КИЇВСЬКИЙ УНІВЕРСИТЕТ ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ

Кафедра міжнародного та приватного права

КВАЛІФІКАЦІЙНА РОБОТА

за темою:

«МІЖНАРОДНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

Виконала:
здобувачка 2 курсу, групи ММ-21з
спеціальності 293 «Міжнародне право»
Бабенко Єлизавета Костянтинівна

Науковий керівник:
Пилипенко Володимир Пилипович
доктор юридичних наук, доцент, кафедри
міжнародного та приватного права
Робота допущена до захисту в ЕК
«__»_____2026р.

В.о. завідувач кафедри міжнародного та
приватного права,
Чернега Віталій Миколайович,
доктор юридичних наук, професор

КИЇВ-2026 р.

АНОТАЦІЯ

Бабенко Є. К. Міжнародно-правове забезпечення інформаційних технологій

Кваліфікаційна робота здобувача другого (магістерського) рівня вищої освіти містить 3 розділи, 9 підрозділів; її загальний обсяг 111 сторінок, включно зі списком використаних джерел, який містить 101 найменування.

Об'єктом дослідження є міжнародно-правові відносини, що пов'язані з інформаційними технологіями.

Предметом дослідження є міжнародно-правове забезпечення інформаційних технологій.

Мета кваліфікаційної роботи полягає в дослідженні міжнародно-правового забезпечення інформаційних технологій.

Методологічну основу кваліфікаційної роботи формують теоретичні, емпіричні, історичні, математична статистика, індукції та дедукції, формально-юридичний (догматичний), порівняльно-правовий аналіз, правове прогнозування, які задіяні в трьох розділах.

Стислий опис результатів кваліфікаційної роботи: в першому розділі кваліфікаційної роботи висвітлено теоретично-правові засади міжнародно-правового забезпечення інформаційних технологій. Розглянуто та проаналізовано поняття, ознаки, види інформаційних технологій, становлення міжнародно-правового регулювання та застосовні у цій сфері принципи міжнародного права. В другому розділі висвітлено міжнародно-правові механізми регулювання забезпечення інформаційних технологій. Розкрито роль міжнародних організацій та співробітництва у сфері кібербезпеки, механізми міжнародно-правового захисту персональних даних, приватності та цифрових прав. В третьому розділі окреслено перспективи розвитку міжнародно-правового забезпечення інформаційних технологій. Охарактеризовано міжнародно-правове регулювання штучного інтелекту, великих даних, цифрових платформ та інформаційні технології в міжнародній безпеці.

Практичне значення отриманих результатів кваліфікаційної роботи. Здобутки, втілені в ній, можуть бути використаними в різних сферах: в міжнародному праві (для формування нових досліджень за даною сферою); в практичній сфері вищої освіти та правозастосовній діяльності, як навчальні матеріали щодо практичної оцінки відповідних позицій.

Ключові слова: міжнародне право, національне право, кібербезпека, інформаційні технології, протидія кіберзлочинності, міжнародні організації, приватність, цифрові права людини, захист персональних даних, збройні конфлікти, загрози міжнародній безпеці.

ABSTRACT

Babenko Yelyzaveta International Legal Framework for Information Technology

The qualification work of an applicant for the second (master's) level of higher education contains 3 sections, 9 subsections; its total volume is 111 pages, including the list of sources used, which contains 101 items.

The object of the study is international legal relations related to information technologies.

The subject of the study is the international legal support of information technologies.

The purpose of the qualification work is to study the international legal support of information technologies.

The methodological basis of the qualification work is formed by theoretical, empirical, historical, mathematical statistics, inductions and deductions, formal-legal (dogmatic), comparative-legal analysis, and legal forecasting, which are involved in three sections.

A brief description of the results of the qualification work: the first section of the qualification work highlights the theoretical and legal foundations of international legal support for information technologies. The concepts, characteristics, types of information technologies, the formation of international legal regulation, and the principles of international law applicable in this area are considered and analyzed. The second section highlights international legal mechanisms for regulating the provision of information technologies. The role of international organizations and cooperation in the field of cybersecurity, mechanisms for international legal protection of personal data, privacy, and digital rights are revealed. The third section outlines the prospects for the development of international legal support for information technologies. The international legal regulation of artificial intelligence, big data, digital platforms, and information technologies in international security is characterized.

The practical significance of the obtained results of the qualification work. The achievements embodied in it can be used in various areas: in international law (to form new research in this area); in the practical sphere of higher education and law enforcement activities, as training materials for the practical assessment of relevant positions.

Keyword: international law, national law, cybersecurity, information technology, countering cybercrime, international organizations, privacy, digital human rights, personal data protection, armed conflicts, threats to international security.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 5
ВСТУП 6
РОЗДІЛ 1 9
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ МІЖНАРОДНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ 9
1.1 Поняття, ознаки та види інформаційних технологій у сучасному міжнародному праві 9
1.2 Становлення міжнародно-правового регулювання інформаційних технологій 18
1.3 Принципи міжнародного права у сфері використання інформаційних технологій 27
Висновки до розділу 1 35
РОЗДІЛ 2 36
МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ 36
2.1 Роль ООН, Ради Європи, Європейського Союзу та інших міжнародних організації у сфері інформаційних технологій 36
2.2 Міжнародно-правовий захист персональних даних, приватності та цифрових прав людини 43
2.3 Міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинності 58
Висновки до розділу 2 65
РОЗДІЛ 3 66
ПЕРСПЕКТИВИ РОЗВИТКУ МІЖНАРОДНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ 66
3.1 Правове регулювання штучного інтелекту, великих даних та цифрових платформ у міжнародному праві 66
3.2 Інформаційні технології в умовах збройних конфліктів та загроз міжнародній безпеці 74
3.3 Перспективи вдосконалення міжнародно-правового регулювання інформаційних технологій в Україні та світі 83
Висновки до розділу 3 93
ВИСНОВКИ 94
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 97
ДОДАТКИ 109

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

США – Сполучені Штати Америки

ЗМІ – Засоби масової інформації

НАТО - Організація Північноатлантичного договору

ООН – Організація Об’єднаних Націй

ЄС – Європейський Союз

КНР – Китайська Народна Республіка

ШОС (Шанхайська організація співробітництва)

AI - штучний інтелект

ШІ – штучний інтелект

LLM – мовні моделі

ІТ – інформаційні технології

АЕС – атомна електростанція

ECCC - Європейський центр компетенцій з кібербезпеки

HADEA - Європейське виконавче агентство з питань охорони здоров’я та цифрових технологій

EIT - Європейський інститут інновацій та технологій

IFIP - Міжнародна федерація з обробки інформації

ВОІВ - Всесвітня організація інтелектуальної власності

ITU - Міжнародний союз електрозв'язку

GDPR - Загальний регламент захисту даних Європейського Союзу

ЄСПЛ - Європейського суду з прав людини

EDPB - Європейська рада із захисту даних

EDPS - Європейський наглядач із захисту даних

OSCE - Організації з безпеки і співробітництва в Європі

ЄКПЛ - Європейської конвенції з прав людини

NATO CCDCOE - Об’єднаний центр передових технологій з кібероборони НАТО

ВСТУП

Актуальність теми. У сучасному інформаційному суспільстві міжнародно-правове забезпечення інформаційних технологій є одним з напрямків, який стрімко розвивається та є одним з найбільш не врегульованих законодавчо. Міжнародне право намагається адаптувати існуючі норми до нових реалій цифрового простору, враховуючи специфіку галузі.

Тому ступінь сучасного стану дослідження полягає в відсутності єдиного уніфікованого міжнародно-правового забезпечення у сфері інформаційних технологій. Водночас це призводить до фрагментації підходів різних держав на тлі появи нових глобальних загроз: кібератак, інформаційних воєн, порушень приватності та конфіденційності, викликів щодо правових механізмів взаємодії, захисту даних, попередження кіберзлочинів, а також недостатній визначеності ролі міжнародних організацій у регулюванні та контролі інформаційних технологій в цілому.

Об’єкт дослідження: міжнародно-правові відносини, що пов’язані з інформаційними технологіями.

Предмет дослідження: є міжнародно-правове забезпечення інформаційних технологій.

Мета дослідження: полягає в дослідженні міжнародно-правового забезпечення інформаційних технологій.

Завдання дослідження:

1. Проаналізувати поняття, ознаки та види інформаційних технологій у сучасному міжнародному праві.
2. Дослідити становлення міжнародно-правового регулювання інформаційних технологій.
3. З’ясувати принципи міжнародного права у сфері використання інформаційних технологій.

4. Встановити роль ООН, Ради Європи, Європейського Союзу та інших міжнародних організації у сфері інформаційних технологій.
5. Дослідити міжнародно-правовий захист персональних даних, приватності та цифрових прав людини.
6. Визначити міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинності.
7. Провести аналіз правового регулювання штучного інтелекту, великих даних та цифрових платформ у міжнародному праві.
8. Проаналізувати інформаційні технології в умовах збройних конфліктів та загроз міжнародній безпеці.
9. Дослідити перспективи вдосконалення міжнародно-правового регулювання інформаційних технологій в Україні та світі.
10. Підвести підсумки проведеного дослідження та сформувати висновки.

Методи дослідження: застосовано 8 методів, які формують дослідження: теоретичні – використано для аналізу наукових досліджень та міжнародно-правових норм; емпіричні – використано для порівняння міжнародно-правових норм; історичні – використано для аналізу становлення міжнародно-правового регулювання; індукції та дедукції – використано для узагальнення дослідження; математичної статистики – використано для аналізу міжнародно-правової інформації; формально-юридичний (догматичний) – використано для виявлення формального змісту міжнародно-правових норм; порівняльно-правовий аналіз – використано для аналізу міжнародно-правових норм; правове прогнозування – використано для прогнозування подальшого розвитку міжнародно-правових норм правового забезпечення в ІТ.

Інформаційна база дослідження: складається з наукових досліджень таких науковців (Бабенко В.В., Бабенко Є.К., Бабенко К.М., Форманюк В.В., Деркач В.Г., Прокопович-Ткаченко Є.Д., Руденко Є.Г., Прохазка Г.А., Корольова В.В., Чорна В.О., Пазюк А.В.), нормативної бази міжнародного та національного права в галузі інформаційних технологій, які стосуються її міжнародно-правового забезпечення.

Наукова новизна одержаних результатів дослідження: полягає в тому, що в даній кваліфікаційній роботі вперше комплексно проаналізовано теоретичні аспекти, пов’язані з міжнародно-правовим та національним забезпеченням у сфері інформаційних технологій. Розкрито основні правові засади, наведено виклики та окреслено загальні перспективи.

Практичне значення одержаних результатів дослідження: полягає у використанні в освітньому середовищі (проведення дисциплін, розробці навчальних матеріалів або курсів), для фахівців з права або фахівців у сфері інформаційних технологій.

Апробація та публікація результатів дослідження: під час навчання та проведення кваліфікаційної роботи магістра прийнято участь у низці наукових заходів та опубліковано наукові роботи в збірниках наукових конференцій (Апробація відображена в списку використаних джерел за номерами з 2 по 15): «Правові аспекти імплементації інформаційних систем в умовах євроінтеграції» (с. 16 – 18) в збірнику VIII Міжнародної науково-практичної конференції «Реалії та перспективи розбудови правової держави в Україні та світі» (м.Київ, 12-13 травня 2025 року). «Етичні норми використання штучного інтелекту в контексті бізнесу» (с. 324 – 327) в збірнику Міжнародної науково-практичної конференції «Синергія інновацій: політика, економіка та менеджмент в цифровому світі» (18 квітня 2025 року).

Додатково, паралельно з проведенням дослідження, було підвищено кваліфікацію та отримано нові навички за допомогою: курсів (Prometheus, Web of Science Academy), навчальних проєктів (Erasmus напрямок Жанн Моне), тренінгів, наукових конференцій, вебінарів (Clarivate Essential, УГСПЛ) на яких було отримано сертифікати, як підтвердження про участь.

Структура та обсяг кваліфікаційної роботи: складається зі вступу, трьох розділів, дев’яти підрозділів, висновків, списку використаних джерел, який містить 101 найменувань. Загальна кількість 111 сторінок, з яких основний тексту складає 91 сторінку.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ МІЖНАРОДНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1 Поняття, ознаки та види інформаційних технологій у сучасному міжнародному праві

Інформаційні технології варто вважати поняттям динамічним та багатогранним, яке в сучасному міжнародному праві не має єдиного універсального трактування, але є ключовим елементом глобального інформаційного суспільства [20; 23].

Водночас у широкому розумінні інформаційні технології являють собою сукупність методів, засобів і способів збору, накопичення, обробки, передачі, зберігання та використання інформації за допомогою технічних пристроїв і програмного забезпечення [18; 27].

Згідно з національними стандартами України та міжнародними підходами, інформаційні технології включають процеси та інструменти, що забезпечують роботу з даними в електронному вигляді [19].

Окрім того, ЮНЕСКО підкреслює суттєвість ролі у формуванні інформаційного суспільства, де технології стають основою економіки, управління та комунікацій [70].

У контексті міжнародного інформаційного права інформаційні технології розглядаються як комплексна категорія, охоплюючи технічні засоби, транснаціональні інформаційні потоки та правовідносини в кіберпросторі.

Міжнародне інформаційне право, в свою чергу, трактує інформаційні технології як предмет правового регулювання, поєднуючий в комплексі публічно-правові (безпека, суверенітет держав) та приватно-правові (захист даних, інтелектуальна власність) аспекти [23; 26].

Більш широкого поширення термін «інформаційні технології» набув наприкінці двадцятого століття у зв'язку з розвитком комп'ютерної техніки та

на той час так званих телекомунікаційних систем (наразі формулювання було замінено на законодавчому рівні на комунікаційні). Водночас у загальному розумінні інформаційні технології являють собою «сукупність методів, процесів, програмно-технічних засобів і комунікаційних мереж, що використовуються для отримання, обробки, накопичення, зберігання, пошуку та поширення інформації» [67, с.5].

Відповідно до положень Закону України «Про Національну програму інформатизації», інформаційна технологія визначається як «цілеспрямована організована сукупність інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки інформації та доступ до джерел даних» [39].

Однак, у міжнародно-правовому аспекті цього періоду інформаційні технології розглядаються не лише як технічний інструмент, але й як об'єкт правового регулювання. Їх використання, зокрема, безпосередньо впливає на реалізацію прав людини, функціонування міжнародних організацій, забезпечення міжнародної безпеки та розвиток міжнародного співробітництва.

Глобальне поширення мережі Інтернет, в свою чергу, стало важливим етапом розвитку інформаційних технологій і самого поняття в цілому. За даними низки джерел міжнародних організацій, слід зазначити, що кількість користувачів мережі Інтернет перевищує п'ять мільярдів осіб, що становить більше половини населення планети [1].

Водночас, вищезазначене свідчить про формування глобального інформаційного простору, який не має державних кордонів та потребує належного міжнародно-правового регулювання та розвиток структури поняття, тому що інформаційні технології в умовах сучасності застосовуються практично у всіх сферах суспільного життя: державному управлінні, митній галузі, міжнародній дипломатії, освіті (зокрема у вишій освіті), медицині, банківській діяльності, електронній комерції, оборонній сфері, діяльності

міжнародних організацій [2; 6; 7; 13]. ІТ-консалтинг, в свою чергу, слід розглядати як конструктивний елемент взаємодії [14].

Хоча важливу роль інформаційні технології відіграють саме у міжнародних відносинах. Сучасна дипломатія активно використовує цифрові платформи для проведення переговорів, обміну інформацією та координації міжнародного співробітництва. Поширення електронного документообігу сприяє підвищенню ефективності діяльності міжнародних організацій, державних установ та автоматизації процесів [15].

Додатково також варто звернути увагу, що на початку двадцять першого століття трактування «інформаційні технології» ототожнювали переважно з «комп'ютерними системами» та «телекомунікаціями», але в умовах сьогодення поняття значно розширилося і включає: штучний інтелект, хмарні технології, блокчейн, Інтернет речей, мережі 5G/6G, квантові обчислення та інші складові [10]. Така еволюція вимагає від міжнародного права докорінної гнучкості та технологічної нейтральності норм.

Водночас для повного розуміння сутності інформаційних технологій необхідно визначити їх характерні ознаки.

В якості першої ознаки слід розглянути інформаційну спрямованість, основна сутність якої полягає в тому, що головним об'єктом впливу інформаційних технологій виступає інформація, незалежно від форми її подання. У процесі функціонування інформаційних систем здійснюються операції зі збору, зберігання, обробки та передачі даних [20].

Другою ознакою є автоматизація інформаційних процесів, тобто використання сучасних програмно-технічних засобів, що дозволяє значною мірою мінімізувати участь людини в обробці великих обсягів інформації.

Третьою ознакою виступає інтегрованість. Сучасні інформаційні технології забезпечують взаємодію різних інформаційних систем, баз даних та комунікаційних мереж у межах єдиного інформаційного простору.

Четвертою ознакою є глобальність. Завдяки мережі Інтернет інформаційні ресурси стали доступними незалежно від географічного

розташування користувачів. Це створює нові можливості для міжнародного співробітництва та одночасно породжує нові виклики для міжнародного права.

П'ятою ознакою є інноваційність. Інформаційні технології постійно вдосконалюються, що обумовлює необхідність регулярного оновлення правового регулювання.

Шостою ознакою є транскордонний характер інформаційних потоків: дані можуть передаватися між державами практично миттєво, що значно ускладнює питання юрисдикції та захисту інформації.

Завершити формулювання слід сьомою ознакою, яка виступає в якості так званого високого рівеня залежності від кібербезпеки. Порушення роботи інформаційних систем може призвести до значних економічних, соціальних та політичних наслідків.

Водночас, в загальному контексті, наведені ознаки доволі доцільно визначають специфіку міжнародно-правового регулювання інформаційних технологій та обумовлюють необхідність розробки спеціальних міжнародних стандартів у сфері інформаційної безпеки.

Додатково варто зауважити, що наукова спільнота пропонує розподіл ознак на дві групи: основні та додаткові. В цілому поділ не несе суттєвого значення в міжнародному аспекті, але як джерело інформації заслуговує на особливу увагу дослідників.

З власної позиції погоджуюсь з баченням науковців Корольовою В.В. та Чорною В.О., що інформаційні технології в загальному контексті є частиною інформаційного права, а отже, слід звернути увагу, що його ознаки мають поширюватися на інформаційні технології як напрям / галузь в повній мірі [38, с.20].

Серед основних ознак варто виокремити наступні, зокрема, в контексті регулятивного методу як невід'ємну складову:

- «регулювання інформаційних правовідносин;
- комплексно-системний характер, що в загальному розумінні характеризується наявністю сукупності взаємопов'язаних способів

чи методів, які безпосередньо впливають на відносини, у результаті чого такі відносини в повній мірі набувають інформаційно-правових властивостей);

- органічне поєднання імперативного та диспозитивного способів нормативно-правового регулювання суспільних правових відносин;
- зумовленість функціями інформаційного права;
- гарантування засобами державного примусу (юридичною відповідальністю)» [38, с.20].

Загалом, розглядаючи інформаційні технології в контексті об'єкта міжнародного права, який для регулювання потребує застосування норм міжнародного законодавства в повній мірі. В цьому разі варто виокремити як ознаки дотичні до інформаційних технологій:

- Транскордонність або екстериторіальність, в цілому полягає в тому, що віртуальний інформаційний простір й цифрові мережі не обмежуються межами державних кордонів. Транскордонні інформаційні потоки чи кібератаки в якості передачі даних майже миттєво охоплюють значний масив користувачів різних континентів. В цьому разі міжнародне регулювання відносин вимагає безпосереднього укладення, в більшості випадках, саме багатосторонніх договорів та, зокрема, так званої уніфікації норм.
- Об'єктивність та нематеріальність водночас полягає в тому що, незважаючи на те, що інформаційні технології базово опираються на фізичні носії інформації, але самі процеси зберігання чи обробки баз даних нематеріальні. В цьому разі об'єктом правових відносин слід безпосередньо вважати сам інформаційний ресурс та сукупність взаємопов'язаних з цим послуг, по своїй суті слід вважати викликом для визначення питань правового регулювання в міжнародному аспекті.
- Багатосуб'єктність, в основному полягає в тому, що у створенні та забезпеченні подальшого функціонування інформаційних технологій приймають участь не лише фізичні особи чи міжнародні організації, а й безпосередньо держави, як суб'єкти міжнародного права, приватні

підприємства, установи, організації та/або корпорації, в тому числі провайдери.

