем управління ризиками, періодичного оцінювання вразливостей, забезпечення інформаційної безпеки та безперервності послуг. Також установлено обов'язок повідомляти про кіберінциденти до національних компетентних органів або CSIRT у встановлені строки через стандартизовану процедуру нотифікації [207].

Важливою інституційною новацією стало створення Європейської мережі органів кіберкризового управління (EU-CyCLONe), покликаної координувати дії держав-членів під час масштабних інцидентів і криз. Цей механізм посилює взаємодію між національними структурами та Європейським агентством з кібербезпеки (ENISA) [223]. Директива запроваджує єдину систему нагляду й санкцій, яка забезпечує ефективність правозастосування. Для суб'єктів, віднесених Директивою (ЄС) 2022/2555 до категорії *essential entities*, встановлено граничні розміри адміністративних штрафів до 10 млн євро або 2% від загального річного обороту підприємства. Для суб'єктів категорії *important entities* передбачено санкції до 7 млн євро

або 1,4% річного обороту. Таке розмежування рівнів відповідальності відповідає принципу пропорційності, що є однією з ключових засад регуляторної політики Європейського Союзу [207]. Держави-члени зобов'язані визначити національні компетентні органи, забезпечити дієві механізми моніторингу, ухвалити національні програми імплементації директиви та встановити узгоджені формати взаємодії з Європейським агентством з кібербезпеки (ENISA), мандат і функції якого унормовано правом ЄС [207; 227].

Директива NIS 2 відображає перехід ЄС від декларативного до юридично зобов'язувального режиму кіберрегулювання, у якому кібербезпека трактується як складова публічного порядку. Її структура демонструє прагнення ЄС забезпечити баланс між наднаціональною уніфікацією стандартів і збереженням компетенцій держав-членів у практичному контролі. Разом із тим, різниця у рівнях адміністративної спроможності держав може зумовити варіативність імплементації положень директиви, що створює потребу в посиленому методичному супроводі з боку ENISA та регулярному моніторингу практики виконання [215].

Директива (ЄС) 2022/2557 (CER) є комплементарним актом до NIS 2, який поширює концепцію стійкості на некіберсфери критичної інфраструктури. Вона спрямована на підвищення загальної стійкості критичних суб'єктів (critical entities resilience) у таких секторах, як енергетика, транспорт, охорона здоров'я, водопостачання, управління відходами, космічні послуги тощо. Головна мета акта – створити уніфіковані підходи до оцінювання ризиків і планування заходів стійкості на рівні підприємств і держав.

Директива зобов'язує держави-члени:

–ідентифікувати критичних суб'єктів у відповідних секторах;
–прийняти національні стратегії забезпечення їхньої стійкості;
–забезпечити обмін інформацією між уповноваженими органами та координацію на рівні Союзу.

Ключовою концептуальною ідеєю CER є інтеграція підходів до управління ризиками у фізичній і цифровій площинах, що формує єдиний континуум кіберної та фізичної безпеки. Такий підхід відповідає сучасній доктрині «resilience-based security governance», за якою превентивні та адаптаційні заходи становлять основу безпеки критичних систем [230].

CER зміцнює взаємозв'язок між цифровими та фізичними аспектами безпеки, але її реалізація залежить від рівня інституційної готовності держав-членів і узгодженості зобов'язань за NIS 2. Наявний ризик асиметрії імплементації – відмінностей у методах ідентифікації критичних суб'єктів та якості національних планів стійкості. Водночас обидві директиви разом формують системну основу правового режиму кібер- та фізичної стійкості в межах ЄС, поєднуючи зобов'язувальний характер норм із гнучкими механізмами адаптації на національному рівні [207; 230].

Регламент (ЄС) 2022/2554 (*Digital Operational Resilience Act*, DORA) становить спеціальний правовий акт у системі фінансового права ЄС, який закріплює обов'язкові вимоги до управління інформаційно-комунікаційними ризиками у фінансовому секторі [229]. Його ухвалення стало реакцією на посилення цифрової залежності банків, страхових компаній, бірж, інвестиційних установ та інших фінансових організацій від зовнішніх ІТ-провайдерів. Документ спрямований на забезпечення операційної стійкості фінансових послуг, тобто здатності фінансових суб'єктів витримувати, реагувати та відновлюватися після кіберінцидентів без втрати критичних функцій.

Регламент поширюється на всі фінансові установи, підконтрольні Європейським наглядовим органам (EBA, ESMA, EIOPA), а також на «критичних постачальників ІК-послуг» (critical ICT third-party providers), які забезпечують ключові цифрові функції для таких установ. Таким чином, він формує наднаціональну правову рамку цифрової операційної стійкості, що доповнює базові обов'язки, передбачені NIS 2 [207; 229; 230].

Серед основних вимог DORA – запровадження політик управління ІК-ризиками, тестування цифрової операційної стійкості (digital operational resilience testing), встановлення процедур реагування на інциденти та звітності перед компетентними органами [229; 173]. Документ встановлює деталізовані вимоги до виявлення, класифікації та аналізу кіберінцидентів, а також до їх обов'язкового повідомлення у встановлені строки [229; 216; 223].

Запроваджено на рівні ЄС наглядовий режим щодо ІК-постачальників, які забезпечують критичні сервіси для фінансового сектору [229]. Такий контроль здійснюється через Спільний наглядовий форум (Joint Oversight Forum), до складу якого входять представники трьох європейських фінансових органів (EBA, ESMA, EIOPA) [229; 173]. Цей механізм покликаний забезпечити єдині підходи до оцінки ризиків, узгодження вимог до тестування та посилення прозорості взаємовідносин між фінансовими організаціями й технологічними провайдерами [229; 173].

Регламент DORA має подвійне значення. З одного боку, він конкретизує загальні вимоги NIS 2 у межах фінансового сектору, забезпечуючи галузеву деталізацію стандартів кіберстійкості [229; 207; 173]. З іншого – створює новий рівень правового контролю за ІК-постачальниками, що зменшує ризики системної залежності від приватних технологічних компаній [229; 173]. Водночас реалізація DORA потребує узгодження фінансового та кіберрегуляторного нагляду, щоб уникнути колізій компетенцій між національними фінансовими регуляторами та європейськими наглядовими органами [229; 207; 173]. У цьому контексті Регламент демонструє характерну для права ЄС тенденцію – зміщення від секторального нагляду до інтегрованої наднаціональної моделей управління ризиками [221; 229; 207; 173].

Регламент (ЄС) 2024/2847 (Cyber Resilience Act, CRA) запроваджує горизонтальні вимоги до безпеки продуктів із цифровими елементами, що розповсюджуються на всій території ЄС [230]. На відміну від DORA, який стосується конкретного сектору, CRA встановлює загальні стандарти

кіберстійкості для будь-яких товарів, що містять програмне забезпечення або підключення до мережі [229; 230; 173]. Таким чином, акт формує нормативну основу для захисту споживачів і ринку від уразливостей у цифрових продуктах [230; 173]. Регламент визначає коло зобов'язаних осіб – виробників, імпортерів і розповсюджувачів цифрових продуктів, та встановлює їхні обов'язки щодо забезпечення кібербезпеки на всіх етапах життєвого циклу продукту: від проєктування та розробки до післяпродажного оновлення й технічної підтримки [230]. Вимоги включають:

– упровадження принципів «безпеки за замовчуванням» (security by default) і «безпеки за задумом» (security by design);

– проведення оцінювання відповідності (conformity assessment);

– повідомлення про виявлені вразливості через визначені на рівні ЄС платформи [230; 227].

Ключова новація CRA полягає у встановленні єдиних мінімальних стандартів безпеки цифрових продуктів і створенні умов для єдиного ринку «безпечного ПЗ». Акт тісно пов'язаний із Cybersecurity Act (Регламент (ЄС) 2019/881), який заклав основу європейських сертифікаційних схем для ІКТ-продуктів [227; 230; 173].

На відміну від DORA, CRA має загальнорегуляторний характер і формує горизонтальну правову основу для безпеки цифрових технологій [229; 230; 173]. Його прийняття свідчить про перехід від секторального до продуктово-орієнтованого регулювання, де акцент зміщено з поведінки суб'єктів на властивості самих продуктів [230; 173]. Основна перевага – створення уніфікованої системи мінімальних вимог для всіх учасників ринку [230]. Водночас певним викликом є практична узгодженість механізмів оцінки відповідності та сертифікації, передбачених Cybersecurity Act, що потребує додаткової методичної координації з боку ENISA [227; 223; 224].

Регламент (ЄС) 2022/2065 (*Digital Services Act*, далі – DSA) є ключовим нормативним актом, що визначає нову архітектуру відповідальності та підзвітності онлайн-посередників у межах внутрішнього ринку ЄС [228; 173].

Він спрямований на підвищення прозорості, підзвітності та безпечності цифрового середовища, зокрема у діяльності «дуже великих онлайн-платформ» (VLOPs) та «дуже великих онлайн-пошукових систем» (VLOSEs). Хоча DSA за своєю природою належить до регуляторних актів у сфері цифрових послуг, його положення мають безпосереднє значення для забезпечення кіберстійкості, оскільки вперше в праві ЄС закріплюють обов'язок системної оцінки ризиків, пов'язаних із функціонуванням цифрових платформ. До таких ризиків віднесено, зокрема, поширення незаконного контенту, маніпуляцію інформацією, зловживання алгоритмічними системами, а також загрози безпеці цифрової інфраструктури, які потенційно можуть мати кібервимір [228; 215; 230].

Регламент запроваджує вимогу до провайдерів великих платформ здійснювати регулярне управління ризиками (risk management), включно з розробленням процедур виявлення, оцінювання та пом'якшення системних ризиків, а також проходити незалежний зовнішній аудит [228; 300]. За результатами оцінок ризиків платформи зобов'язані вживати коригувальні заходи і звітувати перед наглядовими органами та Європейською комісією [228]. У частині кібербезпеки положення DSA узгоджуються з рамками NIS 2 і CRA, формуючи єдиний простір управління ризиками для цифрових послуг [207; 228; 230]. Якщо NIS 2 визначає обов'язки для операторів критичних послуг, а CRA – вимоги до безпеки продуктів, то DSA встановлює організаційно-управлінський рівень відповідальності за системні ризики на онлайн-платформах загального користування [207; 228; 230]. У системі європейського кіберправа DSA є актом превентивного характеру, спрямованим на регулювання поведінкових ризиків, а не технічних параметрів кіберзахисту [173; 220]. Його сильна сторона – запровадження регулярного аудиту ризиків і наглядової відповідальності платформ перед Європейською комісією [173; 228]. Разом із тим, DSA залишає широке тлумачення категорії «системного ризику», що може створювати

неоднозначність у кваліфікації кіберінцидентів і потребуватиме узгодження з технічними вимогами, передбаченими NIS 2 та CRA [173; 207; 230].

Регламент (ЄС) 2025/38 (Cyber Solidarity Act) формує операційний рівень колективної кіберстійкості Європейського Союзу [231]. Його ухвалення стало логічним продовженням політики ЄС у сфері спільного реагування на масштабні кіберінциденти, започаткованої в межах NIS 2 і рішень Європейської комісії щодо створення єдиної системи кризового управління [207; 220; 223; 231]. Регламент передбачає створення транскордонної мережі європейських центрів операційної безпеки (EU-SOCs), які забезпечують постійний моніторинг кіберзагроз, обмін технічними індикаторами та раннє виявлення масштабних атак [231; 215]. Другою інституційною новацією є Європейський кіберрезерв (EU Cyber Reserve) – пул сертифікованих постачальників послуг реагування, які можуть бути оперативно залучені державами-членами для локалізації та ліквідації інцидентів [231; 223].

Окрім технічного виміру, акт передбачає створення механізмів фінансової підтримки для держав-членів у разі великих інцидентів і запроваджує принцип солідарності у кіберпросторі як правову засаду взаємодопомоги. Таким чином, він інституціоналізує механізм колективної кіберстійкості, що поєднує технічні, фінансові та правові інструменти реагування на загальноєвропейському рівні [231].

Cyber Solidarity Act заповнює структурну прогалину між нормативним рівнем (NIS 2, CER) та практичним реагуванням. Його ключовою перевагою є формування операційної спроможності спільного реагування, однак актуальним залишається виклик координації між EU-SOCs та національними CSIRTs, що потребує деталізації процедур обміну інформацією та узгодження стандартів її захисту [207; 223]. У перспективі цей акт може стати основою для європейської системи кризового реагування з наднаціональним координаційним центром [231].

Регламент (ЄС) 2019/881 (*Cybersecurity Act*) установив постійний мандат Європейського агентства з кібербезпеки (ENISA) та заклав європейську систему сертифікації ІКТ-продуктів і послуг [227]. Документ став фундаментом інституційної архітектури кібербезпеки ЄС, у межах якої ENISA виконує аналітичні, координаційні та методичні функції.

Регламент визначає компетенції ENISA у трьох напрямах:

– сертифікація ІКТ-продуктів, послуг і процесів, що забезпечує взаємне визнання сертифікатів у межах ЄС [227];

– аналітика та оцінювання ризиків, включно з підготовкою щорічних оглядів загроз (ENISA Threat Landscape) [215; 217];

– методична та освітня підтримка держав-членів, включно з розробленням рекомендацій, проведенням навчань і симуляцій (Cyber Europe Exercises) [223; 224; 225].

ENISA є центральною ланкою між «жорстким» правом ЄС (NIS 2, CRA, DORA) та його практичною імплементацією на національному рівні, формуючи м’яке регуляторне поле (soft law) у сфері кібербезпеки [207; 229; 230]. Хоча Агентство не має прямих наглядових повноважень, його методичні, аналітичні та сертифікаційні механізми істотно впливають на регуляторні практики держав-членів. Основний виклик полягає у забезпеченні балансу між координуючою роллю ENISA та суверенними компетенціями держав-членів, що відповідає моделі «кооперативного суверенітету» в європейській кібербезпеці [142; 46; 139].

До цього аналізу слід також додати, що Європейські стандарти кіберстійкості знаходять конкретне втілення у національних моделях держав-членів, котрі поєднують правове регулювання з практичною координацією [34; 224; 225]. Розглянемо декілька з них.

Федеративна Республіка Німеччина послідовно розбудовує багаторівневу систему інституційного забезпечення кібербезпеки, що поєднує міжвідомчу координацію, партнерство з приватним сектором і формування культури кіберстійкості [145; 156; 237]. Її ядром є Національний

центр кібероборони (Nationales Cyber-Abwehrzentrum, Cyber-AZ), створений як міжвідомчий вузол оперативної взаємодії між федеральними відомствами у разі кіберінцидентів. Центр координує обмін ситуаційною інформацією, підготовку спільних оціночних звітів і рекомендацій, що забезпечує узгоджене реагування державних органів на загрози кібербезпеці на федеральному рівні [167]. Важливим елементом німецької моделі є UP KRITIS –інституціоналізоване державно-приватне партнерство, орієнтоване на захист критичної інфраструктури. Воно функціонує як платформа для системної взаємодії державних органів, операторів критичних секторів і галузевих асоціацій, сприяючи розробленню спільних стандартів безпеки, обміну досвідом і проведенню спільних навчань [16; 168; 226]. Третім компонентом є ініціатива Allianz für Cyber-Sicherheit, створена Федеральним відомством з безпеки інформаційних технологій (BSI) як мережа обміну знаннями між бізнесом і державою. Програма охоплює інформаційні бюлетені, попередження про загрози, тренінги та галузеві рекомендації, що сприяє масштабуванню практик кіберзахисту в приватному секторі [170; 226].

Стратегічні орієнтири німецької кіберполітики зафіксовані у *Стратегії кібербезпеки для Німеччини 2021 року* (Cyber-Sicherheitsstrategie für Deutschland 2021), ухваленій Федеральним міністерством внутрішніх справ (BMI), яка визначає пріоритети розвитку спроможностей держави, посилення співрегулювання з бізнесом, удосконалення правової бази та розширення ролі федеральних структур у гарантуванні кіберстійкості [224; 225; 237]. Німецька модель демонструє практичну реалізацію принципів директив NIS 2 та CER, зокрема в частині розмежування повноважень і багаторівневої координації, а її особливістю є поєднання державного контролю з партнерським управлінням ризиками – характерна риса європейського підходу до «кооперативної безпеки» [181; 207; 223; 226].

У Французькій Республіці функції національного компетентного органу з питань кібербезпеки виконує Національне агентство з безпеки

інформаційних систем (Agence nationale de la sécurité des systèmes d'information, ANSSI). Агентство поєднує нормативно-координаційні та технічні функції, виступаючи ключовим інструментом імплементації вимог ЄС у національну практику [156; 157]. Його діяльність охоплює сертифікацію та кваліфікацію рішень безпеки, підтримку державного сектору у впровадженні стандартів кіберзахисту, організацію реагування на інциденти та розроблення методичних матеріалів для суб'єктів критичної інфраструктури [157].

Модель ANSSI є прикладом інституційного втілення Cybersecurity Act і NIS 2, у якому центральна роль компетентного органу поєднується з технічною експертизою і безпосередньою підтримкою державних структур [173; 207; 220; 227]. Це забезпечує ефективний баланс між регуляторною владою та практичною спроможністю, хоча вимагає значних ресурсів для підтримки постійної технічної готовності [173; 181].

Швеція реалізує кіберполітику через Шведське агентство з надзвичайних ситуацій (MSB), яке відповідає за координацію національної системи кіберстійкості. Урядова Національна стратегія кібербезпеки 2024 року (Sweden's National Cybersecurity Strategy 2024) визначає пріоритети на 2025–2029 рр., серед яких – посилення спроможностей державного сектору, розвиток державно-приватної взаємодії та інтеграція європейських нормативних вимог (зокрема NIS 2) у національні режими управління ризиками [322; 207; 224]. Шведський підхід характеризується високим рівнем узгодження з європейськими директивами, при цьому робиться акцент не лише на нормативній імплементації, а й на розвитку «операційної готовності» – здатності реагувати на інциденти в реальному часі [322; 223].

Естонська Республіка належить до піонерів європейської кіберполітики. Її Стратегія кібербезпеки на 2024–2030 роки (Cybersecurity Strategy 2024–2030) передбачає розвиток «cyber-conscious» управління ризиками, удосконалення планування стійкості критичних секторів і посилення міжвідомчої взаємодії [309; 254]. Центральну роль у впровадженні

державної політики відіграє Департамент інформаційних систем (RIA) при Міністерстві економіки та комунікацій, який координує реалізацію вимог NIS 2, веде щорічну звітність про стан національної кіберстійкості й здійснює загальне управління національною інфраструктурою безпеки [309; 311; 207]. У його структурі функціонує національна команда реагування CERT-EE, що виконує роль Single Point of Contact у разі кіберінцидентів, забезпечує обмін технічними індикаторами та рекомендаціями для операторів «життєво важливих послуг» [254; 311].

Естонська модель державно-приватного партнерства охоплює широкий спектр механізмів співпраці – від спільного розроблення рекомендацій для приватного сектору до навчань і моделювання кризових сценаріїв [254; 224; 226]. Особливе місце посідає політика Government Relations у сфері кібербезпеки, яка забезпечує сталу інтеграцію державних і бізнес-структур на засадах довіри. Уряд співпрацює з провідними приватними компаніями, такими як Guardtime і CybExer Technologies, залучаючи їх до проєктів з кіберзахисту критичних об’єктів та електронного врядування, зокрема у сфері медичних даних (e-Health) та тестування кіберстійкості інфраструктури [254; 210; 284].

Естонська цифрова інфраструктура базується на технологічній платформі X-Road і застосуванні криптографічного засвідчення цілісності даних, що гарантує довіру до електронних послуг та державних реєстрів [298; 254]. Розбудова партнерських зв’язків підтримується через Естонський кібертехнологічний кластер (Eesti CyberTech klaster), який об’єднує державні, приватні й академічні структури, забезпечуючи обмін досвідом, навчання та поширення інновацій у сфері кіберзахисту [210; 254].

Естонська модель є прикладом системної інтеграції правових і технічних засад кіберзахисту, що поєднує чітку регуляторну базу з високим рівнем цифрової культури. Її особливість – постійний моніторинг імплементації стратегій і відкритість даних, що відповідає принципам прозорості та підзвітності, закріпленим у DSA і NIS 2 [309; 228; 207; 224].

ЄС сформував інтегровану, багаторівневу екосистему кіберстійкості, у якій «hard law» акти (NIS2, CER, DORA, CRA, DSA, Cyber Solidarity Act) вибудовують послідовний ланцюг: від базових обов'язків управління ризиками та інцидент-репортингу для критичних і важливих суб'єктів – до секторальної деталізації у фінансовій сфері, горизонтальних вимог до безпеки цифрових продуктів і управління системними ризиками платформ [207; 227; 229–231; 228; 230]. Операційний рівень забезпечується механізмами колективного реагування, а методичну конвергенцію й «soft law» формує ENISA через керівництва, навчання та сертифікаційні схеми [215; 223–225; 226]. Така архітектура поєднує наднаціональну уніфікацію з національною відповідальністю за нагляд і виконання, зменшуючи регуляторну асиметрію на внутрішньому ринку [173; 220].

Національні моделі держав-членів демонструють різні траєкторії імплементації цієї рамки. Проте, попри відмінності ресурсів і інституційної спроможності, спільним є посилення відповідальності за ланцюги постачання та інтеграція фізичної й цифрової стійкості. У підсумку, європейська модель кіберзахисту еволюціонувала від декларативних підходів до нормативно зобов'язувальної системи з операційними інструментами солідарності. Її цінність – у зв'язці «policy - compliance - assurance - response», що одночасно задає вимоги, забезпечує їх перевірку й створює спроможності для спільного реагування.

Сполучені Штати Америки: політика «регуляторизації» кібербезпеки через виконавчі укази (Executive Orders, EO), секторальні директиви безпеки (Security Directives, SD) та стандарти. Сполучені Штати Америки упродовж останніх років сформували послідовну модель забезпечення кібербезпеки, засновану на поєднанні стратегічного планування, адміністративного регулювання та стандартизації. Її концептуальне ядро становлять Національна стратегія кібербезпеки США 2023 року та План її реалізації (*Implementation Plan*), що маркують перехід від переважно добровільного до нормативно зобов'язувального режиму

забезпечення кіберстійкості [324; 325]. Цей підхід узгоджується із тенденцією «регуляторизації» кібербезпеки, яку в українській науковій літературі також розглядають як еволюційний перехід від декларативних до операційно-обов'язкових механізмів забезпечення стійкості [29; 7; 6].

Ключовою ідеєю Стратегії є перерозподіл відповідальності між державою, приватним сектором і громадянами: головний тягар управління кіберризиками має нести той, хто володіє найбільшими ресурсами та технічною спроможністю – розробники програмного забезпечення, постачальники цифрових сервісів і оператори критичної інфраструктури [324]. У документі визначено п'ять стратегічних напрямів (pillars):

Оборона критичної інфраструктури (Defend Critical Infrastructure);

Протидія зловмисним акторам (Disrupt and Dismantle Threat Actors);

Формування ринку відповідальності (Shape Market Forces to Drive Security and Resilience);

Інвестиції в інновації та стійкість (Invest in a Resilient Future);

Розвиток міжнародного партнерства (Forge International Partnerships to Pursue Shared Goals) [324].

План реалізації конкретизує завдання за кожним напрямом і визначає відповідальних виконавців, серед яких CISA, DOJ, DOE, DoD, FCC, FTC, NIST, OMB [325]. Таке інституційне розмежування відображає перехід США до моделі «спільної відповідальності» (shared responsibility), у межах якої держава не лише координує, а й установлює мінімальні обов'язкові стандарти кібербезпеки для критичних секторів економіки. Подібний підхід до визначення суб'єктів і розподілу відповідальності також простежується в українських дослідженнях щодо моделювання системи кібербезпеки [150; 61].

Практичну основу цієї системи закладено Executive Order 14028 of May 12, 2021 "Improving the Nation's Cybersecurity" [351]. Указ започаткував комплексну модернізацію безпеки федеральних інформаційних систем і ланцюгів постачання програмного забезпечення, визначивши вимоги до

архітектури Zero Trust, багатофакторної автентифікації та Software Bill of Materials (SBOM) для федеральних органів і постачальників програмного забезпечення. ЕО 14028 також установив вимоги до звітування про кіберінциденти постачальниками федеральних органів, що згодом лягло в основу загальнонаціональної системи CIRCIA 2022 [349], а також започаткував розроблення єдиних критеріїв безпечної розробки програмного забезпечення.

Виконання Указу покладено на National Institute of Standards and Technology (NIST), який підготував низку методичних документів, ключовим серед яких є NIST SP 800-218 Secure Software Development Framework (SSDF) – фундамент стандартів безпечної розробки в США [304]. У наукових працях українських дослідників неодноразово підкреслюється, що саме стандартизація та обов'язковість процедур оцінювання безпеки становлять основу ефективних моделей кіберстійкості та слугують орієнтиром для України [47; 59; 63].

Після кібератаки на Colonial Pipeline у 2021 році США впровадили модель «секторальної обов'язковості», реалізовану через Security Directives Транспортного управління безпеки [326]. Серія директив Pipeline-2021-01 установила конкретні вимоги для визначених операторів трубопровідної інфраструктури, що підпадають під регуляторну юрисдикцію TSA [326]. Ці вимоги включають призначення цілодобового координатора з кібербезпеки, своєчасне інформування CISA про інциденти, проведення оцінювання ризиків і розроблення планів підвищення кіберстійкості у встановлені строки [326; 349]. Директиви мають імперативний характер, перебувають під контролем TSA і регулярно оновлюються з урахуванням технологічного розвитку та зміни спектра загроз [326]. Їхня дія поширюється не на всі об'єкти трубопровідного транспорту, а лише на тих операторів, яких TSA визначає як критично важливих для енергетичної безпеки країни [326].

Запровадження такого механізму створило прецедент адміністративного регулювання, який дозволяє надавати приписам

юридичної сили без ухвалення окремого закону Конгресом. Фактично, Сполучені Штати сформували модель швидкого реагування, у якій виконавча влада здатна оперативно встановлювати обов'язкові стандарти безпеки в окремих секторах критичної інфраструктури [269; 270; 324].

