УДК 351.861:004.056
DOI https://doi.org/10.32782/ln.2025.25.48

Колесник О.О.
аспірант
Науково-дослідний інститут публічного права

МІЖНАРОДНІ СТАНДАРТИ ТА УКРАЇНСЬКА ПРАКТИКА КІБЕРЗАХИСТУ: УРОКИ ВІЙНИ

Актуальність теми. Повномасштабна агресія проти України остаточно утвердила кіберпростір як самостійний театр сучасної війни, у межах якого поєднуються технічні операції, інформаційно-психологічні впливи та специфічні режими міжнародно-правової відповідальності держав і недержавних акторів. Хвилі спрямованих кібератак на органи державної влади, критичну інфраструктуру та бізнес набули системного характеру і стали інструментом гібридного тиску, що прямо корелює з ключовими індикаторами національної безпеки та стійкості держави [1; 7; 8]. За цих умов ефективність кіберзахисту визначається не поодинокими технологічними рішеннями, а узгодженістю трьох взаємозумовлених рівнів: (1) міжнародно-правові стандарти належної поведінки в кіберпросторі; (2) європейські регуляторні рамки ризик-менеджменту (насамперед NIS2) та інституційна підтримка ENISA і НАТО; (3) національна імплементація – норми, інституції, процедури реагування та відновлення, здатні працювати в режимі воєнного часу [17–20; 14–16].

Воєнний досвід 2022–2024 рр. продемонстрував необхідність переходу до ризик-орієнтованого регулювання для операторів критичних і важливих послуг, процедуризації публічної атрибуції інцидентів, формалізації міжвідомчої координації та сталої взаємодії держави з приватним сектором і міжнародними партнерами [3; 4; 5; 6; 11; 12; 13]. Саме інтеграція цих компонентів – від нормотворчості до операційних протоколів і кадрової спроможності – формує сучасну архітектоніку національного кіберзахисту, що відповідає євроатлантичним стандартам і вимогам безпекового середовища періоду війни.

Аналіз останніх досліджень і публікацій. У сучасній вітчизняній правовій науці проблематика кібербезпеки набуває системного характеру й розглядається на стику публічно-правової доктрини, безпекових студій та інформаційного права. Вагомий внесок у її розроблення зробили українські дослідники, які визначили ключові вектори еволюції правового регулювання у сфері національної та міжнародної кібербезпеки. Так, С. Мазепа обґрунтував сучасні виклики та напрями вдосконалення законодавства у сфері кіберзахисту [2]; А. Марущак розкрив правові засади реалізації Стратегії кібербезпеки України, акцентувавши увагу на механізмах її імплементації [3]; А. Лисеюк і Т. Свінцицька дослідили специфіку правового забезпечення кібербезпеки в умовах воєнного стану та євроінтеграції [4]; К. Петров проаналізував практику міжнародного співробітництва України у сфері кіберзахисту [5]; В. Тіщенко та Є. Логвиненко розкрили особливості правового режиму забезпечення кібербезпеки у період воєнного стану [6].

Соціально-правовий вимір кіберстійкості та її вплив на систему національної безпеки висвітлено у працях О. Крета та співавт., а також у дослідженнях О. Остапенка і П. Берназа [7; 8]. На мікрорівні поведінкові аспекти кіберзахисту, зокрема формування культури кібергігієни, розкрито у працях Я. Шестака [9]. Практичну основу воєнного досвіду відображають галузеві аналітичні огляди та комп-

лексне видання *Digital Security in Wartime*, що узагальнює найкращі практики кібероборони у період гібридної агресії [10; 13].

Нормативно-методологічне підґрунтя досліджень становлять міжнародно-правові акти: Будапештська конвенція Ради Європи про кіберзлочинність [14], документи ООН (OEWG 2021; APR 2024) [15; 16], директива NIS2 та *Cybersecurity Act* ЄС, а також керівні матеріали ENISA [17–19]. У контексті євроатлантичної інтеграції особливого значення набувають положення Політики кібероборони НАТО (2021) [20] та напрацювання провідних фахівців у галузі міжнародного права кіберпростору (Tallinn Manual 2.0, праці H. Koh, O. Hathaway, R. Crootof, M. Roscini, M. Finnemore, D. Hollis) [21–25].

