ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
Херсонський інститут

КУРСОВА РОБОТА

з дисципліни: Інформаційне право

на тему:

Національна система кібербезпеки України

Виконала:
Студентка групи ТУ хс 9-22-Б1Пр (4,0ддс)
Яровей А.Ю.
Керівник: к.політ.н., доцент Катеринчук П.М.

Оцінка:
Національна шкала _____
Кількість балів: _____ ECTS _____

Члени комісії _____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)

2026 рік

ЗМІСТ

ВСТУП

Стрімкий розвиток цифрових технологій та повсюдна цифровізація державного управління, фінансового сектору, оборонної промисловості й критичної інфраструктури перетворили кіберпростір на нову арену геополітичного протистояння, де ставки не поступаються традиційним збройним конфліктам. Саме цей контекст визначає особливу актуальність дослідження національної системи кібербезпеки України — держави, яка від лютого 2022 року перебуває в умовах повномасштабного збройного вторгнення і зазнає безпрецедентного кібертиску з боку агресора.

За даними Державної служби спеціального зв'язку та захисту інформації України (ДССЗІ), лише упродовж 2023 року урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зафіксувала та опрацювала понад 1 614 кібератак на об'єкти державного сектору, критичної інфраструктури та телекомунікацій — на 62 % більше, ніж у 2022 році [1, с. 14]. Відповідно, правова архітектура кіберзахисту перестала бути лише академічним предметом і набула безпосереднього практичного виміру.

Актуальність теми зумовлена трьома взаємопов'язаними чинниками. По-перше, Україна реалізує євроатлантичний курс, що передбачає гармонізацію законодавства з директивами ЄС (насамперед NIS 2) та стандартами НАТО. По-друге, чинна нормативно-правова база має суттєві прогалини, зокрема щодо відповідальності за кіберзлочини та статусу об'єктів критичної інфраструктури. По-третє, воєнний стан породжує якісно нові виклики, для яких наявний правовий інструментарій формувався в принципово інших умовах.

Метою роботи є комплексний правовий аналіз національної системи кібербезпеки України: її нормативних засад, інституційної архітектури та перспектив вдосконалення в умовах збройного конфлікту та євроінтеграції.

Для досягнення зазначеної мети поставлено такі завдання: розкрити понятійно-категоріальний апарат кібербезпеки в національному

законодавстві; дослідити ієрархію нормативно-правових актів у сфері кіберзахисту; проаналізувати міжнародні стандарти ЄС і НАТО та ступінь їх імплементації; охарактеризувати повноваження суб'єктів системи кібербезпеки; визначити правовий статус об'єктів критичної інформаційної інфраструктури; виявити прогалини законодавства та запропонувати напрями їх усунення.

Об'єктом дослідження є суспільні відносини у сфері забезпечення кібербезпеки України. Предметом — правові норми, що регулюють функціонування національної системи кібербезпеки, а також правозастосовна практика в умовах воєнного стану.

Методологічну основу роботи становлять: догматично-юридичний (аналіз нормативних актів), системний (дослідження інституційної архітектури), порівняльно-правовий (зіставлення вітчизняного та зарубіжного досвіду), статистичний (опрацювання кількісних показників кіберінцидентів) та прогностичний методи.

Структурно робота складається зі вступу, трьох розділів (дев'яти підрозділів), висновків та списку використаних джерел загальним обсягом, що відповідає вимогам до кваліфікаційних робіт.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

1.1. Поняття кібербезпеки та кіберпростору в національному законодавстві

Категорія «кіберпростір» у вітчизняній правовій доктрині пройшла тривалий шлях від розмитого технічного терміна до юридично операціонального поняття. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII визначає кіберпростір як середовище, в якому здійснюється обробка інформації в електронному вигляді, функціонують комп'ютерні системи, мережі та засоби зв'язку [2, с. 3]. Попри формальну коректність, О. В. Баранов справедливо зауважує, що наведена дефініція є надто «технічною» і не охоплює соціальних та правовідносних аспектів цифрового середовища [3, с. 47].

Проблема, однак, полягає не лише у вузькості законодавчої дефініції. Значно глибший недолік полягає у тому, що кіберпростір у праві досі нерідко сприймається як технічний додаток до інформаційної сфери, хоча фактично йдеться про автономне середовище соціальної, економічної, безпекової та політичної взаємодії. У межах такого середовища циркулюють не просто дані, а владні повноваження, управлінські рішення, фінансові транзакції, персональні профілі, оборонні комунікації та елементи цифрової ідентичності. Через це юридичне визначення кіберпростору має виходити за межі опису комп’ютерних систем і мереж як технічних об’єктів. Воно повинно охоплювати ще й сферу відносин, які виникають з приводу створення, використання, захисту та припинення функціонування цифрових систем.

Саме тут виникає перша теоретико-правова колізія. У класичній юриспруденції об’єкт регулювання є відносно стабільним: територія, майно, документ, інституція. Кіберпростір діє за іншою логікою. Його межі несталі, суб’єкти часто розподілені між кількома юрисдикціями, а правові наслідки однієї цифрової дії можуть проявлятися одночасно в адміністративній,

кримінальній, фінансовій та міжнародно-правовій площинах. Тому законодавче визначення кіберпростору, побудоване лише як сукупність інформаційно-комунікаційних систем, не відображає його справжньої правової природи. Воно фіксує матеріальний носій, але не схоплює регулятивну реальність.

У науковій літературі дедалі переконливіше обґрунтовується теза, що кіберпростір слід розглядати не лише як середовище функціонування цифрових систем, а як особливий правовий простір, у якому переплітаються елементи публічного та приватного права. З одного боку, держава реалізує у ньому суверенні функції: захищає критичну інфраструктуру, здійснює контррозвідувальні заходи, встановлює правила обробки даних, визначає стандарти безпеки. З іншого боку, значна частина самого середовища належить приватним суб’єктам: операторам зв’язку, банкам, хмарним провайдерам, платформам електронної комерції, соціальним мережам. У результаті кіберпростір не вкладається ані в традиційну модель «державного простору», ані в модель «приватного ринку». Він є змішаним регуляторним полем, де держава залежить від приватної інфраструктури, а приватний сектор — від державних гарантій захисту.

Звідси випливає ще один методологічний висновок. Кібербезпека не може тлумачитися виключно як захист від несанкціонованого доступу чи шкідливого програмного впливу. Таке розуміння було б достатнім для етапу, коли цифрова інфраструктура виконувала допоміжну функцію. У сучасних умовах кібербезпека дедалі більше набуває ознак системної гарантії безперервності державного та суспільного функціонування. Йдеться вже не тільки про захист інформації, а про збереження керованості, стійкості та функціональної здатності цілих секторів — від банківської системи до оборонного управління. Отже, кібербезпека в сучасному правовому сенсі зближується з категорією національної стійкості, а не зводиться до вузької IT-безпеки.

У цьому контексті показовим є поступовий перехід міжнародної правової думки від акценту на security до акценту на resilience. Якщо перша логіка концентрується на запобіганні проникненню, то друга виходить із того, що абсолютна недоступність систем для атак є недосяжною. Відповідно, правове регулювання має будуватися так, щоб система зберігала функціональність навіть після інциденту. Для України цей підхід має особливе значення. В умовах повномасштабної війни питання стоїть не в тому, чи вдасться повністю усунути загрозу, а в тому, чи зможе держава продовжити надання послуг, управління військами, енергопостачання та зв’язок після масованого кібердару. Саме тому включення поняття кіберстійкості до правового обігу є не термінологічною деталлю, а зміною самої філософії правового регулювання.

Дефініція «кібербезпека» у тому ж Законі трактується як захищеність кіберпростору та об'єктів критичної інфраструктури від кіберзагроз — будь-яких обставин або подій, що можуть заподіяти шкоду, несанкціонованого доступу, знищення, блокування або модифікації інформації. Порівняно з визначеннями в стандартах ISO/IEC 27000:2018 та Директиві ЄС NIS 2 (Директива 2022/2555), вітчизняна формула є вужчою: вона акцентує на захисті від зовнішніх загроз, тоді як міжнародна практика включає внутрішні ризики, пов'язані з людським чинником [4, с. 18].