Методологічну основу національної системи кібербезпеки Сполучених Штатів становлять стандарти та рамкові документи Національного інституту стандартів і технологій (National Institute of Standards and Technology, NIST). Оновлена редакція NIST Cybersecurity Framework 2.0 (2024) визначає шість ключових функцій – *Identify, Protect, Detect, Respond, Recover, Govern*, причому остання функція *Govern* є нововведенням, що розширює рамку управлінським виміром. Документ виступає універсальною основою для управління кіберризиками як у державному, так і в приватному секторах [304]

Рамка виконує роль «спільної мови» (*common language*) між регуляторами, аудиторами, операторами критичної інфраструктури та постачальниками технологічних рішень, забезпечуючи узгодженість підходів до оцінювання, управління та зниження ризиків [205].

Паралельно діє NICE Framework (NIST SP 800-181 Rev.1), яка систематизує компетентності, знання та професійні ролі фахівців у сфері кібербезпеки. Вона закріплює кадровий вимір кіберстійкості, визначаючи стандартизовані профілі посад і вимоги до кваліфікації для освітніх програм, сертифікації та державних служб. Обидві рамки належать до інструментів «м'якого права» (soft law), однак через їх інтеграцію у федеральні контракти, процедури закупівель, аудити та програми акредитації вони фактично набувають обов'язкового статусу для учасників ринку [205; 304; 324].

Організаційним центром реалізації державної політики кібербезпеки виступає Агентство з кібербезпеки та безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency, CISA), яке відповідно до офіційних документів позиціонується як ключовий координаційний орган у сфері захисту критичної інфраструктури [200]. На його базі у 2021 році створено

Joint Cyber Defense Collaborative (JCDC) – постійну оперативно-координаційну платформу спільного планування, координації та реагування, що об'єднує державні органи, операторів критичної інфраструктури, технологічні компанії та міжнародних партнерів [200; 202]. JCDC не є окремим законодавчо встановленим органом, а функціонує в межах CISA як механізм стратегічної взаємодії та обміну інформацією для посилення колективної кіберстійкості [202].

Разом із цим CISA забезпечує функціонування механізму Automated Indicator Sharing (AIS), який дозволяє здійснювати автоматизований обмін технічними індикаторами компрометації (*Indicators of Compromise, IoC*), а також підтримує діяльність мережі Information Sharing and Analysis Centers (ISACs) – галузевих центрів обміну аналітичними матеріалами, попередженнями та найкращими практиками реагування на кіберінциденти [201].

Секторальний вимір кіберполітики Сполучених Штатів Америки реалізується через відомчі стратегії та програми, що конкретизують загальнонаціональні пріоритети на рівні окремих галузей. Ключовим документом у сфері енергетики є *DOE Cybersecurity Strategy (2024)*, яка формує цілісну рамку управління кіберризиками в межах Міністерства енергетики США (Department of Energy, DOE) та визначає його роль як агентства управління ризиками сектора (Sector Risk Management Agency, SRMA) [330]. Стратегія спрямована на забезпечення єдиної, узгодженої та ефективної системи кіберзахисту у всіх підрозділах DOE та у взаємодії з енергетичним сектором.

Документ визначає п'ять стратегічних "стовпів" (pillars), що конкретизують завдання у середньостроковій перспективі:

– *Understand the Risk* – оцінювання ризиків, виявлення критичних систем і взаємозалежностей для пріоритизації заходів захисту;

– *Mitigate Risk* – зменшення ризиків шляхом застосування принципів Zero Trust Architecture та посилення управління вразливостями;

– *Enable Mission Resilience* – підвищення стійкості місій DOE через інтеграцію внутрішнього управління та зовнішньої взаємодії;

– *Develop the Cyber Workforce* – розвиток компетентностей і спроможностей персоналу в галузі кібербезпеки;

– *Protect Critical Energy Infrastructure* – зміцнення кіберстійкості критичної енергетичної інфраструктури у партнерстві з іншими федеральними структурами, секторальними агентствами та приватним сектором [330].

Стратегія передбачає узгодження планування, програмування, бюджетування та підготовки кадрів у межах DOE, а також партнерство з національними лабораторіями, енергетичними підприємствами та міжнародними партнерами з метою посилення кіберстійкості енергосистем США. У поєднанні з базовим документом *Roadmap to Achieve Energy Delivery Systems Cybersecurity* (2011), який започаткував дослідницько-інноваційний вимір безпеки енергопостачання, нова стратегія забезпечує інституційне продовження розвитку секторальної політики кібербезпеки DOE [331].

Важливою операційною формою взаємодії держави з приватним сектором є спільні консультативні повідомлення (Joint Cybersecurity Advisories), які публікуються Агентством з кібербезпеки та безпеки інфраструктури (CISA) у співпраці з іншими федеральними органами. Показовим прикладом є CISA Advisory AA22-011A (2022), підготовлений спільно з Федеральним бюро розслідувань (FBI) та Агентством національної безпеки (NSA) [182].

Документ містить узагальнені технічні рекомендації щодо виявлення, попередження та пом’якшення наслідків державних кібератак, спрямованих проти об’єктів критичної інфраструктури. Такі консультативні акти не створюють прямих юридичних зобов’язань, однак формують стандарт належної обачності (due diligence) для операторів критичних секторів, виконуючи роль інструменту реалізації публічно-приватної відповідальності у межах національної системи кібербезпеки.

У цілому американська модель кіберзахисту побудована на багаторівневому поєднанні правових та квазиправових механізмів. Президентські укази (Executive Orders, EO) ініціюють міжвідомчу нормотворчість і змінюють умови державних закупівель [351]; секторальні директиви (Security Directives, SD) установлюють прямі обов'язки для операторів критичної інфраструктури [326]; стандарти Національного інституту стандартів і технологій (NIST) та рамка NICE визначають технічні й кадрові орієнтири [304]; а інституційні структури CISA – насамперед JCDC, AIS та ISACs – забезпечують обмін інформацією та координацію реагування [200; 201; 202]. У такій конфігурації формується режим «де-факто обов'язковості», заснований на взаємодії адміністративних, договірних і нормативно-технічних засобів. У межах цієї системи CISA виконує переважно координаційно-операційні функції, тоді як NIST забезпечує технічне нормотворення, яке набуває юридичної сили через державні контракти, аудити та регуляторні відсилання [324].

Модель кібербезпеки США характеризується практичною спрямованістю та високою адаптивністю. Вона досягає обов'язковості не стільки через законодавчі приписи, скільки завдяки виконавчим актам (EO, SD) [351; 326], стандартам NIST [304], вимогам федеральних закупівель та постійному інформаційному обміну під егідою CISA [200; 201]. Завдяки цьому забезпечується узгодження державної політики, технічного комплаєнсу й оперативного реагування, що формує цілісну екосистему національної кіберстійкості [324].

НАТО: політичні зобов'язання, оборонна координація, правова релевантність. Комплексна політика кібероборони НАТО (Comprehensive Cyber Defence Policy, 2021; оновлена довідкова сторінка – 30 липня 2024 р.) закріплює інтеграцію кіберсфери у стратегічне та оперативне планування оборони Альянсу, визначає принципи колективної стійкості, обміну інформацією та розвитку національних спроможностей, а також підтверджує, що серйозні кіберінциденти за певних обставин можуть становити загрозу

безпеці Альянсу і стати підставою для консультацій та навіть можливого застосування статті 5 Північноатлантичного договору (рішення – на розсуд Північноатлантичної ради) [292].

На практичному рівні ці положення знайшли відображення у *Statement by NATO Heads of State and Government* (Брюссель, 24 березня 2022 р.), у якій союзники засудили збройну агресію РФ проти України та наголосили на посиленні оборонних і технологічних спроможностей, включно з кібероборони [294]. У своєму вступному зверненні перед початком цього саміту Генеральний секретар НАТО Єнс Столтенберг підкреслив необхідність посилення системи стримування та оборони, зміцнення східного флангу та інвестування у кіберспроможності [208].

Подальший розвиток політичної позиції Альянсу зафіксовано у *Washington Summit Declaration* (Вашингтон, 10 липня 2024 р.), у якій підтверджено підтримку України, зокрема у зміцненні кіберстійкості, виявленні та реагуванні на кіберінциденти, а також у розширенні практичної взаємодії між українськими інституціями та структурами НАТО [295]. Зазначені орієнтири конкретизовано у *Summary of the NATO-Ukraine Innovation Cooperation Roadmap* (2024), що визначає напрями партнерства у сферах технологічних інновацій, цифрової безпеки та кіберзахисту, включно з інтеграцією України в екосистему DIANA [296].

Сукупність цих документів формує політичну рамку кіберполітики НАТО: кіберпростір визнається повноцінним виміром колективної безпеки, а партнерські інструменти – засобом нарощування спроможностей та взаємної сумісності між державами-членами та партнерами [321].

Розбудова кіберспроможностей у межах НАТО здійснюється на основі системної координації між державами-членами, спрямованої на забезпечення взаємної сумісності, розвиток навичок реагування та узгодження технічних і організаційних стандартів. У цьому контексті важливе місце посідають навчальні програми, спільні тренування та кібернавчання (*cyber exercises*),

які забезпечують відпрацювання процедур реагування на інциденти й кризові ситуації відповідно до спільних протоколів Альянсу [292].

Ключовим елементом інституційної архітектури НАТО є мережа центрів передового досвіду (Centres of Excellence, COE), що функціонують у співпраці з Альянсом. Зокрема, Кооперативний центр кібероборони (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE), розташований у м. Таллінн, є акредитованим НАТО міжнародним військовим центром, який забезпечує навчальну, аналітичну та методичну підтримку держав-членів і партнерів у сфері кібероборони. CCDCOE проводить курси, тренінги та спільні кібернавчання, спрямовані на розвиток спроможностей і взаємної сумісності союзників і партнерів [290].

Важливим напрямом діяльності Центру є участь у розробленні методичних рекомендацій для держав щодо формування національних стратегій кібербезпеки. За участю CCDCOE підготовлено міжнародний документ *Guide to Developing a National Cybersecurity Strategy* (Second Edition, 2021), який містить узагальнені принципи побудови стратегій, підходи до оцінювання ризиків, визначення ролей основних стейкхолдерів, а також практичні моделі взаємодії державного, приватного секторів і громадянського суспільства [288]. Зазначені напрацювання сприяють гармонізації національних політик у межах єдиного стратегічного простору НАТО та партнерських держав, забезпечуючи узгодженість термінології, методів управління ризиками та механізмів міжінституційної координації.

У сфері міжнародного публічного права Кооперативний центр кібероборони НАТО (CCDCOE) здійснює науково-аналітичну підтримку держав-членів та партнерів, зокрема як партнер консорціумного проєкту Cyber Law Toolkit – відкритого електронного ресурсу, що систематизує позиції держав і правові тлумачення щодо застосування норм *jus ad bellum* і *jus in bello* у кіберпросторі, включно з питаннями визначення порогу «застосування сили» (*use of force*) та «збройного нападу» (*armed attack*) у контексті кібероперацій [287]. Матеріали ресурсу формуються на основі

оприлюднених державних позицій і правових оцінок, оновлюваних консорціумом партнерських установ за участю CCDCOE, та відображають еволюцію підходів до кваліфікації кіберінцидентів відповідно до норм міжнародного права [178; 317].

Попри відсутність обов'язкової юридичної сили, Cyber Law Toolkit є аналітичним і навчальним ресурсом, який розвивається у форматі міжнародного консорціуму за участю Кооперативного центру кібероборони НАТО (CCDCOE). Він містить приклади правових тлумачень, гіпотетичні кейси та узагальнені позиції держав щодо застосування норм міжнародного публічного права до кібероперацій. За даними CCDCOE, ресурс широко використовується урядовими радниками, міжнародними організаціями, дослідницькими центрами та академічною спільнотою для порівняльного аналізу, розроблення аргументації та навчання у сфері міжнародного кіберправа [287; 317; 278].

Матеріали Cyber Law Toolkit сприяють розвитку праворозуміння у галузі *jus ad bellum* і *jus in bello*, відображаючи еволюцію *opinio juris* та узагальнюючи елементи *state practice* держав [178; 287; 312]. У цьому вимірі CCDCOE виступає інституційним центром експертизи, який забезпечує порівняльний аналіз, консолідацію й інтерпретацію правових позицій, підвищуючи передбачуваність і правову визначеність у сфері міжнародної кібербезпеки [179; 317; 319].

Важливим інструментом формування спільного розуміння сучасних викликів у кіберпросторі виступає журнал NATO Review, який публікує експертні статті, інтерв'ю та коментарі з питань міжнародної безпеки [321]. У матеріалах останніх років систематизуються взаємозв'язки кіберзагроз із гібридними впливами, інформаційними кампаніями та стратегічним суперництвом провідних держав, а також аналізується адаптація політики НАТО до умов стратегічної конкуренції у цифровому середовищі [292; 294]. Зміст цих матеріалів не має нормативного характеру й не становить офіційну позицію Альянсу, проте вони відображають узгоджені політичні тенденції,

пріоритети оборонного планування та стратегічні орієнтири, що згодом трансформуються в офіційні документи та комюніке керівних органів НАТО [208; 295]. Таким чином, аналітичні публікації *NATO Review* функціонують як комунікаційний інструмент, що формує спільне бачення пріоритетів кіберполітики та сприяє узгодженню стратегічних наративів у межах євроатлантичного безпекового простору.

На відміну від правового порядку Європейського Союзу, у межах якого директиви та регламенти встановлюють безпосередньо зобов'язувальні вимоги (зокрема, NIS2, CER, Cybersecurity Act, DSA, DORA, CRA, Cyber Solidarity Act) та передбачають нормативно визначені механізми їх виконання [207; 227; 228; 229; 230; 231], рішення органів НАТО у сфері кібероборони мають переважно політичний характер: кожна держава-союзник несе відповідальність за власний кіберзахист, а Альянс виконує координаційну функцію, забезпечує платформу для обміну інформацією, підготовку кадрів і взаємну підтримку [292; 293; 290].

У Сполучених Штатах нормативне середовище формують стратегічні документи, стандарти та виконавчі інструменти з чітким визначенням відповідальних суб'єктів і процедур. National Cybersecurity Strategy (2023) та Implementation Plan (2023) задають напрям регуляторної реформи та перерозподілу відповідальності між державою й приватним сектором [324; 325], узгоджуючись зі стандартами NIST та актами виконавчої влади, серед яких ключовим є Executive Order 14028 "Improving the Nation's Cybersecurity" (2021) [351]. Оборонний вимір деталізовано у DoD Cyber Strategy (2023), що інтегрує кіберспроможності в доктрину стримування й спільних операцій [350].

У такій перспективі підхід НАТО полягає у виробленні спільних політичних рамок, процедур сумісності та механізмів колективної готовності, залишаючи імплементацію правових зобов'язань на рівні внутрішніх правопорядків держав-членів і партнерів [292; 294].

Узагальнюючи результати порівняльного аналізу, можна зазначити, що ЄС сформував нормативно зобов'язувальну систему кібербезпеки з єдиними стандартами та механізмами колективної стійкості [207; 227; 231]; США реалізують практичну модель регуляторного управління через стандарти, виконавчі акти та державно-приватне партнерство [324; 351; 201]; НАТО забезпечує політичну координацію, оборонну взаємодію та розвиток спроможностей союзників [290; 292]. У сукупності ці підходи створюють взаємодоповнювальну систему міжнародного кіберзахисту.

З огляду на це, подальший аналіз доцільно спрямувати на визначення місця України у цій системі та окреслення шляхів її інтеграції у міжнародну архітектуру кібербезпеки, що розглядається у підпункті 3.2.

3.2. Інтеграція України у міжнародно-правову систему кібербезпеки

Інтеграція України до європейського та глобального режиму кібербезпеки здійснюється у двох взаємопов'язаних площинах – через виконання міжнародно-правових зобов'язань і гармонізацію національного законодавства з правом Європейського Союзу (acquis ЄС). Конституція України визначає основоположні принципи правопорядку, діяльності органів державної влади та забезпечення національної безпеки [52]. На цій конституційній основі сформовано розгалужену систему нормативно-правових актів, що регулюють питання кіберзахисту та цифрової стійкості держави.

Ключові засади державної політики у сфері кібербезпеки закріплено в Законі України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII, який визначає структуру сектору безпеки та інтеграційні орієнтири співпраці з ЄС і НАТО [107], а також у Законі України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII (у редакції Закону № 4336-

IX від 27 березня 2025 р.), що оновив систему державного управління у сфері кіберзахисту та встановив механізми державного нагляду за критичною інформаційною інфраструктурою [111; 81].

Міжнародно-правовою основою інтеграції виступає Конвенція Ради Європи про кіберзлочинність (Будапешт, 2001), ратифікована Законом України від 7 вересня 2005 р. № 2824-IV [116]. Її положення забезпечили гармонізацію криміналізації кіберправопорушень і створили правові засади для міжнародної взаємодії у розслідуваннях кіберзлочинів. У 2022 р. деякі положення Конвенції були імплементовані у процесуальну систему через Закон України № 2137-IX від 15 березня 2022 р. «Про внесення змін до Кримінального процесуального кодексу України…» [85].

Європейський вектор державної політики у сфері цифрової безпеки було також закріплено Планом заходів з виконання Угоди про асоціацію між Україною та ЄС, затвердженим постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106, у якому кібербезпека визначена серед пріоритетів цифрової трансформації та гармонізації нормативно-правових підходів із Європейським Союзом [96].

Інституційну координацію у сфері кібербезпеки здійснює Рада національної безпеки і оборони України (РНБО) та створений при ній Національний координаційний центр кібербезпеки (НКЦК), утворений Указом Президента України від 7 червня 2016 р. № 242/2016 [112]. Згідно з оновленнями, внесеними Указом Президента № 547/2025, статус Центру уточнено з урахуванням посилення його координаційної ролі у співпраці з структурами ЄС, НАТО та Європейського агентства з кібербезпеки (ENISA) [87].

Операційно-технічну взаємодію на міжнародному рівні забезпечує Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ), правовий статус якої визначено Законом України № 3475-IV від 23 лютого 2006 р. [89]. На її базі функціонує CERT-UA, яка взаємодіє з європейськими мережами CSIRTs Network та EU-CyCLONe у форматах

кооперації та обміну інформацією (за підтримки ENISA), без формального членства, передбаченого для держав-членів ЄС. Участь України у відповідних ініціативах відбувається на підставі окремих домовленостей [215; 223; 224].

З 2020 р. нормативна база України системно та поступово наближається до вимог директив ЄС NIS2 (ЄС 2022/2555) та CER (ЄС 2022/2557). Основні положення реалізовано у постановах Кабінету Міністрів України від 9 жовтня 2020 р. № 943 «Деякі питання об’єктів критичної інформаційної інфраструктури» [23] та № 1109 «Деякі питання об’єктів критичної інфраструктури» [24], а також у постанові від 29 грудня 2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту» [98]. Ці акти регламентують класифікацію критичних послуг, процедури оцінки їх стійкості та порядок реагування на кіберінциденти відповідно до європейських стандартів управління кіберризиками.

У сфері електронної ідентифікації та довірчих послуг національне законодавство узгоджене з Регламентом (ЄС) № 910/2014 (eIDAS) через Закон України «Про електронні довірчі послуги» від 5 жовтня 2017 р. № 2155-VIII [92] та постанову КМУ від 16 вересня 2020 р. № 827 [86], що забезпечує взаємне визнання електронних підписів і засобів автентифікації між Україною та ЄС. Додатково Закон України «Про хмарні послуги» від 17 лютого 2022 р. № 2075-IX [130] встановив принципи безпечного використання хмарних технологій у державному секторі відповідно до рекомендацій Європейської комісії.

Стратегічну рамку кіберполітики визначає Стратегія кібербезпеки України, затверджена Указом Президента № 447/2021 [117], та План її реалізації, схвалений постановою Кабінету Міністрів № 158 від 23 лютого 2022 р. [121]. Їх мета – гармонізація національної системи кіберзахисту з європейськими директивами NIS2 [207], CER, DORA [229] та CRA [230], а також розбудова механізмів спільної кіберстійкості з партнерами ЄС і НАТО. Річні плани заходів, зокрема План на 2025 рік, забезпечують послідовність

імплементації та моніторинг виконання зобов'язань у сфері цифрової безпеки [97].

Таким чином, чинна нормативно-правова база України у сфері кібербезпеки характеризується високим ступенем узгодженості з європейськими стандартами та інституційною вбудованістю в міжнародну архітектуру цифрової стійкості. Національні закони та підзаконні акти забезпечують функціонування сумісних з ЄС механізмів управління ризиками, реагування на інциденти та інформаційного обміну, а ключові інституції – РНБО, НКЦК, ДССЗЗІ та CERT-UA – активно залучені до спільних платформ ЄС і НАТО [111; 112; 98].

Інституційне наближення України до європейських структур кібербезпеки супроводжується розвитком двосторонніх і багатосторонніх форматів дипломатичної взаємодії. Ключовим майданчиком цього процесу виступає Кібердіалог Україна–ЄС, який забезпечує політичну координацію, обмін оцінками кіберзагроз та узгодження нормативних і стратегічних підходів до кіберзахисту. За результатами четвертого раунду діалогу (Київ, 16 жовтня 2025 р.) сторони підтвердили спільну мету – інтеграцію України до європейського кіберпростору через імплементацію положень Директиви NIS2 [207], посилення захисту критичної інфраструктури, реалізацію 5G Cybersecurity Toolbox, а також розвиток співпраці у сфері кібердипломатії, санкційної політики та боротьби з кіберзлочинністю. У спільній заяві наголошено, що ЄС і Україна розвиватимуть технічну взаємодію з ENISA [224], Europol, Європейським коледжем безпеки та оборони, а також у межах Tallinn Mechanism –нового інструменту оперативної взаємодії держав-членів і партнерів ЄС для протидії масштабним кібератакам [144].

Особливої ваги набуло рішення про поступове залучення України до ініціативи EU Cybersecurity Reserve, яка створюється відповідно до Cyber Solidarity Act (ЄС 2025/38) [231]. Цей інструмент покликаний забезпечити швидке реагування на міждержавні кібератаки через використання спільних європейських ресурсів і технічних команд. Участь України у цій системі

відкриває можливість інтеграції національної команди реагування CERT-UA у механізми спільного реагування ЄС, що посилює стійкість критичної інфраструктури та уніфікує процедури інцидент-менеджменту [98].

Поглиблення співпраці відображає ширшу тенденцію формування європейського режиму колективної кіберстійкості, який, за аналітичними матеріалами Євроінфоцентру Верховної Ради України, базується на поєднанні правового регулювання, стратегічного планування та державно-приватної взаємодії [34]. Такий підхід створює інституційну основу для інтеграції України у спільну цифрову екосистему ЄС, у межах якої відбувається обмін технічними індикаторами компрометації, узгодження протоколів реагування та взаємне визнання інструментів кіберзахисту в мережах CSIRT Network і CyCLONe, що координуються ENISA [223; 224].

У сучасних наукових дослідженнях підкреслюється, що посилення міжнародного співробітництва у сфері кібербезпеки є не лише технічною, а й політико-правовою необхідністю для України. Таке співробітництво забезпечує інтеграцію національної системи кіберзахисту у глобальну архітектуру цифрової безпеки та створює умови для уніфікації правових механізмів реагування на кіберзагрози. Як зазначають М. Гуцалюк та О. Клименко, міжнародна взаємодія у сфері кібербезпеки сприяє підвищенню спроможності держави протидіяти складним і багатовекторним кібератакам, формує єдині стандарти фіксації та доказування кіберзлочинів, а також забезпечує ефективну участь України у спільних розслідуваннях і транскордонному обміні цифровими доказами [18]. Дослідники наголошують, що взаємодія у форматах Ради Європи, ЄС і НАТО створює передумови для синхронізації кримінально-процесуальних інструментів та підвищення довіри між національними компетентними органами [18].

Подібну позицію висловлює М. Сливка, який розглядає участь України у європейських і глобальних ініціативах (зокрема в межах ЄС, НАТО та ООН) як чинник інституційного зміцнення сектору національної безпеки. Учений підкреслює, що залучення до міжнародних програм підготовки

фахівців, обміну кіберіндикаторами та реалізації спільних навчань сприяє формуванню стійкої системи кібероборони, здатної діяти у координації з партнерами [138]. У цьому контексті міжнародне партнерство виступає не лише інструментом технічного посилення, а й засобом підвищення легітимності України у світовому безпековому просторі.

Важливим аспектом міжнародної інтеграції є регіональний вимір розвитку кіберспроможностей, на чому наголошує О. Зінченко. На думку дослідника, безпекова ситуація у Східній Європі має безпосередній вплив на рівень кіберзагроз у Європейському Союзі, оскільки інформаційні атаки та гібридні впливи у регіоні мають транскордонний характер [39]. У подальших працях Зінченко зазначає, що активна участь України у формуванні європейських механізмів протидії кібертероризму сприяє зміцненню колективної безпеки та розширює практичні можливості обміну інформацією між національними центрами реагування [40]. Дослідник також підкреслює, що досвід України у протидії масованим кібератакам на критичну інфраструктуру використовується європейськими партнерами як приклад формування кіберстійкості у кризових умовах [41].

Таким чином, у науковому дискурсі домінує підхід, за яким міжнародне співробітництво у сфері кібербезпеки розглядається не як факультативний компонент, а як структуроутворюючий елемент національної безпеки України. Воно забезпечує одночасно правову інтеграцію, інституційну спроможність і політичну передбачуваність у реагуванні на сучасні кіберзагрози, що є визначальними ознаками європейської моделі цифрової стійкості [107; 111; 117].

У дисертаційному дослідженні О. Зінченко обґрунтовує, що участь України в міжнародних ініціативах із протидії кібертероризму має не лише політичне, а й правове значення, адже сприяє формуванню нового міжнародно-правового порядку у сфері кібербезпеки. Науковець доводить, що залучення держав до спільних механізмів протидії кіберзагрозам створює підґрунтя для вироблення універсальних принципів поведінки у

кіберпросторі та розвитку міжнародних норм, які регулюють питання відповідальності, юрисдикції й співробітництва у боротьбі з кіберзлочинами [41]. Таким чином, міжнародна активність України у цій сфері постає як складова процесу кодифікації сучасного міжнародного права кібербезпеки.