Попри суттєвий поступ у нормативному та доктринальному осмисленні проблеми, відкритими залишаються низка питань, що мають як теоретичне, так і прикладне значення: визначення меж державного суверенітету та принципу невтручання у цифровому середовищі; конкретизація стандартів *due diligence*; розроблення процесуальних моделей публічної атрибуції кібератак; формування метрик результативності регулювання відповідно до вимог NIS2 та уточнення порядку нагляду і відповідальності операторів критичних послуг у національному праві [17; 21–25].

Метою статті є на підставі міжнародних стандартів (ООН, РЄ, ЄС, НАТО) та української практики воєнного часу здійснити узагальнення «уроків війни» для системи національного кіберзахисту й запропонувати концептуальні орієнтири подальшої імплементації: (а) ризик-орієнтоване регулювання і нагляд відповідно до NIS2; (б) процедуризація міжвідомчої координації та публічної атрибуції інцидентів; (в) інституціоналізація сталого обміну даними з міжнародними партнерами; (г) розвиток кадрової екосистеми та кібергігієни як елементів національної стійкості [1–6; 11–20; 21–25].

Виклад основного матеріалу.

1. Міжнародні стандарти кіберзахисту: еволюція норм і принципів

ООН: принципи поведінки держав і due diligence. Із середини 2010-х рр. напрацьована в межах ООН лінія узгоджених норм відповідальної поведінки держав у кіберпросторі отримала подальший розвиток у підсумковому звіті Відкритої робочої групи (OEWG, 2021), який підтвердив застосовність міжнародного права до ІКТ-середовища, а також наголосив на необхідності запобігання шкідливій діяльності проти критичної інфраструктури, обміну інформацією, підвищення прозорості та довіри [15]. Щорічне просування тематики у 2021–2024 рр. (Annual Progress Report 2024) фіксує поступовий консенсус щодо базових принципів, включно з повагою до суверенітету, невтручанням, недопустимістю застосування сили, а також із обов'язком держав вживати належних заходів (due diligence) для недопущення використання їхньої території як плацдарму кібератак проти інших держав [16]. У сукупності ці документи не лише кодифікують мінімальні стандарти поведінки, але й задають очікувані напрями національної імплементації: розвиток механізмів попередження, виявлення, обміну та допомоги, у тому числі на рівні національних CERT/CSIRT і контактних пунктів для інцидентів КІ [15; 16].

Міжнародне право: суверенітет, невтручання, заборона сили. У сучасній доктрині міжнародного права кіберпростору сформувалася концептуальна рамка, що спирається на фундаментальні норми Статуту ООН: принцип суверенної рівності держав, заборону погрози силою та її застосування, а також принцип невтручання у внутрішні справи. Застосування цих положень у цифровому середовищі набуло особливої актуальності у зв'язку з транснаціональним характером кібероперацій, складністю атрибуції та потенційним масштабом завданої шкоди. Гарольд Кох обґрунтовано наголосив на безпосередній дії міжнародного права у сфері кібе-

роперацій і необхідності переосмислення класичних принципів крізь призму технологічної специфіки сучасного середовища – транскордонності, анонімності суб'єктів, швидкості інформаційних процесів [22].