- Подвійне призначення чи дуальний характер водночас полягає в тому, що цифрові технології як частина інформаційних технологій може бути придатною до використання одночасно як у мирних так і у воєнних цілях (комерція, наука, кіберзброя, дезінформація), що в певній мірі дозволяє розглядати інформаційні технології в контексті гуманітарного права.
- Глобальні ризики породжують вразливість, тому що інформаційні технології слід вважати безпосереднім інструментом для створення загроз міжнародній безпеці (тероризм, кіберзлочинність та інше). Наразі створення дієвих механізмів захисту та контролю безпеки.

Слід зауважити, що наведений перелік ознак інформаційних технологій в контексті міжнародно-правових відносин не є вичерпним.

Окрім цього, у сучасному міжнародному праві науковці виокремлюють низку видів інформаційних технологій, кожен з яких має власні особливості та потребує відповідного міжнародно-правового регулювання, а розвиток цифрового суспільства в цілому посприяв подальшому їх вдосконаленню та популяризації продуктів розроблених на основі тих чи інших технологій.

Найбільш поширеними слід вважати комп'ютерні та мережеві технології як вид інформаційних технологій, що слід вважати складною системою технічних, програмних та організаційних засобів, призначених для роботи з інформацією.

До них належать: програмне забезпечення, комп'ютерні системи, локальні та глобальні мережі, а також комунікаційна інфраструктура. У сучасному світі вони виступають одним із ключових інструментів розвитку міжнародних відносин, економіки, науки та державного управління [33].

Основою сучасного інформаційного суспільства, в свою чергу, стала глобальна мережа Інтернет, яка забезпечує обмін інформацією між мільярдами користувачів у різних країнах світу. Саме завдяки Інтернету стало можливим

функціонування міжнародної електронної комерції, дистанційної освіти, електронного урядування та цифрової дипломатії [20].

З міжнародно-правової точки зору використання мережевих технологій пов'язане з необхідністю забезпечення: свободи доступу до інформації; захисту персональних даних; кібербезпеки; авторських прав; безпеки електронних комунікацій.

Особливу увагу міжнародне співтовариство приділяє питанням забезпечення стабільності функціонування глобальної мережевої інфраструктури, оскільки порушення її роботи може мати негативні наслідки для міжнародної безпеки та економіки в цілому.

Хмарні технології та великі дані слід розглянути як один із найважливіших напрямів розвитку інформаційних технологій, яким стали хмарні обчислення.

Хмарні технології, зокрема, передбачають надання користувачам доступу до обчислювальних ресурсів, програмного забезпечення та сховищ даних через мережу Інтернет. Основною перевагою хмарних сервісів є можливість віддаленого доступу до інформаційних ресурсів незалежно від місця перебування користувача.

У міжнародному праві використання хмарних технологій породжує низку викликів, пов’язаних безпосередньо з: визначенням юрисдикції щодо даних; забезпеченням конфіденційності інформації; захистом персональних даних; транскордонна передача інформації; відповідальність постачальників послуг.

Однак особливого значення набуває проблема зберігання даних на серверах, розташованих у різних державах. У таких випадках виникає питання, законодавство якої країни повинно застосовуватися до інформації, що обробляється.

Доволі тісно пов'язаними з хмарними технологіями є технології великих даних. Зазвичай під великими даними розуміють масиви структурованої та неструктурованої інформації, які неможливо ефективно обробляти традиційними методами.

Наразі технології великих даних використовуються: у державному управлінні; у банківській сфері; у охороні здоров'я; у міжнародній торгівлі; у діяльності міжнародних організацій та, окрім цього, накопичення великих обсягів інформації створює ризики порушення права людини на приватність та потребує додаткових міжнародно-правових гарантій захисту персональних даних в цілому [22].

З іншої сторони, одним із найперспективніших напрямів розвитку сучасних інформаційних технологій є штучний інтелект. Зазвичай під штучним інтелектом розуміють сукупність програмних та апаратних засобів, здатних виконувати функції, які традиційно потребують людського інтелекту. До таких функцій слід відносити: аналіз інформації; прогнозування; розпізнавання образів; автоматичне прийняття рішень; машинне навчання.

В еру цировізації, системи штучного інтелекту активно використовуються в міжнародній торгівлі, транспорті, медицині, фінансовій сфері та державному управлінні [34].

Особливого значення набуває застосування штучного інтелекту у сфері міжнародної безпеки, а автономні системи можуть використовуватися для: моніторингу кордонів; кіберзахисту; аналізу розвідувальної інформації; управління безпілотними системами.

Зазвичай, використання штучного інтелекту породжує низку правових викликів: відповідальність за рішення, прийняті алгоритмом; захист прав людини; недопущення дискримінації; забезпечення прозорості алгоритмів; контроль над автономними системами озброєння та інших.

Варто зауважити, що саме тому міжнародні організації активно працюють над створенням спеціальних правових механізмів регулювання штучного інтелекту в цілому як технології, що стрімко розвивається.

Окремим важливим різновидом сучасних інформаційних технологій слід виділити технології блокчейн. Загалом, технологія блокчейн являє собою розподілену базу даних, у якій інформація зберігається у вигляді взаємопов'язаних блоків та захищена криптографічними методами, що в

повній мірі захищає від несанкціонованого копіювання чи зміни даних в цілому [24].

Основними перевагами блокчейну слід вважати: децентралізація; захищеність інформації; прозорість операцій; неможливість несанкціонованого внесення змін.

В сучасності технологія блокчейн активно використовується для функціонування цифрових активів та криптовалют, а їх поширення створило нові виклики для міжнародного права, серед яких: боротьба з відмиванням коштів; фінансування тероризму; міжнародне оподаткування цифрових активів; правове визначення криптовалют [21].

Технологія IoT, в свою чергу, як і технологія ШІ є важливим інтрументом автоматизації процесів [3].

Наразі більшість держав працюють над створенням правових механізмів регулювання цифрових активів на національному та міжнародному рівнях, в тому числі поєднуючи зусилля для подолання викликів.

Водночас зростання залежності суспільства від цифрових технологій обумовило необхідність розвитку технологій кібербезпеки як окремого виду інформаційних технологій.

Кібербезпека, зазвичай, являє собою систему заходів, спрямованих на захист інформаційних ресурсів, комп'ютерних систем та мереж від несанкціонованого доступу, пошкодження або знищення [16]. До основних технологій кібербезпеки належать: криптографічний захист інформації; електронний цифровий підпис; системи аутентифікації користувачів; антивірусні програми; міжмережеві екрани; системи виявлення кіберзагроз.

У сучасних умовах кібербезпека стала важливим елементом міжнародної безпеки, а масштабні кібератаки можуть бути спрямовані проти: державних органів; банківської системи; транспортної інфраструктури; енергетичних об'єктів; систем зв'язку. В зв’язку з цим міжнародні організації, в свою чергу, приділяють значну увагу розвитку механізмів міжнародного співробітництва у сфері кібербезпеки та боротьби з кіберзлочинністю [26].

Інформаційні технології у діяльності міжнародних організацій слід виділити наступним видом, завершуючи вище наведений перелік видів інформаційних технологій.

В цифрову епоху сучасні міжнародні організації активно використовують інформаційні технології для виконання своїх функцій. Основними напрямами їх застосування слід вважати: електронний документообіг; цифрові архіви; відеоконференції; автоматизовані системи управління; інформаційно-аналітичні платформи [11].

Особливого значення цифрові технології, як вид інформаційних технологій набули з початком пандемії ковіду, коли значна частина міжнародних заходів проводилася в дистанційному форматі.

Таким чином, використання інформаційних технологій сприяє суттєвому підвищенню ефективності міжнародного співробітництва та забезпечує оперативний обмін інформацією між державами та міжнародними організаціями.

1.2 Становлення міжнародно-правового регулювання інформаційних технологій

Становлення міжнародно-правового регулювання інформаційних технологій, характеризується довготривалим періодом розвитку, який пройшов доволі складний шлях.

Початковою стадією розвитку слід вважати епоху до та після 1970 років. Період пов’язаний з появою розробки комп’ютера та інших інформаційних технологічних винаходів, та процесів прикладного, та юридичного регулювання, які сформували сьогодення.

До цієї доби віднесено також період становлення нормативних документів, підставою формування яких слід вважати характерні внутрішні та зовнішні політичні події, нагальна потреба нових розробок та досліджень, які, в свою чергу, посприяли створенню відповідних стандартів, законів та низки інших правових документів: Розробка ENIAC (1946); перший у світі

комерційний комп'ютер випущений під назвою UNIVAC-I (1951); Токійська фондова біржа та Nomura Securities Квиткова компанія представляє UNIVAC-120 (1955); Створення агентства проектів (1951); IBM, мейнфрейм-комп'ютер та відкриття на комп'ютері System/360 випущеного в той же період (1964); Банк Міцуї зараз Банківська корпорація Сумітомо Міцуї лінія, система онлайн-банкінгу введено TEM (1965); США: Концептуалізація гіпертексту шоу (1965) та AT&T Bell Laboratories, Початок досліджень UNIX та заснування ARPANET прототип сучасного інтернету (1969); Перші випадки комп’ютерних злочинів (1970); Випуск перших у світі мікропроцесорів Intel (1971); Розробка перших мов програмування С (1972); Випуск публічного сервісу комунікації TELNET (1974); Створення стандартів методів шифрування (1977) [29].

В загальному контексті, думки науковців суттєво різняться щодо часових меж формування історичних етапів особливо в частині становлення сучасного міжнародно-правового регулювання інформаційних технологій. Зазвичай виокремлюють три нижченаведених періоди.

Перший етап (1990–2000 рр.): Концепція правового вакууму та кіберлібертаріанство здебільшого вважається початковим етапом становлення інформаційних технологій, як об’єкта міжнародно-правового осмислення, який збігся в часі з демілітаризацією глобального політичного простору після закінчення Холодної війни та комерціалізацією мережі Інтернет. У цей період у науковій спільноті та серед перших розробників архітектури Всесвітньої мережі (World Wide Web) панувала ідеологія кіберлібертаріанства. Її ключовим маніфестом стала «Декларація незалежності кіберпростору» Джона Перрі Барлоу (1996 р.), проголошена на Всесвітньому економічному форумі в Давосі. Автор декларації звертався до урядів індустріального світу зі словами: «Уряди промислового світу, ви, втомлені гіганти з плоті та сталі, я прийшов до вас із Кіберпростору — нової домівки Розуму... У нас немає обраного уряду, і навряд чи він колись з'явиться... Ви не маєте суверенітету там, де ми збираємося» [29].

З юридичної точки зору цей підхід спирався на теорію правового вакууму (legal vacuum theory). Її прибічники стверджували, що кіберпростір є окремою, саморегульованою юрисдикцією (lex informatica), яка функціонує за власними правилами (кодами, мережевими протоколами TCP/IP), створеними інженерною спільнотою (зокрема, IETF — Internet Engineering Task Force). Передбачалося, що традиційні географічні кордони держав не мають жодного значення для транскордонних пакетів даних, а отже, спроби застосувати норми класичного міжнародного права, заснованого на Вестфальській системі територіального суверенітету, є онтологічно неможливими та заздалегідь приреченими на провал.

Держави на цьому етапі займали переважно позицію пасивного спостерігача, розглядаючи інформаційні технології виключно як інструмент економічного зростання та наукового обміну. Регуляторна активність на міжнародному рівні мала вузькоспеціалізований, технічний характер і здійснювалася через такі інституції: Міжнародний союз електрозв'язку, який фокусувався на розподілі радіочастотного спектра та стандартизації телекомунікаційного обладнання; Всесвітня організація інтелектуальної власності: у 1996 році ухвалила Договір про авторське право, який став першою серйозною спробою захистити цифровий контент та врегулювати правову охорону комп'ютерних програм як літературних творів; Корпорація Internet Corporation for Assigned Names and Numbers була створена у 1998 році під егідою Департаменту торгівлі США як приватна некомерційна організація, що перебрала на себе функції управління системою доменних імен та IP-адресацією, закріпивши тим самим американську монополію на технічний контроль над мережею.

Першим сигналом про те, що ера правової анархії добігає кінця, стало усвідомлення криміналізації віртуального середовища. У відповідь на появу перших транскордонних комп'ютерних вірусів (таких як «ILOVEYOU» у 2000 році, який завдав глобальних збитків на суму понад 10 мільярдів доларів) Рада Європи розпочала розробку документа, що мав об’єднати зусилля

правоохоронних органів різних держав [72]. Це заклало фундамент для переходу до наступного, значно більш реалістичного етапу взаємовідносин між державою та ІТ.

Другий етап історичного становлення (2000–2015 рр.): Мілітаризація кіберпростору та перші спроби правового обмеження характеризується тим, що на початку двадцять першого століття романтизм кіберлібертаріанства був повністю нівельований прагматичними інтересами національної безпеки провідних світових держав. Цей етап характеризується мілітаризацією кіберпростору, його офіційним визнанням (поруч із суходолом, морем, повітрям та космосом) п'ятим доменом ведення бойових дій та усвідомленням того, що інформаційні технології є критично вразливими елементами життєзабезпечення суспільства в цілому.

Водночас важливою нормативною віхою початку цього етапу стало підписання Будапештської конвенції про кіберзлочинність 2001 року. Це був перший юридично обов'язковий міжнародний договір, який гармонізував національне кримінальне законодавство щодо комп'ютерних злочинів, визначив правила збору електронних доказів та заклав основи транскордонного співробітництва правоохоронних органів. Конвенція доречно продемонструвала: держави повернулися в кіберпростір і готові застосовувати там свій каральний апарат [20].

Проте справжній геополітичний зсув відбувся внаслідок серії подій, які довели руйнівний потенціал інформаційних технологій як інструментів міждержавного протистояння, а саме:

– Кібератаки на Естонію (2007 рік): У відповідь на перенесення пам’ятника «Бронзовий солдат» у Таллінні, державні установи, банки та ЗМІ Естонії зазнали скоординованої масованої DDoS-атаки, яка на 22 дні фактично паралізувала цифрову інфраструктуру країни. Цей прецедент змусив НАТО вперше серйозно розглянути питання: чи може кібератака активувати Статтю 5 про колективну оборону [52, с.37-38].

– Кібератаки на Грузію (2008 рік): Вперше в історії збройних конфліктів кібератаки на урядові сайти та інформаційні ресурси Грузії здійснювалися синхронно з кінетичним (фізичним) вторгненням регулярних військ супротивника. Це в повній мірі продемонстрував концепт інтеграції інформаційних технологій у доктрину гібридної війни [73].

– Розгортання хробака Stuxnet (2010 рік): Спільна операція спецслужб США та Ізраїлю (Олімпійські ігри) призвела до ураження шкідливим програмним забезпеченням комп'ютерних систем збору даних німецького виробництва Siemens на іранському ядерному об'єкті в Натанзі. Вірус фізично розкрутив та зруйнував близько тисячі центрифуг для збагачення урану. Stuxnet став першою підтвердженою кіберзброєю, яка викликала матеріальні руйнування, аналогічні конвенційному бомбовому удару [74].

Окрім цього, слід зауважити, що у цей самий період становлення на рівні ООН сформувався глибокий ідеологічний розкол щодо правового регулювання інформаційних технологій, а саме: Західна коаліція (США, країни Європейського Союзу, НАТО): відстоювала позицію, що створення нових міжнародних договорів є недоцільним, оскільки чинне міжнародне публічне право, включаючи Статут ООН (особливо статті 2(4) та 51) та Міжнародне гуманітарне право, автоматично адаптуються до кіберпростору [40, ст.2, ст.51].

Головним завданням вони бачили кодифікацію звичаєвих норм. Авторитарний блок (КНР та країни ШОС (Шанхайська організація співробітництва) виступили проти застосування Міжнародного гуманітарного права до кіберсфери, аргументуючи це тим, що визнання законів війни в кіберпросторі легалізує кібервійну. Натомість вони щорічно просували концепцію Конвенції ООН про забезпечення міжнародної інформаційної безпеки, під приводом якої намагалися легітимізувати державну цензуру, обмеження свободи слова та встановлення тотального контролю урядів над контентом у межах своїх національних кордонів (залишилася на стадії проекту).

Однак дискусія частково вирішилася в рамках Груп урядових експертів ООН, які у своїх доповідях 2013 та 2015 років змогли досягти компромісу, зафіксувавши фундаментальну тезу: міжнародне право застосовне до сфери інформаційних технологій.

Третій етап (2015 р. до сьогодення): Системна кодифікація та виклики штучного інтелекту. Сучасний етап розвитку міжнародно-правового регулювання інформаційних технологій характеризується переходом від теоретичних дискусій про застосовність права до системної практичної кодифікації конкретних норм та адаптації правових інститутів до технологій так званої «четвертої промислової революції».

Загалом, провідною доктринальною подією початку цього етапу став вихід у 2017 році Талліннського посібника 2.0, яке сформувало чітку систему з 95 правил, що детально розписують як саме норми про суверенітет, державну відповідальність, дипломатичне право та право збройних конфліктів накладаються на кібероперації, також паралельно зазнала трансформації і практика міждержавних протистоянь. Замість поодиноких вірусів світ зіткнувся зі скоординованими операціями стратегічного рівня серед яких варто виокремити: Атаки на енергосистему України (2015–2016 рр.), Епідемія NotPetya (2017 рік), Втручання у президентські вибори в США (2016 рік) [37].

Атаки на енергосистему України (2015–2016 рр.): вперше в історії хакери (угруповання Sandworm) здійснили успішні атаки на українські обленерго Прикарпаття, дистанційно відключивши підстанції та позбавивши світла сотні тисяч громадян в розпал зими. Це суттєво продемонструвало вразливість критичної промислової інфраструктури [75].

Епідемія NotPetya (2017 рік): шкідливе програмне забезпечення, замасковане під програму-вимагач, було запущене через компрометацію українського софту для звітності M.E.Doc. Вірус миттєво поширився світом, паралізувавши роботу глобальних логістичних гігантів, фармацевтичних компаній та банківських систем, завдавши сумарних збитків на понад 10 мільярдів доларів. Цей випадок став хрестоматійним для вивчення

транскордонних наслідків кібератак у міжнародному праві та застосування принципу належної обачності (due diligence) [76].

Втручання у президентські вибори в США (2016 рік): використання технологій зламу та зливу даних (hack-and-leak) щодо Демократичної партії США, поєднане зі скоординованими кампаніями дезінформації через фабрики ботів у соціальних мережах (Facebook, Twitter), змусило міжнародних юристів переосмислити класичний зміст принципу невтручання у внутрішні справи (non-intervention) [77].

Станом на 2026 рік архітектура міжнародно-правового регулювання IT зіткнулася із якісно новим технологічним викликом — стрімким розвитком та впровадженням Генеративного Штучного Інтелекту (AI), великих мовних моделей (LLM) та автономних систем озброєнь (LAWS — Lethal Autonomous Weapons Systems). Поява алгоритмів, здатних самостійно приймати рішення про ураження цілей на полі бою без участі людини (human-out-of-the-loop), підірвала класичний постулат міжнародного гуманітарного права про індивідуальну кримінальну відповідальність за воєнні злочини, адже програму чи нейромережу неможливо притягнути до суду.

У відповідь на ці виклики почалося формування нової парадигми регулювання, заснованої на контролі за ризиками. Історичним проривом стало ухвалення у 2024 році Закону Європейського Союзу про штучний інтелект (EU AI Act), який став першим у світі комплексним транскордонним актом, що розділив системи ШІ за чотирма рівнями ризику (від неприйнятного до мінімального) та назавжди заборонив використання систем когнітивного маніпулювання людьми, соціального скорингу та масового біометричного стеження в реальному часі [28].

Хоча, на сучасному етапі міжнародне цифрове право трансформується з вузької підгалузі національної безпеки на всеохоплюючу систему, що намагається врегулювати (когнітивний суверенітет) людини в умовах інформаційного достатку та протидіяти монополізації цифрового простору глобальними Big Tech корпораціями, чий фінансовий та технологічний ресурс

часто перевищує можливості більшості суверенних держав світу варто виділити як окремий період становлення четверний етап.

Четвертий етап (2022 р. - 2026 р.): Перша повномасштабна кібервійна та криза конвенційного захисту цивільних осіб. Повномасштабне вторгнення в Україну у лютому 2022 року та подальший перебіг бойових дій ознаменували початок принципово нової ери — першої у світовій історії повномасштабної, інтегрованої кібервійни (Full-Scale Cyber Warfare). Цей етап остаточно спростував кабінетні теорії про те, що цифрові операції повністю замінять кінетичну зброю. Натомість практика 2022–2026 років продемонструвала повну синхронізацію кібератак із ракетними ударами, артилерійськими обстрілами та сухопутними наступами, що змусило міжнародне співтовариство переглянути базові пороги застосування Міжнародного гуманітарного права [50].