У науковій літературі наголошується, що порівняльний аналіз практик провідних держав світу – зокрема США, Канади, Німеччини та Фінляндії – має значний вплив на формування української моделі кіберзахисту. В. Акульшина підкреслює, що фінська система кібербезпеки базується на ефективному поєднанні державного управління, діяльності спеціалізованих центрів реагування, участі приватного сектору та академічних інституцій, що забезпечує високий рівень національної стійкості [1]. Така модель демонструє ефективність горизонтальної взаємодії між усіма суб'єктами безпеки, що поступово імплементується і в Україні.

Дослідження О. Климчука та Н. Ткачука підтверджують, що у державах із розвиненою системою кіберзахисту ключову координаційну роль відіграють спеціальні служби та правоохоронні органи, які поєднують аналітичні, технічні й оперативні функції, забезпечуючи сталий обмін інформацією та запобігання загрозам [43]. У контексті України подібний підхід реалізується через взаємодію Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ), Служби безпеки України (СБУ) та Національного координаційного центру кібербезпеки (НКЦК) при РНБО, які формують багаторівневу систему реагування на кіберінциденти та координації між відомчими структурами [111; 112].

У зовнішньополітичному вимірі кібербезпека дедалі виразніше набуває рис цифрової дипломатії, що перетворюється на вагомий інструмент утвердження міжнародного авторитету України та зміцнення її позицій у європейських безпекових процесах [67; 138; 220; 285]. Аналітичні матеріали МЗС України та дослідження міжнародного співробітництва у сфері кібербезпеки підкреслюють, що сучасна дипломатія вимагає поєднання традиційних переговорних практик із новітніми цифровими засобами

комунікації, оскільки кіберзагрози дедалі частіше стають предметом міждержавних перемовин, санкційних режимів та правових домовленостей [138; 186; 191; 301; 342]. Звідси випливає, що формування сталої системи кібердипломатії розглядається як природне продовження зовнішньої політики України, орієнтованої на поглиблення інтеграції до європейського безпекового простору та участь у виробленні міжнародних норм поведінки держав у кіберпросторі [67; 138; 220; 285].

Європейська практика переконливо свідчить: ефективна політика кібербезпеки можлива лише за умови узгодженості правового регулювання й технологічного розвитку [173; 181; 224]. На цьому наголошують М. Саєнко, Є. Савела та Ю. Тополянський, які підкреслюють, що у країнах –членах ЄС результативність боротьби з кіберзлочинністю забезпечується насамперед стандартизацією правових процедур, уніфікацією протоколів обміну інформацією та злагодженою роботою національних центрів реагування [134; 215; 216].

Цю думку продовжує Т. Сліпченко, яка наголошує, що кібербезпека повинна бути інтегрованою частиною загальної системи національної безпеки, узгодженою з політикою оборони, правопорядку та захисту прав людини. На її переконання, правове забезпечення у цій сфері не може розвиватися відокремлено від інституційної структури держави, а має функціонувати як невід’ємний елемент комплексного механізму захисту національних інтересів [107; 119; 139].

Порівняльні дослідження А. Тарасюка показують, що у провідних державах світу – США, Канаді, Великій Британії, Німеччині – система кіберзахисту ґрунтується на мультиакторному підході, коли держава, приватний сектор, наука та громадянське суспільство діють у взаємодії, спільно реагуючи на інциденти й виробляючи політику у сфері цифрової безпеки [145; 149; 239]. Такий формат взаємодії дозволяє системам кібербезпеки бути гнучкими, адаптованими до технологічних змін і швидкої еволюції загроз.

П. Яковлєв підкреслює, що у моделях державного регулювання кібербезпеки, які реалізують США, Канада, Німеччина та Франція, поєднуються централізовані стандарти із широкою автономією приватного сектору в питаннях технічного захисту інформації. Такий баланс державного контролю та ринкової ініціативи забезпечує оперативність реагування, підвищує технологічну гнучкість і сприяє сталому розвитку інноваційних підходів у сфері цифрової безпеки [156; 226; 239].

З урахуванням цих підходів можна стверджувати, що українська модель кібербезпеки еволюціонує у напрямі європейського типу врядування, у якому поєднуються нормативна визначеність, технологічна інноваційність і широка міжсекторна взаємодія [34; 47; 64; 173; 231]. Розвиток кібердипломатії, уніфікація правових процедур, зростання ролі наукової спільноти й приватних акторів поступово формують той стратегічний фундамент, на якому вибудовується сучасна державна політика України у сфері кібербезпеки. Проте, попри помітну динаміку зближення з європейськими стандартами, українська модель кібербезпеки стикається з низкою системних викликів, подолання яких є передумовою повноцінної інтеграції у спільний безпековий простір ЄС. Розглянемо основні з них.

Фрагментація врядування та розмежування повноважень. Європейська нормативна рамка встановлює для держав-членів чіткі вимоги щодо визначення компетентних органів, секторної координації та процедур державного нагляду у сфері кібербезпеки (насамперед Директива (ЄС) 2022/2555 – NIS2 та суміжні акти Союзу у сфері цифрової й операційної стійкості критичних суб’єктів) [34; 207; 220; 227–229]. Наукові дослідження наголошують, що успішна імплементація цих вимог залежить від інституційної цілісності режиму врядування, уникнення «перекриття мандатів» між безпековими відомствами та узгодження повноважень на національному й наднаціональному рівнях [173; 181; 221; 224; 225]. Для України це означає завершити чітку делімітацію повноважень основних суб’єктів національної системи кібербезпеки та вибудувати стабільні канали

взаємодії з операторами послуг з урахуванням багаторівневого нагляду, передбаченого NIS2 (класифікація суб'єктів, повідомлення про інциденти, санкційні механізми) [29; 47; 61; 106; 111; 207; 256].

Операційна готовність до кіберкриз та транскордонних інцидентів. В ЄС інституціоналізовано кризовий контур реагування (мережа CSIRTs, Європейська мережа з управління кіберкризами EU-CyCLONe) та запроваджено інструменти спільного реагування в межах політики кіберстійкості, включно з механізмами Регламенту про кіберсолідарність (Cyber Solidarity Act) [220; 223; 227; 231]. Європейське агентство з кібербезпеки (ENISA) кодифікувало найкращі практики кризового менеджменту, координації між органами влади та приватним сектором і типових процедур обміну інформацією [215; 217; 223; 224; 226]. Для України пріоритетним є посилення спроможностей до спільних транскордонних розслідувань і створення дієвого «єдиного вікна» оперативної взаємодії з операторами критичної інфраструктури та міжнародними партнерами – з урахуванням уроків масштабних транскордонних атак, на які системно вказують регулятори США (CISA, FBI, NSA) у спільних консультативних документах щодо загроз критичній інфраструктурі [182; 183; 198–203.

Досвід Європейського Союзу та Північної Америки переконливо демонструє: без усталеної рамки професій, функціональних ролей і компетентностей неможливо забезпечити сталість процесів нагляду, тестування, аудиту та реагування на кіберінциденти. Релевантними орієнтирами для розгортання національної кадрової політики у сфері кібербезпеки виступають NICE Workforce Framework for Cybersecurity (NIST SP 800-181r1) та інші міжнародні стандарти управління кіберризиками, що визначають стандартизовані ролі, навички й моделі професійного розвитку фахівців [257; 260; 304; 320].

У науковій та аналітичній літературі також підкреслюється, що системні програми підвищення обізнаності, освіти та підготовки кадрів у сфері кібербезпеки становлять базову складову кіберстійкості як на рівні

окремих організацій, так і на рівні держави загалом. Як зазначає F. Aloul, ефективна кібербезпека неможлива без формування сталої культури інформаційної безпеки серед користувачів, що передбачає регулярне навчання, оцінювання рівня обізнаності та впровадження поведінкових стандартів кібергігієни [158]. Аналогічний підхід простежується у стратегіях кібербезпеки держав ЄС, зокрема Німеччини, де розвиток професійних компетентностей і цифрової грамотності суспільства визначено одним із ключових напрямів забезпечення національної кіберстійкості [215; 223; 237], а в українських дослідженнях кібергігієна розглядається як необхідна умова підвищення стійкості до сучасних загроз [133; 155]. Ці джерела акцентують, що людський фактор є водночас найвразливішою і найважливішою ланкою системи безпеки, а отже, інвестиції в освіту, підвищення кваліфікації та просвітницькі кампанії є критично необхідними для стійкого розвитку цифрового середовища [61; 139; 155].

Правова інтероперабельність та електронні докази. Поглиблення участі України у транскордонних розслідуваннях потребує послідовної імплементації процедур Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція, 2001) та її Пояснювальної доповіді [187; 188], а також Другого додаткового протоколу (2022) щодо посилення співробітництва та розкриття електронних доказів [189]. Відповідні міжнародні зобов’язання вже відображено в українському законодавстві про ратифікацію Конвенції [116], проте необхідне подальше узгодження кримінального процесуального законодавства й спеціальних законів у частині процедур швидкого збереження, запиту та передачі даних [81; 85; 94; 103; 106; 107]. Зазначені документи встановлюють правові механізми прямого запиту даних від іноземних провайдерів, спрощеного збереження цифрових доказів і взаємної правової допомоги у максимально стислі строки, що має бути системно імплементовано в український процесуальний простір [184; 187–189; 256]. Наукові дослідження звертають увагу на наявність «сірої зони» між національними стандартами кримінального процесу і технічною

швидкістю доступу до даних у хмарних середовищах, що створює ризики фрагментації практики та правової невизначеності; відповідні аспекти потребують уточнення під час адаптації процедур доказування до сучасних міжнародних підходів до електронних доказів [173; 184; 256; 269; 273].

Цифровий суверенітет і сертифікація. Європейська дискусія щодо балансу між відкритістю цифрового ринку, забезпеченням стратегічної автономії та дотриманням вимог до безпечності «продуктів із цифровими елементами» підкреслює визначальну роль сертифікації, управління ланцюгами постачання та єдиних стандартів довіри [161; 162; 173; 220]. Регламент (ЄС) 2019/881 (EU Cybersecurity Act) закріпив постійний мандат ENISA та створив європейські рамки сертифікації кібербезпеки для ІКТ-продуктів і послуг, тоді як Регламент (ЄС) 2024/2847 (Cyber Resilience Act) запровадив обов'язкові вимоги до кіберстійкості цифрових виробів і відповідальність виробників за управління вразливостями протягом життєвого циклу продукту [173; 227; 230]. Для України пріоритетним є узгодження національних схем сертифікації та оцінки відповідності з європейськими, зокрема у сфері хмарних і SaaS-рішень, а також мінімізація адміністративних бар'єрів для виробників і державних замовників [59; 130; 220; 273]. Це дозволить забезпечити прозорість ринку, підвищити довіру до вітчизняних технологічних продуктів і сприятиме інтеграції України у спільний цифровий простір ЄС [34; 59; 63].

Стандарти та інтероперабельність державних сервісів. Досвід Естонії та інших країн Північної Європи (зокрема екосистема X-Road і забезпечення сумісності державних реєстрів) демонструє, що ефективна технічна інтеграція ґрунтується на відкритих протоколах, стандартизованих інтерфейсах обміну даними та узгоджених архітектурних принципах цифрового врядування [254; 284; 298; 309]. Відповідно до методичних рекомендацій ENISA та Центру передового досвіду з питань кібероборони НАТО (CCDCOE), розроблення й реалізація національних стратегій кібербезпеки мають спиратися на повний цикл політики – планування,

впровадження, моніторинг і періодичне оновлення – що виступає гарантією ефективності та запобіжником формалізму [223; 224; 225; 288].

Міжнародна координація та кібердипломатія. Європейський Союз послідовно розвиває інструментарій кібердипломатії, зокрема механізми санкційного реагування в межах EU Cyber Diplomacy Toolbox, що вимагає від партнерів процесуальної сумісності для проведення атрибуції та доведення кібератак [186; 191; 220; 285]. У трансатлантичному вимірі зберігається потреба у функціональній координації ЄС—США, де спільні підходи сприяють посиленню стримування, взаємній підтримці та спрощенню обміну інформацією [160; 197; 299].

Оцінювання спроможностей і зовнішні індекси. Дані Global Cybersecurity Index Міжнародного союзу електрозв'язку (МСЕ) та порівняльні аналітичні огляди засвідчують, що формальна наявність законів і стратегій ще не гарантує ефективності без належних операційних практик, інвестицій у виконання та незалежного аудиту [164; 235; 258]. Для підвищення рівня зрілості національної системи кібербезпеки потрібні сталі метрики результативності, що дозволяють об'єктивно оцінювати динаміку розвитку [215; 223; 258].

Секторальні та геополітичні ризики. Сфери енергетики, транспорту та космічної діяльності залишаються зонами підвищеної вразливості й регуляторної неповноти, попри наявність дорожніх карт і стратегічних документів [194; 237; 275; 309; 331]. Повномасштабна війна проти України продемонструвала, що кібероперації дедалі тісніше поєднуються з фізичними атаками на критичну інфраструктуру, посилюючи взаємозалежність енергетичних, логістичних і комунікаційних систем [71; 166; 195; 206; 222; 282]. Цей досвід підтвердив, що кіберпростір стає ключовим полем стратегічної конкуренції та гібридного впливу, а ефективне реагування можливе лише за умов інтегрованих стандартів і колективних механізмів підтримки [206; 215; 292]. Відповідно, НАТО визначає кіберпростір як сферу колективної стійкості, що потребує глибшої

сумісності стандартів партнерів і готовності до спільного реагування на масштабні інциденти [292; 294; 295; 321].

Міжсекторна взаємодія та державно-приватне партнерство (ДПП). Європейська практика демонструє, що ефективна кіберстійкість є результатом узгодженої взаємодії держави, бізнесу та суспільства. Зокрема, моделі UP KRITIS та Allianz für Cyber-Sicherheit у Німеччині, а також діяльність Nationales Cyber-Abwehrzentrum функціонують як сталі механізми державно-приватної взаємодії у сфері захисту критичної інфраструктури та реагування на кіберінциденти [167; 168; 170]. Українська наукова та аналітична література також підкреслює стратегічну важливість формування національної моделі ДПП для переходу до європейських стандартів кіберстійкості [13; 16; 21; 53; 77].

З огляду на значення державно-приватної взаємодії для інтеграції України до європейської системи кібербезпеки, питання формування національної моделі ДПП розглянуто окремо в підрозділі 3.3, де проаналізовано його механізми, правові засади та міжнародні стандарти реалізації.

На підставі цього, можна визначити такі пріоритети, реалізація яких сприятиме подальшому зближенню України з правовими, інституційними та операційними рамками Європейського Союзу:

Завершити делімітацію повноважень і формування процедурного ланцюжка державного нагляду відповідно до вимог NIS2 та CER, забезпечивши ризик-орієнтованість, пропорційність контролю та ефективне застосування санкційних механізмів [207].

Інституціоналізувати механізми державно-приватного партнерства для обміну даними – за зразком UP KRITIS та Allianz für Cyber-Sicherheit – доповнивши їх правовими гарантіями добровільного інформаційного обміну, сумісними з підходами ISAC/ISAO та практиками AIS/JCDC, що застосовуються у США [170; 201; 202].

Розвинути кадрову рамку на основі моделей NICE та NIST CSF 2.0, доповнивши її широкими програмами підвищення кіберобізнаності у державному та приватному секторах [304].

Гармонізувати сертифікаційні схеми та вимоги до кіберпродуктів і ланцюгів постачання відповідно до Регламентів (ЄС) 2019/881 і 2024/2847, забезпечуючи поступове взаємне визнання стандартів між Україною та ЄС [227; 230].

Поглибити операційну інтеграцію до механізмів кризового реагування ЄС, зокрема мереж CSIRTs, EU-CyCLONe та інструментів Cyber Solidarity Act, що формують загальноєвропейську систему координації та взаємної допомоги [223; 231].

Забезпечити процесуальну сумісність у сфері електронних доказів з урахуванням вимог Другого додаткового протоколу до Будапештської конвенції [189], а також узгодити національні позиції з інструментами кібердипломатії ЄС [285].

Зазначені орієнтири відповідають методичним підходам ENISA щодо розбудови національних систем кібербезпеки та міжсекторної взаємодії [223; 224; 226], а також рекомендаціям і практикам NATO CCDCOE, спрямованим на підвищення рівня кіберстійкості та нормативної узгодженості держав [288; 178]. Вони узгоджуються з практикою країн із розвиненими режимами кібербезпеки – Німеччини, Естонії, Канади, США та Великої Британії [237; 254; 286; 239; 338]. Їх поступове впровадження може стати логічним кроком у процесі поглиблення інтеграції України до правового й операційного простору кібербезпеки Європейського Союзу.

3.3. Державно-приватне партнерство як інструмент кіберстійкості

Моделі державно-приватного партнерства у сфері кібербезпеки: порівняльно-правовий аналіз США та ЄС. У сучасній євроатлантичній практиці державно-приватне партнерство (ДПП) у сфері кібербезпеки розглядається як система правових, організаційних і технічних механізмів взаємодії держави з операторами послуг, постачальниками ІКТ, виробниками програмних рішень та іншими суб'єктами цифрової інфраструктури з метою запобігання, виявлення й реагування на кіберзагрози. Така співпраця охоплює не лише обмін інформацією, а й спільне планування, проведення навчань, вироблення галузевих стандартів і сертифікаційних схем, що презентується в наукових дослідженнях і аналітичних оглядах, присвячених розбудові механізмів ДПП у сфері кібербезпеки. [16; 21; 38; 53; 77; 281; 320]

Правові засади ДПП у державах Європейського Союзу значною мірою визначені Директивою (ЄС) 2022/2555 (NIS2), яка встановлює вимоги до управління ризиками, компетентні органи та обов'язки «essential» і «important» суб'єктів, а також комплексом актів ЄС щодо стійкості критичних суб'єктів і захисту критичної інфраструктури, що аналізуються в європейській та українській доктрині права ЄС у сфері кібербезпеки. [34; 173; 207] Їх доповнює Регламент (ЄС) 2019/881 (Cybersecurity Act), який визначає постійний мандат ENISA та засновує європейські схеми сертифікації ІКТ-продуктів і послуг. [173; 227]

У європейській практиці кіберстійкість вибудовується через партнерство держави, бізнесу та академічного сектору, що включає розгортання платформ обміну загрозовою інформацією, розвиток сертифікаційних механізмів та спільне інвестування у цифрову інфраструктуру, що підтверджується рекомендаціями ENISA щодо організації кіберкризового менеджменту та державно-приватної взаємодії. [223; 226]. Аналогічний принцип закріплено в Рекомендації OECD щодо управління цифровими ризиками, де цифрова безпека інтегрується в загальне

управління ризиками, а відповідальність розглядається як спільна між державою, приватним сектором і суспільством. [232; 300]

У доктрині НАТО кооперація з промисловістю розглядається як невід'ємна складова колективної оборони в кіберпросторі, що відображено в офіційних документах та аналітичних матеріалах Альянсу щодо кібероборони та стратегічної конкуренції в цифровому середовищі [292; 321]. Ініціатива NATO Industry Cyber Partnership (NICP), започаткована на Конференції з кібероборони НАТО 17 вересня 2014 р., закріпила стратегічні підходи до взаємодії між Альянсом, національними структурами кіберзахисту та приватним сектором, зокрема через створення формалізованих каналів співпраці з промисловими партнерами [293]. Документальні матеріали щодо NICP визначили, що ефективна кібероборона неможлива без довіри, своєчасного обміну інформацією про загрози, спільних навчань і координації технічних стандартів між урядовими та промисловими партнерами, що загалом відповідає концепції «public–private cybersecurity», розробленій у сучасній науковій літературі [213; 226]. У межах NICP передбачено створення постійних механізмів діалогу з ІКТ-компаніями, а також залучення приватних інновацій до спільних оборонних ініціатив, що корелює з європейськими та національними моделями державно-приватного партнерства у сфері кібербезпеки [21; 226; 281; 320]. Подальший розвиток цих засад відображено в оновленій політиці НАТО у сфері кібероборони (Comprehensive Cyber Defence Policy) та підсумкових заявах самітів НАТО щодо підтримки України й зміцнення кіберстійкості євроатлантичного простору через поглиблення партнерства між державами, оборонною промисловістю та технологічними компаніями [292; 294; 295].

Еволюція концепції «collaborative cyber defence» (2010–2024)

2010–2015. Формується стратегічна основа публічно-приватної взаємодії у США. Документ *International Strategy for Cyberspace* (2011) уперше на рівні офіційної стратегії визначив партнерство держави й бізнесу як один із пріоритетів національної безпеки у цифровій сфері, поєднуючи

цілі безпеки, економічного розвитку та захисту прав людини в мережевому середовищі [334]. У секторі енергетики *Roadmap to Achieve Energy Delivery Systems Cybersecurity* (DOE, 2011) закріпила обов'язкову участь операторів критичної інфраструктури у плануванні та реалізації заходів кіберзахисту, включно з управлінням ризиками, обміном інформацією та спільним виробленням галузевих стандартів [331; 275].

2016–2020. Відбувається інституціоналізація співпраці через створення та розвиток національних команд реагування на комп'ютерні інциденти (CSIRT), формування кризових процедур і методик управління кіберінцидентами на європейському та національному рівнях [215; 223]. Європейське агентство з кібербезпеки (ENISA) опублікувало низку практичних рекомендацій, зокрема *NCSS Good Practice Guide* (2016) та *National Cybersecurity Strategies – Practical Guide v2.0* (2023), що визначили стандарти розбудови партнерства між державними й приватними акторами, ролі операторів критичної інфраструктури та механізми їх залучення до національних систем кібербезпеки [224; 225; 226]. У цих документах публічно-приватна взаємодія розглядається як ключовий інструмент підвищення кіберстійкості та готовності до криз, що узгоджується з висновками українських та зарубіжних досліджень щодо ДПП у секторі безпеки [21; 281; 320].

2021–2024 (США). Президентський указ № 14028 *On Improving the Nation's Cybersecurity* (2021) започаткував формування Joint Cyber Defense Collaborative (JCDC) під егідою Агентства з кібербезпеки та безпеки інфраструктури (CISA) як постійного механізму спільного планування, обміну інформацією та координації реагування між державними структурами, операторами критичної інфраструктури та провідними IT-компаніями [351; 202; 200]. Паралельно розвивалися операційні моделі обміну інформацією ISACs та ISAOs, які інституціоналізували взаємодію між державними органами, бізнесом і галузевими об'єднаннями на основі спеціальних правових режимів та програм захисту інформації [201; 204]. У

2020-х роках NIST оновив ключові рамкові документи у сфері кібербезпеки (зокрема NICE Framework), посиливши блоки щодо партнерської взаємодії, розподілу ролей і відповідальності та управління ризиками у ланцюгах постачання, що відображено в акценті на спільній відповідальності держави й бізнесу за стійкість цифрової інфраструктури [304; 324].

2022–2025 (ЄС). Європейський Союз ухвалив низку актів, що суттєво посилили правові засади цифрової стійкості, нагляду за критичними постачальниками ІКТ-послуг та колективного реагування на кіберінциденти. *Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA)* запроваджує вимоги до кіберстійкості фінансових установ, включно з управлінням ІКТ-ризиками, тестуванням, аутсорсингом та взаємодією з постачальниками критичних ІКТ-послуг [229; 173]. *Regulation (EU) 2024/2847 – Cyber Resilience Act (CRA)* установлює обов'язкові вимоги до безпеки «продуктів із цифровими елементами» й відповідальність виробників за управління вразливостями протягом життєвого циклу продукту [230; 227]. *Regulation (EU) 2025/38 – Cyber Solidarity Act* формує механізми солідарного реагування на кіберінциденти, включаючи створення Європейських центрів підтримки реагування та спільні платформи моніторингу й аналізу кіберзагроз [231; 215]. У сукупності ці акти закріплюють модель «collaborative cyber defence» на рівні ЄС, яка базується на інституціоналізованому партнерстві держави, операторів критичної інфраструктури та ІКТ-промисловості, що є важливим орієнтиром і для української моделі державно-приватної взаємодії у сфері кібербезпеки [21; 34; 226].

У National Cybersecurity Strategy Сполучених Штатів зафіксовано принцип «перенесення тягаря кібербезпеки» (shifting the burden), який передбачає зміщення основної відповідальності за безпеку цифрових систем із кінцевих користувачів на розробників програмного забезпечення, постачальників цифрових послуг та операторів критичної інфраструктури [324; 269; 213]. Такий підхід покликаний забезпечити системний

перерозподіл ризиків і формування стійких партнерств між державними органами, приватними компаніями та власниками цифрових платформ як ключової умови управління кіберризиками [324; 205; 213]. Реалізацію цих положень деталізовано у National Cybersecurity Strategy Implementation Plan (липень 2023 р.), який визначає механізми координації між урядовими структурами, регуляторами та приватним сектором у сферах реагування на інциденти, розроблення технічних стандартів і підвищення цифрової стійкості національної інфраструктури [325; 205].

У Cybersecurity Strategy for the Digital Decade (2020) Європейська Комісія наголошує, що забезпечення цифрової стійкості Європейського Союзу ґрунтується на партнерському підході, який передбачає взаємодію між державними органами, бізнесом, науковими установами та громадянським суспільством [220; 181]. Такий підхід охоплює: розвиток європейських схем сертифікації відповідно до положень Регламенту (ЄС) 2019/881 (Cybersecurity Act), який установлює єдині стандарти довіри для ІКТ-продуктів і послуг [227; 173; 220]; створення та підтримку платформ обміну інформацією про кіберзагрози через Information Sharing and Analysis Centres (ISACs) з метою оперативного реагування та підвищення ситуаційної обізнаності [226; 223; 201]; підтримку дослідницьких та інноваційних ініціатив у межах європейської мережі центрів компетенцій у сфері кібербезпеки, що забезпечує координацію наукових розробок і впровадження передових технологій у безпекову політику [220; 226; 231].

У 2021 р. Агентство з кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency, CISA) створило Joint Cyber Defense Collaborative (JCDC) – інституційний механізм координації зусиль державних і приватних суб’єктів у сфері національної кібероборони [200; 202]. Метою JCDC є уніфікація планування та проведення кіберзахисних операцій шляхом спільної роботи федеральних органів, відомств штатів і територій (SLTT-партнерів), операторів критичної інфраструктури та

провідних IT-компаній для виявлення, запобігання та реагування на зловмисну кібердіяльність, що загрожує національним системам [200; 198; 202].