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations деталізував підстави, за яких втручання у інформаційні системи може розглядатися як порушення суверенітету або принципу невтручання, а також запропонував критерії оцінки порогів «використання сили» та «збройного нападу» у цифровому вимірі – з урахуванням характеру цілей, інтенсивності наслідків і контексту кіберінциденту [21]. О. Гетевей та Р. Крутоф, розвиваючи підходи до співвідношення норм *jus ad bellum* і *jus in bello* у кіберпросторі, акцентували на важливості вироблення уніфікованих доказових стандартів для атрибуції та пропорційності контрзаходів [23]. У цьому ж контексті М. Роскіні запропонував концепцію «функціональної еквівалентності» наслідків кібероперацій до кінетичних дій, доводячи, що виведення з ладу критичної інфраструктури – енергетики, транспорту чи систем охорони здоров'я – може мати юридичні наслідки, співмірні із застосуванням фізичної сили [24].

Проблематика «публічного приписування» (public attribution) отримала подальший розвиток у працях М. Фіннемор і Д. Голліса, які розкрили взаємозв'язок між прозорістю процесу атрибуції, легітимністю міжнародно-правової реакції та ефективністю режимів відповідальності держав [25].

У практичному вимірі це означає, що держави мають забезпечити наявність внутрішніх процедур правової кваліфікації кіберінцидентів (*legal review*), впровадити стандартизовані механізми публічної комунікації атрибуції та бути готовими до застосування міжнародно-правових інструментів реагування – дипломатичних демаршів, контрзаходів, а також взаємодопомоги в межах багатосторонніх механізмів [21–25].

Європейський Союз: NIS2 як еталон ризик-менеджменту; Cybersecurity Act і роль ENISA. ЄС інституціоналізував підхід «від принципів до спроможностей», перетворивши вимоги безпеки на обов'язкові управлінські практики для широкого кола суб'єктів. Директива NIS2 (2022) суттєво розширила перелік секторів і категорій операторів (essential/important entities), запровадила ризик-орієнтовані заходи (управління вразливостями, безперервність, ланцюги постачання), жорсткіші строки та процедури повідомлення про інциденти, а також уніфіковані підходи до нагляду і санкцій [17]. Cybersecurity Act (2019) закріпив постійний мандат ENISA та заснував загальноєвропейські рамки сертифікації безпеки ІКТ-продуктів і послуг, що створює спільний ринок довіри та підвищує порівнюваність рівнів захисту [18]. Керівництва ENISA щодо національних стратегій кібербезпеки (NCSS) слугують методичною «дорожньою картою» для держав-членів і партнерів: від визначення ролей і відповідальності, через побудову процесів управління ризиками, до індикаторів результативності та циклу перегляду політик [19]. Для України, що взяла курс на гармонізацію з acquis ЄС, NIS2/ENISA задають практичні стандарти для регуляторів і операторів послуг – від обов'язкових мінімальних вимог безпеки до аудиту, нагляду та персональної відповідальності менеджменту [11; 12; 17–19].

НАТО: кібероборона, партнерство, колективна відповідальність. Актуалізована Політика кібероборони НАТО (2021) закріплює кіберпростір як сферу операцій Альянсу, визнає можливість застосування положень статті 5 у разі кіберінциденту відповідного масштабу, підсилює механізми взаємної підтримки та спільної підготовки, а також акцентує на стійкості, обміні інформацією й протоколах взаємодії з приватним сектором та партнерами [20]. У практичній площині для держав-партнерів (зокрема України) це означає інкорпорацію сумісних процедур реагування, участь у навчаннях і розбудову інтероперабельності, що прямо

корелює з вимогами NIS2 та кращими практиками ENISA [5; 11; 12; 19; 20].

Будапештська конвенція: кримінально-правова база протидії кіберзлочинності. Конвенція Ради Європи про кіберзлочинність (2001) забезпечує уніфікацію складів кіберзлочинів, процесуальні інструменти збирання електронних доказів та канали міжнародної правової допомоги. Вона лишається ключовим «мінімальним стандартом» для гармонізації кримінального законодавства і практики транскордонного переслідування правопорушень у сфері ІКТ [14]. Для воєнного часу її значення лише посилюється, оскільки гібридні операції часто поєднують елементи державної активності з кримінальною діяльністю недержавних акторів, і саме інструментарій Конвенції дозволяє ефективніше працювати з доказами та взаємодіяти з іноземними юрисдикціями [8; 11; 14].