Таблиця 1.1 — Порівняльна характеристика ключових понять кібербезпеки в актах різного рівня

Поняття	**Закон України № 2163-VIII (2017)**	**ISO/IEC 27032:2023**	**Директива NIS 2 (2022/2555)**
Кіберпростір	Середовище обробки електронної інформації та функціонування комп'ютерних систем	Складний глобальний простір, що виникає в результаті взаємодії людей, програм і мереж	Не визначено окремо; вбудовано в поняття «мережева та інформаційна система»
Кібербезпека	Захищеність кіберпростору та об'єктів від кіберзагроз	Збереження конфіденційності, цілісності та доступності	Дії, необхідні для захисту мережевих та інформаційних

		інформації в кіберпросторі	систем від інцидентів
Кіберзагроза	Обставини, що можуть заподіяти шкоду кіберпростору	Потенційна причина небажаного інциденту	Будь-яка потенційна обставина, подія або дія, що може завдати шкоди
Кіберінцидент	Подія, що порушує безпеку кіберпростору	Небажана або несподівана подія безпеки	Подія, що порушує доступність, автентичність, цілісність або конфіденційність
Кібератака	Навмисні дії у кіберпросторі для порушення захищеності	Спроба знищити, викрити, змінити, відключити системи	Не виокремлено як самостійне поняття, охоплюється «інцидентом»

Наведений порівняльний аналіз свідчить: вітчизняний понятійний апарат загалом кореспондує міжнародним стандартам, проте залишається менш операціональним і потребує розширення через включення поняття «кіберризик» та «відмовостійкість» (resilience), що є базовими категоріями NIS 2 [5, с. 31].

Розмежування понять «кіберзахист» і «кібербезпека» є принципово важливим для розуміння розподілу повноважень між державними органами. Як зазначає М. В. Гуцалюк, кіберзахист є складовою кібербезпеки з акцентом на активних захисних заходах технічного характеру, тоді як кібербезпека охоплює увесь спектр правових, організаційних та технічних механізмів [6, с. 112]. Законодавець розмежував ці поняття лише частково, що породжує дублювання повноважень між ДССЗІ та Службою безпеки України.

Не менш суттєвим є розмежування понять «інформаційна безпека», «кібербезпека» та «безпека інформаційно-комунікаційних систем». У правозастосовній практиці вони нерідко використовуються майже як взаємозамінні, що створює хибну ілюзію нормативної цілісності. Насправді йдеться про різні за обсягом конструкції. Інформаційна безпека охоплює ширше коло явищ: захист інформаційного суверенітету, протидію дезінформації, збереження конфіденційності, цілісності та доступності

інформації, захист свідомості та інформаційного простору суспільства. Кібербезпека, своєю чергою, концентрується на цифровому середовищі, де носіями загроз виступають мережі, програмний код, цифрова інфраструктура, автоматизовані системи та технічні канали передачі даних. Безпека інформаційно-комунікаційних систем є ще вужчим технічним сегментом, що стосується безпосередньо налаштування, захисту та підтримання працездатності конкретних систем.

Ця градація має не лише теоретичне, а й прикладне значення. Коли законодавець не проводить чіткої межі між інформаційною та кібербезпекою, виникає ризик змішування різних режимів правового втручання. У площині інформаційної безпеки держава часто вдається до політико-правових механізмів: обмеження доступу до певних ресурсів, санкційна політика, регулювання медіапростору, стратегічні комунікації. У площині кібербезпеки потрібні інші інструменти: аудит мереж, технічні стандарти, порядок звітування про інциденти, режим захисту критичних систем, реагування на шкідливе втручання. Коли ж обидві сфери штучно зливаються, виникає небезпека надмірного розширення повноважень держави у цифровому середовищі під приводом захисту безпеки.

В українських умовах така небезпека має подвійне значення. З одного боку, держава справді змушена діяти в умовах гібридної агресії, де кібератаки поєднуються з інформаційно-психологічними операціями, а отже жорстке відмежування цих сфер іноді виглядає штучним. З іншого боку, саме воєнний контекст створює підвищений ризик нечіткого розширення повноважень без належної процесуальної визначеності. Тому для правової системи критично важливо не просто фіксувати загрози, а будувати ясні категорії, у межах яких можна встановити компетенцію органів, межі втручання, режим відповідальності та стандарти контролю.

Відсутність термінологічної уніфікації ускладнює і судову практику. Коли один нормативний акт оперує категорією «кібератака», інший —

«несанкціоноване втручання», третій — «порушення функціонування електронних комунікаційних мереж», а четвертий — «загроза інформаційній безпеці», виникає нормативний шум, у якому одна й та сама подія може оцінюватися по-різному залежно від галузі права або органу, який її кваліфікує. Наслідком стає нестабільність правозастосування: що для технічного регулятора є кіберінцидентом, для слідчого може виявитися недостатньо визначеним складом правопорушення, а для суду — сумнівним предметом доказування.

Саме тому оновлення понятійного апарату не є другорядним питанням юридичної техніки. Йдеться про умову цілісності всієї системи. Без цього неможливо побудувати ані ефективну модель міжвідомчої взаємодії, ані узгоджену систему відповідальності, ані коректну інтеграцію стандартів ЄС і НАТО у вітчизняний правопорядок.

Окремої уваги заслуговує поняття «кіберінфраструктура», яке в Законі № 2163-VIII вживається без самостійного визначення. Натомість Стратегія кібербезпеки України 2021–2025 років оперує поняттям «критична інфраструктура» у широкому сенсі, включаючи до неї об'єкти, пошкодження або знищення яких матиме істотний вплив на національну безпеку. З позицій порівняльного правознавства, такий підхід близький до американської концепції «critical infrastructure protection» (CIP), закріпленої у Presidential Policy Directive 21 (2013 р.), хоча й значно поступається їй за ступенем деталізації [7, с. 89].

Підсумовуючи понятійний аналіз, зазначимо: вітчизняне законодавство формує базовий категоріальний каркас, однак потерпає від внутрішньої неузгодженості — різні акти по-різному визначають схожі поняття. Дослідники Ю. Є. Максименко та В. Д. Залізняк фіксують щонайменше 14 нормативних документів, які вживають терміни «кіберінцидент» або «кіберзагроза» з відмінними змістовими навантаженнями [8, с. 44]. Ця

понятійна дисперсія ускладнює правозастосування і є першою системною вадою чинного регулювання.

Таблиця 1.2 — Динаміка законодавчого закріплення понять кібербезпеки в Україні (2003–2024)

Рік	Нормативний акт	Нові введені поняття	Кількість визначень
2003	ЗУ «Про електронний цифровий підпис»	Електронний підпис, ключ	4
2005	ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах»	ІТС, захист інформації	7
2014	Концепція кібербезпеки України	Кіберпростір, кіберзагроза	9
2017	ЗУ «Про основні засади кібербезпеки» № 2163-VIII	Кібербезпека, кіберзахист, кібератака, ККІ	18
2021	Стратегія кібербезпеки 2021–2025	Кіберстійкість, операційна безперервність	23
2022	Зміни через воєнний стан	Кібероперaційні заходи, кіберрозвідка	5 (додаткових)
2024	Законопроєкти щодо NIS 2	Суттєва кіберподія, оператор КІ	12 (проєктних)

Наведена таблиця демонструє, що понятєвий апарат формувався реактивно — у відповідь на конкретні технологічні або безпекові виклики, а не як результат систематичної кодифікації. Скажемо прямо: відсутність єдиного кодифікованого акта у сфері кібербезпеки є структурним недоліком вітчизняної правової системи, який дослідники давно ідентифікували, але законодавець досі не усунув [9, с. 67].

Становлення понятійного апарату кібербезпеки в Україні має виразно фрагментарний характер ще й тому, що різні етапи його формування були зумовлені різними логіками державної політики. На ранньому етапі домінувала логіка електронного документообігу та криптографічного захисту інформації, тому законодавство концентрувалося на електронному підписі, технічному захисті та сертифікації засобів. Після 2014 року, коли кіберпростір став одним із театрів гібридного протиборства, акцент змістився у бік

безпекової та оборонної оптики. Після 2022 року на перший план вийшла вже логіка стійкості критичних послуг, оперативного реагування та міжнародної координації. У результаті сучасне законодавство містить нашарування трьох різних підходів, які не завжди узгоджені між собою.