Характерними рисами та ключовими прецедентами цього періоду, що змінили ландшафт міжнародного цифрового права, стали: Синхронізація «кібер-кінетика» тобто практика вторгнення виявила чітку тактичну координацію між військовими хакерами і регулярними військами. Хрестоматійним прикладом стала кібератака на супутникову мережу Viasat 24 лютого 2022 року, здійснена за кілька годин до перетину кордону танковими колонами. Метою атаки було повне засліплення системи зв’язку Збройних Сил України. Водночас вона спричинила каскадні цивільні руйнування по всій Європі, відключивши тисячі вітрових електростанцій у Німеччині, що актуалізувало дискусію про невибірковий характер кіберзброї згідно зі Статтею 51(4) Додаткового протоколу I до Женевських конвенцій [41, ст.51].

У 2023–2025 роках ця стратегія еволюціонувала: хакери здійснювали злом муніципальних систем, камер відеоспостереження та логістичних вузлів безпосередньо перед або під час масованих ракетних обстрілів для коригування вогню та фіксації наслідків руйнувань у реальному часі.

Феномен «Кіберармії» та розмивання статусу комбатанта: найбільшим викликом для міжнародного гуманітарного права стала безпрецедентна за

масштабами мобілізація цивільних фахівців. Створення Міністерством цифрової трансформації України ІТ-армії України, що об'єднала сотні тисяч волонтерів-айтівців з усього світу для проведення наступальних DDoS-атак та кібердиверсій проти спільного ворога, що підірвало класичний принцип розрізнення (distinction).

Цей феномен змусив Міжнародний Комітет Червоного Хреста піти на радикальний крок: у жовтні 2023 року він вперше у своїй історії оприлюднив 8 правил для цивільних хакерів у війні, вимагаючи від волонтерів припинити атаки на лікарні, гуманітарні об'єкти та здійснювати розрізнення між військовими та цивільними серверами.

В їхньому розширеному звіті за листопад 2025 року було чітко констатовано: цивільні особи, які здійснюють кібероперації проти ворога, визнаються такими, що беруть безпосередню участь у воєнних діях (Direct Participation in Hostilities), а отже, юридично втрачають свій цивільний імунітет і стають легітимними об'єктами для фізичного знищення з боку супротивника [78].

Атаки на цивільні дані як злочин проти людяності: до 2022 року вважалося, що кібератаки спрямовані лише на залізо або софт. Однак атака на найбільшого українського мобільного оператора «Київстар» у грудні 2023 року продемонструвала нову стратегію: тотальне знищення віртуальної інфраструктури (баз даних, конфігурацій систем), що призвело до відключення зв'язку, систем оповіщення про повітряну тривогу та банкоматів для мільйонів громадян. Станом на 2025–2026 роки у Міжнародному кримінальному суді в Гаазі сформувався консенсус щодо кваліфікації подібних дій. Forensic-експертизи довели, що масштабні кібератаки, спрямовані на повне відключення життєво важливих систем цивільного населення взимку (опалення, водопостачання, зв'язок), підпадають під юрисдикцію Римського статуту Міжнародного кримінального суду і можуть розглядатися як воєнні злочини або злочини проти людяності, оскільки їхні наслідки ідентичні фізичній блокаді чи знищенню міст [54].

В цілому, становлення сучасності щодо сьогоденних перспектив даного періоду характеризує формування нових історичних істотних змін характерними новими підходами, переосмисленням нормативної бази та її практичної ефективності. Особливо даний спектр вважливий на міжнародному рівні оскільки охоплює національну безпеку.

1.3 Принципи міжнародного права у сфері використання інформаційних технологій

Базові загальносистемні принципи міжнародного права застосовні у сфері інформаційних технологій закріплені у Декларації про принципи міжнародного права 1970 року та Статуті ООН, діють у кіберпросторі зі своєю певною специфікою [40; 99].

Загалом варто зауважити, що в числі перших слід зазначити принцип суверенної рівності держав та концепція кіберсуверенітету.

Згідно з Правилами 1–5 Талліннського посібника 2.0, державний суверенітет у сфері ІТ має два виміри: внутрішній суверенітет, що означає право держави здійснювати виключний контроль та регулювання над інформаційно-технологічною інфраструктурою (сервери, волоконно-оптичні кабелі, базові станції, супутникові термінали), яка розташована на її сухопутній, морській та повітряній території, а також над цифровою діяльністю фізичних і юридичних осіб у межах її юрисдикції; зовнішній суверенітет, в свою чергу означає, що право держави самостійно, без зовнішнього тиску, вести свою цифрову зовнішню політику та управляти своїми інформаційними ресурсами [37, с.11-29].

Однак, станом на 2026 рік навколо цього питання ведеться активна правова дискусія: чи є порушення суверенітету окремим міжнародним правопорушенням у кіберсфері, чи воно стає таким лише тоді, коли переростає у втручання у внутрішні справи якоїсь конкретної держави. Водночас такі країни, як Велика Британія, історично схилялися до думки, що суверенітет - лише принцип, а не самостійна норма, порушення якої тягне відповідальність.

Проте більшість держав (включно з Україною, США, Францією, Німеччиною) офіційно зафіксували у своїх правових позиціях, що будь-яке несанкціоноване проникнення в державні ІТ-системи з боку іноземних органів є прямим порушенням державного суверенітету.

Окремо слід звернути увагу, що як результат дискусії щодо юридичної природи кіберсуверенітету сформувалися дві основні школи мислення:

– Концепція суверенітету як принципу (Sovereignty as a Principle): Прибічники цієї теорії (зокрема Велика Британія та ряд англосаксонських дослідників) стверджують, що суверенітет є лише загальним принципом, парасолькою для інших норм. Відповідно, транскордонний злам державних серверів іноземною розвідкою є політично недружнім кроком, але сам по собі не становить самостійного міжнародного правопорушення, якщо він не призвів до фізичних руйнувань чи елементів примусу.

– Концепція суверенітету як самостійної норми (Sovereignty as a Rule): Цю позицію займає більшість держав світу, включаючи офіційну правову позицію України (зафіксовану в заяві Міністерства закордонних справ 2021 року), США, Франції, Нідерландів та Німеччини. Згідно з цим підходом, суверенітет є конкретною нормою прямої дії. Будь-яке несанкціоноване проникнення іноземного уряду в комп'ютерну мережу іншої держави (навіть без завдання матеріальних збитків (наприклад, з метою кібершпигунства чи встановлення «сплячих» вірусів)) де-юре вважається порушенням суверенітету, що тягне за собою міжнародно-правову відповідальність.

Наступний Принцип незастосування сили або загрози силою в кіберпросторі.

Стаття 2(4) Статуту ООН встановлює імперативну норму (jus cogens), згідно з якою всі члени ООН утримуються в своїх міжнародних відносинах від загрози силою або її застосування, що категорично забороняє державам вдаватися до сили проти територіальної цілісності чи політичної незалежності інших країн [40, ст.2(4)]. Оскільки автори Статуту 1945 року під «силою» розуміли виключно кінетичну, військову силу (танки, артилерію, авіабомби),

тривалий час залишалося неврегульованим питання: чи підпадає під цю заборону використання шкідливого програмного коду (вірусів, троянів, логічних бомб). Головний виклик, зокрема, полягав у тому, чи можна вважати силою програмний код (шкідливе ПЗ, віруси чи щось інше), який не має фізичної маси та кінетичної енергії. Для вирішення цієї дилеми міжнародне право ухвалило підхід, заснований на наслідках (effects-based approach), детально викладених в Правилі 14 Талліннського посібника 2.0 [37, с.84-87].

В загальному розумінні викладеного, юридична кваліфікація цифрової операції як «застосування сили» залежить не від інструменту (код чи ракета), а від масштабів та характеру наслідків (scale and effects): якщо цифрова операція призводить до наслідків, які за своїми масштабами та характером аналогічні наслідкам класичного кінетичного удару (руйнування майна, вибухи, аварії, каліцтва чи смерть людей), вона кваліфікується як застосування сили.

Наприклад: Злом за допомогою вірусу системи охолодження АЕС, що спричинив розплавлення активної зони, або відключення цифрових систем життєзабезпечення в масштабах країни, прирівнюється до військового нападу. Відповідно, якщо масштаби руйнувань досягають критичного рівня, постраждала держава отримує право на індивідуальну чи колективну самооборону на підставі Статті 51 Статуту ООН [40, ст.51]. Це право дає можливість відповісти агресору як дзеркально (кібератакою), так і звичайними конвенційними засобами збройних сил (авіаудари, артилерія та інше).

Принцип невтручання у внутрішні справи (Non-intervention). Цей принцип випливає з концепції державного суверенітету та забороняє державам прямо чи опосередковано втручатися у внутрішні чи зовнішні справи іншої держави, які входять до її внутрішньої компетенції (domaine réservé). Специфіка реалізації цього принципу в ІТ-сфері полягає в обов'язковій наявності двох кумулятивних елементів, зафіксованих у практиці Міжнародного Суду ООН (зокрема, у знаковій справі «Нікарагуа проти США», 1986 р.): втручання має стосуватися питань, рішення щодо яких

держава, згідно з принципом суверенітету, може ухвалювати абсолютно вільно (обрання політичної системи, релігійні та культурні стандарти, ведення зовнішньої політики); наявність елементу примусу (coercion) [27].

Загалом, у сучасному цифровому середовищі примус рідко виглядає як пряма погроза. Найчастіше він реалізується через деструктивні інформаційні технології (цифрове втручання у виборчі процеси): злом електронних систем підрахунку голосів, несанкціоноване проникнення в сервери виборчих комісій з метою модифікації списків виборців, або масоване злиття конфіденційної інформації кандидатів (hack-and-leak) за кілька днів до голосування, що координується іноземною державою.

Штучна дестабілізація, в свою чергу, як елемент примусу, проявляється через алгоритми: використання генеративного штучного інтелекту, дипфейків (deepfakes) вищого керівництва держави та скоординованої неавтентичної поведінки (бот-мереж) у соціальних мережах для штучного провокування масових заворушень, фінансової паніки чи зриву мобілізаційних заходів.

Загалом, якщо іноземна цифрова операція позбавляє державу можливості вільно ухвалювати рішення у сфері її внутрішньої компетенції, така дія кваліфікується як міжнародне правопорушення у вигляді протиправного втручання.

Принцип міжнародно-правової відповідальності держав та проблема атрибуції. Основоположний принцип міжнародного права, який встановлює, що будь-яка міжнародно-протиправна дія держави тягне за собою її міжнародну відповідальність (кодифіковано у Статтях про відповідальність держав за міжнародно-протиправні діяння 2001 року) [56].

Загалом, держава несе повну відповідальність за кібероперації, які здійснюють її офіційні структури: збройні сили (кіберкомандування), спецслужби або дипломатичні представництва [16]. Однак головною архітектурною проблемою цифрового міжнародного права є проблема атрибуції (Attribution): юридичного та технічного доведення того, що конкретна шкідлива цифрова дія була вчинена саме конкретною державою.

Зазвичай, через використання анонімайзерів, проксі-серверів у третіх країнах та технологій підробки цифрового сліду (false flag operations), встановити першоджерело атаки вкрай складно.

Окрім цього, держави часто використовують приватні хакерські угруповання, APT-групи (Advanced Persistent Threat) або кримінальні синдикати для досягнення своїх геополітичних цілей, зберігаючи тактику «правдоподібного заперечення» (plausible deniability). Для подолання цієї проблеми міжнародна юридична практика застосовує стандарти приписування дій приватних осіб державі, закріплені у Правилі 15 Талліннського посібника 2.0 [37, с.87-92]:

1) Тест на «ефективний контроль» (Effective control test): Дії приватних хакерів приписуються державі, якщо буде доведено, що державні органи не просто фінансували чи координували їх загалом, а здійснювали безпосереднє керівництво, планування та контроль над конкретною деструктивною кібероперацією.
2) Схвалення дій (Acknowledgement and adoption): Відповідно до прецедентного права (справа про «Заручників у Тегерані», 1980 р.), якщо приватні хакери здійснили атаку самостійно, але згодом керівництво держави офіційно похвалило їх, визнало ці дії корисними для національних інтересів та відмовилося видавати зловмисників, держава де-юре приймає на себе повну відповідальність за цей напад.

Зокрема, у випадку неможливості довести прямий зв'язок між урядом та хакерами, включається Принцип належної обачності (Due Diligence), визнаний ООН у 2021 році.

Згідно з цим принципом, жодна держава не має права свідомо дозволяти використовувати свою цифрову інфраструктуру (сервери, мережі зв’язку) для дій, які завдають шкоди правам інших держав. Якщо держава отримала офіційну скаргу, що з її території здійснюється кібератака на критичні системи сусідньої країни, але проігнорувала запит і не вжила технічних заходів для

блокування шкідливого трафіку, вона несе міжнародну відповідальність за власну протиправну бездіяльність.

Додатково, слід зауважити, що відповідно до принципу міжнародно-правової відповідальності держав, проблеми атрибуції, згідно зі звичаєвим міжнародним правом визначається, що кожна держава несе відповідальність за кібероперації своїх офіційних органів (армії, розвідки). Навіть, якщо держави використовують тактику «правдоподібного заперечення» (plausible deniability), залучаючи до атак підконтрольні кримінальні хакерські угруповання (проксі-суб'єкт). Для притягнення держави до відповідальності застосовується стандарт «ефективного контролю» (effective control), вироблений Міжнародним Судом ООН, та положення Правила 15 Талліннського посібника 2.0 і таким чином, якщо буде доведено, що приватні хакери діяли за вказівкою, під керівництвом або під безпосереднім контролем державних органів, їхні дії юридично стають діями самої держави [37, с.87-92].

В цьому разі, процес імплементації норм міжнародного публічного права у віртуальний простір зіткнувся з онтологічною проблемою: принципи, створені для фізичного світу (де є чіткі кордони, матеріальні об'єкти та видимі суб'єкти), мають регулювати децентралізоване, транскордонне та переважно анонімне середовище. Як зазначено у коментарях до Талліннського посібника 2.0, ключові засади міжнародного правопорядку, закріплені у Статуті ООН, діють у кіберпросторі не як нові норми, а як звичаєві принципи, що набувають специфічних форм реалізації [16; 40].

У разі початку міжнародного або неміжнародного збройного конфлікту (Jus in bello), будь-які ІТ-операції, пов'язані з веденням бойових дій, підпадають під дію Женевських конвенцій 1949 року та Додаткового протоколу І 1977 року [41; 42].

В цілому, при цифрових атаках держави юридично зобов'язані дотримуватися чотирьох фундаментальних принципів міжнародного гуманітарного права: принципу розрізнення (Distinction), принципу

пропорційності (Proportionality), принципу військової необхідності (Military Necessity), принципу заборони завдання надмірних страждань та Застереження Мартенса. В цілому, принцип розрізнення (Distinction) сформульований у Статті 48 Додаткового протоколу I [42, ст.48]. Сторони конфлікту повинні завжди розрізняти цивільні та воєнні об'єкти.

В загальному аспекті об'єкти: Військові сервери, системи зв'язку командування, радари ППО можна вважати легітимними військовими цілями для кібератак. Натомість цивільні комп'ютерні мережі, сервери Пенсійного фонду, логістичні системи залізниць (що перевозять виключно цивільне населення) атакувати категорично заборонено. Окремий абсолютний захист мають медичні інформаційні системи лікарень, шпиталів та об’єктів прирівняних до них.

Суб'єкти (статус цивільних хакерів): з початком повномасштабних воєнних дій у світі поширився феномен волонтерських «ІТ-армій». Міжнародний Комітет Червоного Хреста у своїх роз'ясненнях доречно зазначає: цивільні програмісти, які здійснюють кібератаки проти супротивника, втрачають свій імунітет цивільної особи, оскільки беруть безпосередню участь у воєнних діях (Direct Participation in Hostilities). Вони стають легітимними цілями для атак (включаючи фізичне ураження місць їхнього перебування) і після затримання не мають автоматичного права на статус військовополоненого, якщо не входять до складу регулярних збройних сил.

Принцип пропорційності (Proportionality) закріплений у Статті 51(5)(b) Протоколу I [40, ст. 51]. Заборонено напад, який може спричинити випадкові втрати життя серед цивільного населення та шкоду цивільним об'єктам, які були б надмірними щодо очікуваної безпосередньої воєнної переваги.

Специфіка в ІТ, зокрема, полягає в тому, що шкідливий програмний код має властивість неконтрольованого самокопіювання та поширення. В цілому, якщо військова кібероперація спрямована проти логістичної програми Міністерства оборони супротивника, але архітектура вірусу дозволяє йому

вирватися у відкриту мережу Інтернет та паралізувати цивільні енергомережі по всьому світу, такий напад є непропорційним і воєнним злочином. Класичним прикладом у доктрині розглядається атака вірусу NotPetya (2017 р.), яка завдала мільярдних збитків цивільному сектору по всьому світу.

Принцип військової необхідності (Military Necessity) дозволяє застосовувати силу лише в тих обсягах, які необхідні для досягнення легітимної військової мети з найменшими витратами ресурсів та часу. Кібератаки не можуть проводитися з метою помсти, залякування цивільного населення чи дезорганізації суспільства, якщо це не дає чіткої переваги на полі бою.

Принцип заборони завдання надмірних страждань та Застереження Мартенса полягає в тому, що заборонено використовувати цифрові інструменти, які за своєю природою завдають жорстоких, негуманних та непотрібних страждань (наприклад, маніпулювання даними про групи крові в базах даних поранених бійців). Однак, в умовах появи автономної кіберзброї на базі штучного інтелекту, яка здатна самостійно обирати цілі та писати код для атак без контролю людини, особливого значення набуває Застереження Мартенса (включене до Протоколу I) [42]. Воно проголошує, що у випадках, не передбачених конкретними договорами, цивільне населення та комбатанти залишаються під захистом принципів міжнародного права, що випливають із установлених звичаїв, принципів гуманності та вимог суспільної свідомості.

Окрім обов'язкових конвенційних принципів робоча група відкритого складу ООН у своїй Доповіді 2021 року кодифікувала 11 добровільних глобальних норм відповідальної поведінки держав (специфічні норми відповідальної поведінки держав (м'яке право ООН). Вони формують надбудову над класичним міжнародним правом і включають три такі принципи:

– Принцип належної обачності (Due Diligence): Держава зобов'язана не допускати, щоб її територія, інфраструктура або IP-адреси свідомо

використовувалися для здійснення транскордонних кібератак іншими державами чи терористичними угрупованнями [37, 30-50].

– Принцип недоторканність CERT: Держави не повинні здійснювати кібератаки на національні групи реагування на комп'ютерні надзвичайні ситуації (Computer Emergency Response Teams — CERT) інших країн та не мають використовувати їх для маскування шпигунства.

– Повага до прав людини онлайн: Держави підтверджують, що всі права людини, які діють в офлайні (свобода вираження поглядів, право на приватність), мають бути повністю захищені в онлайні.

Висновки до розділу 1

1. Отже, основны поняття, ознаки та види інформаційних технологій відіграють достатньо суттєву роль як теоретична основа у формуванні їх міжнародно-правового регулювання.

2. Підводячи підсумок варто зауважити, що та нормативна база, яка була сформована на початкових етапах, суттєво сприяла більшому осмисленнню правового врегулювання питань ніж ті, що наразі впроваджуються, забуваючи про важливість юридичної бази в цілому як галузі, яка повинна зосереджуватися на чітко встановлених поверхневих судженнях не враховуючи практичну реалізацію таких норм.

3. Отже, принципи міжнародного права у сфері інформаційних технологій формуються з базових загальносистемних принципів міжнародного права, які закріплені у відповідних нормах та діють в цій специфічній сфері з певною особливістю.

РОЗДІЛ 2
МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.1 Роль ООН, Ради Європи, Європейського Союзу та інших міжнародних організації у сфері інформаційних технологій

Роль ООН, Ради Європи, Європейського Союзу та інших міжнародних організацій у сфері інформаційних технологій проявляється через різний підхід до взаємодії відповідних установ, співпрацю, нормативні документи, які регулюють ці питання, або інші реалізаційні кроки формування простору в даній міжнародній площині. Міжнародні організації можна розподілити за основними складовими на ті, що здійснюють свою діяльність в сфері інформаційних технологій, а за додатковими складовими на ті, що створені виключно для діяльності в цій сфері.