Основними спроможностями JCDC визначено:

– всеохопне національне планування для управління ризиками як у штатному режимі, так і під час кіберінцидентів;

– спільну ситуаційну обізнаність і аналітичну підтримку державних та приватних партнерів для прийняття узгоджених рішень;

– інтегровані кіберзахисні спроможності для захисту критичної інфраструктури;

– інституціоналізовані навчання та оцінювання ефективності спільних планів і процедур;

– гнучкі механізми взаємодії із секторними регуляторами (Sector Risk Management Agencies, SRMAs) для розроблення галузевих планів управління ризиками [202; 200; 198; 223].

Нормативне підґрунтя цієї моделі утворює розгалужена система актів стратегічного та процедурного характеру, зокрема: Executive Order 14028 (2021) щодо безпеки ланцюгів постачання, архітектури Zero Trust та обміну інцидентною інформацією [351; 200]; Cybersecurity Information Sharing Act (2015), який забезпечує правові механізми добровільного обміну кіберіндикаторами між державою і бізнесом [204; 213]; програма Protected Critical Infrastructure Information (PCII), що гарантує конфіденційність даних операторів критичної інфраструктури [332; 275]; і Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), який запровадив обов’язкове звітування про серйозні кіберінциденти [349; 324]. У межах Joint Cyber Defense Collaborative (JCDC) CISA об’єднує федеральні відомства, операторів критичної інфраструктури та провідні IT-компанії для спільного планування, вироблення оперативних «плейбуків» і реагування на кібератаки, зокрема на державні загрози [200; 202; 182].

Комплексну основу системи доповнюють міжнародні стандарти та рамкові документи з кібербезпеки, зокрема рекомендації ISO/IEC та NIST щодо управління кіберризиками й розвитку кадрового потенціалу у сфері кіберзахисту, які підкреслюють ключову роль партнерств у забезпеченні кіберстійкості [257; 260; 205; 304].

Європейські моделі публічно-приватної взаємодії.

Німеччина (BSI): UP KRITIS і Allianz für Cyber-Sicherheit. Німецька модель державно-приватного партнерства у сфері кіберзахисту ґрунтується на інституційній ролі Федерального відомства з інформаційної безпеки (BSI), яке координує взаємодію держави з операторами критичної інфраструктури. Платформа UP KRITIS розглядається як одна з найбільш сталих форм співпраці держави та бізнесу у питаннях обміну інформацією, підготовки до інцидентів і вироблення галузевих стандартів захисту критичних систем [16; 21; 145]. Додатковий вимір кооперації забезпечує ініціатива Allianz für Cyber-Sicherheit, що формує мережу довіри між державними інституціями та приватними компаніями, спрямовану на поширення попереджень, рекомендацій і найкращих практик кіберзахисту [13; 21]. Взаємодія на оперативному рівні підсилюється діяльністю Національного центру кіберзахисту, який виконує функції міжвідомчої координації та підтримки реагування на інциденти [16; 77]. Правові засади цієї моделі, зокрема щодо повноважень BSI та процедур взаємодії з приватним сектором, узагальнено у профільних аналітичних дослідженнях, присвячених зарубіжним механізмам кіберзахисту та регулювання критичної інфраструктури [21; 145].

Велика Британія: програма Industry 100 (i100). У британській моделі державно-приватного партнерства у сфері кібербезпеки особлива увага приділяється інтеграції людського потенціалу державного та приватного секторів. Програма Industry 100 (i100), координована Національним центром кібербезпеки (NCSC), створює умови для тимчасового залучення фахівців приватних компаній (secondments) до спільної роботи з державними командами у межах NCSC. Такий формат дозволяє формувати спільні робочі

середовища для обміну знаннями, практичним досвідом і аналітичними підходами до виявлення та протидії кіберзагрозам, що підвищує взаємну довіру між державою та індустрією [16; 77; 320].

Нормативну основу діяльності операторів основних послуг (*Operators of Essential Services*) у Сполученому Королівстві визначають The Network and Information Systems Regulations 2018, які імплементують положення Директиви (ЄС) 2016/1148 (NIS Directive) у національне законодавство. Ці норми встановлюють обов'язки суб'єктів критично важливих секторів щодо управління кіберризиками, повідомлення про інциденти та співпраці з компетентними органами у сфері національної кібербезпеки [338].

Естонська модель публічно-приватної взаємодії у сфері кібербезпеки ґрунтується на створенні комплексної технологічної та правової інфраструктури довіри між державними та приватними інформаційними системами. Її функціонування інтегроване у загальну архітектуру е-урядування, визначену в Digital Agenda for Estonia (Estonia's Digital Agenda 2030) та актах, що регулюють державні інформаційні системи, які закріплюють принципи сумісності державних і приватних інформаційних систем [284; 309]. Центральним елементом цієї моделі є платформа X-Road, яка забезпечує захищений обмін даними та інтероперабельність між державними установами, фінансовими організаціями, страховими компаніями й іншими постачальниками цифрових послуг [298; 284]. Архітектура X-Road побудована на принципах мінімізації даних (data minimisation), повного журналювання транзакцій (comprehensive logging) та взаємної автентифікації сторін за допомогою електронних сертифікатів, що унеможливлює несанкціонований доступ і забезпечує повну простежуваність інформаційних обмінів [298]. Інституційне управління розвитком платформи здійснює Nordic Institute for Interoperability Solutions (NIIS) – міжурядова організація, створена Естонією та Фінляндією з метою координації технічних стандартів, безпеки та відкритості коду системи [298]. Правову основу функціонування X-Road становить Public Information Act, який визначає

принципи обміну публічною інформацією, порядок доступу до неї та вимоги до безпечної взаємодії державних інформаційних систем [310]. Стратегічне планування та розвиток екосистеми кіберзахисту координуються через Cybersecurity Strategy 2024–2030 та щорічні звіти Information System Authority (RIA), що забезпечують моніторинг ефективності, оцінку ризиків і вдосконалення нормативної бази [309; 254; 311].

Порівняльний аналіз практик США, Європейського Союзу, Великої Британії, Німеччини та Естонії свідчить про формування у євроатлантичному регіоні уніфікованої концепції «collaborative cyber defence» – співзахисної моделі взаємодії держави, бізнесу та громадянського суспільства. Її сутність полягає у спільному управлінні цифровими ризиками на основі правової визначеності, технічної взаємодії та довіри між учасниками кіберекосистеми, що відображено у стратегічних підходах ЄС, НАТО, держав-членів та США до розвитку кіберстійкості й публічно-приватної взаємодії [220; 226; 288; 292; 324].

Інституційне оформлення партнерства. У досліджених державах ДПП набуло ознак сталої інституційної системи. Сполучені Штати реалізували її через створення Joint Cyber Defense Collaborative (JCDC) під егідою CISA, що поєднує можливості державних відомств та провідних ІКТ-компаній у сфері обміну інформацією про загрози та спільного планування оборонних заходів [200; 202; 324; 351]. Європейський Союз розвиває мережеву модель координації через CSIRTs Network, механізми ISACs та регуляторні рамки NIS2, які закріплюють обов’язки операторів послуг і механізми обміну інцидентною інформацією [207; 223; 226]. Німеччина інституціоналізувала ДПП у форматі UP KRITIS та Allianz für Cyber-Sicherheit, що функціонують під координацією BSI і поєднують операторів критичної інфраструктури, профільні об’єднання та державні органи [168; 170; 171; 237]. Велика Британія запровадила програму Industry 100 (i100), яка інтегрує фахівців з приватного сектору в операційну діяльність National Cyber Security Centre (NCSC) для спільної оцінки загроз і розроблення рекомендацій [286].

Естонія, у свою чергу, забезпечує інституційне оформлення партнерства завдяки інфраструктурі довіри X-Road та її інтеграції в національну стратегію кібербезпеки й систему правового регулювання публічної інформації [284; 298; 309; 310]. В усіх випадках партнерство є постійно діючим механізмом координації, що забезпечує обмін інформацією, спільне планування та навчання як ключові інструменти «collaborative cyber defence» [220; 226; 288].

Нормативна кодифікація спільної відповідальності. Євроатлантична правова база закріплює спільну відповідальність держави, операторів критичної інфраструктури та постачальників цифрових послуг за кіберстійкість, поєднуючи вимоги до управління ризиками, звітності та реагування на інциденти [220; 300]. У США це відображено в *National Cybersecurity Strategy* (2023), яка прямо проголошує принцип *shifting the burden* – перенесення основної відповідальності за безпеку цифрових систем із кінцевих користувачів на розробників програмного забезпечення, провайдерів послуг та операторів критичної інфраструктури [324]. В ЄС аналогічний підхід реалізовано через Директиву (ЄС) 2022/2555 (NIS2), а також Регламенти (ЄС) 2022/2554 (DORA), 2024/2847 (Cyber Resilience Act) та 2025/38 (Cyber Solidarity Act), які разом формують нормативне ядро колективної цифрової стійкості та визначають обов'язки суб'єктів щодо управління кіберризиками і реагування на інциденти [34; 207; 229–231].

Операційна інтеграція публічних і приватних спроможностей. Державно-приватне партнерство дедалі частіше функціонує не лише як політична або консультативна платформа, а як елемент оперативної кібероборони та спільного управління інцидентами [223; 226]. У США *Joint Cyber Defense Collaborative (JCDC)* забезпечує спільне планування, обмін інформацією та координацію реагування між федеральними органами, зокрема профільними секторними органами (SRMAs), операторами критичної інфраструктури та провідними ІКТ-компаніями [200; 202; 203]. У Німеччині подібні завдання підтримуються через міжвідомчо-приватні

платформи UP KRITIS та Allianz für Cyber-Sicherheit, що функціонують під координацією Федерального відомства з інформаційної безпеки (BSI) і забезпечують структурований діалог з операторами критичної інфраструктури та бізнесом [167; 168; 170; 237]. В ЄС оперативну взаємодію в інцидентному вимірі здійснюють національні CSIRTs, роботу яких у межах мережі CSIRTs координує ENISA як секретаріат відповідно до NIS2 та рамкових документів щодо кризового менеджменту і класифікації інцидентів [207; 216; 223; 227].

Довіра як фундамент партнерства. Естонська модель X-Road демонструє, як інституційна довіра між державою, бізнесом і громадянами підкріплюється технічними гарантіями – взаємною автентифікацією суб'єктів, повним журналюванням транзакцій, розподіленою архітектурою та принципом мінімізації даних у державних інформаційних системах [254; 284; 298; 311]. Це підтверджує, що сталий правовий порядок у кіберпросторі можливий лише за умови технічної прозорості, чіткого визначення ролей суб'єктів та юридичного закріплення їхньої відповідальності у сфері цифрової безпеки [173; 220; 227; 300].

Узгодження підходів до стандартів і сертифікації. Регламент (ЄС) 2019/881 (Cybersecurity Act) визначає постійний мандат ENISA та створює рамку європейських схем сертифікації; у США орієнтиром залишається NIST CSF 2.0. Підходи сторін комплементарні, але без офіційного взаємного визнання сертифікації [160; 205; 227].

Кіберстійкість як публічне благо. У стратегічних документах НАТО (у т.ч. Вашингтонська декларація 10 липня 2024 р.) кіберстійкість подається як спільна відповідальність і предмет системної кооперації держав-союзників, індустрії та наукової спільноти [292; 293; 321]. В ЄС це закріплено у Стратегії кібербезпеки 2020 та подальших регуляторних актах [220; 227; 229; 230; 231], а в США – у National Cybersecurity Strategy 2023 [324].

Узагальнюючи, можемо стверджувати, що євроатлантична модель державно-приватного партнерства у сфері кібербезпеки характеризується

нормативною зрілістю, інституційною сталістю та високим рівнем довіри між сторонами. Її визначальні принципи – правова визначеність, спільна відповідальність, прозорість обміну та технологічна довіра – забезпечують ефективне функціонування системи колективної кіберстійкості [16; 21; 160; 213; 226; 281; 320].

Зазначені підходи формують методологічну основу для подальшого дослідження питань адаптації євроатлантичних моделей ДПП до української правової системи, зокрема у частині правового статусу операторів критичної інфраструктури, процедур обміну кіберіндикаторами та розвитку національної архітектури довіри у цифровому просторі [21; 38; 53; 69; 88; 95; 106; 111; 201; 204; 256].

Адаптація євроатлантичних підходів ДПП/ДПВ до української правової системи. Кібербезпека посідає одне з ключових місць у системі пріоритетів державної політики національної безпеки України [26; 61; 107]. Зростання кількості та складності кібератак на критичні, урядові та корпоративні ресурси актуалізує необхідність нормативного закріплення механізмів партнерства держави й приватного сектору [36; 75; 215]. Як зазначає С. Гнатюк, у вітчизняній практиці відбувся поступовий перехід від ситуативної співпраці до інституційного оформлення державно-приватної взаємодії у сфері кібербезпеки, що проявляється у створенні стратегічних документів, міжвідомчих форматів та секторальних ініціатив [13; 21; 53; 88].

У порівняльному вимірі В. Григоренко підкреслює, що ефективне державно-приватне партнерство ґрунтується на довірі, прозорості, розподілі відповідальності та обміні інформацією в режимі реального часу [16; 226]. У країнах ЄС ці принципи реалізуються через інституційні механізми CSIRTs Network, ISACs, платформи публічно-приватної співпраці, а також через обов’язкові стандарти кіберстійкості, зокрема NIS2, DORA та CRA [201; 207; 229; 230]. Їх імплементація в Україні потребує узгодження з вимогами законодавства про критичну інфраструктуру та державну таємницю [90; 95; 106; 111].

Аналітична доповідь НІСД під загальною редакцією Д. Дубова підкреслює, що держава має стимулювати участь бізнесу у забезпеченні кіберстійкості не лише через нормативні вимоги, а й через економічні інструменти –кіберстрахування, спільні тренінги, участь у кіберполігонах та проєктах практичної готовності [21]. Цей підхід відповідає євроатлантичній моделі “whole-of-society approach”, що передбачає залучення держави, бізнесу, академічного та громадського сектору [224; 292; 300; 324].

Дослідження О. Дідич та О. Наумко демонструє, що в умовах воєнного стану ДПП перетворюється на чинник обороноздатності, забезпечуючи створення оперативних форматів співпраці між державою та ІТ-компаніями для протидії кіберагресії [27; 71]. Такі підходи корелюють із практикою США, зокрема моделлю Joint Cyber Defense Collaborative (JCDC) [200; 202].

Ю. Заскока звертає увагу на наявні проблеми правового регулювання: відсутність законодавчого визначення державно-приватного партнерства у сфері кібербезпеки, неврегульованість питань розподілу ризиків та захисту інформації, отриманої від приватних суб’єктів, а також нечіткість процедур реагування на інциденти [38; 53]. Ця фрагментарність створює бар’єри для практичного запуску партнерських механізмів у сферах із підвищеними вимогами до захисту даних [17; 64; 111].

С. Г. Петров обґрунтовує, що ефективна ДПВ передбачає формування сталих правових та організаційних механізмів координації, які дозволяють державі виконувати не контрольну, а фасилітаторну функцію, забезпечуючи умови для обміну інформацією та узгоджених дій учасників [80; 98]. Науковець наголошує, що відсутність постійно діючих платформ координації негативно впливає на стійкість системи кіберзахисту [80; 111].

Б. Панасюк стверджує, що державно-приватне партнерство у сфері кібербезпеки має розглядатися як ключовий механізм забезпечення кіберстійкості держави на основі моделі “shared responsibility”, що інтегрує відповідальність держави та бізнесу відповідно до європейських та євроатлантичних стандартів [77; 226; 281; 320].

Таким чином, аналіз наукових, нормативних та аналітичних джерел засвідчує, що формування ефективної моделі державно-приватної взаємодії (ДПВ) у сфері кібербезпеки України потребує комплексного поєднання правових, інституційних та організаційних механізмів [13; 16; 21; 38; 56; 57; 58; 77; 141; 142; 281; 320].

Кодифікація правових засад ДПП/ДПВ – шляхом ухвалення спеціального закону, який визначатиме статус учасників, їхні права, обов'язки та відповідальність у сфері кібербезпеки [13; 21; 38; 77; 88].

Гармонізація національного законодавства з правом ЄС – із урахуванням положень директив і регламентів NIS2, DORA та CRA [207; 229; 230].

Інституційне закріплення форматів співпраці – через створення постійного національного координатора (Single Point of Contact) та галузевих центрів обміну інформацією (ISAC), що відповідає європейській моделі багаторівневої взаємодії держави та приватного сектору [21; 226; 281; 320].

Розвиток ДПВ повинен базуватися на принципах: спільної відповідальності (shared responsibility), «безпеки за дизайном» (security-by-design), системного управління ризиками. Ці підходи відповідають сучасним міжнародним практикам кіберстійкості й підтверджені дослідженнями OECD та галузевими моделями співпраці [141; 142; 281; 320].

Українська правова система вже містить ключові акти, що формують політико-правове підґрунтя для ДПВ у сфері кібербезпеки: Закон України «Про національну безпеку України» [107]; Закон України «Про основні засади забезпечення кібербезпеки України» [111]; Закон України «Про критичну інфраструктуру» [106]; Стратегія кібербезпеки України (Указ Президента № 447/2021) [117]; План заходів на 2025 рік з реалізації Стратегії (КМУ № 204-р) [97]; План реалізації Стратегії кібербезпеки (Указ № 37/2022) [121]; Закон України від 27.03.2025 № 4336-IX (оновлення сфери кіберзахисту) [81]; Постанова КМУ № 1426 [98]. Разом вони визначають рамкові засади взаємодії держави з приватними суб'єктами, але поки не

встановлюють чітких процедур і форматів співпраці. Відповідно, виникає об’єктивна потреба у спеціальному нормативному акті, який би деталізував механізми ДПВ та забезпечив їх практичну реалізацію.

Саме цю прогалину покликаний усунути спеціальний законопроєкт про ДПВ у сфері кібербезпеки. Законопроєкт № 14150 розроблено на виконання Плану реалізації Стратегії кібербезпеки та спрямовано на системне впорядкування державно-приватної взаємодії [88; 97; 117; 121].

Пояснювальна записка законопроєкту акцентує на таких положеннях:

– модель ДПВ у кібербезпеці не передбачає передачі ризиків чи майна, як у класичному державно-приватному партнерстві;

– вона є некомерційною, ґрунтованою на добровільності, рівності сторін, недискримінації;

– взаємодія охоплює обмін інформацією, консультації, спільні навчання, реагування на інциденти, експертну підтримку та участь у розробленні стандартів [88].

Законопроєкт закладає перехід від адміністративно-контрольної моделі державного регулювання до партнерської парадигми взаємодії у сфері кібербезпеки. [13; 21; 38; 77; 88]. Відповідно до статті 2 законопроєкту №14150, метою акта є впорядкування та розвиток державно-приватної взаємодії у сфері кібербезпеки, спрямоване на зміцнення довіри між суб’єктами, підвищення координації дій, стимулювання інновацій та розвиток національного ринку кіберпродуктів і послуг. Законопроєкт ґрунтується на принципах рівності сторін, добровільності участі, заборони дискримінації, юридичної рівності державних і приватних учасників, а також захисту конфіденційної інформації (ст. 3), що засвідчує перехід від адміністративно-контрольної моделі державного регулювання до партнерської парадигми співпраці у сфері кібербезпеки [88].

Документ уперше на законодавчому рівні систематизує ключові поняття, необхідні для функціонування публічно-приватних форматів у кіберпросторі: «державно-приватна взаємодія у сфері кібербезпеки»,

«державний учасник», «приватний учасник», «проект державно-приватної взаємодії» та «проект за нагальною потребою (ad hoc)» [88]. Сфера дії законопроєкту обмежена суто відносинами інформаційно-комунікаційного співробітництва та спільного реагування на інциденти. Закон прямо передбачає, що його норми не поширюються на класичні державно-приватні партнерства з інвестиційною складовою, на процедури публічних і оборонних закупівель, міжнародну технічну допомогу чи благодійну діяльність. Таким чином, законопроєкт чітко відмежовує державно-приватну взаємодію від фінансово-майнових режимів, фокусуючись на співпраці у сфері обміну даними, підвищенні обізнаності, моніторингу загроз і забезпеченні кіберстійкості [88].

Форми реалізації державно-приватної взаємодії передбачені статтею 7 і охоплюють три базові моделі: укладення договорів або угод, підписання протоколів чи меморандумів без створення цивільно-правових зобов'язань, а також приєднання до умов, затверджених державним учасником [88]. Важливим елементом законопроєкту є закріплення гарантій прав учасників (Стаття 10). Окремий розділ законопроєкту присвячено захисту інформації. Стаття 11 встановлює, що дані, отримані в межах проєктів ДПВ, можуть використовуватися виключно для досягнення визначених цілей. Інформація приватних учасників визнається конфіденційною, а порядок передачі службових відомостей визначається Кабінетом Міністрів України [88]. Таким чином, законопроєкт формує комплексний правовий режим обробки даних, який поєднує захист комерційної та службової інформації з вимогами державної безпеки.

Узагальнюючи, слід відзначити, що законопроєкт №14150 «Про державно-приватну взаємодію у сфері кібербезпеки» формує цілісну нормативну основу для розвитку публічно-приватних форматів співпраці та закладає інституційні передумови для формування сталої екосистеми кіберзахисту. Його значущість полягає у переході від фрагментарних та переважно добровільних ініціатив до правово визначеної моделі взаємодії

держави та бізнесу, побудованої на принципах довіри, добровільності, рівності сторін і прозорості [88].

Водночас окремі положення законопроєкту потребують додаткового узгодження з європейськими стандартами, зокрема щодо процедур інформаційного обміну, режиму відповідальності учасників, інтеграції запропонованих механізмів у національну систему кіберстійкості та сумісності з вимогами NIS2, DORA і CRA. Ці аспекти, а також інші можливі напрями вдосконалення, розглядатимуться у наступному блоці питань.

Узагальнення та рекомендації щодо адаптації євроатлантичних підходів до української правової системи.

Нормативне врегулювання. Одним із ключових напрямів подальшої адаптації євроатлантичних підходів є впорядкування інституційної архітектури державно-приватної взаємодії. Доцільним видається розгляд можливості запровадження окремої статті або пункту в законопроєкті, який би визначав центрального координатора державно-приватної взаємодії у сфері кібербезпеки. Такий інститут забезпечив би системність процесів та зняв би наявні проблеми фрагментації повноважень, що наразі розподілені між кількома державними органами без чіткого центру відповідальності, про що свідчить структура ст. 5 проєкту. Запровадження інституту координатора дозволило б: здійснювати стратегічне та операційне планування ДПВ; вести єдиний реєстр проєктів та ініціатив; розробляти та затверджувати типові умови, меморандуми, процедури та методики оцінювання; забезпечувати постійну комунікацію з приватним сектором і професійними спільнотами; здійснювати аудит дотримання умов взаємодії у межах Закону –без дублювання контрольних чи наглядових повноважень інших органів.

Обгрунтування: подібна сервісно-координаційна модель застосовується у низці європейських держав (напр., RIA в Естонії [311], NCSC у Нідерландах [241], ANSSI у Франції [157]), де інституційний центр допомагає із стандартизацією процесів, прозорістю звітності та

впорядкованим обміном інформацією між державними та приватними учасниками.

Доцільно розглянути можливість уточнення статті 4 законопроєкту шляхом доповнення її класифікацією основних типів державно-приватної взаємодії у сфері кібербезпеки. Такий підхід дозволив би впорядкувати напрями, уже визначені в частині першій статті, у більш структуровану систему форматів співпраці, що відповідає європейській практиці. Зокрема, можна було б передбачити шість узагальнених типів: інформаційно-аналітична (обмін даними про загрози, аналітика ризиків, ситуаційна обізнаність); інцидентна (спільне реагування, діяльність CERT/CSIRT, відновлення систем); освітньо-кадрова (навчання, стажування, підвищення кваліфікації); дослідницько-інноваційна (розроблення нових технологій і засобів кіберзахисту); сервісна (надання кіберзахисних або аналітичних послуг державним структурам); політико-нормотворча (участь у розробленні стратегій, стандартів і регуляторних документів).

Обґрунтування. Подібна структуризація вже використовується у країнах Європейського Союзу. Так, у Німеччині в межах ініціатив UP KRITIS та Alliance for Cyber Security (BSI, 2023) запроваджено модель публічно-приватної співпраці, що передбачає класифікацію проєктів за напрямами взаємодії держави й бізнесу [170]. В Естонії під координацією RIA [254] функціонує національна мережа партнерств у сфері кібербезпеки, яка поєднує обмін інформацією, інцидентне реагування, освітні та інноваційні програми. Саме така типізація форматів взаємодії підвищує передбачуваність, сталість і результативність партнерства між державним та приватним секторами.

Доцільно уточнити статті 8 і 11 законопроєкту, встановивши обов’язок повідомляти державного координатора або CERT-UA про інциденти в межах проєктів ДПВ із визначенням строків, каналів і формату звітності. Також варто передбачити можливість створення спільних public–private incident teams із визначеними повноваженнями, складом і правилами обробки даних.

Умови співпраці мають містити мінімальні вимоги до захисту каналів зв’язку та правила деперсоналізації інформації відповідно до національних стандартів.

Обґрунтування. Європейські акти – Директива (ЄС) 2022/2555 (NIS2) [207] та Регламент (ЄС) 2025/38 «Cyber Solidarity Act» [231] – вимагають узгодженого циклу «обмін - реагування - відновлення». Поточна редакція ст. 11 не забезпечує цієї послідовності, тому уточнення сприятиме оперативній координації та відповідності європейським стандартам кіберстійкості.

Доцільно доповнити статтю 5 та Прикінцеві положення законопроєкту положеннями про: щорічний публічний звіт координатора щодо стану державно-приватної взаємодії (кількість і типи проєктів, показники ефективності, виявлені бар’єри); можливість залучення незалежних експертів та громадських організацій до оцінювання результативності у межах відкритих даних; створення єдиного електронного реєстру проєктів ДПВ з відкритою та захищеною частинами.