Еволюція міжнародних стандартів – від декларативних принципів ООН до регуляторних механізмів ЄС і оперативних рамок НАТО – сформувала принципову модель належної поведінки держав та операторів послуг у кіберпросторі. Водночас ці стандарти не є самодостатніми: вони вимагають гнучкої національної імплементації, що поєднує правові норми, інституційну спроможність і ризик-менеджмент на рівні конкретних організацій (операторів критичних і важливих послуг). Для України, яка діє в умовах триваючої війни, пріоритетами є: (1) повномасштабна гармонізація з NIS2 і впровадження методичних підходів ENISA; (2) інтероперабельність з механізмами НАТО; (3) використання Будапештської конвенції як процесуальної опори для транскордонних розслідувань; (4) інституціоналізація процедур правової оцінки, атрибуції та публічної комунікації інцидентів відповідно до доктрини міжнародного права та узгоджених норм ООН [11–21; 14–20; 22–25].

2. Українська система кіберзахисту: від нормативних основ до практики війни

Національна сучасна система кіберзахисту України сформувалася на базі Закону *«Про основні засади забезпечення кібербезпеки України»* та Стратегії кібербезпеки на 2021–2025 роки, що визначили засади державної політики, систему суб'єктів і механізми координації. Як зазначають С. Мазепа та А. Марущак, саме цей період ознаменував перехід від декларативного до функціонального підходу, коли кібербезпека стала складовою національної безпеки і політики оборони держави [2; 3]. У практичному вимірі, за даними IFES, ключовим кроком стало впровадження ризик-орієнтованого регулювання, орієнтованого на стандарти ЄС і вимоги директиви NIS2 [11; 12]. Під час воєнного стану система довела спроможність до оперативного реагування. Як відзначають В. Тіщенко та Є. Логвиненко, основна увага була зосереджена на забезпеченні безперервності управлінських процесів, захисті державних реєстрів і критичної інфраструктури, а також на розширенні повноважень органів безпеки у межах правового режиму війни [6]. Важливим координатором стала Державна служба спеціального зв'язку та захисту інформації, яка організовувала обмін інформацією, роботу урядової команди реагування CERT-UA та співпрацю з міжнародними партнерами [1]. Одночасно було посилено участь Служби безпеки України, Міністерства оборони, Національного банку та інших органів, що реалізують галузеві функції кіберзахисту [7; 8].

Євроінтеграційний курс визначає стратегічну рамку подальшого розвитку. Як слушно підкреслюють А. Лисеюк і Т. Свінцицька, гармонізація із NIS2 та впровадження європейських механізмів аудиту, сертифікації й нагляду є передумовою інтеграції України до спільного кіберпростору ЄС [4]. Сьогодні міжнародна співпраця набуває системного характеру: участь у кібернавчаннях і спільних ініціативах з ЄС та НАТО забезпечує уніфікацію процедур реагування і підвищує стійкість національних інституцій [5; 20]. Водночас у воєнний час особливого значення набули питання кадрової готовності та кібергігієни,

які, за спостереженням Я. Шестака, стали необхідною умовою функціональної безпеки органів державної влади [9].

Узагальнюючи, слід зазначити, що українська модель кіберзахисту еволюціонувала від нормативної систематизації до практичної реалізації європейських стандартів. Її стійкість забезпечується поєднанням правових основ, інституційної координації та міжнародної інтеграції, що дозволило у воєнний період зберегти керованість, оперативність і довіру партнерів [1–6; 9; 11–13; 17–20].