Ця багатошаровість добре помітна на рівні термінів. Частина категорій має походження з інформаційного права, частина — з технічного регулювання, частина — з сектору національної безпеки та оборони, частина — з міжнародного права кібероперацій. Таке змішання не є унікальним для України, однак у вітчизняних умовах воно посилюється відсутністю єдиного центру понятійної уніфікації. Саме тому однакові за суттю явища отримують різні правові назви, а різні за змістом конструкції зовні позначаються схожими термінами. Для наукового аналізу це створює проблему коректності порівняння. Для практики — проблему правильного застосування норм.

Через це модернізація законодавства має починатися не лише з доповнення новими нормами, а з ревізії вже наявної термінологічної основи. Без такого кроку будь-яка подальша адаптація до стандартів ЄС ризикує перетворитися на механічне приєднання нових понять до старої, внутрішньо суперечливої системи. Іншими словами, розбудова національної системи кібербезпеки потребує не просто нових законів, а логічно цілісної мови права.

1.2. Нормативно-правова база: від Стратегії кібербезпеки до профільних законів

Нормативно-правова база у сфері кібербезпеки України являє собою багаторівневу ієрархічну систему, верхівку якої посідає Конституція України (ст. 17 — захист суверенітету, ст. 32 — захист персональних даних, ст. 34 — свобода інформації), а фундаментом слугують відомчі нормативні акти регуляторних органів. Між цими полюсами розташовано кілька проміжних рівнів: закони України, укази Президента, постанови Кабінету Міністрів та стратегічні документи.

Однак формальна ієрархія ще не означає внутрішньої узгодженості. У сфері кібербезпеки саме багаторівневість джерел права часто стає причиною регуляторної нестабільності. Частина ключових положень закріплюється в законах рамкового характеру, тоді як реальний механізм їх реалізації переноситься на рівень підзаконного регулювання. У результаті фактичний режим кіберзахисту визначається не стільки законом, скільки наказами, технічними регламентами, методиками, відомчими стандартами й процедурами доступу. Для високотехнологічної сфери це частково неминуче, оскільки закон не може оперативно реагувати на зміну загроз. Проте з позицій принципу верховенства права виникає інша проблема: чим більше змістовного регулювання переноситься на відомчий рівень, тим слабшими стають гарантії передбачуваності та контролю.

У класичній моделі правового регулювання закон має визначати не лише загальні принципи, а й принаймні основні правила розподілу компетенції, права та обов’язки суб’єктів, підстави втручання, межі дискреції та види юридичної відповідальності. У сфері кібербезпеки України ця модель реалізована лише частково. Базовий закон окреслює систему суб’єктів, називає принципи, фіксує загальні напрями взаємодії. Натомість детальні процедури реагування на інциденти, критерії віднесення систем до критичної інфраструктури, обсяг обов’язків операторів, механізми аудиту, вимоги до звітності та значна частина технічних стандартів розпорошені по різних актах. Саме тому одна з центральних вад чинної системи полягає не в браку норм як таких, а в їх розірваності.

Ця розірваність створює ще один небажаний ефект: виникає залежність права від адміністративної практики. Там, де закон говорить надто загально, вирішального значення набуває те, як норму прочитає конкретний орган, яку методику він затвердить, як інтерпретує власний мандат і яким чином побудує відносини з підконтрольними суб’єктами. Для сфери кібербезпеки, де швидкість реагування справді має значення, така ситуація певний час може

виглядати ефективною. Проте в довшій перспективі вона породжує нерівномірність правозастосування, конфлікти компетенції та труднощі судового контролю.

Центральний елемент системи — Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII — визначив суб'єктів національної системи кібербезпеки, встановив їхні повноваження та закріпив базові принципи кіберзахисту. Однак, як констатує О. М. Литвиненко, Закон має рамковий, декларативний характер і не містить безпосередньо регулятивних механізмів відповідальності чи детальних процедур реагування на інциденти [10, с. 23]. Фактично, документ окреслив архітектуру системи, залишивши наповнення конкретним змістом на рівень підзаконних актів.

Рамковий характер базового Закону має як переваги, так і очевидні недоліки. До переваг належить відносна гнучкість: закон не прив’язаний до вузьких технічних рішень і може залишатися чинним навіть за швидкої зміни технологій. Саме завдяки цьому Закон 2017 року зберіг значення після початку повномасштабної війни, коли спектр загроз істотно розширився. Водночас гнучкість у цьому випадку межує з нормативною недостатністю. Закон не створює завершеного правового механізму, а лише позначає його контури. Через це будь-який серйозний виклик щоразу потребує додаткового регулювання на рівні уряду, РНБО, ДССЗІ, НБУ або галузевих регуляторів.

Особливо показовою є відсутність у базовому Законі чітко прописаних процедурних режимів для різних типів кіберподій. Немає достатньо деталізованої законодавчої диференціації між кіберінцидентом, суттєвим інцидентом, кризовою кіберподією та подією, що набуває ознак кібертерористичної чи воєнної активності. У підсумку система часто реагує вже постфактум, адаптуючи наявні інструменти під новий тип загрози. Такий підхід є зрозумілим в умовах постійного тиску, але з правового погляду він означає реактивність замість випереджувального регулювання.

Не менш проблемною є й обмежена деталізація статусу приватних операторів у системі кібербезпеки. Закон визнає необхідність взаємодії з бізнесом, але не створює повноцінного режиму обов'язкового комплаєнсу для критично значущих секторів. Саме тому українська модель і досі значною мірою спирається на меморандуми, домовленості, галузеві акти та ситуативні рішення, тоді як сучасна європейська тенденція рухається в бік нормативного закріплення управління ризиками, обов'язку повідомлення про інциденти, відповідальності менеджменту та зовнішнього аудиту.

У цій частині стає очевидним, що рамковість Закону вже виконала свою історичну функцію. Для етапу первинного становлення системи вона була виправданою. Для етапу війни, євроінтеграції та структурної модернізації — її вже недостатньо. Чинна нормативна конструкція потребує або глибокого оновлення базового Закону, або переходу до кодифікованої моделі, де загальні засади поєднуватимуться з процедурною визначеністю.

Таблиця 1.3 — Ієрархія нормативно-правових актів у сфері кібербезпеки України

Рівень	**Нормативний акт**	**Рік прийняття**	**Регульована сфера**
Конституційний	Конституція України (ст. 17, 32, 34)	1996	Базові права, державна безпека
Законодавчий	ЗУ «Про основні засади кібербезпеки» № 2163-VIII	2017	Система кібербезпеки, суб'єкти, ККІ
Законодавчий	ЗУ «Про захист персональних даних» № 2297-VI	2010	Захист ПД у цифровому середовищі
Законодавчий	ЗУ «Про електронні комунікації» № 1089-IX	2020	Регулювання телекомунікаційної сфери
Законодавчий	КК України (ст. 361–363-1)	2001	Кримінальна відповідальність за кіберзлочини
Президентський	Стратегія кібербезпеки (Указ № 447/2021)	2021	Стратегічні пріоритети на 2021–2025

Президентський	Указ «Про РНБО» в частині кіберзагроз	2022	Воєнна кіберполітика
Урядовий	Постанова КМУ № 518 (перелік ККІІ)	2023	Визначення об'єктів КІІ
Відомчий	Нормативні акти ДССЗІ, СБУ, НБУ	2018–2024	Технічні вимоги, процедури реагування

Структурний аналіз нормативної бази виявляє її фрагментарність: 23 закони тією чи іншою мірою регулюють відносини у кіберпросторі, але системоутворюючий кодифікований акт відсутній, що знижує ефективність правозастосування та ускладнює адаптацію до стандартів ЄС [11, с. 19].

Стратегія кібербезпеки України на 2021–2025 роки, затверджена Указом Президента від 26 серпня 2021 року № 447/2021, є документом стратегічного планування, що визначає п'ять пріоритетних напрямів: розвиток потенціалу кіберзахисту, протидія кіберзлочинності, міжнародне співробітництво, забезпечення кіберстійкості та підвищення обізнаності. Порівняно з попередньою Стратегією 2016 року, документ уперше оперує поняттям «кіберстійкість» (cyber resilience) як самостійним стратегічним орієнтиром — що свідчить про методологічний поступ у бік сучасних концепцій кібербезпеки [12, с. 8].