Зокрема, Організація Об'єднаних Націй (ООН) відіграє багатогранну роль у розвитку та використанні інформаційних технологій у сучасному світі. Вона активно сприяє поширенню інформаційних технологій, забезпечує інформаційну безпеку, співпрацює з національними урядами та ІТ-сектором для досягнення цілей сталого розвитку та надає освітні можливості у сфері інформаційних технологій. ООН також використовує інформаційні технології для реагування на кризи та підтримки вразливих груп населення [79].

Організація має програму розвитку, яка використовує інформаційні технології не лише для досягнення цілей сталого розвитку, а й долучається до ІТ-проєктів, спрямованих на подолання глобальних викликів, наприклад, пандемії COVID-19. Фонди ООН реалізують соціальні проєкти, пропонуючи безкоштовні ІТ-курси для вразливих груп населення, таких як жінки, які постраждали від насильства, для їхнього працевлаштування та соціальної інтеграції.

При детальному огляді діяльності ООН, як ключовий міжнародний орган, відіграє значну роль у формуванні глобального інформаційного суспільства. Організація постійно адаптується до швидких змін у сфері інформаційних технологій, визнаючи їхній потенціал для розвитку та водночас усвідомлюючи пов'язані з ними виклики.

ООН активно співпрацює з різними стейкхолдерами для інтеграції інформаційних технологій у глобальні процеси. Наприклад, Глобальний договір ООН в Україні, ініціатива Генерального секретаря ООН, закликає компанії будувати свою діяльність та стратегію з урахуванням принципів сталого розвитку, що охоплює й IT-сферу. Міністерство цифрової трансформації України об'єднує зусилля з Мережею Глобального договору ООН для розвитку IT-сектору, зокрема у східному регіоні країни.

Міжнародна організація активно здійснює поширенням інформаційних технологій, визначаючи умови для ефективності своїх дій та перешкоди, які потрібно подолати; зосереджують окрему увагу на забезпеченні інформаційної безпеки в умовах діджиталізації та розповсюдження соціальних мереж; налагоджують партнерство з національними установами, такими як Міністерство цифрової трансформації України, для розвитку IT-сектору, зокрема в регіонах.

У сучасному світі, де діджиталізація та соціальні мережі створюють нові можливості, ООН приділяє значну увагу питанням інформаційної безпеки. Це включає розробку політик та стандартів для захисту інформаційних систем та даних.

ООН підтримує освітні та навчальні програми у сфері інформаційних технологій. Прикладом є проєкт Фонду ООН, який надає безкоштовні IT-курси для досить суттєвої кількості жінок по всій Україні, що постраждали від насильства, навчаючи їх програмуванню, вебдизайну, тестуванню та проєктному менеджменту. Це сприяє їхній економічній самостійності та інтеграції у ринок праці.

Рада Європи відіграє важливу роль у сфері інформаційних технологій. Вона, як одна з провідних організацій, здійснює діяльність в сфері ІТ в напрямку захисту прав людини, демократії та верховенства права, активно адаптує свою діяльність до викликів та можливостей, які створюють інформаційні технології. Її роль полягає у формуванні інформаційної політики, забезпеченні інформаційної безпеки та розробці стандартів у медіасфері, зважаючи на швидкий розвиток цифрових технологій. Організація координує законодавство країн-учасниць для дотримання норм ліберальної демократії та прав людини у цифровому просторі

Ключовими сферами діяльності Ради Європи слід вважати здійснення регулювання питань у сфері викликів в інформаційній політиці, які пов’язані із забезпеченням інформаційної безпеки в епоху глобальних інформаційно-технологічних змін; розроблення стандартів в сфері медіа, які враховують вплив інформаційних технологій на засоби масової інформації та необхідність скоординованих зусиль для вирішення спільних проблем; координація законодавства країн-учасниць для забезпечення норм ліберальної демократії, викладених у Європейській конвенції з прав людини, що поширюється й на цифрову сферу; забезпечення незалежності засобам масової інформації та вирішувати питання, які виникають внаслідок використання інформаційних технологій у медіапросторі [65].

Водночас, якщо детальніше аналізувати Раду Європи, то варто виділити її в трьох акцентних напрямках діяльності, таких як інформаційна політика та безпека, стандарти у сфері медіа і інформаційних технологій та захист прав людини у цифровому просторі.

Інформаційна політика та безпека у контексті швидкого розвитку інформаційних технологій: Рада Європи ідентифікує ключові виклики, які стосуються інформаційної політики. Одним з пріоритетних напрямків є забезпечення інформаційної безпеки. Це включає розробку стратегій для захисту даних, боротьбу з дезінформацією та кіберзлочинністю, а також підтримку відкритого та безпечного цифрового простору.

Стандарти у сфері медіа та інформаційних технологій: Рада Європи в даному напрямку відіграє важливу роль у встановленні стандартів для медіа, враховуючи вплив інформаційних технологій. ЗМІ (Засоби масової інформації) все більше стикаються з ідентичними проблемами, пов'язаними з використанням інформаційних технологій, що вимагає аналогічних та скоординованих зусиль на міжнародному рівні. Ці стандарти спрямовані на захист свободи вираження поглядів, забезпечення плюралізму медіа та незалежності журналістики в цифрову епоху.

Захист прав людини у цифровому просторі наразі здійснюється, як основна місія, що поширюється й на сферу інформаційних технологій. Організація працює над тим, щоб принципи ліберальної демократії та права людини, закріплені в Європейській конвенції, були дотримані й у віртуальному середовищі. Це передбачає вирішення питань, пов'язаних з приватністю, свободою слова онлайн, доступом до інформації та захистом від дискримінації у цифровому світі.

Загалом, Рада Європи є ключовим гравцем у формуванні нормативно-правової бази для цифрового простору в Європі, зосереджуючись на правах людини та демократії. Її діяльність допомагає країнам-учасницям адаптувати своє законодавство до викликів, пов'язаних з інформаційними технологіями, забезпечуючи інформаційну безпеку та свободу слова. Стандарти та рекомендації Ради Європи у сфері медіа сприяють незалежності та плюралізму ЗМІ в умовах цифрової трансформації. Робота Ради Європи у сфері інформаційних технологій підкреслює важливість міжнародної співпраці для вирішення глобальних інформаційно-технологічних викликів.

Роль Європейського союзу у сфері інформаційних технологій полягає в тому, що вона реалізується відповідно створеним агентствам, які сприяють її здійсненню через відповідні категорії, а зокрема їх відносять до децентралізованих агентств:

– Європейський центр компетенцій з кібербезпеки (ECCC) Румунія: разом із Мережею національних координаційних центрів є новою

структурою Європи для підтримки інновацій та промислової політики у сфері кібербезпеки;

– Європейське виконавче агентство з питань охорони здоров'я та цифрових технологій (HADEA) Бельгія: звертає увагу на амбіції, зокрема, на цифровізаційну стійкість для відповідності поточним і майбутнім викликам;
– Європейський інститут інновацій та технологій (EIT) Угорщина: спрямований на збільшення інновацій через співпрацю між промисловістю та освітніми організаціями [30; 31].

Європейський Союз запровадив «Міжнародну цифрову стратегію» для посилення технологічної конкурентоспроможності Європи, одночасно підтримуючи цифрову трансформацію країн-партнерів, також характерні три основні цілі: розширення співпраці через «Мережу цифрових партнерів», створення «Технологічної бізнес-пропозиції Європейського Союзу» та просування глобального цифрового управління.

Водночас вони надають технічну та наукову підтримку у вирішенні конкретних завдань та питань, які стосуються певних сфер діяльності Європейського Союзу, також вони сприяють взаємодії між різними інституціями та країнами, що допомагає у створенні спільної стратегії та плануванні дій і вони забезпечують обмін інформацією, аналітичними даними та кращими практиками, що сприяє покращенню якості та результативності роботи Європейського Союзу.

Крім цього, агентства підтримують розвиток та впровадження європейських політик та стандартів, сприяють відкритому обміну ідеями та досвідом між країнами, а також сприяють підвищенню ефективності та довіри до суспільства Європейського Союзу. Агентства сприяють співпраці між країнами Європейського Союзу шляхом координації роботи інституцій Європейського Союзу та національних урядів. Вони також можуть надавати консультації та рекомендації для рішень відповідно до галузі своєї компетенції.

Загалом, агентства Європейського Союзу відіграють ключову роль у забезпеченні ефективності та координації роботи Європейського Союзу, сприяючи досягненню його цілей, покращенню якості життя громадян та забезпеченню стабільності та процвітання всієї Європейської спільноти, продовжуючи рости та збільшувати свій вплив на формування та реалізацію європейських політик зі створення нових агентств, які спеціалізуватимуться на нових аспектах сучасного життя і вимогах суспільства.

Водночас щодо інших наявних міжнародних організацій, які здійснюють безпосередню діяльність в сфері інформаційних технологій та відіграють ключову роль у розвитку, стандартизації та регулюванні інформаційних технологій на глобальному рівні, то ці організації охоплюють широкий спектр діяльності, від розробки технічних стандартів до формування політики та сприяння співпраці у сфері інформаційних технологій.

Міжнародна федерація з обробки інформації (IFIP) є всесвітньою організацією для дослідників та фахівців, що працюють в галузі інформаційних та комунікаційних технологій. Міжнародна федерація з обробки інформації є глобальною некомерційною організацією, заснованою під егідою ЮНЕСКО у 1960 році. Вона об'єднує національні науково-технічні товариства з обробки інформації з 56 країн. Місія Міжнародної федерації з обробки інформації полягає у розвитку науки та технологій в галузі інформатики та інформаційно-комунікаційних технологій, сприянні дослідженням, освіті та застосуванню інформаційних технологій для блага суспільства [82].

Всесвітня організація інтелектуальної власності (ВОІВ) займається захистом інтелектуальної власності, включаючи комп'ютерні програми та передачу даних через інформаційні мережі. Всесвітня організації інтелектуальної власності є глобальним форумом для послуг, політики, інформації та співпраці у сфері інтелектуальної власності. В умовах інформатизації, однією з ключових задач всесвітньої організації інтелектуальної власності є захист прав інтелектуальної власності на

комп'ютерні програми та дані, що передаються через інформаційні мережі. Це допомагає стимулювати інновації та творчість у сфері інформаційних технологій [84].

Роль наступних міжнародних організацій безпосередньо направлена на діяльність, пов’язану зі взаємодією з відповідними технологіями.

Наприклад, міжнародний союз електрозв'язку (International Telecommunication Union), спеціалізована установа ООН, займається стандартизацією та регулюванням міжнародного зв'язку, включаючи радіо, телебачення та інтернет. Міжнародний союз електрозв'язку (ITU) є найстарішою міжнародною організацією, яка займається питаннями зв'язку, заснованою у 1865 році [85].

Загалом, це спеціалізована установа ООН, відповідальна за координацію глобального використання радіочастотного спектру, сприяння міжнародній співпраці у виділенні супутникових орбіт, розробку технічних стандартів для забезпечення безперебійного з'єднання мереж та технологій, а також покращення доступу до інформаційно-комунікаційних технологій для громад у всьому світі.

Міжнародна організація зі стандартизації (International Organization for Standardization) – це міжнародна організація створена в 1947 році, яка спеціалізується на стандартизації та суміжних видах, пов’язаних зі стандартизацією технічних об’єктів. Роль організації полягає в уніфікації правил та стандартів до єдиного виду того чи іншого процесу технологічної розробки до відповідності [86].

Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers) одна з масштабніших міжнародна організація, яка створена в 1963 році. Організація також орієнтована на ключову роль здійснення розвитку технологій, розробці та підтримки стандартизації технічних об’єктів [87].

Інтернет корпорації з призначення доменних імен та номерів (Internet Corporation for Assigned Named and Numbers): міжнародна корпорація

створена в 1998 році, здійснює роль в сфері керування доменними іменами, IP-адресами [88].

Консорціум Всесвітнього павутиння (World Wide Web Consortium): міжнародна організація, яка створена в 1994 році. Роль організації спрямована на стабілізацію мережі інтернету, встановлюючи відповідні для цього стандарти [90].

Рада з інтернет-інженерії (Internet Engineering Task Force) відкрита до міжнародного співробітництва та створена в 1986 році. Роль організації в сфері інформаційних технологій спрямована на розвиток мережевих технологічних рішень зі встановленням відповідних стандартів для забезпечення відповідного рівня якості [91].

Існують також національні та регіональні IT-асоціації, які співпрацюють на міжнародному рівні, наприклад, Українська асоціація фахівців інформаційних технологій (УАФІТ) та Асоціація «ІКТ-Маркетинг» в Україні.

Загалом спеціалізовані міжнародні організації, міжнародні організації у сфері інформаційних технологій охоплюють широкий спектр діяльності від технічної стандартизації до правового регулювання та захисту інтелектуальної власності. Участь у роботі цих організацій дозволяє країнам та компаніям впливати на глобальні стандарти та політику в інформаційних технологіях.

Вони сприяють співпраці між дослідниками, фахівцями та урядами для вирішення спільних викликів та використання можливостей, які надають інформаційні технології. Захист інтелектуальної власності в цифровій сфері є ключовим завданням для таких організацій, як Всесвітня організація інтелектуальної власності, що стимулює інновації.

2.2 Міжнародно-правовий захист персональних даних, приватності та цифрових прав людини

Дослідження щодо міжнародно-правового захисту персональних даних, приватності та цифрових прав людини відіграє суттєву роль в умовах сьогодення.

В загальному розумінні, персональні дані являють собою будь-яку інформацію, що прямо або опосередковано стосується ідентифікованої або такої, що може бути ідентифікована, щодо фізичної особи [26; 64].

До персональних даних включаючи, але не обмежуючись відносяться: ім'я та прізвище, дата народження, місце проживання, паспортні дані, номер телефону, електронна пошта, IP-адреса, біометричні дані, геолокаційна інформація [8].

Право на приватність, в свою чергу, охоплює можливість особи самостійно визначати межі доступу до інформації про своє особисте життя. Класичне розуміння права на приватність бере свій початок від фундаментальної праці Семюеля Воррена та Луї Брандайса «The Right to Privacy» (1890 р.), де воно визначалося як «право бути залишеним у спокої» (the right to be let alone) [92]. На етапі індустріального суспільства приватність розглядалася переважно у просторовому та фізичному аспектах як недоторканність житла, таємниця листування та захист від фізичного проникнення у приватне життя особи.

З появою перших електронно-обчислювальних машин та автоматизованих баз даних у другій половині двадцятого століття концепція зазнала суттєвої трансформації. У 1983 році Федеральний конституційний суд Німеччини у своєму історичному рішенні щодо проведення перепису населення (Volkszählungsurteil) сформулював Доктрину інформаційного самовизначення (informational self-determination) [101].

Згідно з цією концепцією, індивід має право самостійно вирішувати, коли, як і в яких межах інформація про його приватне життя може стати доступною іншим особам, організаціям чи державним органам.

У двадцятому столітті, в умовах існування соціальних мереж, хмарних обчислень та Інтернету речей, приватність перестала бути просто можливістю сховатися від суспільства. Сьогодні це, по суті, право на контроль за своїм «цифровим слідом» (digital footprint), захист від автоматизованого

профайлінгу (складання цифрового портрету особи для маніпуляції її поведінкою) та право на анонімність у глобальній мережі.

Водночас право на приватність є одним із базових прав людини. Воно забезпечує захист особистого життя від неправомірного втручання з боку держави, приватних компаній або інших осіб.

У цифрову епоху зміст цього права значно розширився та включає:

– захист електронних комунікацій;
– конфіденційність листування;
– захист цифрової ідентичності;
– контроль над використанням персональних даних.

Особливу роль у розвитку права на приватність відіграє практика Європейського суду з прав людини. Однак основу міжнародно-правового захисту приватності становлять міжнародні акти у сфері прав людини.

Серед низки міжнародних нормативних документів особливе значення займають:

– Загальна декларація прав людини 1948 року [89];
– Міжнародний пакт про громадянські і політичні права 1966 року [84];
– Європейська конвенція про захист прав людини і основоположних свобод 1950 року [65];
– Конвенція Ради Європи №108 [24];
– Загальний регламент захисту даних Європейського Союзу (GDPR) [22].

Зокрема, Загальна декларація прав людини ООН (1948 р.): Відповідно до Статті 12, ніхто не може зазнавати безпідставного втручання в його особисте і сімейне життя, безпідставного зазіхання на недоторканність його житла, таємницю його листування чи на його честь і репутацію.» [89, ст.12].

Аналогічні положення містить стаття 17 Міжнародного пакту про громадянські і політичні права (1966 р.) [83, ст.17]. Стаття 17 дублює та посилює положення Декларації, накладаючи на держави-учасниці позитивне зобов'язання не лише утримуватися від неправомірного втручання, а й

ухвалити законодавчі акти для захисту осіб від таких посягань з боку третіх сторін [89].

Конвенція про захист прав людини і основоположних свобод (1950 р.): Стаття 8 «Право на повагу до приватного і сімейного життя» стала найбільш динамічним інструментом захисту приватності у світі завдяки широкому та еволюційному тлумаченню її положень Європейським судом з прав людини [65, ст.8].

Відповідно до статті 55 Статуту ООН, яка передбачає, що повага та розвиток людської гідності є важливою метою Організації Об'єднаних Націй [40, ст.55]. Стаття 12 Загальної декларації прав людини, прийнятої Генеральною Асамблеєю ООН 10 грудня 1948 року, забороняє свавільне або незаконне втручання в особисте життя, сім'ю, житло чи комунікації будь-якої особи, а також забороняє навмисні посягання на репутацію та честь будь-якої особи [89, ст.12].

Однак, цифрові права людини все ж являють собою сукупність прав і свобод, що реалізуються в цифровому середовищі, включаючи право на доступ до Інтернету, захист персональних даних, свободу вираження поглядів онлайн та право на цифрову безпеку, а міжнародно-правовий інститут захисту персональних даних виокремився із загального права на приватність наприкінці 1970-х років, коли стало зрозуміло, що традиційні механізми не здатні врегулювати транскордонні потоки комп'ютеризованої інформації.

В свою чергу, Конвенцію Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (Конвенція 108+ або Конвенція № 108) та її модернізацію слід вважати першим юридично обов'язковим міжнародним договором у цій сфері [24]. Даний документ став відкритим для підписання у Страсбурзі з 28 січня 1981 року. Ця Конвенція заклала універсальні принципи обробки даних, які згодом лягли в основу національних законодавств низки країн світу (включаючи Закон України «Про захист персональних даних»).

Окремо, зважаючи на тотальну зміну технологічного підходу, у 2018 році було ухвалено Модернізований протокол, який трансформував документ у Конвенцію 108+. Оновлений текст договору впровадив такі інновації:

- Посилення вимог щодо легітимності обробки (принцип прозорості та явна згода суб'єкта).
- Розширення категорій «чутливих даних» (sensitive data), до яких тепер віднесено генетичні та біометричні дані.
- Обов'язковість повідомлення про витік даних (data breach notification) контролюючим органам.
- Створення сильних, незалежних наглядових органів із широкими повноваженнями щодо накладення санкцій.

Водночас Конвенція 108+ залишається єдиним глобальним міжнародним договором, до якого можуть приєднуватися держави, що не є членами Ради Європи, що робить її універсальним містком для гармонізації світових стандартів приватності [24].

Загальний регламент про захист даних Європейського Союзу (GDPR) був ухвалений у 2016 році та введений в дію 25 травня 2018 року (Регламент ЄС 2016/679 (General Data Protection Regulation)) [22].

Загалом він став найбільш жорстким, прогресивним та впливовим документом у сфері цифрового права. Юридична унікальність цього Регламенту полягає в його екстратериторіальній дії (стаття 3) [22, ст.3]. Водночас його дія поширюється на компанії, розташовані за межами Європейського Союзу, якщо вони пропонують товари чи послуги суб'єктам даних в Європейському Союзі або здійснюють моніторинг їхньої поведінки в цілому.

По суті, Регламент закріпив шість фундаментальних принципів обробки персональних даних, які станом на 2026 рік визнані золотим стандартом світового інформаційно-технологічного комплаєнсу:

- Принцип законності, справедливості та прозорості здебільшого полягає в тому, що дані мають оброблятися на законних підставах, а

суб'єкт повинен чітко знати, хто, навіщо і як довго використовує його персоналізовану інформацію [22, ст. 6].