3. Уроки війни: практика, ризики, кібергігієна

Воєнний досвід засвідчив якісну зміну профілю загроз: поряд із масованими DDoS, фішингом та зловмисними кампаніями проти публічних реєстрів і КІ зросла частка комбінованих операцій із використанням соціальної інженерії та ланцюгів постачання; ці тенденції відображено у галузевих оглядах за 2021–2023 рр. і узагальненнях практик воєнного часу [10; 13]. Ефективне реагування забезпечувалося там, де вибудувано постійні канали обміну даними та чітку рольову модель «держава–оператор–постачальник» (індикатори компрометації, playbooks, тестування відновлення), що відповідає підходам ризик-менеджменту, рекомендованим IFES та європейськими керівництвами [11; 12; 19]. Критичною умовою стало «заздалегідь узгоджене» партнерство з приватним сектором: спільні навчання, швидка передача технічних артефактів, відпрацьовані процедури інцидент-репортингу [13; 11].

Людський чинник виявився вирішальним: мінімізація успішних атак корелює з упровадженням базових практик кібергігієни (MFA, політики доступів, сегментація, резервування, дисципліна оновлень), що підтверджено як практичними кейсами, так і академічними висновками щодо освіти та поведінкових стандартів (Шестак) [9; 10; 13]. На правовому рівні режим воєнного стану вимагав оперативних процедур реагування, але з дотриманням принципу пропорційності та захисту даних; відповідні акценти щодо меж повноважень та процесуальних гарантій обґрунтовано у Лисеюк і Свінцицької та у Тіщенка і Логвиненка [4; 6]. Для бізнесу та операторів критичної інфраструктури ключовими стали управління ризиками ланцюгів постачання, аудит готовності, уніфікація процесів інцидент-менеджменту й узгодження з вимогами NIS2/ENISA, що випливає з аналітики IFES і практичних рекомендацій воєнного періоду [11; 12; 17–19; 13]. Узгоджена міжнародна взаємодія (ЄС/НАТО) підвищила інтероперабельність та пришвидшила обмін технічною інформацією, що напряму вплинуло на стійкість до складних багатовекторних атак [5; 20].

Війна підтвердила потребу у «повному циклі» кіберстійкості: від індивідуальної кібергігієни та підготовленості персоналу – до методично оформлених процесів управління ризиками на рівні організацій та інституційної координації держави з міжнародними партнерами. Саме поєднання практик оперативного обміну, правових процедур воєнного часу, євроінтеграційних стандартів NIS2/ENISA та регулярних навчань забезпечує відтворювану здатність системи протистояти загрозам і відновлюватися після інцидентів [4–6; 10–13; 17–20].

Висновки. Узагальнюючи результати дослідження, слід констатувати, що війна стала каталізатором становлення в Україні повноцінної моделі кіберзахисту, інтегрованої у систему євроатлантичних стандартів. Міжнародні норми (ООН, РЄ, ЄС, НАТО) задали нормативно-правову рамку відповідальної поведінки держав і операторів у кіберпросторі, а національна практика довела ефективність їх гнучкої імплементації в умовах гібридної агресії. Поєднання ризик-орієнтованого регулювання за NIS2, процедур правової атрибуції, інституційної координації органів влади та розвитку кібергігієни як складової національної стійкості забезпечує не лише оперативне реагування на загрози, а й формує стратегічну спроможність держави діяти проактивно у гло-

бальному цифровому середовищі. Подальший розвиток системи кібербезпеки України має ґрунтуватися на методичній сумісності з європейськими механізмами сертифікації, постійному обміні даними з партнерами та формуванні кадрової екосистеми, здатної підтримувати сталу кіберстійкість суспільства і держави.