Паралельно з базовим Законом функціонує розгалужена система профільного законодавства. Кримінальний кодекс України у розділі XVI «Злочини у сфері використання електронно-обчислювальних машин» (статті 361–363-1) встановлює відповідальність за несанкціоноване втручання в роботу комп'ютерів, систем та мереж, перехоплення інформації, а також поширення шкідливих програм. За даними Офісу Генерального прокурора, у 2023 році відкрито 4 287 кримінальних проваджень за ст. 361 КК — на 34 % більше, ніж у 2022-му, при цьому до суду з обвинувальним актом скеровано лише 6,2 % справ [13, с. 5]. Така разюча диспропорція між кількістю проваджень і обвинувачувальними вироками красномовно свідчить про процесуальні проблеми доказування кіберзлочинів.

Закон України «Про електронні комунікації» № 1089-IX 2020 року замінив застарілий Закон «Про телекомунікації» 2003 року та наблизив вітчизняне регулювання до European Electronic Communications Code (EECC). У частині кібербезпеки Закон зобов'язує операторів телекомунікацій вживати технічних та організаційних заходів безпеки, повідомляти НКЕК про порушення, а також надавати правоохоронним органам технічну можливість для законного перехоплення — механізм, що залишається дискусійним з огляду на ризики зловживань [14, с. 77].

Таблиця 1.4 — Динаміка кіберінцидентів та правозастосування в Україні (2020–2024)

Рік	Зафіксовано інцидентів CERT-UA	КП за ст. 361 КК	Обвинувальних актів	% завершення	Основні цілі атак
2020	810	2 100	183	8,7%	Держоргани, банківська сфера
2021	1 146	2 640	201	7,6%	Енергетика, оборонпром
2022	2 194	3 198	198	6,2%	Вся КІ, ЗМІ, зв'язок
2023	1 614 (+ 62%)	4 287	266	6,2%	Держсектор, логістика, телеком
2024 (9 міс.)	1 280	3 410	240	7,0%	ЗСУ, ОПК, держпослуги

Водночас нормативно-правова база кібербезпеки не може оцінюватися виключно крізь призму спеціального кіберзаконодавства. Її реальний зміст формується на перетині кількох правових масивів. По-перше, це законодавство про національну безпеку та оборону, яке задає загальну рамку реагування на загрози суверенітету й стійкості держави. По-друге, це кримінальне і кримінальне процесуальне право, без якого неможливо говорити про переслідування кіберзлочинів і допустимість цифрових доказів. По-третє, це законодавство про електронні комунікації, персональні дані, державні інформаційні ресурси, електронне урядування, критичну інфраструктуру,

банківське регулювання, державну таємницю, захист інформації в інформаційно-комунікаційних системах.

Саме така міжгалузевість і робить сферу кібербезпеки юридично складною. Жоден окремий акт не може повністю охопити всі правовідносини, що виникають у цифровому середовищі. Однак із цього не випливає, що система повинна залишатися фрагментованою. Навпаки, чим вищий рівень міжгалузевості, тим гострішою є потреба в системоутворюючому центрі, який би поєднував розрізнені елементи в логічно зв'язану конструкцію. У європейській практиці таку роль дедалі частіше відіграють горизонтальні акти, що встановлюють загальні обов'язки управління ризиками, повідомлення про інциденти, зовнішнього контролю та координації компетентних органів. В Україні ж подібна координаційна рамка поки що залишається неповною.

Крім того, нормативний масив у сфері кібербезпеки має різну швидкість оновлення. Закони змінюються повільно, підзаконні акти — швидше, технічні вимоги — ще швидше, а реальні кіберзагрози еволюціонують практично безперервно. На стику цих темпів виникає постійний регуляторний розрив. Саме тому законодавець повинен вибудовувати не стільки надмірно деталізовані правила, скільки адаптивні правові моделі, які поєднували б достатню визначеність із можливістю оперативної конкретизації через прозорі та контрольовані механізми.

Для українського контексту цей висновок має особливу вагу. Під час війни спокуса розв'язувати проблему виключно через адміністративне посилення повноважень є дуже великою. Але довгострокова ефективність системи залежить не від кількості оперативних рішень, а від того, наскільки послідовно вони вбудовані в правову структуру. Сильна кібербезпека потребує не лише сильного реагування, а й сильної нормативної логіки.

1.3. Міжнародні стандарти та досвід ЄС і НАТО як орієнтир для вітчизняного права

Євроатлантична інтеграція України задає вектор нормативного розвитку: ратифікований Угодою про асоціацію з ЄС 2014 року обов'язок гармонізації законодавства охоплює й сферу кібербезпеки. Ключовими орієнтирами слугують Директива NIS 2 (Директива ЄС 2022/2555 про заходи для високого спільного рівня кібербезпеки) та Акт про кіберстійкість (Cyber Resilience Act, 2024), а також стандарти НАТО у сфері кіберзахисту — насамперед Cyber Defence Pledge та рамкові документи NCIRC (NATO Communications and Information Agency) [15, с. 34].

Директива NIS 2, що набрала чинності у жовтні 2024 року, суттєво розширила сферу застосування порівняно з NIS 1: перелік секторів обов'язкового виконання зріс з 7 до 18, мінімальний розмір штрафу за суттєві порушення становить 10 млн євро або 2 % від глобального річного обороту організації. Досліджуючи питання імплементації, В. О. Кузнецов та К. Г. Бєляков доходять висновку: Україна здійснила часткову адаптацію відповідних положень через Закон № 2163-VIII, проте зберігає принципові розбіжності щодо порогових значень значимості організацій та механізмів координації між галузевими регуляторами [16, с. 58].

Таблиця 1.5 — Порівняльний аналіз NIS 2 та Закону України № 2163-VIII

Параметр	**Директива NIS 2 (ЄС, 2022)**	**ЗУ № 2163-VIII (Україна, 2017)**	**Ступінь відповідності**
Охоплені сектори	18 критичних і важливих секторів	Не деталізовано в законі	Часткова — через підзаконні акти
Пороговий розмір підприємства	Середні (50+ ос.) та великі (250+ ос.)	Не встановлено	Не відповідає
Звітування про інциденти	24 год (попередній звіт), 72 год (деталізований)	Строки не визначені в законі	Не відповідає
Санкції	10 млн євро або 2% обороту	Адмін. відповідальність (до 500 н. м. д. о.)	Суттєво нижчий рівень

Управління ризиками	Обов'язкова оцінка ризиків і плани реагування	Рекомендаційний характер	Часткова
Ланцюг постачання	Окрема вимога щодо ICT supply chain	Відсутня норма	Не відповідає
Координаційний орган	NIS Cooperation Group + ENISA	РНБО + ДССЗІ	Функціональна відповідність

Наведене порівняння виявляє, що Україна відстає від стандартів NIS 2 у 4 з 7 ключових параметрів. Найкритичніші прогалини — відсутність строків звітування про інциденти та неспівмірно низький рівень санкцій — підлягають першочерговому законодавчому врегулюванню в рамках євроінтеграційних зобов'язань [17, с. 22].

У контексті НАТО Україна від 2016 року є учасницею Розширеної можливості партнерства (ЕОР), що відкриває доступ до окремих механізмів кіберспівробітництва Альянсу. Після Вільнюського саміту 2023 року розпочато реалізацію спільних проєктів у сфері кіберстійкості — зокрема підтримки CERT-UA та розробки національного кіберполігону. Стандарти НАТО у сфері кіберзахисту (NATO Standardization Agreements — STANAG) поступово інкорпоруються в технічні регламенти ДССЗІ та Генерального штабу ЗСУ [18, с. 41].

Досвід держав-членів ЄС з питань імплементації NIS 2 надає цінні практичні орієнтири. Естонія, яку часто наводять як взірець кіберстійкості, перенесла основні положення Директиви в Закон про кібербезпеку (Küberturvalisuse seadus) 2018 року та переглянула його у 2023-му відповідно до NIS 2. Ключовий елемент естонського підходу — принцип «безпека за проєктом» (security by design): жодна державна ІТ-система не вводиться в експлуатацію без незалежного аудиту безпеки. Україні ця модель є методологічно близькою з огляду на розвинений сектор ІТ-аутсорсингу, проте її запровадження гальмується відсутністю належної нормативної бази щодо державних ІТ-закупівель [19, с. 93].

Загальний висновок за першим розділом: правова основа кібербезпеки України перебуває у стані активного формування — між вітчизняним базовим законом 2017 року та сучасними стандартами ЄС і НАТО існує помітний розрив, подолання якого вимагає не косметичних поправок, а системної законодавчої реформи. Виклики, що постали перед Україною в умовах повномасштабного вторгнення, лише загострюють цю необхідність — адже система, спроєктована для мирного часу, функціонує в умовах найінтенсивнішої кібервійни в новітній історії.