- Принцип обмеження мети здебільшого полягає в тому, що персональні дані збираються для чітко визначених легітимних цілей і не можуть оброблятися у спосіб, несумісний з цими цілями.
- Принцип мінімізації даних здебільшого полягає в тому, що оброблятися мають лише ті дані, які є дійсно необхідними для виконання поставленого завдання (нічого зайвого) [22, ст. 5].
- Принцип точності здебільшого полягає в тому, що неточні або застарілі дані мають бути негайно видалені або виправлені [22, ст. 5].
- Принцип обмеження зберігання здебільшого полягає в тому, що дані не повинні зберігатися довше, ніж це необхідно для цілей їх обробки [22, ст. 5].
- Принцип цілісності та конфіденційності здебільшого полягає в тому, що забезпечення належного технічного та організаційного захисту від несанкціонованої обробки, втрати чи знищення є критично важливим [22].

Феномен впливу Загального регламенту захисту даних Європейського Союзу (GDPR) на законодавство інших країн (таких як Бразилія з її LGPD, Каліфорнія з CCPA/CPRA, або оновлені закони Японії та Південно-африканської республіки) отримав у міжнародному праві назву «Ефект Брюсселя» (The Brussels Effect), коли стандарти Європейського Союзу де-факто стають обов'язковими для глобального бізнесу, який прагне зберегти доступ до європейського ринку [22].

Водночас норми міжнародних конвенцій залишалися б декларативними без динамічного судового тлумачення. Практика Європейського суду з прав людини (ЄСПЛ) та Суду Справедливості Європейського Союзу сформували сучасні межі допустимого втручання держави у цифрове життя громадян.

Європейський суд з прав людини (ЄСПЛ) розглядає Статтю 8 Європейської конвенції з прав людини як «живий інструмент» (living

instrument), який має адаптуватися до умов сучасного інформаційного суспільства. Суд сформував розлогу практику щодо неприпустимості тотального масового стеження без чітких законодавчих меж та судового контролю [65, ст.8].

Зокрема, справа «Big Brother Watch та інші проти Великої Британії» (2021 р.): Велика палата Європейського суду з прав людини (ЄСПЛ) визнала, що режим масового перехоплення електронних комунікацій (bulk interception), який практикувався спецслужбами, порушував Статтю 8 Європейської конвенції з прав людини через відсутність належного незалежного нагляду та чітких критеріїв відбору даних для аналізу. Суд підкреслив, що метадані (час дзвінка, геолокація, тривалість з'єднання) слід вважати не менш чутливими, ніж сам зміст розмови, оскільки дозволяють скласти інтимний портрет життя людини [43].

Суд Справедливості ЄС відіграв ключову роль у захисті європейських стандартів приватності від зазіхань з боку спецслужб третіх країн через розгляд позовів австрійського юриста та активіста Максиміліана Шремса.

По суті, вище зазначений суд у цих справах виступив як (конституційний захисник) фундаментальних прав Європейського Союзу (статті 7, 8 та 47 Хартії фундаментальних прав ЄС розкриває право на приватність, захист персональних даних та ефективний судовий захист) [43; 60 ст.7, 8, 47].

Варто зауважити, що він (суд), встановив важливий стандарт: рівень захисту персональних даних у третій країні повинен бути «essentially equivalent» суттєво еквівалентним рівню захисту в Європейському Союзі і це стало обов’язковим критерієм для будь-яких транскордонних передач даних.

Окрім цього відбулося зміцнення принципу верховенства прав людини над економічними та безпековими інтересами: відповідно даний суд чітко дав зрозуміти, що масовий доступ спецслужб до даних європейців без індивідуальних підозр, без пропорційності та без ефективних засобів правового захисту є несумісним з європейським правопорядком. Це рішення має яскраво виражений правозахисний характер і посилює позицію

Європейського Союзу у глобальному дискурсі щодо балансу між національною безпекою та приватністю.

Додатково слід зазначити, що набуло подальшого розвитку міжнародне інформаційне право, а в свою чергу, Суд Справедливості ЄС підтвердив, що існуюче міжнародне право (зокрема, положення Міжнародного пакту про громадянські і політичні права, Конвенції 108+/ Загальний регламент Європейського Союзу про захист даних) застосовується до кіберпростору. Він підкреслив, що національна безпека не є абсолютним виправданням для масового стеження за іноземцями [24; 25; 84].

Проблеми, які виявив Суд Справедливості Європейського Союзу посилили роль міжнародного права та продемонстрували:

– відсутність ефективних судових засобів захисту для неамериканських громадян у США;
– недостатню незалежність механізмів оскарження (наприклад, Privacy Shield Ombudsperson);
– надмірну широту повноважень американських спецслужб.

Значення для міжнародного права безпосередньо полягає в тому, що Рішення стало прецедентом для інших регіонів і країн, які прагнуть високих стандартів захисту даних. По суті, воно посилило позицію Ради Європи (Конвенція 108+) та ООН у дискусіях щодо права на приватність у цифрову епоху та підкреслело фрагментацію глобального регулювання даних і необхідність нових міжнародних угод (на кшталт EU-US Data Privacy Framework, який також піддається критиці та можливим майбутнім позовам Шремса) [24; 45].

Загалом, через позови Максиміліана Шремса Суд Справедливості Європейського Союзу став одним із найвпливовіших міжнародних судових органів у сфері цифрових прав. Він не просто скасував два механізми передачі даних, а сформував новий глобальний стандарт: пріоритет фундаментальних прав людини над комерційними інтересами та державною безпекою третіх

країн. Це класичний приклад того, як регіональний суд може суттєво впливати на розвиток міжнародного права.

В загальному аспекті саме ці судові прецеденти змусили США реформувати систему нагляду за власними спецслужбами та створити спеціальний Суд із перегляду питань захисту даних (Data Protection Review Court (DPRC)) для іноземних громадян, що продемонструвало прямий вплив міжнародного цифрового права на національне оборонне законодавство наддержав.

Водночас цифрові права людини в умовах сучасності розглядаються як права нового покоління. Відповідно у сучасній правовій доктрині триває дискусія щодо класифікації поколінь прав людини. Традиційні три покоління (громадянські/політичні; економічні/соціальні; колективні права) сьогодні доповнюються четвертим поколінням: цифровими та біометричними правами, які випливають із віртуального існування особи та розвитку біотехнологій.

Право бути забутим (The Right to be Forgotten): Вперше легалізоване Судом Європейського Союзу у знаковій справі Google Spain проти AEPD та Маріо Костеха Гонсалеса (2014 р.), а згодом закріплене у Статті 17 Загального регламенту захисту даних Європейського Союзу (GDPR) як «право на стирання» [22, ст.17].

Суть справи: Особа має право вимагати від пошукових систем та інтернет-платформ видалення посилань на персональну інформацію про неї, якщо ці дані є застарілими, неточними, надмірними або втратили законні підстави для обробки.

Правова колізія: Це право постійно перебуває в стані делікатного балансу із правом на свободу вираження поглядів та свободу інформації (Стаття 10 Європейської конвенції з прав людини). Міжнародні суди чітко визначили, що «право бути забутим» не є абсолютним і не застосовується, якщо інформація має високу суспільну значущість (наприклад, дані про злочини політиків чи історичні події) [23, ст.10; 65].

Право на захист від автоматизованого прийняття рішень та профайлінгу:

Стаття 22 Загального регламенту захисту даних Європейського Союзу (GDPR) та новітні міжнародні стандарти встановлюють, що право особи не підлягати рішенню, яке породжує юридичні наслідки для неї або подібним чином істотно впливає на неї, якщо таке рішення базується виключно на автоматизованій обробці, включаючи профайлінг [22, ст.22].

Суть справи: Якщо банк відмовляє у видачі кредиту, або алгоритм штучного інтелекту відхиляє резюме кандидата при прийомі на роботу, або скорингова система визначає рівень правопорушень особи, то суб’єкт має право вимагати втручання людини (human intervention), висловити власну точку зору та оскаржити рішення робота.

Право на шифрування та анонімність: У 2024–2026 роках на рівні Ради ООН з прав людини розгорнулася гостра боротьба за визнання наскрізного шифрування (end-to-end encryption) базовим елементом права на приватність. Держави, мотивуючи це боротьбою з тероризмом та захистом дітей, намагаються законодавчо зобов'язати месенджери (Signal, WhatsApp, Telegram) створювати «бекдори» (backdoors) для спецслужб.

Проте, варто звернути увагу, що міжнародні інституції захисту прав людини стоять на позиції, що послаблення шифрування для однієї цілі руйнує безпеку всієї мережі Інтернет, роблячи мільярди цивільних громадян уразливими для кіберзлочинців та авторитарних режимів

Зокрема, Організація Об'єднаних Націй розглядає цифрові права як невід'ємну складову прав людини: У резолюції Ради ООН з прав людини 2012 року було підтверджено, що права людини, які існують офлайн, повинні однаково захищатися і в онлайн-просторі, тому ООН в цілому приділяє особливу увагу: захисту свободи слова в Інтернеті; захисту персональних даних; боротьбі з масовим цифровим стеженням; регулюванню штучного інтелекту.

Водночас варто звернути увагу, Європейський Союз як світовий лідер у сфері захисту персональних даних створив одну з найрозвиненіших,

комплексних і впливових систем захисту персональних даних у світі, основними елементами якої слід вважати:

– Загальний регламент захисту даних (GDPR) [22];
– Хартія основних прав ЄС [60];
– практика Суду Європейського Союзу;
– діяльність Європейської ради із захисту даних.

Загалом, ця система базується на поєднанні сильної нормативної бази, високих конституційних стандартів, активної судової практики та ефективних інституційних механізмів. Завдяки цьому Європейський Союз став глобальним еталоном регулювання у сфері захисту персональних даних, а його підходи активно запозичуються іншими країнами та регіонами (так званий Brussels Effect).

Загальний регламент захисту даних (GDPR, Regulation (EU) 2016/679) є центральним елементом європейської системи захисту даних. Він набув чинності нещодавно (25 травня 2018 року), але безпосередньо застосовується в усіх країнах-членах ЄС. Серед ключових особливостей цього Регламенту (GDPR) у контексті захисту персональних даних слід виокремити такі: екстериторіальна дія (ст. 3), що поширюється на компанії з усього світу, якщо вони обробляють дані резидентів Європейського Союзу; сім основних принципів обробки даних (ст. 5): законність, справедливість, прозорість, обмеження метою, мінімізація даних, точність, обмеження зберігання, цілісність і конфіденційність, а також підзвітність (accountability); розширені права суб’єктів даних: право на доступ, виправлення, видалення («право бути забутим»), обмеження обробки, перенесення даних, заперечення проти обробки, у тому числі проти автоматизованих рішень; жорстка відповідальність: штрафи до 20 млн євро або 4% від глобального річного обороту компанії; обов’язок проводити (Data Protection Impact Assessment (DPIA)), призначати (Data Protection Officer (DPO)) та вести реєстр обробки даних [22, ст. 3, ст. 5].

Наступним не менш значущим елементом системи захисту персональних даних Європейського Союзу слід вважати Хартію основних прав Європейського Союзу (2000/2012). Цю Хартію основних прав Європейського Союзу ще знаменують як (Конституційний фундамент системи) [60].

На відміну від багатьох правових систем світу (зокрема США), де доречі приватність розглядається переважно як категорія споживчого права чи захисту від необґрунтованих обшуків, в ЄС захист даних піднесено до рівня невіддільних прав людини (fundamental human rights).

Водночас Хартія основних прав Європейського Союзу (має силу Установчих договорів) розділяє це поняття на дві самостійні правові норми розкриті в таких статтях:

– Стаття 7 (Повага до приватного і сімейного життя): Класичне право «бути залишеним у спокої» (right to be left alone), що захищає житло, таємницю комунікацій та особистий простір від свавільного втручання держави чи третіх осіб [60, ст. 7].

– Стаття 8 (Захист персональних даних): Новаторська норма цифрової епохи. Вона проголошує, що будь-яка обробка даних має здійснюватися лише на законних підставах (наприклад, за згодою), прозоро та для чітко визначених цілей, а головне вона закріплює право кожної людини на доступ до зібраних про неї даних та право на їх виправлення, а також вимагає контролю з боку незалежних органів [60, ст. 8].

– Стаття 47 (Право на ефективний судовий захист) [60, ст. 47].

В цілому, Суд Справедливості Європейського Союзу неодноразово підкреслює, що Загальний регламент захисту даних (GDPR) повинен тлумачитися саме крізь призму цих статей Хартії основних прав Європейського Союзу, що надає захисту даних саме конституційний статус. Хартія має статус конституційного документа ЄС і є найвищим рівнем захисту прав у європейському правопорядку [60; 22].

Практика Суду Справедливості Європейського Союзу розглядається в якості третього елементу системи захисту персональних даних. В комплексі

системи Суд Справедливості Європейського Союзу відіграє роль конституційного суду Європейського Союзу у сфері даних і значно розвинув та посилив положення Загальний регламент захисту даних (GDPR).

Найважливіші рішення: Google Spain (C-131/12, 2014): започаткування «права бути забутим»; Schrems I (2015) та Schrems II (2020): скасування Safe Harbor і Privacy Shield, встановлення стандарту «essential equivalence»; Meta (Facebook): штраф 1,2 млрд євро (2023) та рішення C-446/21 (2024) щодо обмеження використання даних для персоналізованої реклами; Рішення 2023–2025 років щодо нематеріальної шкоди, прозорості алгоритмів та транскордонних передач даних [47; 49].

В цілому, Суд Справедливості Європейського Союзу послідовно проводить лінію на пріоритет фундаментальних прав людини над комерційними інтересами технологічних компаній. Суд Справедливості Європейського Союзу виступає головним «живим» інтерпретатором та захисником європейських стандартів приватності, послідовно обмежуючи посягання як європейських урядів, так і спецслужб третіх країн. Як епохальні судові прецеденти Суду Справедливості Європейського Союзу в якості прикладу слід виокремити наступні:

– Справа Digital Rights Ireland (2014): Суд визнав недійсною Директиву про збереження даних (Data Retention Directive), яка зобов'язувала провайдерів масово та без розбору зберігати метадані комунікацій усіх громадян. Суд постановив: масове стеження без конкретної підозри є непропорційним [46].

– Справа Google Spain (2014): Суд вперше легітимізував «право на забуття», зобов'язавши пошуковий гігант видаляти з видачі застарілі або нерелевантні лінки на персональні дані людини за її запитом [47].

– Серія справ Schrems I (2015) та Schrems II (2020): Суд скасував міжнародні угоди про передачу даних між Європейським Союзом та Сполученими Штатами Америки (Safe Harbor та Privacy Shield), оскільки американське розвідувальне законодавство (FISA Section 702) дозволяло АНБ

здійснювати масове стеження за іноземцями, не надаючи європейцям засобів судового захисту. Цим Суд підтвердив, що права людини в Європейському Союзі не можуть бути предметом політичного чи економічного компромісу в міжнародних договорах [49].

Європейська рада із захисту даних (European Data Protection Board (EDPB) розглядається як четвертий елемент системи захисту персональних даних. Європейська рада із захисту даних це центральний координаційний (регуляторний) орган Європейського Союзу у сфері захисту даних, створений відповідно до Загального регламенту захисту даних (GDPR) [22]. До його складу входять представники національних наглядових органів усіх країн-членів та Європейський наглядач із захисту даних (EDPS). По суті, він об'єднує керівників національних наглядових відомств із захисту персональних даних усіх країн Європейського Союзу (наприклад, таких як CNIL у Франції чи BfDI в Німеччині) та Європейського інспектора з захисту даних (EDPS).

Функціональна роль Європейської ради із захисту даних (EDPB) у системі міжнародного права:

– Єдність правозастосування (Consistency Mechanism): Рада забезпечує однакову інтерпретацію Загального регламенту захисту даних (GDPR) по всьому ЄС. Якщо німецький та ірландський регулятори сперечаються щодо штрафу для великого Big Tech гіганта, остаточне та обов'язкове рішення ухвалює EDPB [22].

– Розробка керівних настанов (Guidelines): Європейська рада із захисту даних (EDPB) видає детальні юридичні роз’яснення щодо складних технологічних питань: як регулювати використання файлів cookies, як захищати дані в хмарних обчисленнях, як трактувати згоду користувача у системах штучного інтелекту чи блокчейн-технологіях.

– Узгодження міжнародних трансферів: Саме Європейська рада із захисту даних (EDPB) оцінює, чи забезпечують треті країни належний рівень захисту даних для того, щоб дозволити туди вільний транскордонний експорт інформації.

Загалом, міжнародно-правовий захист персональних даних, приватності та цифрових прав людини пройшов еволюційний шлях від просторової концепції недоторканності житла до глобальної системи захисту цифрової ідентичності особи. Аналіз сучасного стану цієї сфери дозволяє звернути увагу на низку ключових моментів, а саме: Конвергенція стандартів: Завдяки «Ефекту Брюсселя» та модернізації Конвенції 108 (Конвенція 108+), у світі відбувається поступова уніфікація правил обробки персональних даних. Європейська модель, що базується на пріоритеті прав людини над комерційними інтересами корпорацій, де-факто виграє глобальну конкуренцію в американської ліберальної та китайської тоталітарної цифрових моделей [24].

Другим моментом є Технологічний розрив: Головною проблемою міжнародного цифрового права залишається висока швидкість розвитку технологій порівняно із бюрократичними процедурами ухвалення міжнародних договорів. Поява генеративного штучного інтелекту та нейротехнологій вимагає від міжнародних інституцій переходу від жорстких статичних правил до гнучких рамок регулювання, заснованих на оцінці ризиків (risk-based approach).

Необхідність Універсальної конвенції: Регіональні інструменти (Загальний регламент про захист даних Європейського Союзу (GDPR), акти Ради Європи) є ефективними, проте вони не вирішують проблему глобальних цифрових питань (data havens): країн із низьким рівнем захисту даних, де зловмисники та Big Tech корпорації можуть безконтрольно обробляти інформацію [28].

Міжнародна спільнота під егідою ООН має вийти на рівень підписання Глобальної конвенції про цифрові права людини, яка б зафіксувала право на шифрування, анонімність, захист від безконтрольного ШІ-профайлінгу та когнітивну свободу як універсальні права четвертого покоління для всього людства.

2.3 Міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинності

Міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинності є специфічним середовищем, оскільки воно не має ні національних, ні міжнародних кордонів, тому ефективне співробітництво та регулювання, особливо щодо кіберзагроз, потребує скоординованих дій на глобальному, регіональному та двосторонньому рівнях.

Зокрема, теорія міжнародного співробітництва в кібербезпеці базується на договорах (Будапештська конвенція), м'якому праві (GGE) та принципах міжнародного права. Міжнародне співробітництво в цій сфері регулюється низкою правових документів, до яких, поміж іншого, відносять:

– міжнародні договори (Будапештська конвенція про кіберзлочинність (2001) криміналізує чотири групи злочинів (доступ, перехоплення, втручання в дані/систему, шахрайство, дитяча порнографія); процедури взаємної правової допомоги (MLA)) [20]; Додатковий протокол до Конвенції кіберзлочинність (криміналізація расистських та ксенофобних дій через комп’ютерні системи); Другий додатковий протокол до конвенції про кіберзлочинність (спрощення транскордонного доступу до доказів (електронних даних), пряма співпраця з провайдерами, спільні слідчі групи) [93]; UNTOC (Палермська конвенція) факультативний протокол (форми організованої злочинності) [51]; Африканська конвенція про кібербезпеку (2014)) [53];

– м’яке право, де визначають принципи ООН GGE (2013, 2015, 2021), Рекомендації ITU щодо кібербезпеки, норми відповідальної поведінки держав;

– регіональне право (Закон Європейського Союзу про кібербезпеку (2019), GDPR (2016), Директива NIS2 (2023), Рішення Ради Європи про співпрацю у кіберпросторі) [22];

– принципи міжнародного права визначаються статтею 2 Статуту ООН (Суверенітет, невтручання, заборона застосування сили), статтею 51 (право на самооборону) та принцип взаємної правової допомоги [40, ст.2, ст.51].

Водночас, аналізуючи документи, варто окреслити чотири ключові теоретичні концепції міжнародного співробітництва: територіальний суверенітет, доктринальну «екстериторіальна юрисдикція», регульовані принципи та теорію атрибуції, кожна з них відіграє важливу роль при формуванні загального способу співробітництва в цій сфері безпеки та протидії.