Анотація

Статтю присвячено комплексному теоретико-правовому аналізу міжнародних стандартів кіберзахисту та особливостей їх імплементації в Україні в умовах воєнного стану. Показано, що формування ефективної системи кібербезпеки є складовою національної безпеки держави й невід'ємним чинником її цифрового суверенітету. Встановлено, що розвиток правового регулювання у сфері кіберзахисту зумовлений потребою гармонізації національного законодавства з актами Європейського Союзу, рекомендаціями НАТО та загальновизнаними нормами міжнародного права. Розкрито еволюцію нормативних підходів – від принципів відповідальної поведінки держав, закріплених у документах ООН, до ризик-орієнтованого регулювання, сертифікації та управління кіберризиками відповідно до положень Директиви NIS2, Регламенту Cybersecurity Act і методичних документів ENISA. Методологічну основу дослідження становлять системно-структурний, порівняльно-правовий та інституційний підходи, що дали змогу зіставити міжнародні стандарти з українською практикою та визначити тенденції її подальшого розвитку. Обґрунтовано, що сучасна модель національного кіберзахисту інтегрує правові, організаційні й технологічні засоби реагування на кіберзагрози, забезпечує міжвідомчу координацію й ефективну взаємодію держави з приватним сектором. Зроблено висновок, що війна стала каталізатором становлення в Україні повноцінної моделі кіберзахисту, інтегрованої у систему євроатлантичних стандартів. Міжнародні норми (ООН, РЄ, ЄС, НАТО) задали нормативно-правову рамку відповідальної поведінки держав і операторів у кіберпросторі, а національна практика довела ефективність їх гнучкої імплементації в умовах гібридної агресії. Поєднання ризик-орієнтованого регулювання за NIS2, процедур правової атрибуції, інституційної координації органів влади та розвитку кібергігієни як складової національної стійкості забезпечує не лише оперативне реагування на загрози, а й формує стратегічну спроможність держави діяти проактивно у глобальному цифровому середовищі. Подальший розвиток системи кібербезпеки України має ґрунтуватися на методичній сумісності з європейськими механізмами сертифікації, постійному обміні даними з партнерами та формуванні кадрової екосистеми, здатної підтримувати сталу кіберстійкість суспільства і держави.

Ключові слова: кібербезпека, національна безпека, міжнародні стандарти, кібероборона, воєнний стан, кібергігієна, кіберстійкість.

Kolesnyk O.O. International standards and Ukrainian cyber defense practice: lessons from war

Summary

The article is devoted to a comprehensive theoretical and legal analysis of international standards of cyber security and the features of their implementation in Ukraine under martial law. It is shown that the formation of an effective cybersecurity system is a component of the national security of the state and an integral factor of its digital sovereignty. It is established that the development of legal regulation in the field of cyber security is due to the need to harmonize national legislation with the acts of the European Union, NATO recommendations and generally recognized norms of international law. The evolution of regulatory approaches is revealed - from the principles of responsible behavior of states, enshrined in UN documents, to risk-oriented regulation, certification and management

of cyber risks in accordance with the provisions of the NIS2 Directive, the Cybersecurity Act Regulation and ENISA methodological documents. The methodological basis of the study is the system-structural, comparative-legal and institutional approaches, which made it possible to compare international standards with Ukrainian practice and determine the trends of its further development. It is substantiated that the modern model of national cyber defense integrates legal, organizational and technological means of responding to cyber threats, ensures interagency coordination and effective interaction of the state with the private sector. It is concluded that the war became a catalyst for the formation of a full-fledged model of cyber defense in Ukraine, integrated into the system of Euro-Atlantic standards. International norms (UN, CoE, EU, NATO) set the regulatory and legal framework for responsible behavior of states and operators in cyberspace, and national practice has proven the effectiveness of their flexible implementation in conditions of hybrid aggression. The combination of risk-oriented regulation under NIS2, legal attribution procedures, institutional coordination of authorities and the development of cyber hygiene as a component of national resilience provides not only an operational response to threats, but also forms the strategic ability of the state to act proactively in the global digital environment. Further development of Ukraine's cybersecurity system should be based on methodological compatibility with European certification mechanisms, constant data exchange with partners, and the formation of a human resources ecosystem capable of supporting sustainable cyber resilience of society and the state.

Key words: cybersecurity, national security, international standards, cyber defence, martial law, cyber hygiene, cyber resilience.