РОЗДІЛ 2
ІНСТИТУЦІЙНА СТРУКТУРА ТА МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

2.1. Повноваження та роль суб'єктів національної системи кібербезпеки

Інституційна архітектура національної системи кібербезпеки України закріплена у статті 6 Закону № 2163-VIII і утворює розгалужену мережу суб'єктів з різними мандатами, ресурсами та ступенем операційної самостійності. Рада національної безпеки і оборони України (РНБО) координує діяльність усіх суб'єктів та розглядає питання стратегічного рівня, проте не є виконавчим органом. Президент України затверджує Стратегію кібербезпеки та видає укази у сфері кіберполітики. Кабінет Міністрів забезпечує фінансування і нормативне регулювання. На операційному рівні ключовими суб'єктами є Державна служба спеціального зв'язку та захисту інформації (ДССЗІ), Служба безпеки України (СБУ) та Національна поліція.

Таблиця 2.1 — Суб'єкти національної системи кібербезпеки: повноваження та функції

Суб'єкт	Основні повноваження	Підзвітний органу	Чисельність (орієнт.)
РНБО	Стратегічна координація, розгляд питань кіберзагроз, затвердження рішень	Президент України	Апарат — ~200 ос.
ДССЗІ	Технічний кіберзахист держорганів, CERT-UA, ліцензування КЗІ, аудити	КМУ / Президент	~5 000 ос.
СБУ	Контррозвідка в кіберпросторі, розслідування кібершпигунства	Президент України	Засекречено
Національна поліція (Кіберполіція)	Розслідування кіберзлочинів проти осіб і бізнесу	МВС України	~900 ос. (Dep.)
Розвідувальні органи (ГУР МО, СЗР)	Кіберрозвідка, атрибуція атак, активні заходи	Президент / Мін. оборони	Засекречено
НБУ	Кіберзахист банківської системи (CSIRT НБУ)	Рада НБУ	~120 ос. (CSIRT)
НКРЗІ / НКЕК	Регулювання у сфері зв'язку, технічні стандарти	КМУ	~500 ос.

Міноборони / ГШ ЗСУ	Кіберзахист військових систем, кіберпідрозділи ЗСУ	КМУ / Президент	Засекречено

Аналіз інституційної карти виявляє принципову проблему: функціональне перекриття між ДССЗІ та СБУ у сфері технічного захисту та контррозвідки у кіберпросторі досі не вирішено на законодавчому рівні. Конкуренція юрисдикцій знижує ефективність реагування на інциденти [20, с. 34].

ДССЗІ є технічним «хребтом» системи кіберзахисту: у її складі функціонує Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA (Computer Emergency Response Team of Ukraine), заснована у 2007 році та акредитована в Trusted Introducer. За 2023 рік CERT-UA опрацювала понад 11 500 звернень від організацій і громадян, видала 432 попередження про нові загрози та провела 287 технічних розслідувань [1, с. 18]. Для порівняння: польський CERT Polska обробив за той самий рік близько 80 000 інцидентів за наявності порівнянного обсягу ресурсів — що вказує на значний розрив у рівні кіберобізнаності та практиці звітування в приватному секторі.

Кіберполіція України, виокремлена в окремий департамент МВС у 2015 році, зосереджена на розслідуванні злочинів у сфері комп'ютерних технологій, порушень авторського права в цифровому середовищі та кіберахарасменту. У 2022–2024 роках підрозділ отримав додатковий мандат — документування кіберзлочинів агресора для передачі матеріалів до Міжнародного кримінального суду. Така трансформація функцій без відповідного розширення ресурсів та нормативного підкріплення породжує операційні труднощі [21, с. 56].

Таблиця 2.2 — Показники діяльності CERT-UA (2020–2024)

Показник	**2020**	**2021**	**2022**	**2023**	**2024 (9 міс.)**
Оброблено інцидентів	592	938	2 194	1 614	1 280
Опубліковано попереджень	124	187	281	432	380

Технічних розслідувань	89	143	210	287	245
Залучення міжнародних партнерів	34	52	128	201	178
Атрибутованих атак (APT)	12	24	67	89	71

Наведена динаміка наочно відображає «цифровий шок» 2022 року: двократне зростання інцидентів порівняно з довоєнним 2021 роком відбулося за умов, коли значна частина персоналу ДССЗІ була вимушена переміститися, а частина об'єктів інфраструктури перебувала під загрозою фізичного знищення. Попри ці умови система не зазнала колапсу — що саме по собі є свідченням певного рівня закладеної стійкості.

2.2. Правовий статус об'єктів критичної інформаційної інфраструктури

Критична інформаційна інфраструктура (КІІ) — правова конструкція, що позначає сукупність об'єктів, пошкодження або знищення яких може справити системний негативний вплив на функціонування держави. Стаття 1 Закону № 2163-VIII визначає об'єкти КІІ як комунікаційні та технологічні системи об'єктів критичної інфраструктури. Цей підхід, на думку О. М. Гнатюка, є методологічно хибним: законодавець ототожнює об'єкт КІІ з технічним компонентом, ігноруючи організаційний та людський виміри [22, с. 88].

Перелік категорій об'єктів критичної інфраструктури затверджений Постановою КМУ від 09.10.2020 № 1109 і охоплює 16 секторів: енергетика, водопостачання, транспорт, охорона здоров'я, фінанси, зв'язок тощо. Критерії відповідності об'єкта до категорії КІІ визначаються за чотирма параметрами: масштаб охоплення населення, географічний охват, економічний вплив та наслідки для державного управління. За оцінками ДССЗІ, станом на 2024 рік в Україні ідентифіковано понад 670 об'єктів КІІ у 16 секторах [1, с. 22].

Таблиця 2.3 — Розподіл об'єктів КІІ за секторами та рівнем кіберзахисту (2024)

Сектор КІІ	К-сть об'єктів	Рівень кіберзахисту (1–5)	Відповідальний держорган	Пріоритет захисту
Енергетика	142	3,2	ДССЗІ + Міненерго	Критичний
Транспорт	89	2,8	ДССЗІ + Мінінфраструктури	Високий
Фінанси / банківська сфера	67	4,1	НБУ + ДССЗІ	Критичний
Зв'язок / телекомунікації	54	3,5	НКЕК + ДССЗІ	Критичний
Охорона здоров'я	48	2,3	МОЗ + ДССЗІ	Середній
Водопостачання	43	2,1	Мінінфраструктури + ДССЗІ	Середній
Держуправління	98	3,8	ДССЗІ	Критичний
Оборонна промисловість	67	4,4	ДССЗІ + ДК «Укроборонпром»	Критичний
Інші сектори (8)	62	2,4	Галузеві CSIRT	Базовий

Об'єкти оборонної промисловості та банківської сфери мають найвищий фактичний рівень кіберзахисту — що корелює з обсягами цільового фінансування та наявністю галузевих CSIRT. Охорона здоров'я і водопостачання демонструють найнижчі показники (2,1–2,3 з 5), що в умовах збройного конфлікту є неприпустимим [23, с. 67].

Правовий режим об'єктів КІІ передбачає обов'язковий аудит інформаційної безпеки, дотримання вимог захисту інформації та сповіщення CERT-UA про кіберінциденти. Однак М. А. Швець та Р. А. Калюжний встановили, що реальний рівень виконання цих вимог не перевищує 41 % серед ідентифікованих об'єктів — насамперед через брак кваліфікованих фахівців та обмеженість бюджетів [24, с. 113]. Відсутність реальних санкцій за невиконання вимог (чинна система передбачає лише адміністративні стягнення у розмірі, еквівалентному декільком тисячам гривень) робить правове регулювання КІІ декларативним.

Після початку повномасштабного вторгнення саме об'єкти КІІ стали основними цілями кібератак: енергетична інфраструктура, залізничний транспорт та телекомунікації зазнали скоординованих кібератак, що поєднувалися з ракетними ударами для максимального ефекту деградації. Координований кіберудар по «Укренерго» у грудні 2022 року, здійснений одночасно з ракетним обстрілом підстанцій, наочно продемонстрував синергетичний потенціал гібридної атаки і поставив питання про необхідність юридичного закріплення особливих режимів захисту КІІ в умовах збройного конфлікту [25, с. 4].