Обґрунтування. У чинній редакції статті 5 законопроєкту такі механізми не передбачені: вона зосереджена на плануванні, комунікації та внутрішній оцінці ефективності, без вимог до системної звітності чи публічного доступу до інформації. Водночас у країнах ЄС прозорість забезпечується через інституційні платформи партнерства, які поєднують моніторинг, відкриту звітність та незалежну оцінку – зокрема, Bonn Cyber Security Cluster (Німеччина) [193], Campus Cyber France (Франція) [174], Dutch Security Delta (Нідерланди) [209]. Запровадження подібних інструментів сприятиме відкритості, довірі та підзвітності у реалізації державно-приватних проєктів у сфері кібербезпеки.

Доцільно уточнити статті 6 і 7 законопроєкту, посиливши вимоги до прозорості процедур відбору приватних учасників і запобігання потенційним конфліктам інтересів. Зокрема, варто: доповнити статтю 6 нормою про оприлюднення критеріїв відбору та результатів конкурентних процедур; визначити механізм оскарження у випадку порушення принципів відкритості

чи рівного доступу; передбачити обов'язкове постфактум повідомлення координатора у разі застосування неконкурентних (ad hoc) процедур із коротким строком звітування; уточнити у статті 7, що «умови приєднання» мають містити стандартизовані вимоги до доброчесності учасників, відкритості та недискримінаційності.

Обґрунтування. У чинних редакціях статей 6 і 7 визначено загальні правила щодо конкурентного та неконкурентного відбору, а також форми взаємодії (договір, меморандум, умови приєднання). Однак не передбачено процедур прозорого інформування, оскарження або незалежного моніторингу.

Запровадження цих механізмів узгоджується з принципами належного врядування ЄС (EU Good Governance Principles) [221] і вимогами Директиви (ЄС) 2022/2555 (NIS2) [207] щодо відкритості відбору партнерів і недопущення зловживань при укладенні угод про кіберспівпрацю.

Окрім зазначеного, було б також доцільно передбачити в законопроєкті окремий напрям, присвячений розвитку кадрового потенціалу та інновацій у сфері кібербезпеки, який охоплював би створення спільних освітніх програм, стажувань і лабораторій, а також підтримку стартапів через гранти та регуляторні "пісочниці" для тестування нових рішень. Такий підхід відповідає практиці Campus Cyber France [174] та Cyber Tech Estonia [210; 254], де поєднання освітнього і інноваційного сегментів забезпечує сталість кадрового резерву, сприяє розвитку національних технологій і підвищує загальну кіберстійкість.

У межах подальшого вдосконалення законопроєкту також варто інтегрувати у національне законодавство положення Директив NIS2, CER та Регламентів DORA і CRA, що визначають обов'язки операторів критичних послуг, вимоги до управління ризиками та реагування на інциденти запровадити модель "shared responsibility" (розподіл зобов'язань між державою, операторами критичної інфраструктури й постачальниками цифрових послуг), спираючись на європейські акти та методичні підходи

ENISA до публічно-приватної взаємодії; уточнити та розширити перелік принципів державно-приватної взаємодії, закріпивши поряд із наявними принципами рівності, недискримінації та добровільності також принципи прозорості, підзвітності та процедурної справедливості, що передбачали б належні процедури відбору приватних учасників, можливість оскарження результатів і відкритість інформації про реалізовані проєкти; визначити механізм правової відповідальності та захисту прав учасників ДПВ, у тому числі у випадках невиконання зобов'язань чи неналежного використання конфіденційної інформації, з урахуванням режимів звітування/повідомлення, передбачених актами ЄС [207; 229; 230; 226]. Такі положення узгоджуються з європейською рамкою NIS2–DORA–CRA, яка формує правові та організаційні засади спільної відповідальності держави й приватного сектору та забезпечує поступову гармонізацію українського законодавства з нормами ЄС [207; 229; 230; 226].

Інституційне забезпечення. Європейська практика демонструє, що ефективність ДПВ у сфері кібербезпеки безпосередньо залежить від наявності постійних інституцій координації та довіри між державою і приватним сектором. У країнах ЄС такі функції виконують національні координатори, ISAC-платформи та експертні ради, які забезпечують інтеграцію обміну інформацією, спільне планування й оперативне реагування на інциденти. Їхня імплементація в українську систему ДПВ сприятиме операційній узгодженості, підвищенню швидкості реагування та єдності стратегічного управління [207; 226]. Отже, для ефективного впровадження державно-приватної взаємодії у сфері кібербезпеки доцільно передбачити чітку систему управління та координації, яка забезпечуватиме узгодженість дій, прозорість процесів і сталий розвиток партнерства. Зокрема, пропонується: визначити єдиного національного координатора (Single Point of Contact), уповноваженого організовувати обмін інформацією, координацію дій і оцінювання ефективності партнерства. Ця пропозиція узгоджується з раніше сформульованою ідеєю про запровадження окремої статті, якою

передбачалося нормативно закріпити роль такого координатора. Така функція відповідає підходу, визначеному Директивою (ЄС) 2022/2555 (NIS 2), яка зобов'язує держави-члени призначати центральний орган або контактний пункт для управління кіберінцидентами та міжсекторальної взаємодії [207]; створити секторальні координаційні платформи або ради за участю державних органів, операторів критичної інфраструктури, ІКТ-компаній і наукових установ – за зразком Information Sharing and Analysis Centres (ISACs), що діють у ЄС і США як платформи для обміну інформацією між державними й приватними суб'єктами [201; 207; 226]; сформувати постійно діючі консультативні механізми – експертні ради, спільні аналітичні чи інцидентні групи при РНБО, Мінцифрі або НКЦК, аналогічно до Cybersecurity Councils і Public-Private Advisory Boards, створених у Німеччині, Франції та Нідерландах для координації національної політики у сфері кіберстійкості [157; 174; 193; 209]; унормувати статус зазначених структур у національному законодавстві, визначивши їхні повноваження, порядок взаємодії та звітності, що узгоджується з рекомендаціями ENISA «Public-Private Partnerships in Cyber Security – Recommendations and Best Practices» (2024) [206].

Запропоновані заходи спрямовані на формування цілісної моделі державно-приватної взаємодії у сфері кібербезпеки, яка поєднує євроатлантичні стандарти з особливостями української правової системи, забезпечуючи поступову гармонізацію законодавства, інституційну сталість та підвищення національної кіберстійкості.

Висновки до Розділу 3

1. Здійснено системний огляд і критичний аналіз європейської моделі кіберзахисту як нормативно зобов'язувальної екосистеми, що спирається на узгоджений пакет актів (NIS2, CER, DORA, CRA, DSA, Cyber Solidarity Act,

Cybersecurity Act) та методичну роль ENISA; розкрито їх зміст, інституційні новації та взаємозв'язок із сертифікаційними й soft-law механізмами. Показано національні траєкторії імплементації (Німеччина, Франція, Швеція, Естонія) як приклади поєднання правового регулювання з операційною координацією. Доведено, що європейська модель кіберзахисту еволюціонувала від декларативного підходу до послідовного циклу «політика - виконання - контроль - реагування», формуючи багаторівневу архітектуру кіберстійкості, у якій поєднано наднаціональну уніфікацію стандартів із національною відповідальністю за їх практичну реалізацію.

2. Узагальнено особливості формування та розвитку моделі кібербезпеки Сполучених Штатів Америки. Встановлено, що американський підхід базується на поєднанні стратегічного планування, адміністративного регулювання, стандартизації та тісної взаємодії держави з приватним сектором. Показано перехід від переважно добровільних механізмів забезпечення кіберстійкості до системи нормативно визначених вимог, у якій виконавчі акти, секторальні директиви та стандарти NIST відіграють ключову роль у формуванні єдиних правил і процедур безпеки. Окреслено основні напрями державної політики, визначені *National Cybersecurity Strategy* (2023) та *Implementation Plan* (2023–2024), а також роль провідних інституцій –Агентства з кібербезпеки та безпеки інфраструктури (CISA), Національного інституту стандартів і технологій (NIST) та міжвідомчих платформ обміну інформацією. Підкреслено значення інтеграції стандартів *Cybersecurity Framework 2.0* і *NICE Framework* як основи для уніфікації технічних та кадрових підходів до управління кіберризиками. Доведено, що модель кіберзахисту США характеризується практичною спрямованістю, високою адаптивністю та гнучким поєднанням нормативних, організаційних і технічних інструментів, що забезпечують ефективну взаємодію між державою, бізнесом і суспільством у забезпеченні національної кіберстійкості.

3. Здійснено комплексний аналіз політики кібероборони НАТО. Розкрито зміст ключових декларацій і документів Альянсу, які закріплюють інтеграцію кіберсфери в оборонне планування та визначають принципи колективної стійкості, взаємодопомоги й партнерства. Проаналізовано роль Кооперативного центру кібероборони НАТО (CCDCOE) як провідного осередку аналітичної, навчальної та методичної підтримки. Встановлено, що політика НАТО має передусім політичний, а не нормативно-зобов'язувальний характер: Альянс координує дії союзників, сприяє обміну інформацією, формує стандарти сумісності та розвиває колективну готовність до кіберзагроз. У межах цієї моделі кожна держава-член несе відповідальність за власний кіберзахист, тоді як НАТО забезпечує рамкову синергію оборонних, навчальних і правових ініціатив.

4. Проведено комплексний аналіз процесу інтеграції України у міжнародну систему кібербезпеки, який охоплює правові, інституційні та стратегічні аспекти цього процесу. Встановлено, що національна нормативно-правова база у сфері кіберзахисту поступово гармонізується з європейським правом, насамперед із вимогами директив NIS2 і CER, регламентів DORA, CRA та Cybersecurity Act. На основі конституційних положень і спеціальних законів сформовано сучасну модель державного управління кібербезпекою, що спирається на взаємодію ключових інституцій – РНБО, НКЦК, ДССЗЗІ та CERT-UA – і відображає принципи міжвідомчої координації, притаманні європейському врядуванню.

5. Досліджено міжнародно-правовий і дипломатичний вимір інтеграції України до спільного безпекового простору ЄС і НАТО. Простежено, як через участь у кібердіалозі Україна–ЄС, співпрацю з ENISA, залучення до ініціатив Tallinn Mechanism і підготовку до приєднання до EU Cybersecurity Reserve держава посилює свою інституційну сумісність із європейськими механізмами кіберстійкості. Встановлено, що українська практика кіберзахисту поступово відповідає ключовим європейським стандартам ризик-менеджменту, кризового реагування, сертифікації та обміну технічною

інформацією, що підвищує довіру міжнародних партнерів і зміцнює позиції України в євроатлантичному безпековому середовищі.

6. Доведено, що українська модель кібербезпеки еволюціонує у напрямі європейського типу врядування, який поєднує нормативну визначеність, технологічну інноваційність і розвинену міжсекторну взаємодію. Разом із тим виявлено низку системних викликів, зокрема потребу у завершенні делімітації повноважень між органами державної влади, розвитку кадрового потенціалу, інституціоналізації державно-приватного партнерства та забезпеченні операційної інтеграції у європейські механізми кризового реагування.

7. Запропоновано практичні шляхи подолання окреслених викликів і подальшого поглиблення інтеграції України до європейського кібербезпекового простору. Серед основних пріоритетів визначено вдосконалення інституційної координації та створення єдиного координуючого вузла для управління кіберризиками; розгортання національної кадрової рамки на основі стандартів NICE і NIST; розвиток програм підвищення цифрової обізнаності; формалізацію партнерства між державою та бізнесом у сфері обміну кіберданими; узгодження національних схем сертифікації з вимогами Європейського Союзу; а також активну участь у спільних ініціативах ЄС і НАТО.

8. Здійснено комплексний порівняльно-правовий аналіз моделей державно-приватного партнерства (ДПП) у сфері кібербезпеки в державах євроатлантичного простору – Сполучених Штатах Америки, Європейському Союзі, Великій Британії, Німеччині та Естонії. Розкрито зміст, правові основи, інституційну архітектуру та технічні механізми функціонування партнерств, що забезпечують колективну кіберстійкість. Доведено, що ДПП є не лише формою політичної кооперації, а сталою нормативно визначеною системою спільної відповідальності держави, операторів критичної інфраструктури, постачальників цифрових послуг і технологічних компаній за управління кіберризиками, запобігання та реагування на інциденти.

9. Узагальнено еволюцію підходів до співзахисту у 2010–2025 рр., від початкових декларацій партнерства до створення інституційно оформлених механізмів колективної кібероборони. У США цей процес відобразився у формуванні нормативно закріплених моделей співпраці, таких як Joint Cyber Defense Collaborative (JCDC), ISACs та ISAOs, підкріплених актами EO 14028, CIRCIA і стандартами NIST CSF 2.0. В Європейському Союзі аналогічні принципи закріплено в актах NIS2, CER, DORA, CRA та Cyber Solidarity Act, які створюють правове поле для спільного управління ризиками, сертифікації ІКТ-продуктів і взаємодії національних CSIRTs під координацією ENISA. Установлено, що обидві системи – американська та європейська –еволюціонували до моделі «collaborative cyber defence», де партнерство є постійною операційною складовою, а не факультативним механізмом обміну.

10. Здійснено узагальнення національних практик партнерства як прикладів інтеграції нормативних і технічних рішень. Виявлено, що Німеччина реалізує модель мережевої взаємодії через програми UP KRITIS та Allianz für Cyber-Sicherheit під координацією BSI, Велика Британія – через кадрову інтеграцію в межах програми Industry 100 (NCSC), а Естонія – через створення інфраструктури довіри X-Road, заснованої на правовій сумісності та технологічній прозорості обміну даними. Доведено, що довіра в таких системах забезпечується не лише правовими гарантіями, а й технічними інструментами – взаємною автентифікацією, журналюванням транзакцій, мінімізацією даних та відкритими стандартами взаємодії.

11. Узагальнено, що євроатлантична модель ДПП у кібербезпеці характеризується нормативною зрілістю, інституційною сталістю та високим рівнем взаємної довіри між учасниками. Вона спирається на три ключові принципи – правову визначеність, спільну відповідальність і технологічну прозорість, які забезпечують ефективне функціонування системи колективної кіберстійкості. Доведено, що ця модель поєднує регуляторні та інноваційні підходи, уможливлюючи оперативну інтеграцію публічних і приватних

спроможностей. Сформовано теоретико-прикладне підґрунтя для адаптації елементів євроатлантичних моделей до української правової системи, зокрема у частині створення постійних платформ співпраці, процедур обміну кіберіндикаторами, механізмів сертифікації та розвитку національної інфраструктури цифрової довіри.

12. Здійснено порівняльно-правовий аналіз євроатлантичних підходів до ДПП/ДПВ у кібербезпеці; систематизовано їхні базові принципи (довіра, прозорість, розподіл відповідальності, обмін у реальному часі) та інституційні механізми (CSIRTs Network, ISACs, публічно-приватні платформи), включно з нормативною рамкою NIS2/DORA/CRA. Узагальнено наукові позиції щодо ролі держави, бізнесу й суспільства; показано значення економічних стимулів (кіберстрахування, навчання, кіберполігони) та воєнного контексту, який підсилює функцію ДПП як чинника обороноздатності (аналог JCDC). Ідентифіковано ключові регуляторні прогалини України (відсутність дефініцій, процедур розподілу ризиків, правового режиму даних і інцидентного реагування) та обґрунтовано потребу гармонізації з нормами ЄС і закріплення фасилітаторної ролі держави.

13. Визначено ключові напрями адаптації євроатлантичних підходів до української правової системи у сфері кібербезпеки. На основі аналізу наукових та аналітичних джерел визначено чотири стратегічні вектори реформування: по-перше, кодифікацію правових засад державно-приватної взаємодії шляхом прийняття спеціального закону, який встановлює статус, права та обов’язки учасників; по-друге, гармонізацію національного законодавства з правом ЄС відповідно до вимог директив і регламентів NIS2, CER, DORA, CRA; по-третє, інституційне закріплення постійних форматів співпраці через створення єдиного національного координатора (Single Point of Contact) та галузевих ISAC-платформ; і по-четверте, інтеграцію євроатлантичних принципів “shared responsibility” та “security by design” у державну політику й систему управління кіберризиками.

14. Здійснено нормативно-правовий аналіз чинних актів, що формують підґрунтя державно-приватної взаємодії у сфері кібербезпеки України, та визначено рівень їх відповідності євроатлантичним підходам. Проаналізовано основні документи – закони України «Про національну безпеку», «Про основні засади забезпечення кібербезпеки», «Про критичну інфраструктуру», Стратегію кібербезпеки 2021 року та План її реалізації на 2025 рік. На основі їхнього аналізу встановлено, що правова база є лише рамковою і не забезпечує належного механізму практичної взаємодії держави та приватного сектору – відсутні процедури відбору учасників, порядок обміну інформацією та гарантії конфіденційності.

15. Визначено ключову роль законопроєкту №14150 “Про державно-приватну взаємодію у сфері кібербезпеки” як нормативного інструмента кодифікації та впорядкування форматів партнерства. Доведено, що законопроєкт №14150 формує системну нормативну основу для розвитку публічно-приватних форматів співпраці у кібербезпеці, закладає інституційні передумови сталої екосистеми кіберзахисту та демонструє перехід від фрагментарного регулювання до правово визначеної, партнерської моделі взаємодії. Водночас визначено напрями подальшого вдосконалення – гармонізацію із законодавством ЄС, уточнення процедур інформаційного обміну, врегулювання відповідальності сторін і інтеграцію у національну систему кіберстійкості.

16. Реалізовано всі чотири визначені напрями адаптації євроатлантичних підходів до української правової системи – кодифікаційний, гармонізаційний, інституційний та концептуально-принциповий.

У межах кодифікаційного напряму здійснено конкретизацію змісту та структури спеціального закону «Про державно-приватну взаємодію у сфері кібербезпеки». Сформульовано пропозиції щодо доповнення законопроєкту №14150 новими статтями, поняттями та процедурами, що визначають статус учасників, їхні права, обов’язки та відповідальність. Запропоновано окрему статтю про центрального координатора ДПВ (Single Point of Contact),

створення єдиного реєстру проєктів, типізацію форматів взаємодії (інформаційна, інцидентна, освітня, інноваційна, сервісна, нормотворча), а також посилення прозорості, звітності та доброчесності процедур відбору приватних партнерів. Таким чином, створено концептуально завершену модель правового врегулювання ДПВ.

У межах гармонізаційного напряму проведено зіставлення положень законопроєкту з вимогами європейського права – директив і регламентів NIS2, CER, DORA, CRA. На основі цього запропоновано норми щодо обов'язкових процедур повідомлення про кіберінциденти, спільних команд реагування (public–private incident teams), стандартів обробки та деперсоналізації інформації, а також узгодження термінології з категоріями європейського законодавства (critical entities, digital service providers, operators of essential services). У такий спосіб забезпечено відповідність українського законопроєкту вимогам кіберрегуляторного поля ЄС і принципам ENISA.

У межах інституційного напряму обґрунтовано створення єдиної системи управління ДПВ, яка включає: національного координатора (SPOC), уповноваженого забезпечувати обмін інформацією, планування, оцінювання ефективності та комунікацію з приватним сектором; секторальні ISAC-платформи для обміну інформацією між державними й приватними учасниками; постійно діючі консультативні органи – експертні ради, аналітичні й інцидентні групи при РНБО, Мінцифрі, НКЦК; систему незалежного моніторингу, щорічної публічної звітності координатора та єдиний реєстр проєктів ДПВ.

У межах принципово-концептуального напряму впроваджено євроатлантичні підходи "shared responsibility" та "security by design" у систему української кіберполітики. Підкреслено, що держава має виконувати фасилітаторну функцію – створювати правові, технічні й організаційні умови для безпечного обміну даними, спільного реагування на загрози та підвищення кіберстійкості. Запропоновано закріпити ці принципи в

преамбулі та базових статтях законопроєкту як засадничі для розвитку національної моделі ДПВ, гармонізованої з європейськими стандартами управління ризиками.

ВИСНОВКИ

У дисертаційній роботі представлено теоретичне узагальнення й нове вирішення наукового завдання, яке полягає у всебічному теоретико-правовому аналізі системи кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки, визначенні закономірностей її розвитку в умовах гібридної агресії проти України, виявленні ключових інституційно-правових вразливостей і напрямів підвищення кіберстійкості держави, а також у розробленні науково обґрунтованих пропозицій щодо вдосконалення національної моделі правового регулювання та інституційного забезпечення кіберзахисту з урахуванням євроатлантичних підходів. Одержані результати дослідження дозволили сформулювати висновки, націлені на досягнення поставленої мети, а також відповідні рекомендації та пропозиції.

1. У результаті проведеного дослідження проаналізовано еволюцію наукових підходів до розуміння сутності кібербезпеки, з'ясовано її міждисциплінарну природу та визначено співвідношення з суміжними категоріями – інформаційною безпекою, кіберзахистом і кіберстійкістю. Встановлено, що кібербезпека постає як складне міждисциплінарне соціотехнічне явище, у якому поєднуються технічні, правові, управлінські, соціальні та етичні виміри. Її еволюція від вузької концепції інформаційної безпеки до цілісної системної категорії засвідчує поступовий перехід до ризик-орієнтованої парадигми, яка ґрунтується на інтеграції технократичного, правового, управлінського та соціогуманітарного підходів. Такий інтегрований підхід забезпечує цілісне бачення кібербезпеки як процесу управління ризиками, довірою та стійкістю цифрового середовища, що передбачає синхронізацію правових, технологічних і поведінкових інструментів захисту. З'ясовано наявність дефінітивної невизначеності та фрагментарності термінологічного апарату у сфері кібербезпеки, що зумовлює методологічну неузгодженість і нормативну розпорошеність. Доведено необхідність гармонізації базових понять – «інформаційна

безпека», «кібербезпека», «кіберзахист», «кіберстійкість» – у науковій, освітній та правозастосовній практиці. Підкреслено визначальну роль людського фактора та етики інформації у формуванні культури довіри, відповідальності й прозорості в цифровому просторі. У межах дослідження кібербезпеку визначено як стан і безперервний процес забезпечення правомірного, етично врегульованого та стійкого функціонування цифрового середовища, що досягається через узгоджену взаємодію технологічних, управлінських, правових і поведінкових механізмів захисту даних, інфраструктур, соціальних відносин і публічних функцій держави.

2. Проаналізовано міжнародно-правові основи забезпечення кіберзахисту та виявлено роль і вплив універсальних і регіональних актів – ООН, ОБСЄ, Ради Європи та Європейського Союзу – у формуванні глобальної системи норм і принципів у сфері кібербезпеки. Розкрито, що міжнародне право посідає ключове місце у становленні глобальної архітектури кібербезпеки, виконуючи функції універсального регулятора цифрових відносин і водночас інструмента легітимації державної політики у сфері кіберзахисту. Встановлено, що сучасний міжнародно-правовий режим кібербезпеки ґрунтується на базових принципах міжнародного права — суверенітету, невтручання, заборони сили, належної обачності та поваги до прав людини. Показано, що поєднання норм «твердого» та «м’якого» права, інституційних механізмів довіри, процедур атрибуції та публікації національних позицій формує поліцентричну, але внутрішньо узгоджену модель глобального кіберврядування. Особлива увага приділена впливу регіональних і універсальних інструментів: Будапештської конвенції про кіберзлочинність та Другого додаткового протоколу, санкційних механізмів ЄС, а також відповідних ініціатив ООН і ОБСЄ. Доведено, що саме їх взаємодоповнюваність забезпечує ефективну інтеграцію міжнародних, регіональних і національних механізмів протидії кіберзагрозам і сприяє формуванню глобальної системи норм, принципів і стандартів у сфері кібербезпеки.

3. Розкрито структуру національної системи кібербезпеки України, її законодавчі засади, інституційну архітектуру, повноваження суб'єктів та механізми взаємодії державного і приватного секторів. Системно обґрунтовано, що національна система кібербезпеки є багаторівневою соціотехнічною конструкцією, яка функціонує на принципах верховенства права, законності, пропорційності, підзвітності та ризик-орієнтованості. Встановлено, що сучасна архітектура державної політики у сфері кібербезпеки має стратегічно впорядкований характер і включає: рамкові документи (стратегії та концепції), доменні документи (галузеві та секторальні регламенти), а також операційно-стратегічні акти, які визначають порядок інцидент-менеджменту, реагування, координації та обміну інформацією. Проаналізовано законодавчі засади функціонування системи, що визначають компетенцію ключових суб'єктів – РНБО, Національного координаційного центру кібербезпеки, ДССЗЗІ, СБУ, НПУ, CERT-UA та інших органів, залучених до забезпечення кіберзахисту. Особлива роль належить НКЦК, який виконує функції центрального координатора міжвідомчої взаємодії та забезпечує синхронізацію стратегічних і оперативних процесів. Попри позитивну динаміку оновлення законодавства у 2022–2025 роках, доведено актуальність подальшої уніфікації термінології, процедур реагування, сертифікації засобів захисту та модернізації нормативно-технічної бази відповідно до стандартів Європейського Союзу у сфері управління ризиками та кіберстійкості.

4. Розкрито зміст і класифікацію кібероперацій як інструмента сучасних воєн і конфліктів, зокрема у контексті російської гібридної агресії. З'ясовано, що кіберагресія, кібероперації та кіберзлочинність становлять три взаємопов'язані, але самостійні правові феномени, кожен із яких характеризується власною юрисдикційною природою, суб'єктним складом і механізмами відповідальності. Їхня взаємодія формує багаторівневий простір кіберконфліктності, у якому поєднуються державні, недержавні та транснаціональні актори. Показано, що в умовах сучасних воєн і конфліктів –

насамперед російської гібридної агресії проти України – кібероперації виступають інтегрованим інструментом впливу, що поєднує технічні, розвідувальні, інформаційно-психологічні та логістичні компоненти і функціонує у взаємодії з військово-політичними засобами. Розроблена класифікація кібероперацій за параметрами «цілі – інструменти – очікувані ефекти» дала можливість уніфікувати опис інцидентів, забезпечити порівнюваність їхніх наслідків та узгодити технічні характеристики із правовими режимами реагування. Емпіричний аналіз російських кібероперацій підтвердив валідність цієї моделі, оскільки виявив систематичне поєднання деструктивних, розвідувальних та інформаційних дій у межах гібридної стратегії. Окремо встановлено наявність низки «сірих зон» міжнародного права – щодо суверенітету, невтручання, атрибуції та доступу до цифрових доказів, – які особливо виразно проявилися в російській агресії. Обґрунтовано потребу гармонізації доктринальних підходів до кваліфікації кіберінцидентів, розроблення процедур спільної верифікації технічних даних і створення нормативно визначених механізмів публічно-приватної взаємодії, що забезпечували б баланс між державними повноваженнями та технологічною автономією недержавних акторів.