Список використаних джерел:

1. Державна служба спеціального зв'язку та захисту інформації України. Національна система кібербезпеки функціонуватиме ефективніше. – 2023. URL: https://cip.gov.ua/ua/news/nacionalna-sistema-kiberbezpeki-funkcionuvatime-efektivnishe
2. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства.* 2025. № 2(42). С. 164–172.
3. Марущак А. І. Стратегія кібербезпеки України: правові засади та механізми реалізації. *Вісник Національного університету «Львівська політехніка».* 2024. № 2(38). С. 112–119.
4. 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
5. Петров К. М. Міжнародне співробітництво у сфері кібербезпеки: український досвід. *Актуальні проблеми міжнародних відносин.* 2023. Вип. 157. С. 92–105.
6. Тіщенко В. О., Логвиненко Є. С. Правові засади забезпечення кібербезпеки в умовах воєнного стану. *Протидія кіберзлочинності та торгівлі людьми.* : зб. матеріалів міжнар. наук.-практ. конф. Харків : Харківський національний університет внутрішніх справ, 2023. С. 71–74.
7. Крет О., Крет Р., Кундеус О. Cybersecurity System as a Component of National Security. *Грані.* 2024. Т. 27, № 5. С. 134–142.
8. Остапенко О. В., Берназ П. С. Кіберзлочинність як загроза національній безпеці України. *Науковий вісник Національної академії внутрішніх справ.* 2024. № 1(130). С. 78–86.
9. Шестак Я. І. Кібергігієна в 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.

10. Найпопулярніші види кібератак у 2021. URL: https://10guards.com/ua/articles/the-most-common-types-of-cyber-attacks-in-2021/
11. IFES Ukraine. *Ukraine Cybersecurity Legal Framework: Overview and Analysis.* Kyiv : IFES, 2021. 47 p. URL: https://ifesukraine.org/wp-content/uploads/2021/04/IFES-Ukraine-Cybersecurity-Legal-Framework.pdf
12. IFES Ukraine. *Cybersecurity in Ukraine: Legal Framework Analysis.* – Kyiv : IFES, 2024. 156 p.
13. Thompson, M., Kovalenko, O. (eds.) *Digital Security in Wartime: Ukrainian Experience and International Best Practices.* – Kyiv : Digital Ukraine Institute, 2024. 289 p.
14. Budapest Convention on Cybercrime (ETS No. 185). Council of Europe, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
15. United Nations. *Final Report of the Open-ended Working Group on Security of and in the Use of ICTs (OEWG).* New York : United Nations, 2021URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/067/22/PDF/N2106722.pdf
16. United Nations. *OEWG Annual Progress Report 2024.* New York : United Nations, 2024. URL: https://documents.un.org
17. 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 (NIS2 Directive). *Official Journal of the European Union.* – L 333/80, 27.12.2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
18. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act). *Official Journal of the European Union.* – L 151/15, 07.06.2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881
19. ENISA. *National Cyber Security Strategies: Practical Guide on Development and Execution.* – Heraklion : European Union Agency for Cybersecurity (ENISA), 2016. URL: https://www.enisa.europa.eu/publications/ncss-good-practice-guide
20. NATO. *Cyber Defence Policy 2021.* – Brussels : NATO, 2021. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm
21. Schmitt, M. N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge : Cambridge University Press, 2017. 598 p.
22. Koh, H. H. International Law in Cyberspace. *Harvard International Law Journal (Online Symposium).* 2012. Vol. 54. P. 1–12. URL: https://harvardilj.org/2012/12/online-54-koh/
23. Hathaway, O. A., Crootof, R. International Law and the Future of Cyberspace // *Yale Law Journal.* 2022. Vol. 132. P. 215–259.
24. Roscini, M. *Cyber Operations and the Use of Force in International Law.* – Oxford : Oxford University Press, 2014. 328 p.
25. Finnemore, M., Hollis, D. B. Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. *European Journal of International Law.* 2020. Vol. 31, No. 3. P. 961–989. https://doi.org/10.1093/ejil/chaa052.