З теорії, Глобальний характер кіберзагроз потребує міжнародної взаємодії в цілому. Важливу роль у цьому процесі відіграють міжнародні організації, насамперед НАТО, Європейський Союз та Організація Об'єднаних Націй. Основними напрямами міжнародного співробітництва є: обмін інформацією про кіберзагрози; спільні навчання та тренування; розробка міжнародних стандартів безпеки; координація реагування на кіберінциденти; підготовка фахівців з кібербезпеки, тому міжнародна співпраця сприяє підвищенню рівня кіберстійкості держав та ефективному протистоянню сучасним загрозам.

Водночас виникає колізія між територіальним суверенітетом та транскордонним характером кіберзлочинів у контексті місця вчинення діяння: класичне міжнародне право вимагає згоди держави на юрисдикційні дії на її території, але в кіберпросторі докази часто фізично розташовані за кордоном.

Доктрина «екстериторіальної юрисдикції»: деякі держави (США, Велика Британія) на законному рівні мають право отримувати доступ до транскордонних цифрових доказів через юрисдикційно підконтрольних їм провайдерів; наприклад, американський CLOUD Act (2018) зобов'язує компанії США надавати електронні докази незалежно від місця їх фізичного зберігання [55]. Таким чином, зокрема, впроваджуються нові підходи замість класичного територіального принципу.

Регульовані принципи міжнародного співробітництва: принцип «рівня юрисдикційної лояльності» – компроміс між збереженням суверенітету та необхідністю швидкого доступу до доказів; принцип подвійної кримінальності – діяння має бути злочином у запитуючій та запитуваній

державі; принцип спеціалізації – отримані докази можуть використовуватися лише для тієї справи, з якої надійшов запит; принцип пропорційності – заходи обмеження прав мають бути співмірними з тяжкістю злочину; взаємна правова допомога (MLA) – традиційний механізм, але в кіберспрaвах часто надто повільний.

Теорія «атрибуції» відображається у встановленні відповідальності держави за кібератаки, зокрема, через докази, наприклад, згідно з ILC Draft Articles on State Responsibility (Проєкт статей про відповідальність держав за міжнародно-протиправні діяння (2001 рік)) [56].

Загалом, міжнародне співробітництво у сфері кібербезпеки включає різні підходи щодо формування правової позиції для вирішення та запобігання кіберзлочинності, тому доцільно буде розглянути наступні позиції, механізми та відповідні їх виклики:

– Правова грамотність, як один з ключових компонентів спрямований на узгодження національних законодавств щодо кіберзлочинності та захисту даних [7; 8]. З основних документів варто виокремити Будапештську конвенцію про кіберзлочинність (Рада Європи 2001 року), яка характерна тим, що є одним з перших міжнародних договорів, який регулює та класифікує кіберзлочини, як кримінальні правопорушення (наприклад несанкціонований доступ до даних) та GDPR (документ Європейського Союзу), який регулює питання персональних даних і визначає права та обов’язки суб’єктів таких даних щодо юридичного процесу їх захисту [20, 22];

– Інформаційний обмін, як встановлений процес обміну даними про загрози, інциденти, вразливість, які повинні контролюватися відповідними спеціалізованими міжнародними установами (FIRST, CERT/CSIRT мережі) [94; 95].

– Оперативна співпраця, як безпосередній механізм взаємодії врегулювання кіберпростору під час кіберзагроз, створюючи оперативні розслідування, транскордонний доступ до доказів та інші технічні можливості в даному питанні (Європол та Інтерпол).

– Навчання та розвиток потенціалу щодо вдосконалення процедур міжнародного співробітництва та протидії в кіберпросторі. Їх, зазвичай, організовують міжнародні організації ООН, НАТО, OSCE, які проводять різні тренінги, стажування, обмін технологічними рішення, здійснюючи безпосередню діяльність в сфері міжнародного співробітництва заради зменшення рівня кіберзлочинності шляхом посилення кібербезпеки.

– Публічно-приватне співробітництво на міжнародному рівні щодо питань кооперації різних міжнародних організацій, держав, компаній та інших учасників, які мають вплив на врегулювання даного питання, а для прикладу варто навести компанію Microsoft Digital Crimes Unit, яка спрямовує діяльність підрозділу саме на правову та Інтернет безпеку.

Водночас як ключові міжнародні документи та рамки слід розглянути: Будапештську конвенцію про кіберзлочинність (2001) – перший міжнародний договір, що криміналізує несанкціонований доступ, перехоплення, шахрайство, дитячу порнографію та встановлює процедури співпраці [20]; UN Group of Governmental Experts (GGE) – рекомендації щодо відповідальної поведінки держав у кіберпросторі; NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) – дослідницька та навчальна платформа, участь України з 2023 р.; EU Cybersecurity Act (2019) – створення EU Agency for Cybersecurity (ENISA) та рамок сертифікації [17]; Global Forum on Cyber Expertise (GFCE) – платформа для розвитку потенціалу країн, що розвиваються.

Разом з цим, аналізуючи практичні кейси реалізації кібербезпеки та питань протидії кіберзлочинності, слід звернути увагу на такі: (Операція «Avalanche» (Європол, 2016) – знешкодження ботнету та шкідливого програмного забезпечення, задіяно 30+ країн.; операція «Disrupt» (FBI, 2022) – вилучення інфраструктури програми-вимагача Hive: спільна робота з правоохоронцями 11 країн; проєкт «Keep» (Інтерпол) – щорічні глобальні акції проти фішингу, шахрайства в електронній комерції). Наведений перелік не є вичерпним: бази даних містять значну кількість різних інших судових прецедентів та судових справ за напрямком.

Справа про транскордонний збір доказів: Перша справа стосується прецеденту між Microsoft Corp. v. United States (2016–2018, США), де уряд США вимагав доступу до електронних листів, що зберігалися в Ірландії. Суд першої інстанції: ордер діє лише в територіальних межах; уряд має використовувати механізм взаємної правової допомоги. Апеляційний суд: позицію Microsoft підтримано [57]. Результат: ухвалення CLOUD Act (2018) – дозволяє США отримувати дані від американських провайдерів незалежно від місця зберігання за умови угод з іноземними державами [55].

Друга справа за цим напрямком є «Snowden» (2013) та Європейський суд з прав людини (2018, Big Brother Watch проти Великої Британії), де масове стеження за не громадянами через PRISM. ЄСПЛ визнав порушення ст.8 ЄКПЛ (право на приватність) через відсутність належного нагляду. Вирок створив прецедент для вимог пропорційності та прозорості в транскордонному зборі даних [58].

Третя справа: Сполучені Штати проти Ульбріхта (2015) – Silk Road. Факти: Адміністратор даркнет-майданчика (Росс Ульбріхт) засуджений у США за наркоторгівлю, відмивання коштів, злом. Юрисдикційне обґрунтування: сервери розташовані в США, транзакції через американські банки, жертви – громадяни США. Результат: довічне ув'язнення; підтверджено принцип екстериторіальної юрисдикції за «ефективним» та «територіальним» принципами. Суд визнав юрисдикцію на підставі того, що транзакції відбувалися через сервери в США та впливали на американських громадян. Прецедент для кримінального переслідування міжнародних кіберзлочинців навіть без їхньої фізичної присутності. [59].

Справи про кіберзлочинність та юрисдикцію. Перша справа за напрямком, яка демонструє специфіку прецеденту є R. v. Sheppard (2021, Велика Британія), де хакер із Великої Британії зламав сервери в США та Канаді. Суд визнав британську юрисдикцію на підставі територіального принципу (дії вчинено з території Великої Британії) та ефективного застосування принципу (шкода завдана британським компаніям).

З іншої сторони справа про атрибуцію та державну відповідальність за кібератаки. В даному напрямку є три судових прецеденти, які в повній мірі розкривають специфіку. Перша ICJ – Нікарагуа проти США (1986), однак тут її безпосередньо не відносять до кіберсправ, принцип «ефективного контролю» застосовується до атрибуції кібератак: держава несе відповідальність, якщо вона здійснювала «ефективний контроль» над діями недержавних суб'єктів.

Другий прецедент OPCW – хімічні атаки в Сирії (2013, 2018), кібератаки, як частина гібридних конфліктів; розслідування OPCW-UN демонструють спроби застосувати міжнародне право до кіберінцидентів (атрибуція через технічні докази).

Третій прецедент: агресії Росії проти України – кібератаки на енергосистему (2015-2017) атрибутовані українською стороною (Fancy Bear, Sandworm). Міжнародне співтовариство застосувало санкції на основі доказів (наприклад, санкції ЄС та США 2018–2022).

Четвертий прецедент Естонія (2007), кібератаки на державні установи, приписані Росії. Естонія звернулася до ЄС та НАТО, але без прямого судового розгляду (оскільки немає міжнародного суду з кіберзлочинності) [52].

П'ятий прецедент NotPetya (2017), атрибуція Україною та західними країнами Росії (Sandworm). Кримінальні впровадження порушені в Україні, але міжнародна юрисдикція реалізується через санкції, а не через судові вироки.

Підсумовуючи, судові прецеденти варто охарактеризувати, як різні застосовані механізми (взаємна правова допомога, як офіційний запит через центральні органи; Європейський наказ про розслідування, який застосовується під час збору доказів в кримінальних справах та відповідних прецедентах; спільні слідчі групи, створення міжнародних команд, здійснюючи співпрацю для проведення розслідування; публікація ордерів через cloud Act/ 2nd Protocol до Будапештської конвенції, здійснюючи прямий запит) [20; 55].

Водночас в судовій практиці в просторі міжнародного співробітництва у сфері щодо кіберпростору варто окреслити п’ять викликів:

1) Несумісність темпу правосуддя з технологіями, де судові процеси тривають роками, а кіберзлочинці змінюють інструменти за тижні.
2) Докази в шифрованому вигляді, при якому суди часто не можуть зобов'язати розшифрувати дані без порушення прав людини.
3) Юрисдикційні колізії, де множинність юрисдикцій сприяють виникненню різних прецедентів (наприклад, справа USA v. Assange – одночасно позови США, Швеції, Еквадору).
4) Відсутність універсального суду, через бракування спеціалізованого міжнародного кримінального суду для кіберзлочинів виникає багато суперечливих питань.
5) Як ключовий елемент в якості ризику несанкціонованого використання під час імплементації даних, які завантажуються в датасет, як елемент аналітики під час проведення судової експертизи. Даний аспект повинен враховувати морально-етичні аспекти під час застосування таких технологій [5].

В міжнародному співробітництві Україна активно залучена до спільноти в сфері кібербезпеки. Зокрема, поміж іншого, Україна ратифікувала в 2005 році Будапештську конвенцію про кіберзлочинність; співпрацює з CERT-UA, FIRST, NATO CCDCOE (Об’єднаний центр передових технологій з кібероборони НАТО); учасник EU Cyber Diplomacy Toolbox, а з 2022–2025 рр. відіграє важливішу роль в контексті «цифрового фронту», який спрямовує не тільки як отримання технічної допомоги, а головне створює нові практичні прецеденти, надаючи прямий досвід зі протистояння гібридним атакам.

Підсумовуючи, міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинності має критичне значення, але стикається з політичними, правовими та технологічними перешкодами. Подальший процес розвитку потребує зміцнення довіри, уніфікації правових норм та посилення оперативної координації. Судова практика, хоча й фрагментарна, але

демонструє тенденцію до розширення екстериторіальної юрисдикції (CLOUD Act), посилення ролі взаємної правової допомоги (2-й Протокол) та спроб атрибуції держав крізь призму відповідальності (стандарт ICJ). Проте ключові виклики: швидкість, технологічність та відсутність єдиного суду – залишаються невирішеними.

Висновки до розділу 2

1. Отже, роль розглянутих міжнародних організації, які здійснюють свою діяльність в даній сфері полягає в тому, що вони сприяють розвитку інновацій, через співпрацю з дослідниками, фахівцями та урядами для вирішення низки суспільних викликів, які формуються з відповідних інформаційних технологій.

2. Міжнародна спільнота під егідою ООН має вийти на рівень підписання Глобальної конвенції про цифрові права людини, яка б зафіксувала право на шифрування, анонімність, захист від безконтрольного ШІ-профайлінгу та когнітивну свободу як універсальні права четвертого покоління для всього людства.

3. Підсумовуючи, варто зазначити, що міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинності має критичне значення, яке стикається з різними викликами та зокрема з політичними, правовими та технологічними перешкодами. Наразі подальші дії здебільшого з орієнтовані на поверхневе вирішення питань, які потребують більшого аналізу та переосмислення навіть на даній стадіїї, що відображається в судові практиці та практичних кейсах щодо таких кіберзлочинів.

РОЗДІЛ 3
ПЕРСПЕКТИВИ РОЗВИТКУ МІЖНАРОДНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

3.1 Правове регулювання штучного інтелекту, великих даних та цифрових платформ у міжнародному праві

Правове регулювання штучного інтелекту, великих даних та цифрових платформ у міжнародному праві є специфічним середовищем особливо зі сторони юриспруденції, що, в першу чергу, дозволяє спостерігати та аналізувати різноманітність підходів, в тому числі щодо правового регулювання у міжнародному праві.

Міжнародно-правове регулювання в контексті штучного інтелекту, великих даних та цифрових платформ у міжнародному праві є важливими питаннями, які потребують детального розгляду та окремого контролю через швидкий розвиток технологій сучасності та їх безпосередній вплив на різні аспекти суспільства.

Загалом, серед головних аспектів міжнародного права, які регулюють правові особливості штучного інтелекту, великих даних та цифрових платформ є: регуляторні рамки; права людини; міжнародне співробітництво; відповідальність і правоохоронні органи; інновації та розвиток.

Регуляторні рамки: технології штучного інтелекту, збору великих даних та врахування специфіки роботи цифрових платформ, що створюють нові виклики для правових систем. В цілому Міжнародні організації, такі як ООН та Європейський Союз, працюють над створенням стандартів і норм, що регулюють ці технології. Наприклад, Загальний Регламент Європейського Союзу про захист даних «General Data Protection Regulation» стає важливим прикладом того, як міжнародні норми можуть впливати на діяльність компаній, що обробляють великі обсяги даних [25].

Права людини: важливо враховувати, як використання штучного інтелекту та великі дані впливають на права людини. Наприклад, питання конфіденційності, права на захист особистих даних, а також можливість дискримінації, яка може виникнути з упередженими алгоритмами. Міжнародне право має забезпечити захист прав осіб у цій новій ері активного розвитку інформаційних технологій [32; 36].

Міжнародне співробітництво: оскільки для штучного інтелекту, великих даних та цифрових платформ невизначено відповідних кордонів, країни мають плідно співпрацювати для створення ефективних механізмів, в тому числі правового регулювання. В умовах сьогодення цей аспект може включати: угоди про обмін інформацією, спільні дослідження та розробку етичних норм для врегулювання використання інформаційних технологій. Наприклад, Кодекс етики штучного інтелекту в подальшому слід врахувати як основу для впровадження міжнародних стандартів [4].

Відповідальність і правоохоронні органи: саме вони визначають юридичну відповідальності за дії, здійснені за допомогою штучного інтелекту (наприклад, в випадку автономних автомобілів або медичної діагностики): це є суттєво важливим питанням. Міжнародне право має розробити чіткі рамки для визначення, хто несе відповідальність за шкоду, заподіяну внаслідок використання технології штучного інтелекту.

Інновації та розвиток: наука і технології повинні «йти в ногу» з правовими нормами. Міжнародні правові системи мають підтримувати інновації, забезпечуючи при цьому відповідний рівень захисту прав та свобод громадян. Це вимагає постійного моніторингу розвитку технологій і адаптації законодавства.

З цього варто виокремити низку міжнародних судових органів (наприклад, Міжнародний суд ООН чи Міжнародний кримінальний суд) щодо штучного інтелекту (Artificial Intelligence), великих даних (Big Data) та цифровий платформ (Digitalization platform), позиції яких ще формуються, при цьому міжнародна судова практика активно розвивається на рівні

національних юрисдикцій, які в сукупності створюють глобальний досвід. Водночас ці національні практики часто обговорюються на міжнародних форумах і впливають на формування майбутніх міжнародних правових норм.

Загалом, разом з цим, в Сполучених Штатах системи штучного інтелекту, такі як COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), використовувалися для оцінки ризику рецидиву злочинців. Однак, це викликало значні дебати та судові розгляди щодо можливої упередженості алгоритмів та дискримінації.

Зокрема справа State v. Loomis у Вісконсині (2016) є яскравим прикладом, де використання оцінки ризику, згенерованої штучним інтелектом, було оскаржено як порушення права обвинуваченого на належну правову процедуру, оскільки алгоритм був запатентованим і його внутрішня логіка не була повністю розкрита стороні захисту. Це підкреслило проблему «чорної скриньки» штучного інтелекту у судочинстві [61].

Водночас британська судова система досліджує використання штучного інтелекту для прискорення процесу перегляду документів у великих комерційних справах (e-discovery), а також для аналізу судових рішень. Хоча штучний інтелект не приймає остаточних рішень, він допомагає юридичним фахівцям ефективніше обробляти величезні обсяги інформації.

Разом з цим Сінгапур активно впроваджує технології штучного інтелекту в свої судові процеси, зокрема для автоматизації рутинних завдань, пошуку інформації у великих текстових документах та підготовки проєктів судових рішень. Це дозволяє підвищити ефективність судочинства.

В умова сьогодення в Україні також обговорюється та впроваджується використання технології штучного інтелекту у судовій практиці. Приклади включають: пошук інформації у великих масивах документів, підготовку релізів судових рішень та аналіз судової практики для забезпечення її єдності. Існують дискусії щодо допустимості використання матеріалів, згенерованих штучним інтелектом, як доказів у суді та їхнього впливу на оскарження вже прийнятих судових рішень.

Низка таких країн як Австралія, Гонконг, Нова Зеландія також активно вивчають та впроваджують цифрові трансформації у своїх судових системах, використовуючи штучний інтелект та великі дані для підвищення ефективності та доступності правосуддя.

Однак, як практичні кейси з правового регулювання технологій варто перерахувати деякі приклади, які демонструють міжнародну судову практику щодо штучного інтелекту, великих даних та рівень зосередження на інтеграції цих технологій у національні судові системи різних держав світу для оптимізації процесів, де наукова спільнота також стикається з фундаментальними правовими питаннями, такими як справедливість, прозорість, відповідальність та захист прав людини. Дискусії та рішення, прийняті в цих національних юрисдикціях формують основу для розробки майбутніх міжнародних стандартів та регулювання в цілому.

Міжнародне право у сфері штучного інтелекту перебуває на етапі активного формування, реагуючи на швидкий розвиток технологій та їхній глобальний вплив. Основна мета полягає у створенні універсальних принципів та норм, які б забезпечували етичне та безпечне використання штучного інтелекту, захищали права людини та сприяли міжнародному співробітництву у цій сфері. Це безпосередньо включає розробку документів такими організаціями, як ЮНЕСКО та Рада Європи, що спрямовані на встановлення етичних рамок та правових конвенцій.

Швидкий розвиток штучного інтелекту, загалом, вимагає створення концептуально нових міжнародно-правових механізмів для регулювання його використання. Хоча ЮНЕСКО у 2021 році ухвалила Рекомендації з етики штучного інтелекту, що стало першим універсальним документом у цій сфері, який встановлює спільні цінності та принципи для етичного розвитку та використання штучного інтелекту, а Рада Європи розробила Конвенцію про штучний інтелект у 2024 році, яка має на меті забезпечити повагу до прав людини, демократії та верховенства права у контексті використання штучного інтелекту та є важливим кроком у міжнародному регулюванні загальні

питання потребують особливої уваги на міжнародному рівні, тому що використання штучного інтелекту порушує питання захисту прав людини, зокрема конфіденційності даних та запобігання дискримінації. [71, 28]. На додаток до цього міжнародне правоохоронне співробітництво також інтегрує штучний інтелект для обміну оперативною інформацією та виявлення загроз, що суттєво автоматизує рутинні процеси та скорочує час для прийняття рішень як політичних так і управлінських.

Разом з цим розвиток штучного інтелекту, великих даних та цифрових платформ кардинально змінює соціальні та правові структури, створюючи нові виклики для міжнародного правового регулювання. Сучасний світ характеризується діджиталізацією, що робить питання регулювання штучного інтелекту та великих даних одним із ключових на міжнародному рівні. Міжнародні ініціативи та інструменти набирають обертів, а разом з цим кілька міжнародних організацій активно працюють над розробкою правових та етичних рамок для штучного інтелекту:

ООН схвалений Глобальний цифровий договір, який є доповненням до Пакту, намагається сформулювати загальні принципи регулювання штучного інтелекту [96].