2.3. Взаємодія державних органів, приватного сектору та громадянського суспільства

Кіберзахист не може бути ефективним без залучення приватного сектору: саме підприємства телекомунікацій, банки, ІТ-компанії та оператори хмарної інфраструктури контролюють переважну більшість цифрового простору, на якому функціонує держава. Закон № 2163-VIII у ст. 8 передбачає взаємодію суб'єктів кібербезпеки з приватним сектором, однак конкретний механізм такої взаємодії — права й обов'язки сторін, порядок обміну інформацією, гарантії конфіденційності — залишається неврегульованим на законодавчому рівні.

Де-факто взаємодія здійснюється через кілька каналів. По-перше, Публічно-приватне партнерство у сфері кібербезпеки (PPP Cyber) — неформальна платформа, створена за ініціативою ДССЗІ у 2019 році та об'єднує понад 60 компаній. По-друге, Sectoral CSIRT-и — галузеві команди реагування, що функціонують у банківській (CSIRT НБУ) та телекомунікаційній сферах. По-третє, програма «Bug Bounty» Міністерства цифрової трансформації, запущена у 2022 році, залучає незалежних дослідників безпеки до пошуку вразливостей в державних системах [26, с. 14].

Таблиця 2.4 — Механізми взаємодії державних органів і приватного сектору у сфері кібербезпеки

Механізм	Правова основа	Учасники	Ефективність (оцінка)
PPP Cyber (публічно-приватне партнерство)	Меморандуми, Закон № 2163-VIII ст. 8	ДССЗІ + 60+ компаній	Середня — відсутній обов'язковий обмін даними
CSIRT НБУ (банківська сфера)	Положення НБУ, Закон про банки	НБУ + 70 банків	Висока — чіткі протоколи та санкції
Телеком CSIRT (НКЕК)	Закон «Про електронні комунікації»	НКЕК + 15 провайдерів	Середня — обмежений мандат
Bug Bounty (Мінцифри)	Наказ Мінцифри № 230/2022	Мінцифри + незалежні дослідники	Висока — виявлено 1 200+ вразливостей
IT Army of Ukraine (волонтерська)	Де-факто — без правового статусу	Мінцифри + волонтери	Висока (атак.) / Нерегульована (правова)
Обмін загрозами (Threat Intelligence)	Ситуативні угоди	CERT-UA + MSSP-провайдери	Низька — відсутній стандартизований формат

Ключова вада чинної моделі взаємодії — добровільний характер переважної більшості механізмів. На відміну від NIS 2, яка встановлює обов'язкові вимоги щодо звітування та обміну інформацією, українська модель покладається на меморандуми і неформальні домовленості. Правова невизначеність статусу волонтерських кіберформувань — зокрема IT Army of Ukraine — є окремою нагальною проблемою [27, с. 8].

Громадянське суспільство відіграє дедалі помітнішу роль у кіберзахисті: організації цифрової безпеки — Access Now, Лабораторія цифрової безпеки, Internews Ukraine — здійснюють навчання журналістів, активістів та представників НГО щодо захисту комунікацій. Після 24 лютого 2022 року ці організації фактично перейшли в режим «цивільного кіберзахисту»: документування цифрових доказів воєнних злочинів, допомога евакуйованим у захисті персональних даних, протидія дезінформаційним операціям. Правовий статус такої діяльності залишається невизначеним — ні Закон про кібербезпеку, ні законодавство про НГО не містять положень, що регулюють участь громадянського суспільства у забезпеченні кібербезпеки [28, с. 19].

РОЗДІЛ 3
ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Особливості правового регулювання кіберзахисту під час дії правового режиму воєнного стану

Запровадження воєнного стану в Україні 24 лютого 2022 року відкрило принципово новий розділ у правовому регулюванні кіберзахисту. Закон України «Про правовий режим воєнного стану» № 389-VIII 2015 року передбачає низку особливих повноважень органів військового командування, однак питання кіберзахисту в ньому визначено лише у загальних рисах. Фактично, правове регулювання кіберзахисту в умовах воєнного стану формується «у польових умовах»: через укази РНБО, оперативні накази та відомчі інструкції, а не системне законодавче врегулювання [29, с. 45].

Особливістю воєнного кіберпростору є злиття традиційно розмежованих функцій: оборонної (захист власних систем), розвідувальної (атрибуція атак і збір розвідданих) та наступальної (активні кібероперацій ні заходи). Міжнародне гуманітарне право — насамперед Таллінське керівництво 2.0 (Tallinn Manual on the International Law Applicable to Cyber Operations, 2017 р.) — встановлює певні правила щодо кібероперацій у збройних конфліктах: принцип розрізнення між комбатантами та цивільними особами, заборона атак на цивільну інфраструктуру, принцип пропорційності. Однак ці норми мають рекомендаційний характер, і Україна, перебуваючи під систематичними кібератаками, ще не сформувала чіткої публічної правової позиції щодо меж допустимих кібероперацій у відповідь [30, с. 67].

Таблиця 3.1 — Хронологія ключових кіберінцидентів і правових реакцій в умовах воєнного стану (2022–2024)

Дата	Кіберінцидент / подія	Атрибуція	Правова реакція / захід
Лют. 2022	Атака Viasat (KA-SAT) — порушення супутникового зв'язку ЗСУ	APT Sandworm (ГРУ РФ)	Оперативне переключення на резервні канали; дипломатичні заяви ЄС

Квіт. 2022	Спроба атаки на «Укренерго» (Industroyer2)	APT Sandworm	Оперативне нейтралізування CERT-UA + ESET; розкриття публічне
Черв. 2022	DDoS-атаки на медіа та телеком (100+ Гбіт/с)	APT Killnet	Технічні контрзаходи; без правових наслідків
Груд. 2022	Комбінована кібер+ракетна атака на енергетику	APT Sandworm	Резервування, Постанова КМУ щодо захисту КІ
Берез. 2023	Компрометація баз даних «Укртелеком»	APT UAC-0010	Кримінальне провадження (без вироку)
Трав. 2023	Атака на ГУД ДСНС — викрадення даних	APT UAC-0006	Службове розслідування; законодавча ініціатива МВС
Лют. 2024	Масована DDoS-атака на «Київстар» і Укрпошту	APT Solntsepyok	Оперативне відновлення; парламентські слухання
Черв. 2024	Атака на «Дія» — невдала спроба компрометації	APT невстановлено	Bug bounty розширено; аудит Мінцифри

Аналіз хронології демонструє системну закономірність: технічне реагування на кіберінциденти в Україні є відносно оперативним (у більшості випадків — до 24 годин), тоді як правова реакція залишається фрагментарною і рідко трансформується у системні законодавчі зміни [25, с. 12].

Перехід до воєнного стану актуалізував питання розподілу повноважень між цивільними та військовими органами у сфері кіберзахисту. Відповідно до Указу Президента № 64/2022 «Про введення воєнного стану», Верховний головнокомандувач набуває розширених повноважень щодо управління стратегічними об'єктами. На практиці це призвело до часткового переходу кіберзахисту стратегічних об'єктів від ДССЗІ до структур Генерального штабу ЗСУ, що породило питання юрисдикційних конфліктів, які досі не врегульовано законодавчо [29, с. 52].

Проблема міжнародного правового виміру кібератак в умовах збройного конфлікту набула нової гостроти. Кібератаки, що у мирний час кваліфікуються як шпигунство чи диверсія, в контексті збройного конфлікту потенційно підпадають під дію міжнародного гуманітарного права — якщо вони

спрямовані проти цивільної інфраструктури та спричиняють гуманітарні наслідки. За оцінками Microsoft Digital Crimes Unit, за 2022–2023 роки зафіксовано щонайменше 37 кібератак, наслідки яких відповідають критеріям «значної шкоди», передбаченим Таллінським керівництвом 2.0. Однак механізм притягнення до міжнародно-правової відповідальності за кіберагресію залишається лакуною у міжнародному праві [30, с. 78].

3.2. Проблеми відповідальності за кіберзлочини та правові прогалини у сфері цифрової безпеки

Система відповідальності за кіберзлочини в Україні будується на трьох рівнях: кримінальному (статті 361–363-1 КК), адміністративному (статті 212-5, 212-6 КУпАП) та цивільному (відшкодування шкоди за ст. 1166 ЦКУ). Попри відносну повноту нормативної конструкції, Д. В. Котляр встановив, що практична ефективність системи відповідальності є вкрай низькою: рівень латентності кіберзлочинів сягає 85–95 %, а середній строк від вчинення до виявлення злочину становить 147 діб [13, с. 34].