5. Проведено емпіричний аналіз основних кібератак проти України у 2014–2024 роках, котрий дав змогу виокремити три фази ескалації російської кіберагресії, що відображають поступове зростання технологічних та організаційних спроможностей противника. Від перших цільових атак на промислові системи керування (BlackEnergy, Industroyer) – до операцій у ланцюгах постачання (NotPetya) та багатовекторних дій періоду повномасштабної війни (wiper-атаки, масові DDoS-операції, ураження супутникових мереж KA-SAT/Viasat). Визначено стратегічні цілі цих операцій: дестабілізація критичної інфраструктури; порушення життєво важливих цифрових сервісів; створення умов для інформаційно-психологічного тиску; послаблення обороноздатності; ускладнення державного управління, логістики та роботи військових систем. Їх масштаби

та наслідки продемонстрували високий рівень інтеграції кібер-, інформаційних і військових засобів у єдине гібридне операційне середовище – характерну рису сучасної російської воєнної доктрини. Розроблені у дисертації аналітичні матриці відповідності «тип атаки – інцидент – джерела», побудовані на принципі подвійної перевірки, забезпечують відтворюваність кейсів, їх правову кваліфікацію та формують стандартизований підхід до аналізу інцидентів. Доведено, що більшість операцій не досягають порогу «застосування сили», але кваліфікуються як міжнародно-протиправні втручання, а практика колективної публічної атрибуції створює емпіричну базу для подальшого усталення стандартів доказування. Отримані уроки для державної політики безпеки включають: необхідність розвитку системної кіберстійкості; уніфікацію стандартів інцидент-репортингу; посилення співпраці між державою, приватним сектором і міжнародними партнерами; удосконалення механізмів атрибуції; посилений захист IT/OT-інфраструктур; створення резервних цифрових каналів для забезпечення безперервності критичних сервісів навіть в умовах масштабних атак.

6. Виявлено основні вразливості критичної інформаційної інфраструктури, державних органів і суспільства в умовах воєнного стану та запропоновано напрями їх мінімізації. Встановлено, що системні вразливості національної кіберстійкості України проявляються на інституційному, технічному та соціально-комунікаційному рівнях і пов’язані з незавершеністю циклу управління ризиками. До ключових інституційних проблем віднесено фрагментацію повноважень, відсутність уніфікованої таксономії інцидентів та недостатній розвиток механізмів публічно-приватного партнерства. Технічні вразливості включають розриви на стику IT/OT-середовищ, залежність від зовнішніх хмарних сервісів та нерівномірність впровадження засобів захисту. На соціально-комунікаційному рівні визначальними чинниками залишаються людський фактор, дезінформаційні кампанії та відмінності у рівнях кадрової

підготовки. Розроблені у дисертації аналітичні матриці «вразливість – прояви – напрями вдосконалення» відтворюють взаємозв'язок між типами загроз і необхідними інституційно-правовими, технологічними та комунікаційними заходами реагування. Запропоновано пріоритетні напрями мінімізації вразливостей, зокрема: гармонізацію національних стандартів із підходами ENISA, NIS2 та CISA/NSA; розбудову систем оперативного обміну інформацією між CSIRT/SOC; укладення типових угод про рівень надання послуг (SLA) для критичних цифрових сервісів; впровадження практики «червоних команд»; унормування взаємодії з волонтерськими кіберспільнотами та розвиток освітніх програм з кібергігієни.

7. Визначено сучасні проблеми протидії кіберзлочинності та кіберагресії та оцінено ефективність нормативно-правових і оперативно-технічних механізмів реагування. Встановлено, що ключовими викликами залишаються фрагментарність правозастосовної практики, недостатня уніфікація процедур інцидент-менеджменту, обмежений доступ до цифрових доказів, несинхронізованість міжвідомчих процесів і нерівномірний розвиток технічних спроможностей органів сектору безпеки й оборони. На підставі узагальнення виявлених закономірностей обґрунтовано потребу переходу від реактивної до проактивної моделі національної політики кіберзахисту, яка передбачає упереджувальний характер дій, стандартизовані протоколи обміну інформацією та розвиток довіри як стратегічного ресурсу цифрової безпеки. Доведено, що поряд із кримінально-правовими інструментами дедалі більшого значення набувають позакримінальні механізми реагування – санкційні, дипломатичні та публічно-атрибуційні, – які виконують функцію колективного стримування та превенції кіберагресії. Запропоновано методологічні орієнтири підвищення процесуальної стійкості атрибуції, що включають створення відтворюваних «кейс-файлів» з уніфікованими індикаторами компрометації (IoC/TTPs), застосування стандартизованих методик збору даних і документування ланцюга збереження доказів (chain of custody). Інституціоналізація публічно-приватного партнерства визначена як

ключовий інструмент подолання інформаційної асиметрії між державними структурами, цифровими провайдерами та громадянським суспільством, що уможливлює створення цілісної, стійкої та правово визначеної архітектури національної кібербезпеки.

8. Здійснено порівняльний аналіз стратегій кіберзахисту США, НАТО та Європейського Союзу та виокремлено їх нормативні, організаційні й технологічні моделі. Проведене дослідження дало змогу сформувати цілісне уявлення про євроатлантичні підходи до забезпечення кібербезпеки, які трансформувалися у складну багаторівневу систему правового, інституційного та технологічного врядування.

Європейська модель кіберзахисту визначена як нормативно зобов'язувальна екосистема, що ґрунтується на узгодженому пакеті актів – NIS2, CER, DORA, CRA, DSA, Cyber Solidarity Act і Cybersecurity Act – у поєднанні з методичною, координаційною та аналітичною роллю ENISA. У структурі цієї моделі чітко простежуються нормативний (регуляторний), організаційний (координаційний) та технологічний (стандартизаційний) виміри. Сформований цикл «політика – виконання – контроль – реагування» забезпечує перехід від декларативних до дієвих механізмів регулювання. Приклади імплементації в державах-членах ЄС (Німеччині, Франції, Швеції, Естонії) підтверджують поєднання наднаціональної уніфікації стандартів із національною відповідальністю за практичну реалізацію.

Модель США має операційно орієнтований характер, що базується на балансі стратегічного планування, адміністративного регулювання та стандартизації у тісній взаємодії з приватним сектором. Її нормативний компонент формується виконавчими актами, секторальними директивами та вимогами CISA; організаційний – міжвідомчими платформами та механізмами співпраці; технологічний – стандартами NIST CSF 2.0 та кадровою рамкою NICE. Модель США демонструє високу адаптивність та ефективність поєднання правових, управлінських і технічних інструментів у сфері управління кіберризиками.

Політика НАТО репрезентує передусім організаційно-координаційну модель, яка інтегрує кіберсферу в оборонне планування та колективну безпекову політику Альянсу. Зміст її інструментарію охоплює розвиток сумісності, партнерства, колективної готовності та взаємодопомоги. Через діяльність Кооперативного центру кібероборони (CCDCOE) реалізуються аналітичні, навчальні та методичні функції, здійснюється розроблення стандартів та забезпечується узгодженість дій у межах колективної кібероборони. НАТО створює «рамкову синергію» між державами-членами, не підмінюючи їхніх національних механізмів, але встановлюючи основу для колективного реагування у цифровому середовищі.

9. Досліджено механізми інтеграції України до міжнародної системи кібербезпеки, зокрема у форматах ЄС, НАТО та Ради Європи, та визначено шляхи гармонізації національного законодавства. Встановлено, що інтеграція України розвивається у напрямі поступового наближення до європейських і євроатлантичних стандартів, що включає адаптацію нормативної бази, інституційну сумісність і участь у міжнародних платформах кіберспівпраці. Показано, що гармонізація нормативно-правової бази з актами Європейського Союзу (NIS2, CER, DORA, CRA, Cybersecurity Act) поєднується з посиленням інституційного потенціалу держави через діяльність РНБО, Національного координаційного центру кібербезпеки, ДССЗЗІ та CERT-UA. Участь України у кібердіалозі Україна–ЄС, співпраця з ENISA, долучення до ініціатив Tallinn Mechanism і підготовка до приєднання до EU Cybersecurity Reserve посилюють інституційну сумісність та довіру міжнародних партнерів. У межах євроатлантичного напряму інтеграції визначено значення співпраці з НАТО – насамперед через участь у програмах, навчаннях і аналітичних проєктах Кооперативного центру кібероборони (CCDCOE) та залучення до механізмів колективної готовності та обміну інформацією. Водночас встановлено, що зберігаються виклики, пов’язані з необхідністю завершення делімітації повноважень між органами влади, розвитку кадрового потенціалу, формалізації державно-приватного

партнерства та розбудови національної системи кризового реагування, інтегрованої з європейськими й євроатлантичними механізмами.

10. Обґрунтовано можливості застосування євроатлантичних практик державно-приватного партнерства як інструмента підвищення кіберстійкості України та сформульовано пропозиції щодо вдосконалення правових засад і процедур такої взаємодії. Встановлено, що ключовим напрямом подальшого зближення з євроатлантичним простором є розвиток державно-приватної взаємодії у сфері кібербезпеки як основи колективної стійкості. Порівняльний аналіз показав, що євроатлантична практика ДПВ/ДПП функціонує як нормативно визначена система спільної відповідальності держави, операторів критичної інфраструктури, постачальників цифрових послуг і технологічних компаній. Модель США та європейська поступово еволюціонували до концепції «collaborative cyber defence», у межах якої партнерство перетворилося з факультативної практики на постійний операційний інструмент забезпечення кіберстійкості. Досвід Німеччини, Великої Британії та Естонії підтверджує, що ефективність таких форматів забезпечується не лише наявністю правових гарантій, а й технологічними засобами довіри: взаємною автентифікацією, аудитом транзакцій, мінімізацією даних і відкритими стандартами взаємодії. На основі дослідження сформовано систему рекомендацій щодо адаптації євроатлантичних підходів до української правової системи, яка охоплює чотири взаємопов’язані напрями:

а) кодифікаційний – доопрацювання та прийняття спеціального закону «Про державно-приватну взаємодію у сфері кібербезпеки» (законопроєкт № 14150), визначення правового статусу, повноважень та відповідальності учасників, створення єдиного національного координатора (Single Point of Contact), ведення реєстру проєктів та типізації форматів співпраці;

б) гармонізаційний – узгодження національного законодавства з правом ЄС відповідно до актів NIS2, CER, DORA, CRA, зокрема у сфері інцидент-репортингу, захисту даних і формування спільних команд реагування;

в) інституційний – створення мережі секторальних ISAC-платформ, консультативних органів і механізмів незалежного моніторингу, що забезпечують прозорість, підзвітність і сталість партнерських форматів;

г) концептуально-принциповий – імплементація засад «shared responsibility» і «security by design» у систему державного управління кіберризиками, що визначає сталий розподіл ролей і відповідальності між суб’єктами.

Узагальнюючи, застосування євроатлантичних практик державно-приватного партнерства створює для України реалістичний і стратегічно вивірений шлях до побудови стійкої, прогнозованої та інтегрованої системи кіберзахисту. Реалізація запропонованих рекомендацій забезпечить практичне зближення з євроатлантичним безпековим простором і посилить здатність держави протистояти сучасним і майбутнім кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акульшина В. Кібербезпека Фінляндії: правовий та інституційний механізми. Медіафорум: аналітика, прогнози, інформаційний менеджмент: збірка наукових праць. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 158–165. URL: http://www.library.univ.kiev.ua/ukr/elcat/new/detail.php3?doc_id=1826345

2. Алексеєва О. А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Інформація і право*, 2023. №4(47). С. 168–176. https://doi.org/10.37750/2616-6798.2023.4(47).291633

3. Арсенович Л. А. Понятійно-категоріальний апарат у сфері підготовки фахівців із кібербезпеки органів державної влади України. *Наукові перспективи*, 2022. № 2. С. 33–53. DOI: https://doi.org/10.52058/2708-7530-2022-2(20)-33-53

4. Бакалінська О. О. Правове забезпечення кіберзахисту в Україні. *Підприємництво, господарство і право*, 2019. № 9. С. 100-108. URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf

5. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*, 2014. № 2(42). С. 54–62. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf

6. Бурячок В. Л., Гнатюк С. О., Корченко О. Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф. (5 квітня 2013 р., м. Київ). Київ : Наук.-вид. центр НА СБ України, 2013. С. 416.

7. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. … канд. юрид. наук : 12.00.07. Університет сучасних знань, 2018. 221 с. URL: http://essuir.sumdu.edu.ua/handle/123456789/70638

8. Вдовенко С., Живило Є., Черноног О., Докіль В. Аналіз особливостей функціонування системи кібероборони. Нормативно-правові

аспекти. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2022. Вип. 74. С. 52–72. https://doi.org/10.17721/2519-481X/2022/74-06

9. Великий тлумачний словник сучасної української мови : 250000. Уклад. та голов. ред. В. Т. Бусел. Київ; Ірпінь: Перун, 2005. VIII, 1728 с.

10. Веселова Л. Понятійно-термінологічний апарат у системі адміністративно-правового забезпечення кібербезпеки. *Scientific Journal of Public and Private Law,* 2019. № 5(1). С. 138–143. DOI:10.32844/2618-1258.2019.5-1.24

11. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*, 2020. № 2. С. 200–203.

12. Гнатченко Д. Д., Гнатченко Т. О., Кальбенко А. С. Державне регулювання у сфері захисту кіберпростору як компонент забезпечення інформаційної безпеки України. Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. Київ : Київ. нац. торг.-екон. ун-т, 2020. – С. 48–50

13. Гнатюк С. Л. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні : аналітична записка. Київ: Національний інститут стратегічних досліджень, 2017. URL: https://niss.gov.ua/sites/default/files/2017-12/kiberbezpek-d3e61.pdf

14. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «кібербезпека» в системі національної безпеки: теоретико-правовий аспект. *Journal of the Academy of Legal Sciences of Uzhhorod University,* 2024. № 5. С. 112–120. DOI: https://doi.org/10.24144/2788-6018.2024.05.73

15. Горліченко С. Особливості сучасного понятійно-термінологічного апарату у сфері підготовки фахівців з кібербезпеки. *Кібербезпека: освіта, наука, техніка,* 2024. № 3(23). С. 171–181. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/547

16. Григоренко В. А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки. *Державне управління: удосконалення та розвиток*, 2021. № 2 (37). URL: https://doi.org/10.37750/2616-6798.2021.2(37).238405

17. Гульванська Ю. А. Правове регулювання кібербезпеки в Україні: сучасний стан та перспективи розвитку. *Інформація і право*, 2024. № 2(49). С. 45–52.

18. Гуцалюк М., Клименко О. Щодо посилення міжнародного співробітництва у сфері забезпечення кібербезпеки. *Становлення та розвиток правової держави: проблеми теорії та практики*, 2023. DOI: https://doi.org/10.36059/978-966-397-359-3-48.

19. Даник Ю. Г. Основи кібербезпеки та кібероборони : підручник. Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – 2-ге вид., перероб. та доп. Одеса : ОНАЗ ім. О. С. Попова, 2019. 320 с.

20. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис,* 2015. № 2. С. 144–147.

21. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналітична доповідь. За заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с. URL: https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf

22. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23 грудня 2020 р. № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF

23. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

24. Деякі питання об’єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

25. Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв’язку: Постанова Кабінету Міністрів України від 14.05.2015 р. № 303. URL: https://zakon.rada.gov.ua/laws/show/303-2015-%D0%BF#Text

26. Дзюндзюк В. Б., Котух Є. В. Кібербезпека як один з пріоритетів національної політики. *Державне будівництво*, 2020. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2020_2_4

27. Дідич О. Р., Наумко О. М. Державно-приватне партнерство у забезпеченні національної безпеки в умовах повномасштабного вторгнення. *Публічне адміністрування та національна безпека*, 2023. № 2. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2023/2_2023/20.pdf

28. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*, 2017. №10. С. 110–116.

29. Діордіца І. В. Адміністративно-правове регулювання кібербезпеки України : дис. … д-ра юрид. наук: 12.00.07. Запоріжжя : Запорізький нац. ун-т, 2018. 519 с.

30. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення : монографія. Херсон: Видавничим дім «Гельветика», 2017. 548 с.

31. Діордіца І. Поняття та зміст національної системи. *Национальный юридический журнал: теория и практика*, 2016. Вип. 6(1). С. 37-42.

32. Довгань О. Д., Тарасюк А. В. Національні інтереси України в кібернетичній сфері. *Інформація і право*, 2021. № 1(36). С. 134–142. DOI: 10.37750/2616-6798.2021.1(36).238194.

33. Довгань О. Д., Тарасюк А. В. Протидія загрозам кібербезпеці держави на глобальному рівні. *Інформація і право*, 2020. № 2(33). С. 85–98. DOI: 10.37750/2616-6798.2020.2(33).208100

34. Європейський інформаційно-дослідницький центр. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. Київ : Верховна Рада України, 2021. URL: https://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf

35. Ємельянов В., Бондар Г. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Публічне управління та регіональний розвиток,* 2019. № 5. С. 493–523. DOI: https://doi.org/10.34132/pard2019.05.02

36. Жарикова А. Кількість кібератак у 2023 році зросла на 16 % – Держспецзв'язку. *Економічна правда*. 31.01.2024. URL: https://www.epravda.com.ua/news/2024/01/31/709355/

37. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. *Інформація і право*, 2021. № 4. С. 129–134. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_4_14

38. Заскока Ю. В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. *Наукові перспективи*, 2021. № 9 (21). URL: http://perspectives.pp.ua/index.php/np/article/view/467/470

39. Зінченко, О. І. Вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського регіону. *Politicus,* 2024. № 5. С. 154–158. DOI: https://doi.org/10.24195/2414-9616.2024-5.21.

40. Зінченко, О. І. Європейські регіональні засоби протидії кібертероризму. *Регіональні студії*, 2024. № 39. С. 94–100. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/73170

41. Зінченко, О. І. Протидія кібертероризму як загрозі сучасній нац. безпеці держав європейського регіону: дис. … канд. політ. наук (PhD). Харків : ХНУ ім. В. Н. Каразіна, 2023. 215 с. URL: https://karazin.ua/storage/static-content/source/documents/aspirantura/zakhysty/Zinchenko/Зінченко%20дисертація.pdf

42. Камчатний М. В. Нормативно-правове закріплення питань кібербезпеки у міжнародному праві. Актуальні проблеми сучасного

міжнародного права : зб. наук. ст. за матеріалами І Харк. міжнар.-прав. читань, присвяч. пам'яті проф. М. В. Яновського і В. С. Семенова, Харків, 27 листоп. 2015 р. : у 2 ч. Харків, 2015. Ч. 1. С. 320–323.

43. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави,* 2015. № 3. С. 75-83. URL: http://nbuv.gov.ua/UJRN/iblsd_2015_3_12.

44. Ковалів М., Скриньковський Р., Назар Ю. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Traektoriâ Nauki,* 2021. № 3(3). С. 65–73. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3731

45. Колесник О.О. Кібербезпека як елемент національної безпеки України в умовах війни. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі:* матеріали міжнародної науково-практичної конференції (Київ, 18–19 лют. 2025 р.). Київ: Науково-дослідний інститут публічного права, 2025. С. 71–73.

46. Колесник О.О. Міжнародні стандарти та українська практика кіберзахисту: уроки війни. *Правові новели*. 2025. № 25. С. 375–382. DOI: https://doi.org/10.32782/ln.2025.25.48

47. Колесник О.О. Нормативно-інституційні засади формування національної системи кібербезпеки України. *Право та державне управління*. 2025. № 1. С. 437–445. DOI: https://doi.org/10.32782/pdu.2025.1.61

48. Колесник О.О. Принципи міжнародного права в системі глобальної кібербезпеки. *Проблемні питання юридичної науки в контексті реформування правової системи України:* матеріали міжнародної науково-практичної конференції (Київ, 19–20 жовт. 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 121–123.

49. Колесник О.О. Сучасний стан і тенденції розвитку правового регулювання національної системи кібербезпеки України. *Актуальні питання науки і практики та шляхи їх вирішення:* матеріали другої

міжнародної науково-практичної конференції (Київ, 4–5 черв. 2025 р.). Київ: Науково-дослідний інститут публічного права, 2025. С. 140–143.

50. Колесник О.О. Теоретико-правові засади формування та еволюції поняття кібербезпеки. Юридичний науковий електронний журнал. 2024. № 7. С. 636–641. DOI: https://doi.org/10.32782/2524-0374/2024-7/154

51. Колесник О.О. Формування поняття «кібербезпека» в сучасній правовій науці: теоретичні орієнтири та методологічні виклики. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність:* матеріали міжнародної науково-практичної конференції (Київ, 4–5 черв. 2024 р.). Київ: Науково-дослідний інститут публічного права, 2024. С. 98–100.

52. Конституція України. Відомості Верховної Ради України, 1996, № 30, ст. 141 (із наступними змінами). URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

53. Костенко І. В., Левченко Д. С, Оксінь В. В. Публічне адміністрування в контексті сталого розвитку: інституційний вимір та стратегічні пріоритети. *Юридичний науковий електронний журнал*, 2025. № 2. С. 646-649.

54. Крет, О., Крет, Р., & Кундеус, О. Система кібербезпеки як складова національної безпеки держави. *Науково-теоретичний альманах Грані*, 2024. № 27(5). С. 92-99. https://doi.org/10.15421/172496

55. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. *Аспекти публічного управління*, 2018. № 6(10). С. 37–46. URL: https://aspects.org.ua/index.php/journal/article/download/435/430

56. Куркова К. М. Інформаційні технології в умовах воєнного стану в контексті оновлення парадигми публічного адміністрування у сфері забезпечення науково-технологічного розвитку в Україні. *Захист та дотримання прав громадян органами Національної поліції України в умовах воєнного стану : матеріали міжнародної науково-практичної конференції*

(Харків, 24 листопада 2023 р.). Харків : Харківський національний університет внутрішніх справ, 2023. С. 40–43. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/651af476-6417-46b4-8294-768958b5b070/content

57. Куркова К. М. Концептуальне розуміння національної безпеки у публічно-інформаційній сфері. *Наукові записки. Серія: Право*, 2025. Вип. 18. С. 343–347. DOI: https://doi.org/10.36550/2522-9230-2025-18-343-347.

58. Левченко Д. Парадигма ідеї глобального цифрового врядування як явища адміністративного права. *Адміністративне право і процес, 2*024. № 4. С. 5–13. DOI: https://doi.org/10.17721/2227-796X.2024.4.01

59. Лисеюк А. М., Свінцицька Т. В. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. *Право та інновації*. 2024. № 4(48). С. 32–34. DOI: https://doi.org/10.37772/2518-1718-2024-4(48)-4.

60. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. 2-ге вид., доп. і перероб. Київ : Текст, 2008. 400 с.

61. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*, 2017. № 5. С. 174–180. URL: http://pgpjournal.kiev.ua/archive/2017/5/40.pdf

62. Лук'янчикова В. Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки. *Гілея: науковий вісник,* 2013. № 72. С. 793–796.

63. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства*, 2025. №2. С. 164–171. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/2142

64. Марущак А. І. Стратегія кібербезпеки України: правові засади та механізми реалізації. *Вісник Національного університету «Львівська політехніка». Юридичні науки*, 2024. № 2(38). С. 112–119.

65. Мельник С. В. Концептуально-категоріальний апарат у системі професійної підготовки майбутніх фахівців з інформаційної та кібербезпеки. *Інформаційні технології і засоби навчання*, 2016. Т. 55, № 5. С. 187–197. DOI: https://doi.org/10.33407/itlt.v55i5.1497

66. Мельник С. В., Тихомиров О. О., Лєсков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. Збірник наукових праць Київського національного університету імені Тараса Шевченка. Київ : ВІКНУ, 2011. Вип. 30. С. 165–172.

67. Міністерство закордонних справ України. Антон Демокін: під час 4-го раунду кібердіалогу Україна та ЄС поглиблюють співпрацю у сфері кібербезпеки. Міністерство закордонних справ України. URL: https://mfa.gov.ua/en/news/anton-demohin-pid-chas-4-go-raundu-kiberdialogu-ukrayina-ta-yes-pogliblyuyut-spivpracyu-u-sferi-kiberbezpeki

68. Мінфін. Кібербезпека бізнесу під час війни. Мінфін, 2025. URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny

69. Науково-практичний коментар до Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29.12.2021 № 1426. Державна служба спеціального зв'язку та захисту інформації України від 11.02.2022 р. URL: https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya-pro-organizaciino-tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini-vid-29-grudnya-2021-r-1426

70. Національна система кібербезпеки функціонуватиме ефективніше. ДССЗЗІ України, 2023. URL: https://cip.gov.ua/ua/news/nacionalna-sistema-kiberbezpeki-funkcionuvatime-efektivnishe

71. Національний інститут стратегічних досліджень, Кіберскладник російсько-української війни: уроки та оцінки міжнародної спільноти, 28.06.2022. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/kiberskladnyk-rosiysko-ukrayinskoyi-viyny-uroky-ta-otsinky

72. Несрін Д., Радомська Л. А. Сучасний стан кібербезпеки в Україні. Вінницький національний технічний університет, 2021. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/37987/90562.pdf

73. Ніконенко У., Халіна О. Організаційно-правовий механізм забезпечення кібербезпеки соціально-економічних систем в умовах викликів сучасності. *Економічний простір*, 2024. № 190. С. 108–113. DOI: https://doi.org/10.32782/2224-6282/190-20

74. Оксінь В. Ю. Левченко Д. С., Костенко І. В Міжнародне співробітництво у сфері підприємницької діяльності з використанням альтернативних джерел енергії. Правові аспекти та перспективи розвитку. *Юридичний науковий електронний журнал,* 2025. №6. С. 293-301.

75. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : річний звіт за 2024 рік. Київ : ДССЗЗІ України, 2024. 24 с. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006

76. Павленко В. С. Сутність кібербезпеки у теорії інформаційного права. *Право та державне управління*, 2021. № 2(47). С. 28–33. DOI: https://doi.org/10.32840/pdu.2021.2.4

77. Панасюк Б. М. Державно-приватне партнерство як механізм забезпечення кіберстійкості держави. *Information Security of the Person, Society and the State*, 2025. № 1 (38). URL: https://journals.uran.ua/ispss/article/view/340013/328076

78. Панченко В. М. Співвідношення понять: інформаційна та кібернетична безпека. *Інформаційна безпека людини, суспільства, держави*, 2013. № 2(12). С. 20–23.

79. Пашорін В.І. Термінологічні та освітні аспекти кібербезпеки. Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр.

наук.-практ. конф. (Київ, 27 берез. 2019 р.). Київ : Київ. нац. торг.-екон. ун-т, 2019. 244 с. С. 28-30.

80. Петров С. Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право*, 2019. № 4 (31). С. 107–113. URL: https://jnas.nbuv.gov.ua/j-pdf/Infpr_2019_4_15.pdf

81. 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 р. № 4336-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4336-20

82. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: Проект Закону № 8087 від 29 вересня 2022 р. Верховна Рада України. 8 сесія IX скликання. – Включено до порядку денного Законом № 4586-IX від 03 вересня 2025 р. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40553

83. Про внесення змін до деяких законів України щодо удосконалення окремих питань діяльності Служби безпеки України та підвищення її ефективності у зв'язку з участю у відсічі і стримуванні збройної агресії проти України»: Закон України від 16.07.2025 р. №4542-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4542-20#Text

84. Про внесення змін до Концепції з IT-централізації у системі управління державними фінансами: Розпорядження Кабінету Міністрів України від 03.03.2020 р. № 215-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/215-2020-%D1%80#Text

85. Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам: Закон України від 15.03.2022 р. №2137-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text

86. Про внесення змін до Положення про інтегровану систему електронної ідентифікації та Положення про Міністерство цифрової трансформації України: Постанова Кабінету Міністрів України від 16.09.2020 р. № 827. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/827-2020-%D0%BF#Text

87. Про внесення зміни до Указу Президента України від 7 червня 2016 р. № 242/2016 «Про Національний координаційний центр кібербезпеки» : Указ Президента України від 24.07.2025 р. № 547/2025. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/547/2025.

88. Про державно-приватну взаємодію у сфері кібербезпеки. Пояснювальна записка до проєкту Закону України. 2025 р. Верховна Рада України. URL: https://itd.rada.gov.ua/994137d0-2158-4bac-a6cd-55fb5a439c8a

89. Про Державну службу спеціального зв'язку та захисту інформації України»: Закон України від 23.02.2006 р. № 3475-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

90. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-xii#Text

91. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

92. Про електронні довірчі послуги: Закон України від 05.11.2017 р. № 2155-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2155-19

93. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/851-iv#Text

94. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1089-20

95. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: постанова Кабінету Міністрів України від 19.06.2019 р. № 518. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

96. Про затвердження плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Постанова Кабінету Міністрів України від 25.11.2017 р. № 1106. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text

97. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 07.03.2025 р. № 204-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/204-2025-%D1%80

98. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

99. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах: Постанова Кабінету Міністрів України від 16.11.2002 р. № 1772. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF

100. Про затвердження Порядку надання послуг конфіденційного зв’язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям: Постанова Кабінету Міністрів України від 11.10.2002 р. № 1519. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1519-2002-%D0%BF

101. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних

ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.2020 р. № 1176. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

102. Про затвердження Технічного регламенту засобів криптографічного захисту інформації: Постанова Кабінету Міністрів України від 21.10.2020 р. № 991. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/991-2020-%D0%BF#Text

103. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

104. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-vi#Text

105. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-xii#Text

106. Про критичну інфраструктуру: Закон України від 16.11.2021 р. №1882-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

107. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-viii#Text

108. Про національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text

109. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2135-xii#Text

110. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 р. № 3341-XII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3341-%D1%85ii#Text

111. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

112. Про Положення про Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України: Указ Президента України від 07.06.2016 р. № 242/2016. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

113. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента від 22.05.1998 р. № 505/98. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text

114. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text

115. Про прийняття за основу проекту Закону України про Кіберсили Збройних Сил України: Постанова Верховної Ради України від 09.10.2025 р. № 4628-IX. Верховна Рада України. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/56055

116. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7.09.2005 р. № 2824-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575

117. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”: Указ Президента України від 26.09.2021 р. № 447/2021. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/n0055525-21#Text

118. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”: Указ Президента від

15.03.2016 р. № 96. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

119. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”: Указ Президента від 14.09.2020 р. №392/2020. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

120. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: Указ Президента України від 13.02.2017 р. № 32/2017. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/32/2017#Text

121. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 01.02.2022 р. № 37/2022. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/37/2022#n5.

122. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14.03.2016 р. № 92/2016. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/92/2016.

123. Про рішення Ради національної безпеки і оборони України від 4 жовтня 2025 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 04.10.2025 р. № 749/2025. Верховна Рада України. URL: https://www.president.gov.ua/documents/7492025-56749

124. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2229-xii#Text

125. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р.

Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

126. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України № 1009 від 06.12.2017 р. № 1009. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

127. Про схвалення Стратегії боротьби з організованою злочинністю: Розпорядження Кабінету Міністрів України від 16.09.2020 р. № 1126-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-%D1%80#Text

128. Про схвалення Стратегії розвитку сфери електронних комунікацій України на період до 2030 року та затвердження операційного плану заходів на 2025–2027 роки: Розпорядження Кабінету Міністрів України від 04.06.2025 р. № 546-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/546-2025-%D1%80

129. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1280-iv#Text

130. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text

131. Проект Закону про Кіберсили Збройних Сил України: законопроєкт 4586-IX від 03.09.2025 р. Верховна Рада України. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/45453

132. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. Європейська Бізнес-Асоціація, 2024. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam

133. Романова О. М. Кібербезпека під час повномасштабного вторгнення РФ. *Часопис Київського університету права*, 2024. № 2. С. 56–59. DOI: https://doi.org/10.36695/2219-5521.2.2024.9.

134. Саєнко, М. І.; Савела, Є. А.; Тополянський, Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія: Право*, 2021. Вип. 64. С. 386–391. DOI: https://doi.org/10.24144/2307-3322.2021.64.71

135. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник НУ «Львівська політехніка». Серія: Юридичні науки*, 2024. № 1(41). С. 314–320. DOI: https://doi.org/10.23939/law2024.41.314.

136. Скибун О. Ж. Кібербезпека систем електронних комунікацій органів державної влади України. *Вісник НАДУ при Президентові України. Серія: Державне управління*, 2021. № 1. С. 30–39. URL: http://nbuv.gov.ua/UJRN/vnaddy_2021_1_6

137. Скрипник Л. В. Щодо кібербезпеки. *СТСЗИ*, 2013. Вип. 2(24). С. 126–130.

138. Сливка, М. М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний науковий електронний журнал*, 2022. № 10. С. 489–491. DOI: https://doi.org/10.32782/2524-0374/2022-10/121

139. Сліпченко, Т. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. Актуальні проблеми правознавства, 2020. 1(1). С. 128–133. DOI: https://doi.org/10.35774/app2020.01.128.

140. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник. Повітряне і космічне право*, 2021. № 2 (59). С. 110–115. DOI: https://doi.org/10.18372/2307-9061.59.15603.

141. Сорока Л. В., Куркова К. М., Боровик А. В. Особливості адміністративно-правового механізму взаємодії суб'єктів забезпечення економічної безпеки України щодо протидії викликам цифрового середовища. *Юридичний науковий електронний журнал*, 2024. № 11. С. 569–573. DOI: https://doi.org/10.32782/2524-0374/2024-11/134.

142. Сорока Л. В., Колесник О. О. Міжнародно-правові принципи регулювання кіберпростору: суверенітет, невтручання та Due Diligence. *Держава та регіони. Серія: Право*, 2025. № 1. С. 166-170.

143. Стець В. Теоретико-правові проблеми визначення кібербезпеки. *Український журнал прикладних наук URAN*, 2019. Том 4 № 80. С. 24–28. DOI: https://doi.org/10.35432/1993-8330appa4802019194098

144. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі. *Урядовий портал*, 2023. URL: https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-tamizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori

145. Тарасюк А. В. Досвід забезпечення кібербезпеки у зарубіжних країнах. *Науковий вісник публічного та приватного права*, 2019. № 4. С. 204–209. URL: http://www.nvppp.in.ua/vip/2019/4/tom_2/41.pdf

146. Тарасюк А. В. Забезпечення кібернетичної безпеки людини: міжнародно-правовий аспект. *Юридичний вісник*, 2020. № 3. С. 254–261.

147. Тарасюк А. В. Понятійно-категоріальний синтез правового забезпечення кібербезпеки України. *Порівняльно-аналітичне право*, 2019. №5. С. 296-298. URL : http://www.pap.in.ua/5_2019/77.pdf

148. Тарасюк А. В. Правовий чинник у попередженні кіберзагроз на міжнародному та національному рівнях. *Вісник Запорізького національного університету. Юридичні науки*, 2020. № 4. Т. 1. С. 168–173.

149. Тарасюк А. В. Пріоритети забезпечення кібербезпеки: досвід окремих країн. *Інтернаука : міжнар. наук. журн. Серія «Юридичні науки»*, 2020. №4. С. 42–49. URL : https://doi.org/10.25313/2520-2308-2020-4-5818.

150. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*, 2020. № 2. С. 119–124. DOI: https://doi.org/10.32838/2707-0581/2020.2-2/23.

151. Тарасюк А. В. Системний підхід у дослідженні правових основ кібербезпеки. *Прикарпатський юридичний вісник*, 2020. № 2. С. 108–111.

152. Тіщенко В. О., Логвиненко Є. С. Правові засади забезпечення кібербезпеки в умовах воєнного стану. Протидія кіберзлочинності та торгівлі людьми. Харків, 2023. С. 71–74.

153. Федченко Д. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *Юридичні Науки*, 2018. № 5(57). С. 653–658. URL: https://molodyivchenyi.ua/index.php/journal/article/view/4603

154. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*, 2012. № 2. С. 162-169.

155. Шестак, Я. І. Кібергігієна у інформаційному просторі в умовах воєнного стану. Інформаційна безпека та комп'ютерні технології: тези V Міжнародної науково-практичної конференції (Кропивницький, 2022). Кропивницький: Центральноукраїнський національний технічний університет, 2022. С. 5–6.

156. Яковлєв П. О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції). *The Journal of V. N. Karazin Kharkiv National University. Series "Law"*, 2020. Вип. 30. С. 106–113. DOI: https://doi.org/10.26565/2075-1834-2020-30-13.

157. Agence nationale de la sécurité des systèmes d'information (ANSSI). *Plan stratégique 2025–2027 de l'ANSSI*. Paris: ANSSI, 2024. URL: https://cyber.gouv.fr/sites/default/files/document/Plan-strat%C3%A9gique-2025-2027-de-lANSSI.pdf

158. Aloul, F. The Need for Effective Information Security Awareness. *International Journal of Intelligent Computing Research (IJICR)*, 2011. Vol. 2, No. 1. P. 116–123. DOI: https://doi.org/10.20533/ijicr.2042.4655.2011.0014

159. Amoroso, E. Cyber Security. New Jersey : Silicon Press, 2006. 420 p. URL: https://dumitrudumbrava.wordpress.com/wp-content/uploads/2012/01/cyber-security.pdf

160. Anagnostakis, D. The European Union–United States cybersecurity relationship: a transatlantic functional cooperation. *Journal of Cyber Policy*, 2021. Vol. 6, No. 2. P. 243–261. DOI: https://doi.org/10.1080/23738871.2021.1916975

161. Balarabe K. Digital Borders and Beyond: Establishing Normative Grounds for Cybersecurity and Sovereignty in International Law. *Computer Law & Security Review*, 2025. Vol. 55.Art. 106180. URL: https://www.sciencedirect.com/science/article/abs/pii/S2212473X25000537

162. Bellanova, R.; Carrapico, H.; Duez, D. Digital/sovereignty and European security integration: an introduction. *European Security*, 2022. Vol. 31, No. 3. P. 337–351. DOI: https://doi.org/10.1080/09662839.2022.2101887

163. Bing, C.; Satter, R. Ukrainian Telecom Company's Internet Service Disrupted by "Powerful" Cyberattack. *Reuters*, 2022. URL: https://www.reuters.com/business/media-telecom/ukrainian-telecom-companys-internet-service-disrupted-by-powerful-cyberattack-2022-03-28

164. Bischoff, P. Cybersecurity Rankings by Country: Which Countries Have the Worst (and Best) Cybersecurity? London: Comparitech, 2024. URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

165. Broeders, D.; Cristiano, F. Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road, 2020. URL: http://dx.doi.org/10.2139/ssrn.3819171

166. Brumfield C. Russia-linked cyber-attacks on Ukraine: A timeline. CSO Online, 2022. URL: https://www.csoonline.com/article/571865/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html

167. BSI. Nationales Cyber-Abwehrzentrum (Cyber-AZ). Bonn : BSI, 2024. URL: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum.html

168. BSI. UP KRITIS: Public-Private Partnership for Critical Infrastructure Protection. Bonn: BSI, 2024. URL:

https://www.bsi.bund.de/EN/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html

169. Buchan R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions. *Journal of Conflict & Security Law*, 2012. Vol. 17, No. 2. P. 211–227. DOI: 10.1093/jcsl/krs017.

170. Bundesamt für Sicherheit in der Informationstechnik (BSI). Allianz für Cyber-Sicherheit. Bonn: BSI, 2024. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Allianz-fuer-Cyber-Sicherheit/allianz-fuer-cyber-sicherheit_node.html

171. Bundesamt für Sicherheit in der Informationstechnik (BSI). Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG). Bonn: BSI, 2021. URL: https://www.gesetze-im-internet.de/bsig_2009/

172. Burgess, M. Mysterious Satellite Hack Has Victims Far Beyond Ukraine. *Wired*. 23 March 2022. URL: https://www.wired.com/story/viasat-internet-hack-ukraine-russia/

173. Bygrave L. A. The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes. *Computer Law & Security Review*, 2025. Vol. 56. Art. 106071. URL: https://www.sciencedirect.com/science/article/pii/S0267364924001377

174. Campus Cyber. About the Campus. Paris : Campus Cyber. Gouvernement français, 2024. URL: https://campuscyber.fr/en

175. Canada. *Statement on International Law Applicable in Cyberspace* (22.04.2022). Ottawa: Global Affairs Canada, 2022. URL: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

176. Canongia, C., Mandarino, R. Cybersecurity: The New Challenge of the Information Society. In: Crisis Management: Concepts, Methodologies, Tools and

Applications. Hershey, PA: IGI Global, 2014. P. 60–80. DOI: http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

177. Cattler, D., Black, D. The Myth of the Missing Cyberwar: Russia's Hacking Succeeded in Ukraine –And Poses a Threat Elsewhere, Too. Foreign Affairs, 2022. URL: https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar

178. CCDCOE. *Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States*. Tallinn, 2025. URL: https://ccdcoe.org/uploads/2025/05/Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf

179. CCDCOE. The Tallinn Manual – Project page (incl. 3.0 update), 2021–2025 Tallinn: NATO CCDCOE. URL: https://ccdcoe.org/research/tallinn-manual/

180. Cerulus, L. Kyiv's Hackers Seize Their Wartime Moment. *Politico*. 10.03.2022. URL: https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group

181. Christou, G. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy.* Basingstoke : Palgrave Macmillan, 2016. 268 c. URL: https://link.springer.com/book/10.1057/9781137400529

182. CISA; FBI; NSA. *Cybersecurity Advisory: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (AA22-011A)*, 2022. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

183. CISA; National Security Agency (NSA). *Control System Defense: Know the Opponent (Joint Cybersecurity Advisory AA22-265A)*, 2022. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-265a

184. Clough, J. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*, 2014. Vol. 40, No. 3. P. 698–736. URL: https://ssrn.com/abstract=2615789

185. Conger, K., Satariano, A. Volunteer Hackers Converge on Ukraine Conflict with No One in Charge. *The New York Times*, 04.03.2022. URL: https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html

186. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. *Official Journal of the European Union*. L 129 I, 17.05.2019. P. 13–19. URL: https://eur-lex.europa.eu/eli/dec/2019/797/oj/eng

187. Council of Europe. Convention on Cybercrime (Budapest Convention, ETS No. 185). Budapest: Council of Europe, 2001. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

188. Council of Europe. *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*. Strasbourg: CoE, 2001. URL: https://rm.coe.int/16800cce5b

189. Council of Europe. *Second Additional Protocol to the Convention on Cybercrime (CETS No. 224)*. Strasbourg : CoE, 2022–2024. URL: https://rm.coe.int/1680a49dab

190. Council of the European Union. Russian Cyber Operations Against Ukraine: Declaration by the High Representative on Behalf of the European Union, 2022. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

191. Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union. L 129 I, 17.05.2019. P. 1–12. URL: https://eur-lex.europa.eu/eli/reg/2019/796/oj/eng

192. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining Cybersecurity. *Technology Innovation Management Review*, 2014. Vol. 4, No. 10. P. 13–21. DOI: http://doi.org/10.22215/timreview/835

193. Cyber Security Cluster Bonn e.V. About us Bonn: Cyber Security Cluster Bonn, 2024. URL: https://www.cyber-security-cluster.eu

194. Cyber security management model for critical infrastructure protection. In: Contemporary Issues in Business, Management and Education: International Scientific Conference, Vilnius, Lithuania, 13–14 May 2021. Vilnius : Vilnius Gediminas Technical University, 2021. DOI: https://doi.org/10.3846/cibmee.2021.611

195. CyberPeace Institute. Ukraine: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects, 2023. URL: https://cyberconflicts.cyberpeaceinstitute.org

196. CyberScoop. Viasat Hack: Russia Behind Cyberattack on Ukraine, Say US, UK and EU, 2022. URL: https://www.cyberscoop.com/viasat-hack-russia-uk-eu-us-ukraine/

197. Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security, 2012. Ottawa–Washington: Public Safety Canada; DHS, 2012. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx

198. Cybersecurity and Infrastructure Security Agency (CISA). Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, 2022. URL: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

199. Cybersecurity and Infrastructure Security Agency (CISA). APT Cyber Tools Targeting ICS/SCADA Devices (Alert Code AA22-103A). Washington, D.C.: CISA, 25 May 2022. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a

200. Cybersecurity and Infrastructure Security Agency (CISA). Improving the Nation's Cybersecurity. Washington, D.C.: U.S. Department of Homeland Security, 2024 URL: https://www.cisa.gov/jcdc

201. Cybersecurity and Infrastructure Security Agency (CISA). Information sharing (ISACs/ISAOs, AIS). Washington, D.C.: U.S. Department of

Homeland Security, 2024. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing

202. Cybersecurity and Infrastructure Security Agency (CISA). Joint Cyber Defense Collaborative: Unifying Cyber Defense Planning and Operations. Washington, D.C.: CISA, August 2021. URL: https://nsarchive.gwu.edu/sites/default/files/documents/qytieo-agiyf/04.pdf

203. Cybersecurity and Infrastructure Security Agency (CISA). *Shields Up: Guidance for Organizations*, 2022. URL: https://www.cisa.gov/shields-guidance-organizations

204. Cybersecurity Information Sharing Act of 2015. *Public Law*, 2015. No. 114-113, div. N, § 104, 129 Stat. 2242. URL: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf

205. Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Inf. Comput. Secur*., 27, 373-392. DOI:10.1108/ICS-10-2018-0122

206. Digital Security in Wartime: Ukrainian Experience and International Best Practices. Ed. by M. Thompson, O. Kovalenko. Kyiv: Digital Ukraine Institute, 2024. 289 p.

207. 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 (NIS 2 Directive). *Official Journal of the European Union*. L 333, 27 Dec. 2022. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

208. Doorstep statement by NATO Secretary General Jens Stoltenberg at the start of the extraordinary Summit of NATO Heads of State and Government. 24 Mar. 2022. URL: https://www.nato.int/cps/en/natohq/opinions_193611.htm

209. Dutch Security Delta (HSD). About HSD. The Hague: Dutch Security Delta, 2024. URL: https://securitydelta.nl

210. Eesti CyberTech klaster – Estonian CyberTech Cluster. URL: https://itl.ee/cybertech

211. Egloff F. J., Public attribution of cyber intrusions. *Journal of Cybersecurity*, 2020. Volume 6, Issue 1. https://doi.org/10.1093/cybsec/tyaa012

212. Eichensehr K. E. Ukraine, Cyberattacks, and the Lessons for International Law. *AJIL Unbound*, 2022, Vol. 116, pp. 145–149. DOI: 10.1017/aju.2022.20

213. Eichensehr, K. E. Public-Private Cybersecurity. *Texas Law Review*, 2017. Vol. 95. P. 467–499. URL: https://texaslawreview.org/public-private-cybersecurity

214. Eichensehr, K. SolarWinds: Accountability, Attribution, and Advancing the Ball. *Just Security*, 16.04.2021. URL: https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball

215. ENISA Threat Landscape 2023. Luxembourg: Publications Office of the European Union, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

216. ENISA. Reference Incident Classification Taxonomy, 2018. URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

217. ENISA. Threat Landscape 2024–2025. URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

218. ESET Research. CaddyWiper: New wiper malware discovered in Ukraine. WeLiveSecurity, 2022 p. URL: https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

219. ESET Threat Report T1 2022. – Bratislava: ESET, 2022. URL: https://web-assets.eset.com/fileadmin/ESET/INT/B2B_Resource_centrum/Reports/T1-2022_Threat-Report.pdf

220. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. The EU's Cybersecurity Strategy for the Digital Decade. Brussels: European Commission, 2020. 22 c. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

221. European Commission. European Governance – A White Paper. Brussels: Commission of the European Communities, 25 July 2001. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0428

222. European Parliamentary Research Service (EPRS). Russia's war on Ukraine: Timeline of cyber-attacks. Authors: Jakub Przetacznik, Simona Tarpova. Brussels : European Parliament, Members' Research Service, 2022. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/icri_BRI(2022)733549_EN.pdf

223. European Union Agency for Cybersecurity (ENISA). Best Practices for Cyber Crisis Management Heraklion: ENISA, 2021. URL: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

224. European Union Agency for Cybersecurity (ENISA). National Cybersecurity Strategies – Practical Guide v2.0. Heraklion : ENISA, 2023. URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/national-cybersecurity

225. European Union Agency for Cybersecurity (ENISA). NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies. Heraklion: ENISA, 2016. URL: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

226. European Union Agency for Cybersecurity (ENISA). Public-Private Partnerships in Cyber Security – Recommendations and Best Practices. Heraklion: ENISA, 2024. URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/public-private

227. European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (The European Union

Agency for Cybersecurity) 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, 7 June 2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

228. European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*. L 277, 27 Oct 2022. P. 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

229. European Union. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (DORA). *Official Journal of the European Union*. L 333, 27 December 2022. P. 1–79. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

230. European Union. 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 (Cyber Resilience Act). *Official Journal of the European Union.* L 2847, 20 Nov 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

231. European Union. Regulation (EU) 2025/38 of 19 December 2024 on a framework for cyber solidarity in the Union (Cyber Solidarity Act). *Official Journal of the European Union*. L 15/1, 2025. URL: https://eur-lex.europa.eu/eli/reg/2025/38/oj

232. Finnemore M.; Hollis D. B. Constructing Norms for Global Cybersecurity. *The American Journal of International Law,* Vol. 110, No. 3 (July 2016), pp. 425-479. Published by: American Society of International Law Stable URL: http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425

233. Finnemore, Martha and Hollis, Duncan B., Beyond Naming and Shaming: Accusations and International Law in Cybersecurity (March 6, 2019).

European Journal of International Law, Temple University Legal Studies Research Paper, 2019. No.14. URL: http://dx.doi.org/10.2139/ssrn.3347958

234. Floridi, L. The Ethics of Information. Oxford: Oxford University Press, 2013. URL: https://doi.org/10.1093/acprof:oso/9780199641321.001.0001

235. Freedom House. Freedom on the Net 2024: The Struggle for Trust Online. Washington, D.C.: Freedom House, 2024. URL: https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

236. Gatlan, S. New CaddyWiper Data-Wiping Malware Hits Ukrainian Networks. *BleepingComputer*. 2022. URL: https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks

237. Germany. Federal Ministry of the Interior and Community. Cyber Security Strategy for Germany 2021. Berlin: BMI, 2021. URL: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile

238. Germany. On the Application of International Law in Cyberspace (Position Paper), 2021. Berlin: Federal Foreign Office. URL: https://documents.unoda.org/wp-content/uploads/2021/12/Germany-Position-Paper-On-the-Application-of-International-Law-in-Cyberspace.pdf

239. Government of Canada. Public Safety Canada. National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. Ottawa: Public Safety Canada, 2018. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybr-scrt-strtgy/index-en.aspx

240. Government of France. International Law Applied to Operations in Cyberspace. Paris : Ministry for the Armed Forces, 2019. 18 p. URL: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf ;

241. Government of the Netherlands – National Cyber Security Centre (NCSC). URL: https://english.ncsc.nl

242. Government of the Netherlands. Letter to the Parliament on the International Legal Order in Cyberspace; Appendix: International Law in Cyberspace. The Hague : Ministry of Foreign Affairs, 5 July 2019. URL: https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Appendix_+International+Law+in+Cyberspace+(Statement+by+the+Netherlands).pdf

243. Greenberg, A. Russia's Sandworm Hackers Attempted Third Blackout in Ukraine. Wired. 12 Apr. 2022. URL: https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/

244. Greenberg, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. 22 Aug. 2018. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

245. Grigsby A. The End of Cyber Norms. Survival, 2017. Vol. 59, No. 6. P. 109–122. DOI: 10.1080/00396338.2017.1399730

246. Hansen, L., Nissenbaum, H. Digital Disaster, Cyber Security, and The Copenhagen School. *International Studies Quarterly*, 2009. Vol. 53, No. 4. P. 1155–1175. DOI: https://doi.org/10.1111/j.1468-2478.2009.00572.x

247. Hathaway O. A., Crootof R., Levitz P., Proctor H., Nowlan A. E., Perdue W., Spiegel J. The Law of Cyber-Attack. *California Law Review*, 2012. Vol. 100, No. 4. P. 817–885. Yale Law & Economics Research Paper No. 453; Yale Law School Public Law Working Paper No. 258. URL: https://ssrn.com/abstract=2134932

248. Henrico, S., & Putter, D. Cyber What Systematic Review. *Journal of Applied Security Research*, 2025. 1–34. https://doi.org/10.1080/19361610.2025.2544184

249. Holland, S., Pearson, J. US, UK: Russia Responsible for Cyberattack Against Ukrainian Banks. *Reuters*. 18.02.2022. URL: https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18

250. Human Rights Council. The promotion, protection and enjoyment of human rights on the Internet: Resolution 20/8. Geneva : United Nations, 16.07.2012. A/HRC/RES/20/8. URL: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

251. Hurwitz R. The Play of States: Norms and Security in Cyberspace. *American Foreign Policy Interests*, 2014. Vol. 36, No. 5. P. 322–331. DOI: 10.1080/10803920.2014.972048.