Зокрема, в умовах сучасності ключові виклики Регулювання штучного інтелекту, великих даних та цифрових платформ стикаються з низкою складних питань:

- права людини, де використання штучного інтелекту може впливати на такі права, як конфіденційність, свобода слова, право на справедливий судовий розгляд та захист від дискримінації.
- відповідальність визначають юридичною відповідальностю за дії, вчинені автономними системами штучного інтелекту, що залишається складним питанням.
- інтелектуальна власність, де існують відповідні суттєві виклики щодо правового регулювання створення об'єктів інтелектуальної власності за допомогою штучного інтелекту.

– міжнародна взаємодія при якій інтеграція штучного інтелекту у міжнародну правоохоронну взаємодію охоплює обмін оперативною інформацією та виявлення загроз, що вимагає гармонізації норм.

Однак варто також порівняти правові методи низки країн та регіонів, які проявляють різні підходи до регулювання штучного інтелекту в цілому. Наприклад, Європейський Союз у 2024 р. ухвалив Акт про штучний інтелект (AI Act), який є першим у світі комплексним законом про штучного інтелекту, що класифікує системи штучного інтелекту за рівнем ризику та встановлює відповідні вимоги. Цей підхід може слугувати моделлю для міжнародних стандартів [28].

Станом на 2025–2026 роки розвиток генеративного штучного інтелекту та нейроінтерфейсів (наприклад, комерційних пристроїв типу Neuralink чи аналогів) вивів загрози для приватності за межі звичного збору анкетних даних. Наразі актуальною постає загроза для ментальної приватності. Алгоритми машинного навчання на основі непрямих цифрових слідів (швидкості друку, рухів очей, лайків, тривалості затримок екрана) здатні реконструювати емоційний стан особи, її політичні уподобання, сексуальну орієнтацію та приховані психологічні вразливості.

Зокрема і в зв’язку з цим на міжнародно-правовому рівні першою комплексною відповіддю став Європейський акт про штучний інтелект (EU AI Act), на який покладаються великі перспективи [28]. Цей акт запровадив жорсткі заборони на використання штучного інтелекту для:

- когнітивного маніпулювання поведінкою людей, що може завдати їм шкоди;
- невибіркового збору зображень облич з інтернету чи камер відеоспостереження для створення баз даних розпізнавання (як це робила компанія Clearview AI).
- систем соціального скорингу (оцінки благонадійності громадян на основі поведінки, за прикладом Китайської Народної Республіки (КНР).

Біометричні дані (шаблони обличчя, відбитки пальців, геометрія сітківки, хода) згідно зі Статтею 9 Загального регламенту Європейського Союзу про захист персональних даних (GDPR) належать до спеціальних категорій даних, обробка яких загалом заборонена без чіткої індивідуальної згоди. Масове використання камер із функцією автоматичного розпізнавання облич у публічних просторах міст фактично знищує концепцію анонімності у громадських місцях [22, ст.9].

В цілому комітет Організації Об'єднаних Націй (ООН) з прав людини у своїх загальних зауваженнях наголошує, що повсюдне використання біометричного трекінгу має так званий «охолоджуючий ефект» (chilling effect) і впливає на реалізацію інших фундаментальних прав, зокрема поміж іншого свободи мирних зібрань, свободи слова та асоціацій, оскільки громадяни уникають участі в мирних протестах через страх бути автоматично ідентифікованими та внесеними до «чорних списків» відповідних органів.

Водночас міжнародно-правове регулювання великих даних створює головний виклик міжнародного права щодо таких даних, а це в якійсь мірі правовий баланс між вільним транскордонним потоком даних (необхідним для глобальної цифровізації та / або діджиталізації) та цифровим суверенітетом держав (захистом національних інтересів та приватності в цілому).

Захист персональних даних та екстериторіальність: Європейський Загальний регламент про захист даних (GDPR) встановив глобальний стандарт, тобто будь-яка передача великих масивів даних за межі Європейського Союзу вимагає від третіх країн аналогічного рівня захисту (принцип Adequacy decision) [25]. Схожі закони ухвалили низка країн світу (наприклад, CCPA (Головний закон штату Каліфорнія про захист персональних даних споживачів) в США, LGPD (Загальний закон Бразилії про захист персональних даних у Бразилії), що фактично сприяло формуванню загального міжнародного звичаєвого права захисту даних [62; 63].

Зазвичай Міжнародне торгове право щодо питанн великих даних регулюються в межах угод про електронну комерцію. Загалом, ключовим

правилом виступає заборона державам вимагати обов'язкової локалізації даних (вимоги зберігати дані виключно на серверах всередині країни) як умови для ведення міжнародного бізнесу, окрім випадків пов’язаних з питаннями національної безпеки.

Крім цього, міжнародне право комплексно захищає великі масиви даних не виокремлюючи як персональні (комерційні бази, супутникові знімки тощо) через інститути інтелектуальної власності (права на бази даних) та Угоду ТРІПС в контексті щодо захисту комерційної таємниці. Угода ТРІПС (Угода Світової Організації Торгівці (СОТ) про торговельні аспекти прав інтелектуальної власності): ключовий міжнародний документ, який зобов'язує держави-учасниці захищати нерозкриту інформацію, в тому числі комерційну таємницю від незаконного отримання, розголошення чи використання третіми особами [66].

Міжнародно-правове регулювання цифрових платформ теж має певні особливості варті додаткової уваги. В умовах сучасності цифрові платформи (соціальні мережі, маркетплейси, пошукові системи) перетворилися на транснаціональних суб'єктів, які де-факто мають власну юрисдикцію (правила модерації, внутрішні суди). Міжнародне право намагається повернути їх у правове поле держав за допомогою трьох інструментів: регулювання контенту та протидія гібридним загрозам, антимонопольне регулювання ринку, міжнародне оподаткування.

Зокрема регулювання контенту та протидія гібридним загрозам полягає в тому, що цифрові платформи безпосередньо несуть міжнародну відповідальність за поширення пропаганди війни, терористичного контенту та кібершахрайства. Міжнародним еталоном в цьому питанні слід вважати Акт про цифрові послуги (DSA). Він зобов’язує платформи відкривати свої алгоритми рекомендацій для міжнародних аудиторів та швидко видаляти нелегальний контент за запитом регуляторів [68].

Поряд з цим антимонопольне регулювання ринку полягає в тому, що великі цифрові платформи отримали статус «гейткіперів» (цифрових

воротарів). Міжнародна спільнота через Організацію економічного співробітництва та розвитку і регіональні акти (наприклад, Акт про цифрові ринки (DMA)) обмежує монополію Великих даних. Їм заборонено надавати перевагу власним продуктам на своїх цифрових платформах та примусово прив'язувати користувачів до однієї екосистеми [69].

Міжнародне оподаткування слід вважати так званим «Історичним проривом» під егідою Організації економічного співробітництва та розвитку (ОЕСР) та G20 (група двадцяти) стало впровадження Двокомпонентного плану (Two-Pillar Solution). Цифрові платформи зобов’язані сплачувати мінімальний глобальний корпоративний податок у тих країнах, де вони фактично отримують доходи, навіть якщо у них немає там фізичних офісів або представництв.

Загалом, з цього варто визначити потребу саме спостерігати за розвитком міжнародних регуляторних ініціатив, таких, як Рекомендації ЮНЕСКО та Конвенція Ради Європи, для розуміння глобальних тенденцій у правовому регулюванні штучного інтелекту.

Однак, окремо варто також враховувати тенденції і національного законодавства, які інтегрують міжнародні принципи, оскільки вони формують основу для майбутніх універсальних норм.

Отже, безпосередню увагу слід акцентувати на питання етики та права людини у будь-якій розробці чи використанні штучного інтелекту, щоб забезпечити відповідність міжнародним стандартам. Також варто враховувати специфічні питання відповідальності та інтелектуальної власності у контексті штучного інтелекту, оскільки ці сфери потребують чітких правових рішень на міжнародному рівні.

3.2 Інформаційні технології в умовах збройних конфліктів та загроз міжнародній безпеці

Нинішні тенденції поширення збройних конфліктів, в певній мірі, породжують нові виклики та створюють загрози для міжнародної безпеки, що

сприяє явному збільшенню їх кількості та призводить до стрімкого розвитку інформаційних технологій, тому доцільно розглянути їх вплив на глобальні процеси міжнародного рівня в цілому.

Загалом, в загальному аспекті розвиток інформаційних технологій спричинив появу нових викликів для міжнародного права. Традиційні норми міжнародного гуманітарного права формувалися в період, коли кіберпростір та цифрові технології ще не існували, тому сьогодні міжнародне співтовариство активно працює над адаптацією існуючих правових механізмів до нових умов сучасних реаліїв.

Окрім того, основою міжнародно-правового регулювання залишаються положення Організації Об'єднаних Націй; Статут Організації Об'єднаних Націй; Женевські конвенції 1949 року; додаткові протоколи до Женевських конвенцій; міжнародні звичаї та принципи міжнародного гуманітарного права [40; 42].

Статут ООН забороняє застосування сили проти територіальної цілісності або політичної незалежності держав. Водночас залишається дискусійним питання, чи може масштабна кібератака розглядатися як акт агресії або збройний напад у розумінні статті 51 Статуту ООН [40, ст.51].

Разом з цим, відповідно до Статті 48 Додаткового протоколу I, сторони конфлікту повинні завжди розрізняти цивільні об'єкти та військові цілі [42, ст.48]. У кіберпросторі цей принцип реалізувати найважче через феномен подвійного призначення (Dual-use інфраструктура). Одинакові сервери, оптоволоконні кабелі, маршрутизатори та хмарні сховища використовуються одночасно цивільними лікарнями, банками та логістичними підрозділами збройних сил.

Крім цього, правова доктрина наголошує: атака на вузол зв'язку подвійного призначення є законною ціллю лише за умови, що його знищення дає чітку військову перевагу, а супутня шкода цивільному населенню не буде надмірною.

В цілому, якщо детальніше аналізувати поняття збройних конфліктів та пов’язаних питань в міжнародній безпеці, то їх об’єднує поняття напад або атака на цифрові дані як головного об’єкту. Він регламентується статтею 49 Додаткового протоколу І, який визначає напад як «акти насильства проти супротивника» [42, ст.49]. Серед міжнародних юристів, науковців триває дискусія: чи є самі по собі цифрові дані «об'єктом», який можна атакувати:

- Консервативна школа права: Дані не є матеріальними, тому їх видалення чи модифікація за допомогою вірусу-Wiper (без фізичного пошкодження жорсткого диска) не є «нападом» у розумінні міжнародного гуманітарного права.
- Прогресивна школа (підтримується МКЧХ (Міжнародний Комітет Червоного Хреста) та Україною): Дані є критичним елементом життєдіяльності сучасного суспільства. Знищення електронних реєстрів прав власності, медичних карток чи баз даних пенсійного забезпечення має такий же руйнівний соціальний ефект, як спалення архівів у фізичному світі. Тому видалення даних має кваліфікуватися як напад і регулюватися міжнародним гуманітарним правом.

Більшість сучасних експертів також погоджується, що кібератака, наслідки якої еквівалентні наслідкам традиційного збройного нападу (наприклад, руйнування електростанцій або загибель людей), може бути підставою для реалізації державою права на самооборону.

Дана Концепція збройних конфліктів та загроз міжнародній безпеці уперше сформульована військовими теоретиками США наприкінці двадцятого століття, передбачала перетворення інформаційної переваги на чинник безпосередньої бойової сили шляхом об’єднання сенсорів (розвідки), систем управління та засобів ураження в єдину мережу.

У двадцять першому столітті ця парадигма еволюціонувала. Інформаційні технології забезпечили перехід від локальних автоматизованих систем управління військами до глобальних бойових екосистем, де кожен

військовослужбовець, дрон або стаціонарний радар функціонують як вузли єдиної інформаційної матриці.

Загалом, кібератаки під час конвенційних бойових дій суттєво відрізняються від кримінального хакерства (ransomware) чи промислового шпигунства. Їх основна мета: дезорганізація державного управління, знищення критичної інфраструктури та деморалізація населення. В основному військові кібероперації поділяють на три ключові категорії:

1) Деструктивні атаки (Wipers): Програмне забезпечення, масковане під здирників, яке безповоротно знищує Master Boot Record (MBR) та файлові системи. Яскравими прикладами сімейства шкідливого програмного забезпечення слід вважати: HermeticWiper, CaddyWiper та AcidRain, використані проти українських державних органів та супутникових терміналів напередодні 24 лютого 2022 року.
2) Атаки на критичну інфраструктуру (OT/ICS attacks): Таргетовані удари по операційним технологіям та системам SCADA. Атаки на енергомережі, гідротехнічні споруди та залізничний транспорт (наприклад, атаки угруповання Sandworm на українську енергосистему).
3) Кібершпигунство (APT-операції): Advanced Persistent Threats (розвинені сталі загрози), спрямовані на довготривале приховане перебування в мережах міністерств оборони та закордонних справ для викрадення планів, даних розвідки та алгоритмів логістики.

В свою чергу, якщо розглядати концептуальну цифрову стійкість, що є одним з прецедентів сучасних воєнних дій, здійснивши демонтаж парадигми «локальних серверних кімнат», фізичне знищення дата-центрів ракетними ударами змусило держави переходити на транскордонну хмарну архітектуру.

Однак загрози таких аспектів міжнародній безпеці та наявність самої кризи міжнародного права демонструє проблематику атрибуції, де визначають головну юридичну та політичну складність кібервійни, яка полягає у проблемі

атрибуції – доведенні причетності конкретного уряду до проведення цифрової атаки.

Концептуалізація кіберзброї та кібератак: у міжнародному праві доктринально тривалий час точилася дискусія щодо того, чи можна кваліфікувати кібератаку як «застосування сили» (use of force) або «збройний напад» (armed attack) в розумінні Статті 2(4) та Статті 51 Статуту ООН [40, ст.2(4), ст.51]. На сьогодні, завдяки кодифікаційній роботі Групи урядових експертів ООН (UN GGE) та виходу Талліннського посібника 2.0 (Tallinn Manual 2.0), сформувався консенсус щодо так званого підходу за наслідками (effects-based approach) [37].

Відповідно до цього підходу, кібероперація прирівнюється до збройного нападу, якщо її наслідки аналогічні наслідкам конвенційного удару: фізичне руйнування інфраструктури, травмування або загибель людей.

Правило 14 Талліннського посібника 2.0: Кібероперація становить застосування сили, коли її наслідки за масштабом і суворістю еквівалентні некогнітивним (фізичним) кінетичним операціям [37, с. 84-87].

Проте сіра зона міжнародного права залишається відкритою для операцій, які не викликають миттєвих фізичних руйнувань, але повністю паралізують державу:

– Масові атаки програм-стерувачів (Wipers), такі як NotPetya (2017) або HermeticWiper (2022), що знищують критичні бази даних міністерств та фінансового сектору.
– Блокування державних комунікацій через розгалужені DDoS-атаки під час розгортання кінетичного наступу.

Гаазькі конвенції забороняють нейтральним державам дозволяти воюючим сторонам відкривати на їхній території радіостанції чи використовувати лінії зв'язку для військових цілей. Проте ці правила стосуються виключно урядів. Вони не забороняють приватним компаніям, розташованим у нейтральних або третіх країнах, надавати послуги воюючим сторонам.

Водночас, коли компанія SpaceX надає Україні термінали Starlink для забезпечення зв'язку Збройними Силами України (ЗСУ), а компанія Palantir інтегрує свої алгоритми штучного інтелекту для коригування артилерійського вогню, виникає правовий прецедент. Ці компанії зареєстровані в США. Сполучені Штати офіційно не є стороною конфлікту. З точки зору класичного міжнародного права дії SpaceX і Palantir є приватними комерційними послугами, що не порушує статус нейтралітету США.

З правової точки зору, такі дії часто балансують на межі між «актом насильства» (attack) та заходами, що не досягають цього порогу, що ускладнює легітимну реалізацію права держави на самооборону.

Держави-агресори активно використовують так звані «проксі-групування» (квазі-незалежні хакерські банди, такі як Killnet чи LockBit), щоб формально зняти з себе відповідальність за порушення міжнародного права. Водночас, якщо ідентифікація джерела атаки за класичними стандартами НАТО раніше тривала тижнями, то бойовий досвід України довів необхідність створення систем атрибуції в реальному часі.

Роль НАТО та Європейського Союзу у якості забезпечення кібербезпеки визначаються після кібератак на державні та критичні об'єкти різних країн, при цьому саме питання кібербезпеки стало одним із пріоритетів міжнародної політики. НАТО визнає кіберпростір окремою операційною сферою поряд із сушею, морем, повітрям та космосом. У 2016 році на саміті НАТО у Варшаві офіційно було проголошено кіберпростір повноцінною сферою ведення операцій.

З іншої сторони Європейський Союз реалізує комплексну політику кіберзахисту, що включає: Директиву NIS2; Європейський акт про кіберстійкість; програми цифрової безпеки; співпрацю між державами-членами у сфері реагування на кіберінциденти [44; 48].

Також, однією з найбільших проблем міжнародного права є встановлення відповідальності за кібератаки. На відміну від традиційних військових дій, у кіберпросторі складно визначити справжнього виконавця

атаки. Зазвичай для цього використовується процедура атрибуції, де відбувається встановлення зв'язку між кібероперацією та конкретною державою.

Проте з огляду на фундаментальні постулати міжнародного кримінального права є принцип персональної відповідальності. За воєнні злочини судять конкретних людей: командирів, які віддали наказ або солдатів, які його виконали.

У випадку використання повністю автономного дрона зі штучним інтелектом, який через галюцинацію алгоритму комп'ютерного зору переплутав цивільний шкільний автобус із військовою вантажівкою та знищив його, виникає вакуум відповідальності:

- Оператор не знав про помилку, бо дрон діяв автономно в умовах РЕБ (радіоелектронна боротьба).
- Командир, який запустив дрон, діяв у межах стандартних процедур.
- Програміст/Розробник, який писав код нейромережі, не міг передбачити всі аномалії вибірки даних (data bias) під час навчання моделі.
- Сам штучний інтелект не є суб'єктом права і не може нести кримінальну відповідальність.

Цей юридичний глухий кут, тобто безвихідь, вважається причиною того, що в межах Конвенції ООН про конкретні види звичайної зброї (CCW) у Женеві вже кілька років тривають запеклі дебати щодо повної заборони або жорсткого регулювання «роботів-убивць». Станом на 2026 рік юридично обов'язкового договору досі не підписано через супротив країн, які є лідерами військово-технологічних перегонів.

Використання генеративного штучного інтелекту (NLP / LLM моделей, дипфейків) у межах психологічних операцій та інформаційного протиборства досягло рівня, коли воно загрожує не лише стабільності окремої держави, а й базовим правам людини [9].

Одним з таких є дипфейки та порушення права на самовизначення, де масове поширення ШІ-генерованого контенту, спрямованого на дестабілізацію виборчих процесів або розпалювання внутрішніх етнічних конфліктів (як це реалізується в межах гібридних операцій РФ проти країн Балтії та Молдови), порушує Міжнародний пакт про цивільні та політичні права, зокрема Статтю 1 (право народів на вільне визначення свого політичного статусу) [97, ст. 1]. Ситуація коли, інформаційне середовище повністю контролюється та спотворюється іноземними ШІ-ботами, громадяни позбавляються можливості робити свідомий, незманіпульований вибір.

В свою чергу, проблема кваліфікації інформаційного геноциду демонструє, що міжнародне право визнає підбурювання до геноциду міжнародним злочином (Стаття III Конвенції про запобігання злочину геноциду та покарання за нього 1948 року) [98, ст.3]. Проте сучасні ІТ-технології дозволяють автоматизувати цей процес. Алгоритми рекомендацій соціальних мереж (таких як Facebook або TikTok) оптимізовані під залучення користувачів через гнів та радикалізацію.

Також історичний прецедент у М'янмі (2017 рік), коли алгоритми Facebook сприяли поширенню мови ворожнечі проти народу рохінджа, що призвело до реального геноциду, продемонстрував, що технологічні платформи можуть ставати інструментами міжнародних злочинів. Це ставить питання про юридичну відповідальність транснаціональних корпорацій перед Міжнародним кримінальним судом (МКС).