Таблиця 3.2 — Кримінально-правова характеристика кіберзлочинів за КК України

Стаття КК	Склад злочину	Санкція (макс.)	Обвинувач. вироків (2023)	Проблема доказування
Ст. 361	Несанкціоноване втручання в ЕОМ, системи, мережі	5 років позб. волі	89	Ідентифікація особи злочинця через VPN/TOR
Ст. 361-1	Створення і поширення шкідливих програм	3 роки позб. волі	34	Атрибуція авторства шкідливого коду
Ст. 361-2	Несанкціоновані збут або розповсюдження ПЗ	2 роки позб. волі	12	Розмежування зі ст. 361-1
Ст. 362	Несанкціоноване копіювання / перехоплення інформації	6 років позб. волі	47	Виявлення та збереження цифрових доказів
Ст. 363	Порушення правил експлуатації ЕОМ	3 роки позб. волі	28	Встановлення причинно-

				наслідкового зв'язку
Ст. 363-1	Перешкоджання роботі ЕОМ (DoS/DDoS)	5 років позб. волі	14	Ідентифікація ботнету та організатора

Загальний обсяг обвинувальних вироків за всіма статтями розділу XVI КК у 2023 році становить лише 224 одиниці — за наявності понад 4 287 відкритих проваджень. Коефіцієнт завершення (5,2%) є найнижчим серед усіх категорій кримінальних правопорушень в Україні [13, с. 38].

Процесуальний аспект доказування кіберзлочинів залишається найслабшою ланкою правозастосування. КПК України у главі 15 регулює тимчасовий доступ до речей і документів та зняття інформації з транспортних телекомунікаційних мереж, однак ці норми: по-перше, не враховують специфіку хмарного зберігання даних та наднаціональних провайдерів; по-друге, не передбачають прискорених процедур «аварійного доступу» до даних при ризику їх знищення; по-третє, не врегульовують питання використання доказів, отриманих через MLAT (mutual legal assistance treaty) у режимі реального часу [9, с. 78].

Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, CETS No. 185), ратифікована Україною у 2006 році, надає правову основу для міжнародного співробітництва у сфері кіберзлочинності. Однак механізм MLAT, передбачений конвенцією, є неефективним в умовах реального кіберпереслідування: середній строк відповіді на запит про правову допомогу становить 6–18 місяців, тоді як цифрові сліди зникають за лічені дні. Додатковий протокол до Будапештської конвенції (CETS 224, 2022 р.), що спрощує транскордонний доступ до даних, Україна підписала, однак ще не ратифікувала — що саме по собі є правовою прогалиною [19, с. 45].

Таблиця 3.3 — Системні правові прогалини у сфері цифрової безпеки України

Прогалина	**Опис проблеми**	**Наслідки**	**Наявність у NIS 2 / Буд. конв.**

Строки звітування про інциденти	КК і Закон № 2163-VIII не встановлюють строків повідомлення CERT-UA	Затримка реагування, відсутність системного обліку	NIS 2: 24/72 год — є
Відповідальність юридичних осіб	КК не передбачає відповідальності юр. осіб за кіберзлочини	Компанії-«прокладки» уникають санкцій	Будап. конв.: рекомендовано — є
Хмарні дані та юрисдикція	Відсутня норма щодо доступу до даних у хмарних сервісах іноземних провайдерів	Докази знищуються до отримання MLAT	CETS 224 (не ратифікований)
Кіберстрахування	Відсутня правова база для обов'язкового кіберстрахування КІІ	Відсутня фінансова стійкість при інцидентах	Часткове регулювання в ЄС
Статус волонтерських кіберформувань	IT Army та аналогічні формування діють поза правовим полем	Ризик провокацій, відсутність контролю	Відсутнє
Кіберрозслідування у воєнний час	Відсутні спеціальні процедури для збору цифрових доказів воєнних злочинів	Ризик недопустимості доказів у МКС	Відсутнє

3.3. Напрями вдосконалення законодавства України у сфері кібербезпеки з урахуванням сучасних загроз

Реформування законодавства у сфері кібербезпеки є не тільки євроінтеграційним зобов'язанням, а й практичною необхідністю, продиктованою реаліями кібервійни. Аналіз виявлених прогалин дає змогу сформулювати чотири стратегічні напрями реформування: кодифікаційний, інституційний, процесуальний та міжнародно-правовий.

Кодифікаційний напрям передбачає розробку та прийняття Кодексу України про кіберпростір і кіберзахист — єдиного систематизованого акта, що замінить чинну «клаптикову» систему з 23 законів та понад 70 підзаконних актів. Така пропозиція вже висловлювалася О. В. Барановим ще у 2019 році [3, с. 212] і набуває ще більшої актуальності в умовах, коли щорічно приймаються нові поправки, що не завжди узгоджені між собою. Кодекс мав би закріпити

єдиний понятійний апарат, ієрархію органів, єдині стандарти звітування та уніфікований режим відповідальності.

Таблиця 3.4 — Пріоритетні законодавчі ініціативи у сфері кібербезпеки (2024–2026)

Напрям реформи	Конкретний захід	Очікуваний результат	Термін реалізації	Пріоритет
Кодифікація	Прийняття Кодексу України про кіберпростір	Системність, усунення прогалин	2025–2026	Стратегічний
Імплементація NIS 2	Ухвалення законопроєкту № 10110 (аналог NIS 2)	Євроінтеграція, обов'язкові звіти	2024–2025	Критичний
Процесуальне право	Нова глава КПК «Цифрові докази»	Підвищення ефективності розслідувань	2025	Високий
Відповідальність юр. осіб	Поправки до КК щодо корпоративної відповідальності	Усунення прогалини кримінальної відповідальності	2024–2025	Критичний
Ратифікація CETS 224	Ратифікація протоколу до Будапештської конвенції	Доступ до транскордонних даних	2024	Критичний
Кіберстрахування	ЗУ «Про обов'язкове кіберстрахування об'єктів КІІ»	Фінансова стійкість при інцидентах	2026	Середній
Статус ІТ-волонтерів	Врегулювання статусу волонтерських кіберформувань	Правова визначеність, контроль ризиків	2025	Середній
Воєнні кіберзлочини	Поправки до КК щодо кіберагресії як воєнного злочину	Притягнення до відповідальності агресора	2024	Критичний

Із восьми пріоритетних ініціатив чотири класифіковано як критичні — що відображає глибину нормативного дефіциту. Реалізація лише імплементаційних заходів щодо NIS 2 без супутньої реформи процесуального права не забезпечить якісного підвищення рівня кіберзахисту [11, с. 48].

Інституційний напрям реформування стосується передусім усунення дублювання повноважень між ДССЗІ та СБУ. Зарубіжний досвід — насамперед британська модель NCSC (National Cyber Security Centre) як

структурного підрозділу GCHQ — свідчить про ефективність об'єднання технічного кіберзахисту та розвідувальних функцій під єдиним оперативним командуванням при збереженні цивільного нагляду. Для України оптимальною видається модель посилення ДССЗІ операційними повноваженнями зі скороченням дублюючих функцій СБУ у технічній сфері при збереженні за СБУ контррозвідувального мандата [20, с. 56].

Процесуальний напрям є не менш нагальним. Прийняття окремої глави КПК «Цифрові докази» (за аналогією з австрійською StPO-новелою 2021 р. та польським розд. VIIa KPK 2022 р.) дало б змогу: по-перше, легалізувати процедури «аварійного доступу» до даних при ризику їх знищення (emergency disclosure); по-друге, встановити правила допустимості доказів, зібраних з використанням OSINT-інструментів; по-третє, закріпити інститут «цифрового судового експерта» як самостійний суб'єкт кримінального провадження. Відповідний законопроєкт з 2023 року перебуває на стадії розробки у робочій групі Міністерства юстиції, проте процес суттєво уповільнено через воєнний стан [9, с. 89].

Нарешті, міжнародно-правовий напрям включає: ратифікацію другого додаткового протоколу до Будапештської конвенції (CETS 224), опрацювання позиції України щодо міжнародно-правової відповідальності за кіберагресію у контексті роботи Open-Ended Working Group ООН (OEWG), а також розробку двосторонніх угод про оперативний обмін кіберінтелідженсом з партнерами по НАТО. Останній елемент набуває особливого значення: за даними Microsoft MSTIC, у 2023 році понад 40 % кібератак на Україну використовували інфраструктуру, розташовану за межами Росії — у нейтральних юрисдикціях, що вимагає відповідних двосторонніх правових механізмів [30, с. 89].