252. IBM Security. Cost of a Data Breach Report 2023. URL: https://www.ibm.com/reports/data-breach

253. ICRC. International humanitarian law and cyber operations during armed conflicts (Position paper, Nov 2019). – Geneva: ICRC, 2019. URL: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

254. Information System Authority (RIA). Cyber Security in Estonia 2024. Tallinn: RIA, 2024. URL: https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf

255. International Committee of the Red Cross. Executive Summary: Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts. *International Review of the Red Cross*, 2022. Vol. 104, No. 919 (June 2022). – P. 1–9. URL: https://international-review.icrc.org/articles/executive-summary-avoiding-civilian-harm-from-military-cyber-operations-919

256. International Foundation for Electoral Systems (IFES). *Ukraine Cybersecurity Legal Framework: Overview and Analysis*. Kyiv : IFES Ukraine, 2021. 47 p. URL: https://ifesukraine.org/wp-content/uploads/2021/04/IFES-Ukraine-Cybersecurity-Legal-Framework-Overview-2020-v2-2021-04-01-Ukr.pdf

257. International Organization for Standardization (ISO); International Electrotechnical Commission (IEC). ISO/IEC 27032:2023 Information Security, Cybersecurity and Privacy Protection – Guidelines for Cybersecurity. Geneva: ISO, 2023. URL:

https://cdn.standards.iteh.ai/samples/76070/be57667fdd0b432490c253ca538c9938/ISO-IEC-27032-2023.pdf

258. International Telecommunication Union (ITU). Global Cybersecurity Index (GCI) 2020 : Measuring Commitment to Cybersecurity. Geneva : ITU, 2024. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

259. Italy, Ministry of Foreign Affairs and International Cooperation. Position Paper on the applicability of international law in cyberspace, 2021. URL: https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2022/02/CronachedalCyberspazio3_2021.pdf

260. ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). URL: http://www.itu.int/rec/T-REC-X.1205-200804-I/en

261. James Pearson and Christopher Bing. Reuters. Factbox: The Cyber War Between Ukraine and Russia, 2022. URL: https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/

262. James Pearson, Raphael Satter, Christopher Bing & Joel Schectman, Exclusive: U.S. Spy Agency Probes Sabotage of Satellite Internet During Russian Invasion, Sources Say, Reuters, 2022 URL: https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11

263. Janczewski R.; Pilarski G.; Marczyk M. Terminology as a barrier to NATO's interoperability in cyberspace operations. *Knowledge-Based Organization*, 2019. Vol. 25, No. 3. P. 31–35. URL: https://sciendo.com/article/10.2478/kbo-2019-0113

264. Japan. Basic Position of the Government of Japan on International Law Applicable to Cyber Operations (28.05.2021). Tokyo: MOFA. URL: https://www.mofa.go.jp/policy/page3e_001114.html

265. Kagubare, I. Intel chair ‘amazed’ Russia hasn’t launched full-scale cyberwarfare. *The Hill*, 2022. URL: https://thehill.com/policy/international/598138-intel-chair-amazed-russia-hasnt-launched-full-scale-cyberwarfare.

266. Kello, L. Cyber Legalism: Why It Fails and What to Do. *Journal of Cybersecurity*, 2021. Vol. 7, Issue 1. DOI: https://doi.org/10.1093/cybsec/tyab014

267. Kemmerer, R. A. Cybersecurity. *Proceedings of the 25th IEEE International Conference on Software Engineering*, 2003. P. 705–715. DOI: 10.1109/ICSE.2003.1201257.

268. Khoronovskyi, O., Orlean, A., Kostenko, I., Melnyk, O., Sokiran, M. Threats to critical infrastructure: A study of transnational organized crime in Ukraine. *Amazonia Investiga*, 2024. Vol. 13, No. 84. P. 118–130. DOI: https://doi.org/10.34069/AI/2024.84.12.7

269. Kosseff, J. Defining Cybersecurity Law. *Iowa Law Review*, 2018. Vol. 103, No. 3. P. 985–1035. URL: https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/ILR-103-3-Kosseff.pdf

270. Kosseff, J. Upgrading Cybersecurity Law. *Houston Law Review*, 2023. Vol. 61. P. 51–53.

271. Kostenko, I. The role of satellite communications in the Russo-Ukrainian war: Legal and ethical implications. In: Brodowski, L., Marcisz-Dynia, A. (eds.). *Stan aktualny i perspektywy rozwoju międzynarodowego prawa lotniczego, kosmicznego oraz nowych technologii*. Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego, 2025. P. 338–352. URL: https://wydawnictwo.ur.edu.pl/produkt/stan-aktualny-i-perspektywy-rozwoju-miedzynarodowego-prawa-lotniczego-kosmicznego-oraz-nowych-technologii

272. Kostenko, Inessa (2020) The Draft Law of Ukraine “On the Extraction and Utilization of Natural Resources of the Moon and Other Celestial Bodies.” *Advanced Space Law*, Volume 6, 29-42. https://doi.org/10.29202/asl/6/4

273. Kravchuk M., Kravchuk V., Hrubinko A., Podkovenko T., Ukhach V. Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security*. 2024. Vol. 2, No. 2. P. 28–38. https://doi.org/10.62566/lps/2.2024.28

274. Lerman, R., Zakrzewski, C. Elon Musk's Starlink Is Keeping Ukrainians Online When Traditional Internet Fails. *The Washington Post*, 19.03.2022. URL: https://www.washingtonpost.com/technology/2022/03/19/elon-musk-ukraine-starlink

275. Lewis, J. A. *Cybersecurity and Critical Infrastructure Protection*. – Washington, DC: Center for Strategic and International Studies, 2006 URL: https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection

276. Limba, T., Plėta, T., Agafonov, K., Damkus, M. Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, 2017. Vol. 4, No. 4. P. 559–573. DOI: https://doi.org/10.9770/jesi.2017.4.4(12).

277. Lonergan, E. D., Lonergan, S. W., Valeriano, B., Jensen, B. Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why. *The Washington Post*, 07.03.2022. URL: https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why

278. Mačák, K. From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers. *Leiden Journal of International Law*, 2017. Vol. 30, No. 4. P. 877–899. DOI: 10.1017/S0922156517000417.

279. Marks, J. 11 reasons we haven’t seen big Russian cyberattacks yet. *The Washington Post*, 03.03.2022. URL: https://www.washingtonpost.com/politics/2022/03/03/11-reasons-we-havent-seen-big-russian-cyberattacks-yet

280. Marks, J. Cybersecurity pros want to stop talking about a ‘cyber 9/11’. *The Washington Post*, 10.09.2021. URL:

https://www.washingtonpost.com/politics/2021/09/10/cybersecurity-pros-want-stop-talking-about-cyber-911/

281. Mekh, Y., Georgiievskyi, I., Ignatchenko, I., Krasnopolska, T., Kostenko, I. Public-private partnership in the security sector: Updating in the conditions of counteracting COVID-19 and armed aggression in eastern Ukraine. *Linguistics and Culture Review*, 2021. Vol. 5, Suppl. 4. P. 1653–1663. DOI: http://dx.doi.org/10.46925//rdluz.37.22

282. Microsoft. *Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine*, 27.04.2022. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

283. Miller, M. The World Holds Its Breath for Putin's Cyberwar. *Politico*, 2022. URL: https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440

284. Ministry of Economic Affairs and Communications (Republic of Estonia). *Estonia's Digital Agenda 2030 (Digiühiskonna arengukava 2030)*. Tallinn: MEAC, 2021. URL: https://www.mkm.ee/sites/default/files/documents/2022-04/Digi%C3%BChiskonna%20arengukava_ENG.pdf

285. Moret, E., Pawlak, P. *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?* Paris: EU Institute for Security Studies, 2017. 8 p. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf

286. National Cyber Security Centre (NCSC). Industry 100 Programme (i100). London: UK Government, 2023. URL: https://www.ncsc.gov.uk/section/industry-100/about

287. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Cyber Law Toolkit – Use of Force: Collection of State Positions*. Tallinn : CCDCOE, 2025. URL: https://cyberlaw.ccdcoe.org/wiki/Use_of_force_in_cyberspace

288. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *National Cybersecurity Strategies: Practical Guide to the Development and Execution*. Tallinn: CCDCOE, 2021. URL: https://ccdcoe.org/uploads/2022/02/2021-NCS-Guide.pdf

289. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *NotPetya*, 2017. URL: https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)

290. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Training and Exercises for Partner Nations*. Tallinn: CCDCOE, 2024. URL: https://ccdcoe.org/training

291. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Ukraine to be accepted as a Contributing Participant to NATO CCDCOE*, 16.03.2022. URL: https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/

292. NATO. *Cyber Defence (including the 2021 Comprehensive Cyber Defence Policy)*. Brussels: NATO, 30.07.2024. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm

293. NATO. *NATO Industry Cyber Partnership launched at the NATO Cyber Defence Conference*. Brussels: NATO, 17.09.2014. URL: https://www.nato.int/cps/en/natohq/news_113121.htm

294. NATO. *Statement by NATO Heads of State and Government*. Brussels : NATO, 24.03.2022. URL: https://www.nato.int/cps/en/natohq/official_texts_193719.htm

295. NATO. *Statement by the North Atlantic Council on Allied Support to Ukraine*. Brussels: NATO, 10.07.2024. URL: https://www.nato.int/en/what-we-do/partnerships-and-cooperation/natos-support-for-ukraine

296. NATO. *Summary of the NATO-Ukraine Innovation Cooperation Roadmap*. 05.08.2024. URL: https://www.nato.int/cps/en/natohq/official_texts_228255.htm

297. New Zealand. Ministry of Foreign Affairs and Trade; Crown Law Office. *Updated position statement: The Application of International Law to State*

Activity in Cyberspace. Wellington, 17.06.2025. URL: https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/New-Zealands-position-statement-on-The-Application-of-International-Law-to-State-Activities-in-Cyberspace.pdf

298. Nordic Institute for Interoperability Solutions (NIIS). *X-Road Governance Model and Legal Framework*. Tallinn: NIIS, 2023. URL: https://www.niis.org

299. Nye, J. S. Jr. *The Regime Complex for Managing Global Cyber Activities*. – Waterloo, ON: Centre for International Governance Innovation (CIGI); London: Chatham House, 2014. 28 p. URL: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities/

300. Organisation for Economic Co-operation and Development (OECD). *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*. Paris: OECD, 2021. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479

301. Organization for Security and Co-operation in Europe (OSCE). *16 cyber/ICT security confidence-building measures.* Vienna: OSCE, 2023. URL: https://www.osce.org/files/f/documents/f/7/555999_1.pdf

302. Organization for Security and Co-operation in Europe (OSCE). *Permanent Council Decision No. 1202: OSCE confidence-building measures to reduce the risks of conflict stemming from the use of ICTs*. Vienna: OSCE, 10.03.2016. PC.DEC/1202. URL: https://www.osce.org/files/f/documents/d/a/227281.pdf

303. Oxford University Press. *Oxford Online Dictionary*. Oxford University Press, 2014. URL: http://www.oxforddictionaries.com/definition/english/Cybersecurity

304. Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., Witte, G. *NIST Special Publication 800-181. Revision 1. Workforce Framework for Cybersecurity*

(NICE Framework). Gaithersburg, MD: National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/NIST.SP.800-181r1

305. Proska, K., Wolfram, J., Wilson, J., Black, D., Lunden, K., Kapellmann Zafra, D., Brubaker, N., McLellan, T., Sistrunk, C. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. *Mandiant / Google Cloud*, 2023. URL: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

306. Protocol Additional to the Geneva Conventions of 12 August 1949 (Protocol I), 1977. URL: https://zakon.rada.gov.ua/laws/show/995_199

307. Raymond, M. Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex. *The Cyber Defense Review*, 2016. Vol. 1, No. 2. P. 81–94.

308. Raymond, M. Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot. *Strategic Studies Quarterly*, 2016. Vol. 10, No. 4. P. 123–149. URL: https://nsarchive.gwu.edu/sites/default/files/documents/5024568/Air-University-Managing-Decentralized-Cyber.pdf

309. Republic of Estonia. *Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia*. Tallinn: Ministry of Economic Affairs and Communications for Estonia, 2023. URL: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

310. Republic of Estonia. *Public Information Act*. Tallinn: Riigi Teataja, 2019. URL: https://www.riigiteataja.ee/en/eli/529032019012/consolide

311. Riigi Infosüsteemi Amet (RIA). Estonian Information System Authority, 2024. URL: https://www.ria.ee/en

312. Roscini, M. *Cyber Operations and the Use of Force in International Law*. Oxford University Press, 2014. 328 p.

313. Sanger, D. E., Barnes, J. E., Conger, K. As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War. *The New York Times*,

28.02.2022. URL: https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

314. Sanger, D. E., Conger, K. Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds. *The New York Times*, 2022. URL: https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html

315. Schatz, D., Bashroush, R., Wall, J. Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, 2017. No. 2. P. 54–74. DOI: https://doi.org/ 10.15394/jdfsl.2017.1476

316. Schiliro, F. Towards a Contemporary Definition of Cybersecurity. *arXiv preprint*, 2023. URL: https://doi.org/10.48550/arXiv.2302.02274

317. Schmitt, M. N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017. 598 p.

318. Schmitt, M. N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013. 282 p.

319. Schmitt, M. N. Grey Zones in the International Law of Cyberspace. *Yale Journal of International Law Online*, 2017. Vol. 42. P. 1–21. URL: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf

320. Soroka Larysa. Collective Security Crisis: Challenges to Space Law and Space Security. Advanced Space Law, 2023. Volume 12, 76-81. https://doi.org/10.29202/asl/12/10

321. Stevens, T., Burton, J. НАТО і стратегічна конкуренція в кіберпросторі. *NATO Review*, 2023. URL: https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/

322. Sweden. Government Offices. *Nationell strategi för cybersäkerhet 2025–2029*. Regeringen, 2025. URL:

https://www.regeringen.se/contentassets/a35c523611834fa1997d1ff5b2297338/nationell-strategi-for-cybersakerhet-20252029-skr.-202425121.pdf

323. Tarhan, K. Historical development of cybersecurity studies: A literature review and its place in security studies. *Przegląd Strategiczny*, 2022. Issue 15. P. 327–345. DOI: https://doi.org/10.14746/ps.2022.1.23

324. The White House. *National Cybersecurity Strategy*. Washington, D.C. : The White House, March 2023. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

325. The White House. *National Cybersecurity Strategy Implementation Plan*. Washington, D.C.: The White House, July 2023. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

326. Transportation Security Administration (TSA). *Security Directive Pipeline-2021-01D*. Washington, D.C.: U.S. Department of Homeland Security, 2021. URL: https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01d.pdf

327. Tsagourias, N. The Legal Status of Cyberspace: Sovereignty Redux? *Research Handbook on International Law and Cyberspace* / eds. N. Tsagourias, R. Buchan. 2nd ed. Cheltenham: Edward Elgar Publishing, 2021. P. 1–25. DOI: 10.4337/9781789904253.00010.

328. Tsagourias, N., Farrell, M. Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, 2020. Vol. 31, No. 3. P. 941–970. DOI: 10.1093/ejil/chaa057.

329. Tzavara, V., Vassiliadis, S. Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, 2024. Vol. 23. P. 1695–1719. DOI: 10.1007/s10207-023-00811-x.

330. U.S. Department of Energy (DOE). DOE Cybersecurity Strategy. Washington, D.C.: DOE, 2024. URL: https://www.energy.gov/sites/default/files/2024-03/EXEC-2023-007090%20-%20DOE%20Cybersecurity%20Strategy%20SB%20S2%20CIO%20012224_508%20Reviewed.pdf

331. U.S. Department of Energy. Roadmap to Achieve Energy Delivery Systems Cybersecurity. Washington, D.C.: U.S. DOE, 2011. URL: https://www.energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

332. U.S. Department of Homeland Security. *Protected Critical Infrastructure Information (PCII) Program: Title 6 Code of Federal Regulations, Part 29*. Washington, DC: DHS, 2023. URL: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program

333. U.S. Department of State. Attribution of Russia's Malicious Cyber Activity Against Ukraine, 2022. URL: https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

334. U.S. Government. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, D.C.: The White House, 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

335. UK Government. Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion, 2022. URL: https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

336. Ukraine. National Cyber Security Index, 2025. URL: https://ncsi.ega.ee/country/ua/

337. United Kingdom Attorney General. *International Law in Future Frontiers* (speech, Chatham House, 19 May 2022). London: UK Government, 2022. URL: https://www.gov.uk/government/speeches/international-law-in-future-frontiers

338. United Kingdom. *The Network and Information Systems Regulations 2018: Statutory Instrument 2018 No. 506 (as amended 2020/2022)*. London: UK Government, 2022. URL: https://www.legislation.gov.uk/uksi/2018/506

339. United Nations General Assembly. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations, 30.07.2010. A/65/201. URL: https://documents.un.org/doc/undoc/gen/n10/469/57/pdf/n1046957.pdf

340. United Nations General Assembly. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations, 24.06.2013. A/68/98. URL: https://dig.watch/wp-content/uploads/A_68_98_E.pdf

341. United Nations General Assembly. *Resolution 70/237 "Developments in the field of information and telecommunications in the context of international security"*. New York : United Nations, 30.12.2015. A/RES/70/237. URL: https://docs.un.org/en/a/res/70/237

342. United Nations Group of Governmental Experts. *Advancing Responsible State Behaviour in Cyberspace*. New York: United Nations, 14.07.2021. A/76/135. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

343. United Nations Group of Governmental Experts. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations, 2015. A/70/174. URL: https://docs.un.org/en/A/70/174

344. United Nations. *Developments in the field of information and telecommunications in the context of international security*. New York: United Nations, 18.03.2021. A/75/816. URL: https://docs.un.org/en/A/75/816

345. United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)*. New York: United Nations, 2001. (ILC Yearbook 2001, vol. II, Part Two; A/56/10). URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

346. United Nations. *Explanatory notes on the draft United Nations convention against cybercrime*. Vienna: UNODC. Ad Hoc Committee, 03.09.2024. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Documents/Explanatory_notes_draft_convention.pdf

347. United Nations. General Assembly. *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, established pursuant to resolution 75/240: Resolution*. New York: United Nations. URL: https://digitallibrary.un.org/record/4071346?v=pdf

348. United Nations. *Open-ended Working Group on Security of and in the Use of ICTs 2021–2025: Third annual progress report*. New York : United Nations, 22.07.2024. A/79/214. URL: https://docs.un.org/en/A/79/214

349. United States Congress. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), Public Law 117-103, 2022. Washington, DC: U.S. Congress. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

350. United States. Department of Defense. *2023 DoD Cyber Strategy: Unclassified Summary*. Washington, D.C.: DoD, 2023. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

351. United States. *Executive Order 14028 of May 12, 2021 on Improving the Nation's Cybersecurity*. Federal Register, 2021. Vol. 86, No. 93. P. 26633–26647. URL: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

352. Vicens, A. Top Ukrainian Cyber Official Praises Volunteer Hacks on Russian Targets, Offers Updates. Cyberscoop. 15.03.2022. URL: https://cyberscoop.com/it-army-ukraine-caddywiper-viasat

353. Volz, D., McMillan, R. In Ukraine, a “Full-Scale Cyberwar” Emerges. *The Wall Street Journal*, 2022. URL: https://www.wsj.com/world/europe/in-ukraine-a-full-scale-cyberwar-emerges-11649780203

354. Von Solms, R., Van Niekerk, J. From information security to cyber security. *Computers & Security*, 2013. Vol. 38. P. 97–102. DOI: 10.1016/j.cose.2013.04.004

355. Zubko A., Sokiran M., Danylenko A., Levchenko D., Oksin V. Determining the nature of digital communication in public law sphere. *International Journal of Religion*, 2024. Vol. 5, No. 5. P. 568–575. DOI: https://doi.org/10.61707/c4xc0981

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Колесник О.О. Теоретико-правові засади формування та еволюції поняття кібербезпеки. Юридичний науковий електронний журнал. 2024. № 7. С. 636–641. DOI: https://doi.org/10.32782/2524-0374/2024-7/154

2. Колесник О.О. Нормативно-інституційні засади формування національної системи кібербезпеки України. *Право та державне управління*. 2025. № 1. С. 437–445. DOI: https://doi.org/10.32782/pdu.2025.1.61

3. Колесник О.О. Міжнародні стандарти та українська практика кіберзахисту: уроки війни. *Правові новели*. 2025. № 25. С. 375–382. DOI: https://doi.org/10.32782/ln.2025.25.48

4. Сорока Л.В., ***Колесник О.О.*** Міжнародно-правові принципи регулювання кіберпростору: суверенітет, невтручання та Due Diligence. *Держава та регіони*. Серія: Право. 2025. № 1. С. 246–253. DOI: https://doi.org/10.32782/1813-338X-2025.1.35

які засвідчують апробацію матеріалів дисертації:

5. Колесник О.О. Принципи міжнародного права в системі глобальної кібербезпеки. *Проблемні питання юридичної науки в контексті реформування правової системи України:* матеріали міжнародної науково-практичної конференції (Київ, 19–20 жовт. 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 121–123.

6. Колесник О.О. Формування поняття «кібербезпека» в сучасній правовій науці: теоретичні орієнтири та методологічні виклики. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність:* матеріали міжнародної науково-практичної конференції (Київ, 4–5 черв. 2024 р.). Київ: Науково-дослідний інститут публічного права, 2024. С. 98–100.

7. Колесник О.О. Кібербезпека як елемент національної безпеки України в умовах війни. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі:* матеріали міжнародної науково-практичної конференції (Київ, 18–19 лют. 2025 р.). Київ: Науково-дослідний інститут публічного права, 2025. С. 71–73.

8. Колесник О.О. Сучасний стан і тенденції розвитку правового регулювання національної системи кібербезпеки України. *Актуальні питання науки і практики та шляхи їх вирішення:* матеріали другої міжнародної науково-практичної конференції (Київ, 4–5 черв. 2025 р.). Київ: Науково-дослідний інститут публічного права, 2025. С. 140–143.

Додаток Б

ЗАТВЕРДЖУЮ
В.о. Президента Науково-дослідного
інституту публічного права,
доктор юридичних наук, професор
Сергій КОРОЄД
«28» листопада 2025 р.

АКТ
упровадження результатів дисертаційного дослідження
Колесника Олександра Олександровича
на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід», поданого на здобуття ступеня доктора філософії зі спеціальності 081«Право» в освітній процес Науково-дослідного інституту публічного права

Комісія в складі: провідного наукового співробітника, доктора юридичних наук, професора Луценко-Миськів Лесі Ігорівни, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Шкарупи Костянтина Вікторовича, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Козіна Сергія Миколайовича склала цей акт про те, що матеріали дисертації Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» (на здобуття ступеня доктора філософії зі спеціальності 081«Право») мають необхідний теоретичний, методологічний рівень і практичну значимість та використовуються в освітньому процесі. Під час обговорення наданих матеріалів комісією було констатовано, що окремі положення дослідження було використано при розробленні лекційних курсів з дисципліни, яка викладається у Науково-дослідному інституті публічного права, а саме «Інформаційні технології у науково-правових дослідженнях», при підготовці відповідних підручників, навчальних посібників, а також у контексті інших дисциплін, які викладаються в Інституті. Лекційний курс окремих тем навчальних дисциплін увібрав положення цього дисертаційного дослідження.

ВИСНОВОК:
результати дисертаційного дослідження на тему: «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» Колесника Олександра Олександровича вважати впровадженими в освітній процес Науково-дослідного інституту публічного права з дисципліни «Інформаційні технології у науково-правових дослідженнях».

Голова комісії: **Леся ЛУЦЕНКО-МИСЬКІВ**

Члени комісії: **Костянтин ШКАРУПА**

Сергій КОЗІН

Додаток В

ЗАТВЕРДЖУЮ
В.о. Президента Науково-дослідного інституту публічного права,
доктор юридичних наук, професор
Сергій КОРОЄД
«26» листопада 2025р

А К Т
впровадження результатів дисертаційного дослідження Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід», поданого на здобуття ступеня доктора філософії зі спеціальності 081«Право» у науково-дослідну діяльність Науково-дослідного інституту публічного права

Комісія в складі: провідного наукового співробітника, доктора юридичних наук, професора Луценко-Миськів Лесі Ігорівни, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Шкарупи Костянтина Вікторовича, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Козіна Сергія Миколайовича склала цей акт про те, що матеріали дисертаційного дослідження Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» мають необхідний теоретичний, методологічний рівень і практичну значимість та використовуються у науково-дослідній діяльності наукових відділів Науково-дослідного інституту публічного права під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки та використовуються Інститутом в межах реалізації науково-дослідної теми «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації №0120U105390).

Використання результатів дисертації сприятиме активізації та підвищенню ефективності наукової роботи працівників відділів та аспірантів Науково-дослідного інституту публічного права.

ВИСНОВОК

Результати дисертаційного дослідження Колесника Олександра Олександровича на тему «Кібербезпека в системі національної безпеки України: правові виклики гібридної війни та міжнародний досвід» вважати впровадженими у науково-дослідну діяльність Науково-дослідного інституту публічного права, під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем кібербезпеки як складової сучасної архітектури національної та міжнародної безпеки.

Голова комісії: **Леся ЛУЦЕНКО-МИСЬКІВ**

Члени комісії: **Костянтин ШКАРУПА**

Сергій КОЗІН