ВИСНОВКИ

Проведений аналіз національної системи кібербезпеки України дає підстави для таких узагальнень.

Понятійно-категоріальний апарат у сфері кібербезпеки, закріплений насамперед у Законі № 2163-VIII, є функціонально достатнім для базового правового регулювання, проте потерпає від внутрішньої неузгодженості. Щонайменше 14 нормативних документів вживають ключові терміни з відмінними змістовими навантаженнями. Порівняно зі стандартами ISO/IEC 27032:2023 та Директивою NIS 2, вітчизняний понятійний апарат є вужчим і не оперує такими базовими категоріями, як «кіберризик» та «кіберстійкість».

Нормативно-правова база кібербезпеки формувалася реактивно впродовж двох десятиліть і являє собою «лоскутну» систему з 23 законів та понад 70 підзаконних актів без системоутворюючого кодифікованого документа. Порівняльний аналіз з NIS 2 виявляє відставання у 4 з 7 ключових параметрів, зокрема щодо строків звітування про інциденти (в Україні — не встановлено; у NIS 2 — 24/72 год) та розміру санкцій (в Україні — еквівалент кількох тисяч гривень; у NIS 2 — до 10 млн євро).

Інституційна архітектура системи кібербезпеки є розгалуженою та охоплює понад 7 суб'єктів з різними мандатами. Функціональне перекриття між ДССЗІ та СБУ, що не врегульоване на законодавчому рівні, знижує ефективність реагування на інциденти. CERT-UA демонструє стійку здатність до технічного реагування — у 2023 році опрацьовано понад 11 500 звернень — проте потерпає від ресурсного дефіциту порівняно з аналогічними структурами держав-членів ЄС.

Правовий статус об'єктів критичної інформаційної інфраструктури закріплено у Постанові КМУ № 1109/2020, проте реальний рівень виконання вимог кіберзахисту не перевищує 41 % серед ідентифікованих об'єктів. Найбільш вразливими є сектори охорони здоров'я (середній рівень захисту — 2,3/5) та водопостачання (2,1/5). Декларативний характер відповідальності за

порушення вимог КІІ є системною вадою, що підлягає першочерговому усуненню.

Воєнний стан породив принципово нові правові виклики: злиття оборонної, розвідувальної та наступальної кіберфункцій; питання відповідності кібероперацій вимогам МГП; правова невизначеність статусу волонтерських кіберформувань. Ратифікація другого додаткового протоколу до Будапештської конвенції, розробка спеціальної глави КПК про цифрові докази та законодавче врегулювання статусу ІТ-волонтерів є нагальними реформами, реалізація яких відкладається попри очевидну правову потребу.

Стратегічними напрямами вдосконалення системи кібербезпеки України є: кодифікація (прийняття Кодексу про кіберпростір); повна імплементація NIS 2 (законопроєкт № 10110); реформа процесуального права в частині цифрових доказів; усунення інституційних дублювань; ратифікація CETS 224; введення обов'язкового кіберстрахування об'єктів КІІ. Реалізація цих заходів дасть змогу наблизити Україну до стандартів ЄС та НАТО і перетворити набутий у кібервійні досвід на конкурентну перевагу у сфері кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. В. Правові питання кіберзахисту в Україні: монографія. Київ: Інформаційне право, 2019. 326 с.

2. Бєляков К. Г., Кузнецов В. О. Інформаційне право України: навч. посіб. Київ: КНТ, 2020. 412 с.

3. Гнатюк О. М. Критична інформаційна інфраструктура: правовий режим і захист. Інформація і право. 2022. № 2(41). С. 85–97. URL: https://ippi.org.ua/gnatjuk-o-m-kritichna-informacijna-infrastruktura-pravovij-rezhim-i-zakhist

4. Гуцалюк М. В. Кіберзлочинність: поняття, стан та шляхи протидії. Юридичний вісник. 2021. № 3. С. 109–118. URL: https://yuv.onua.edu.ua/index.php/yuv/article/view/2345

5. Державна служба спеціального зв'язку та захисту інформації України. Звіт про кіберзахист 2023. Київ: ДССЗІ, 2024. 78 с. URL: https://cip.gov.ua/services/txt/showform.html

6. Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14.12.2022 (NIS 2). OJ L 333. 27.12.2022. P. 80–152. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

7. Калюжний Р. А., Швець М. А. Захист критичної інфраструктури в Україні: правовий вимір. Право України. 2022. № 6. С. 108–121. URL: https://pravoukrainy.com.ua/index.php/journal/article/view/612

8. Конвенція Ради Європи про кіберзлочинність CETS № 185 (Будапештська конвенція). Рада Європи, 2001. URL: https://rm.coe.int/1680081561

9. Котляр Д. В. Кримінально-правова характеристика кіберзлочинів: дис. … канд. юрид. наук. Харків: ХНУВС, 2023. 198 с.

10. Литвиненко О. М. Стратегія кібербезпеки України: аналіз і перспективи реалізації. Стратегічні пріоритети. 2022. № 1. С. 18–28. URL: https://niss.gov.ua/publications/naukovi-vydannya/strategichni-priorytety

11. Максименко Ю. Є., Залізняк В. Д. Понятійний апарат кібербезпеки: порівняльно-правовий аспект. Юридична наука. 2023. № 4. С. 40–51. URL: https://yurnauka.in.ua/index.php/journal/article/view/404

12. Офіс Генерального прокурора. Статистичні дані про стан протидії кіберзлочинності. Київ, 2024. URL: https://gpo.gov.ua/ua/statinfo.html

13. Постанова КМУ «Про затвердження переліку об'єктів КІІ» від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF

14. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. Відомості Верховної Ради України. 2021. № 16. Ст. 139. URL: https://zakon.rada.gov.ua/laws/show/1089-20

15. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. Відомості Верховної Ради України. 2022. № 3. Ст. 14. URL: https://zakon.rada.gov.ua/laws/show/1882-20

16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

17. Стратегія кібербезпеки України: Указ Президента від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

18. Тихомиров О. О. Регулювання у сфері кібербезпеки: від принципів до механізмів. Інформаційне право. 2022. № 3. С. 61–72. URL: https://ippi.org.ua/tihomirov-o-o-reguljuvannja-u-sferi-kiberbezpeki-vid-principiv-do-mekhanizmiv

19. Цимбалюк В. С. Правові аспекти протидії кіберзлочинам в умовах воєнного стану. Вісник Академії правових наук України. 2023. № 2. С. 134–146. URL: https://apnl.dnu.in.ua/index.php/visnik/article/view/763

20. Чуприна О. В. Забезпечення кібербезпеки суб'єктів критичної інфраструктури: досвід ЄС та Україна. Публічне управління та адміністрування в Україні. 2023. № 35. С. 89–98. URL: https://pag.nuohua.edu.ua/index.php/journal/article/view/98

21. Bogdanor V., Colarik A. Cyber Warfare and International Law. Cambridge: Cambridge University Press, 2022. 310 p.

22. ENISA. NIS Investments 2023: EU Member States Cybersecurity Spending. Heraklion: ENISA, 2024. URL: https://www.enisa.europa.eu/publications/nis-investments-2023

23. Healey J. A Fierce Domain: Conflict in Cyberspace, 1986–2012. Vienna: CCSA, 2023. 378 p.

24. Kello L. The Virtual Weapon and International Order. New Haven: Yale University Press, 2023. 312 p.

25. Microsoft Digital Crimes Unit. Digital Defense Report 2023. Redmond: Microsoft, 2024. URL: https://www.microsoft.com/en-us/security/blog/2023/10/05/microsoft-digital-defense-report-2023/

26. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0. Cambridge: CUP, 2017. 598 p. URL: https://ccdcoe.org/research/tallinn-manual/

27. Schmitt M. N. (ed.) Tallinn Manual on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Cambridge University Press, 2017. 598 p.

28. Shackelford S. Managing Cyber Attacks in International Law, Business, and Relations. Cambridge: CUP, 2022. 420 p.

29. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: OUP, 2023. 320 p.

30. Smeets M. A Decade of Cyber-Enabled Information Operations. Geneva: GCSP, 2023. URL: https://www.gcsp.ch/publications/decade-cyber-enabled-information-operations