Відповідно до проєкту статтей про відповідальність держав за міжнародно-протиправні діяння, розробленого Комісією міжнародного права ООН, держава несе відповідальність за дії своїх органів та підконтрольних їй осіб [56].

Однак у випадку кібератак доведення такого контролю є складним процесом, що часто стає предметом різних міжнародних спорів.

Водночас, щодо міжнародного права, що демонструє загрози в питанні міжнародному гуманітарному праві та Талліннському посібнику, де

визначають, що чинне міжнародне право, зокрема Женевські конвенції, було сформоване до цифрової епохи. Наразі ключовим правовим орієнтиром є Талліннський посібник з міжнародного права, застосовного до кібервійни [37]. Цей документ розглядає питання пов’язані з суверенітетом держав у кіберпросторі, відповідальність держав за кібератаки, право на самооборону, контрзаходи у відповідь на кіберінциденти, захист цивільної інфраструктури, правовий статус кібероперацій під час війни.

Талліннський посібник, зокрема, визначає за яких умов кібератака на критичну інфраструктуру може вважатися актом агресії та дає право державі на самооборону відповідно до Статті 51 Статуту ООН [37; 40, ст.51]. Проте, чіткого консенсусу на рівні Ради Безпеки ООН щодо «цифрового порогу» застосування військової сили досі немає, що створює сірі зони для безкарних дій агресорів.

Навесні 2022 року Україна за сприяння технологічних гігантів (Microsoft, Amazon Web Services, Google) провела безпрецедентну в історії міграцію державних реєстрів, критичних баз даних та банківської інфраструктури у «хмару» на території країн НАТО. Це унеможливило фізичне знищення державного цифрового контуру, а AWS надала спеціальні пристрої Snowball – зашифровані портативні обчислювальні комплекси для екстреного копіювання петабайтів даних безпосередньо з урядових об'єктів під обстрілами.

Одним із найнебезпечніших проявів використання інформаційних технологій у конфліктах є кібервійна. Вона передбачає застосування інформаційно-комунікаційних технологій для завдання шкоди інформаційним системам противника, його критичній інфраструктурі, військовим об'єктам та органам державного управління. Основними формами кібервійни слід вважати шість видів: несанкціонований доступ до інформаційних систем; поширення шкідливого програмного забезпечення; DDoS-атаки; викрадення конфіденційних даних; порушення роботи енергетичних, транспортних та фінансових систем; інформаційне шпигунство.

Досвід останніх років свідчить, що кібератаки можуть супроводжувати традиційні бойові дії та бути їх важливою складовою. Особливо небезпечними є атаки на енергетичну інфраструктуру, системи зв’язку та державні інформаційні ресурси.

Україна стала одним із ключових прикладів держави, яка протистоїть масштабним інформаційним та кіберзагрозам. З початку російської агресії українські державні установи, енергетичні компанії, інформаційно-комунікаційні оператори та фінансові організації неодноразово ставали об’єктами кібератак.

Війна стала каталізатором розвитку українського ІТ-сектору та кібербезпеки. Було створено нові механізми реагування на кіберінциденти, посилено захист державних ресурсів, розширено міжнародне співробітництво у сфері кібероборони. Український досвід сьогодні вивчається багатьма країнами світу як приклад забезпечення цифрової стійкості в умовах війни.

Додатково важливо окреслити конфлікт корейського півострову, який здійснив вплив і на інший збройний конфлікт (Російсько-Український), з плином часом модернізувавшись в поєднанні з інформаційними технологіями.

3.3 Перспективи вдосконалення міжнародно-правового регулювання інформаційних технологій в Україні та світі

Інформаційні технології стали одним із ключових чинників розвитку міжнародно-правового регулювання та сучасного суспільства в цілому. Вони забезпечують функціонування державного управління, економіки, фінансової сфери, освіти, науки, охорони здоров'я та міжнародних комунікацій. Глобалізація цифрового середовища сприяла формуванню єдиного інформаційного простору, в якому дані можуть передаватися між державами практично миттєво. Водночас розвиток цифрових технологій супроводжується появою нових загроз, зокрема кіберзлочинності, кібершпигунства, порушення права на приватність, незаконного використання

персональних даних, поширення дезінформації та зловживань штучним інтелектом.

В умовах сьогодення міжнародно-правове регулювання інформаційних технологій набуває особливої актуальності. Його головним завданням є вироблення універсальних правил поведінки держав, міжнародних організацій, суб'єктів господарювання та громадян у цифровому середовищі. Для України питання розвитку міжнародно-правового регулювання ІТ є важливим також у контексті європейської інтеграції, цифрової трансформації держави та протидії кіберзагрозам в умовах воєнного стану [12].

Варто звернути увагу, що система міжнародно-правового регулювання інформаційних технологій перебуває на стадії активного розвитку. На відміну від традиційних галузей міжнародного права, цифрова сфера змінюється надзвичайно швидко, що ускладнює процес створення універсальних правових механізмів.

Загалом, в умовах сьогодення основу міжнародного регулювання становлять міжнародні договори, регіональні нормативно-правові акти, рекомендації міжнародних організацій та національне законодавство окремих держав.

Одним із найважливіших міжнародних документів є Конвенція про кіберзлочинність 2001 року (Будапештська конвенція), яка стала першим міжнародним договором, спрямованим на боротьбу зі злочинами у кіберпросторі. Документ встановлює механізми міжнародної співпраці між правоохоронними органами різних держав та визначає основні види кіберзлочинів [20].

Важливу роль відіграють також документи Організації Об'єднаних Націй, спрямовані на забезпечення міжнародної інформаційної безпеки та мирного використання інформаційно-комунікаційних технологій. Особлива увага приділяється питанням недопущення використання кіберпростору для агресії та втручання у внутрішні справи держав.

Окремий напрям міжнародного регулювання сформувався у межах Європейського Союзу. Найбільш впливовим актом став Загальний регламент Європейського Союзу про захист даних (GDPR) (General Data Protection Regulation), який визначає високі стандарти захисту персональних даних та фактично став міжнародним орієнтиром для багатьох країн світу [22].

Останніми роками значного розвитку набуло правове регулювання штучного інтелекту. Акт про штучний інтелект (AI Act) прийнятий в Європейському Союзі який вважається перший комплексний нормативним актом, що встановлює правила використання систем штучного інтелекту залежно від рівня ризику для суспільства та прав людини [28].

Таким чином, сучасна система міжнародного регулювання інформаційних технологій є багаторівневою та охоплює різні аспекти цифрової діяльності, проте все ще не має єдиного універсального правового механізму.

Загалом, основні проблеми міжнародно-правового регулювання інформаційних технологій полягають в тому, що попри значні досягнення, міжнародне співтовариство стикається з низкою проблем у сфері правового регулювання цифрових технологій.

Першим викликом є швидкість технологічного прогресу. Нові технології виникають значно швидше, ніж розробляються нормативно-правові акти. Це призводить до появи правових прогалин та невизначеності щодо регулювання нових цифрових продуктів і послуг.

Другою проблемою є відсутність єдиного міжнародного підходу до регулювання кіберпростору. Різні держави мають власне бачення цифрового суверенітету, свободи Інтернету та допустимих механізмів державного контролю над інформаційними ресурсами. Це ускладнює міжнародне співробітництво та гармонізацію законодавства.

Третьою проблемою є транскордонний характер кіберзлочинності. Хакерські атаки, викрадення даних та інші кіберзлочини можуть здійснюватися з території однієї держави проти об'єктів, розташованих у низці

інших країн. У таких умовах виникають труднощі щодо визначення юрисдикції та притягнення винних до відповідальності.

Особливої актуальності набувають питання правового регулювання штучного інтелекту. Використання алгоритмів машинного навчання може створювати ризики дискримінації, порушення права на приватність та непрозорого прийняття рішень. Саме тому Акт про штучний інтелект (AI Act) передбачає ризик-орієнтований підхід до регулювання таких систем [28].

Ще однією проблемою є захист персональних даних. Великі цифрові платформи збирають та аналізують величезні обсяги інформації про користувачів. Це створює ризики порушення права на приватність та потребує посилення міжнародних гарантій захисту даних.

Водночас зростання кількості кібератак змушує держави суттєво активізувати міжнародне співробітництво. Одним із перспективних напрямів є створення універсальних міжнародних механізмів реагування на кіберінциденти та оперативний обмін інформацією про кіберзагрози в режимі реального часу.

У якості майбутніх перспектив слід розглядати можливим ухвалення нових міжнародних договорів, які встановлюватимуть правила поведінки держав у кіберпросторі та визначатимуть відповідальність за кібератаки проти критичної інфраструктури.

Окрім цього, міжнародне регулювання штучного інтелекту в якості майбутніх перспектив потребує особливого рівня не лише уваги, а й контролю. Його стрімкий розвиток (програмних рішень розроблених на основі технології штучного інтелекту) зумовив необхідність формування міжнародних стандартів його використання. Основою такого регулювання сьогодні виступає Акт про штучний інтелект (AI Act Європейського Союзу), який слід вважати важливим правовим актом у цій сфері [28].

Разом з цим в якості основних перспектив розвитку міжнародного регулювання технології штучного інтелекту варто виокремити такі:

- запровадження глобальних етичних стандартів;

- забезпечення прозорості алгоритмів;
- захист прав людини від автоматизованих рішень;
- комплексний контроль використання автономних бойових систем;
- міжнародний нагляд за високоризиковими системами розробленими на основі технології штучного інтелекту.

Слід зауважити, що класичні інструменти міжнародного законотворення виявилися критично повільними перед стрімким зростання можливостей штучного інтелекту. Безконтрольний прорив у галузі великих мовних моделей та генеративних нейромереж актуалізував загрози виникнення проблем безпрецедентного масштабу: від автоматизованого створення індивідуалізованого шкідливого програмного коду (кіберзброї) до тотального розмивання поняття об'єктивної істини через використання дипфейків.

В цілому, перспектива розвитку міжнародно-правового регулювання в цій сфері лежить у юридичній площині створення спеціалізованої міжурядової установи під егідою ООН, за безпосередньою аналогією з Міжнародним агентством з атомної енергії (МАГАТЕ). Такий орган, робоча назва якого обговорюється як Міжнародна колегія з питань штучного інтелекту, повинен мати імперативні повноваження щодо обов'язкового правового та технічного аудиту безпеки передових моделей штучного інтелекту ще до моменту появи їхнього комерційного релізу. На міжнародно-правовому рівні в якості регулювання цього питання варто закріпити обов'язкове цифрове маркування (водяні знаки) для будь-якого контенту, згенерованого штучним інтелектом, що дозволить знизити рівень маніпуляцій під час виборчих процесів у демократичних країнах.

Водночас нагальним міжнародно-правовим викликом є врегулювання сфери квантових технологій. Поява працюючих квантових комп'ютерів створює пряму загрозу для глобальної фінансової та дипломатичної безпеки, оскільки такі системи здатні за лічені секунди дешифрувати сучасні асиметричні криптографічні стандарти (зокрема, алгоритм RSA). Перспективи розвитку права в цьому секторі пов'язані з розробкою нової Міжнародної

конвенції про перехід на постквантове шифрування. Цей документ має зобов'язати держави уніфікувати перехід національних банківських систем, реєстрів прав власності та каналів урядового зв'язку на квантовостійкі алгоритми, запобігаючи виникненням ризику глобального інформаційного колапсу.

В свою чергу, посилення захисту персональних даних потребують особливої уваги, тому що у сучасному світі персональні дані набувають статусу стратегічного ресурсу, а міжнародне право поступово рухається до уніфікації правил їх обробки.

Загальний регламент Європейського Союзу про захист даних (GDPR) уже сьогодні впливає на законодавство багатьох країн світу та фактично формує міжнародний стандарт захисту приватності. Подальший розвиток регулювання буде спрямований на вдосконалення механізмів міжнародної передачі даних, посилення відповідальності за їх незаконне використання та підвищення рівня контролю за діяльністю цифрових платформ [22].

Регулювання діяльності цифрових платформ: глобальні цифрові корпорації мають значний вплив на суспільні процеси та інформаційний простір. Саме тому все більше уваги приділяється питанням прозорості алгоритмів соціальних мереж, боротьби з дезінформацією, захисту конкуренції та запобігання монополізації цифрових ринків.

З іншої сторони міжнародне співтовариство поступово формує підходи до відповідальності цифрових платформ за контент та використання персональних даних користувачів.

Разом з цим варто звернути увагу на перспективи міжнародного співробітництва у сфері кібербезпеки, що в умовах сьогодення має суттєве значення в якості перспектив розвитку міжнародно-правового регулювання для інформаційних технологій.

Будапештська конвенція про кіберзлочинність 2001 року, яка тривалий час виступала єдиним ефективним багатостороннім інструментом у цій царині, на сьогодні об'єктивно потребує модернізації [20]. Вона розроблялася,

коли концепцій хмарних обчислень, децентралізованих анонімних криптовалют та транскордонних програм-вимагачів не існувало в промислових масштабах.

Головним напрямом вдосконалення конвенційного режиму є розширення кола учасників та практична імплементація положень Другого додаткового протоколу до Конвенції про кіберзлочинність щодо посиленого співробітництва та розкриття електронних доказів (2022 р.) [93]. Перспектива цього документу полягає в радикальному спрощенні процесу збору цифрових слідів. Правоохоронні органи держав-учасниць отримують право напряму звертатися до приватних сервіс-провайдерів (хостинг-провайдерів, реєстраторів доменних імен, адміністраторів хмарних сховищ) в інших юрисдикціях для негайного отримання інформації про користувачів та трафік. Це дозволяє оминути архаїчні та тривалі процедури взаємної правової допомоги, які зазвичай тривають місяцями, за які зловмисники встигають знищити цифрові докази.

Разом з цим ООН юридично підходить до завершення багаторічного процесу підготовки Всеохоплюючої міжнародної конвенції про протидію використанню інформаційно-комунікаційних технологій у злочинних цілях. Головна перспектива вдосконалення міжнародного права через цей інструмент: створення універсального юридичного містка між країнами Заходу та державами Глобального Півдня. Проте правова доктрина застерігає від надмірного розширення переліку кіберзлочинів у тексті нової конвенції ООН. Новий документ має фокусуватися суто на технічних злочинах (кримінальний хакінг, фішинг, атаки на комп'ютерні системи), але не повинен перетворитися на легітимний інструмент для авторитарних режимів, переслідування політичних дисидентів, блокування незалежних медіа та цензурування вільного Інтернету під приводом боротьби.

Окрім того, перспективи вдосконалення правового регулювання інформаційних технологій в Україні заслуговують на особливу увагу. Разом з курсом на євроінтеграцію Україна активно адаптує своє законодавство до

міжнародних та європейських стандартів у сфері цифрових технологій уже тривалий період [12].

Одним із ключових напрямів є гармонізація національного законодавства з правом Європейського Союзу. Особливого значення набуває імплементація норм щодо захисту персональних даних відповідно до Загального регламенту Європейського Союзу про захист даних (GDPR) та підготовка правової бази для регулювання штучного інтелекту та програмних рішень розроблених на основі цієї технології [22].

Зокрема серед низки напрямків варто виокремити такі:

1) Імплементація Акту про штучний інтелект (AI Act) та вимоги до регулювання технології штучного інтелекту: перед українським ІТ стоїть і зовнішній стратегічний виклик щодо прискорення інтеграції в цифровий простір Європейського Союзу. Це вимагатиме гармонізації українського законодавства з новими європейськими нормами, такими як Акт про штучний інтелект (AI Act) (правила для штучного інтелекту) [28].

2) Директива DSA як модель для гармонізації українського законодавства: стаття присвячена дослідженню Digital Services Act (DSA) як моделі для гармонізації українського законодавства у сфері цифрових послуг [68]. У країнах ЦСЄ імплементація DSA стикається з особливими викликами: від нестачі ресурсів до слабкої інституційної спроможності.

3) Закон «Про інтероперабельність» та European Interoperability Act: Фундаментом стане закон «Про інтероперабельність», який Україна планує впровадити. Це важливий крок для гармонізації українського законодавства з European Interoperability Act.

4) Single Digital Gateway (SDG) та Once-Only Technical System (OOTS): наступний етап як повна гармонізація з європейськими регуляціями Single Digital Gateway (SDG) та Once-Only Technical System (OOTS), що визначені пріоритетами на наступний рік [100].

5) Приєднання до політики ЄС «Роумінг як вдома»: Закон наближає законодавство України до acquis Європейського Союзу. Він посилює умови

для підтримання Україною режиму внутрішнього ринку з Європейським Союзом, шляхом приєднання до єдиної роумінгової зони Європейського Союзу «Роумінг як вдома».

Окрім цього, для України євроінтеграційний вектор виступає безальтернативною необхідністю модернізації всього масиву національного ІТ-права [12]. Чинний Закон України «Про захист персональних даних», ухвалений ще у 2010 році, не в повній мірі враховує стандарти Європейського Союзу [26]. Він (Закон України «Про захист персональних даних») базується на застарілій європейській Директиві 95/46/ЕС і абсолютно не враховує сучасну архітектуру збору даних через мобільні додатки, кукі-файли, алгоритми штучного інтелекту та великі дані [26; 36]. Як наслідок, Європейська Комісія досі не може ухвалити рішення щодо відповідності рівня захисту даних в Україні. Це питання створює серйозні бар'єри для українського ІТ-бізнесу, оскільки європейські контрагенти змушені проходити складні бюрократичні процедури для передачі даних українським розробникам.

Зазвичай, перспектива розв'язання цієї проблеми полягає у невідкладному ухваленні та реалізації положень нової редакції Закону «Про захист персональних даних», текст якого повністю гармонізовано зі стандартом Загального регламенту про захист даних Європейського Союзу (GDPR) [22]. Для України цей крок передбачає радикальну перебудову її національної системи:

1) Інституційна реформа: Функції контролю за захистом даних мають бути вилучені з компетенції Уповноваженого Верховної Ради з прав людини, який не має достатніх технічних та кадрових ресурсів. Замість цього передбачено створення принципово нового органу (Незалежної комісії з питань захисту персональних даних та доступу до публічної інформації), який за своїм статусом відповідатиме європейським наглядовим інституціям.

2) Впровадження нових корпоративних стандартів: Українські державні органи (включаючи Мінцифри (Міністерство цифрової трансформації

України), Міністерство внутрішніх справ (МВС), Міністерство охорони здоров’я (МОЗ)) та приватні компанії великого бізнесу будуть зобов'язані ввести посаду інспектора з захисту даних (DPO (Data Protection Officer)).

3) Економічна відповідальність: Закон запровадить дієві, європейського зразка фінансові санкції за витік або незаконну обробку даних. Замість нинішніх символічних адміністративних штрафів компанії ризикуватимуть мільйонними стягненнями, що змусить корпоративний сектор реально інвестувати в інформаційну безпеку.

У той же час в умовах повномасштабної війни важливим завданням є зміцнення кібербезпеки держави, що створює додаткові виклики для держави та захисту її інтересів. Для України це питання має не просто теоретичне, а безпосередньо має нагальне значення. Перебуваючи в епіцентрі першої у світі повномасштабної кібервійни та одночасно реалізуючи стратегічний курс на повноправне членство в Європейському Союзі, наша держава вимушена модернізувати національне законодавство в ультракороткі терміни.

Завдяки цьому, побудова передової цифрової держави (екосистема «Дія») та широке впровадження воєнних технологій (MilTech) потребують надійного правового фундаменту, який би повністю корелював із найновішими стандартами ЄС, такими як Загальний регламент про захист даних (GDPR) та Акт про штучний інтелект (EU AI Act) [22; 28]. Усе це має важливе значення для подальшого розвитку України та міжнародно-правового регулювання в цілому.

В цілому, Україна активно співпрацює з міжнародними партнерами у сфері захисту критичної інфраструктури, протидії кібератакам та обміну інформацією про кіберзагрози.

Окрім того, перспективним напрямом для України слід вважати також формування національної стратегії розвитку штучного інтелекту та впровадження дієвих механізмів контролю й контролю за тими, хто бде контролювати тих, хто триматиме розробки на основі цієї технології під контролем.

Висновки до розділу 3

1. Отже, правове регулювання відповідних технологій в міжнародному праві тільки починає формувати підгрунття для врегулюванні низки питань, які фокусують увагу на трьох ІТ-напрямках: ШІ, великі дані та цифрові платформи. Ці напрямки є найбільш суперечливими з поміж інших інформаційних технологій та потребують швидкого врегулювання для сворення подальшого правового орієнтиру у вирішенні питань сучасності щодо інших технологій.

2. Отже, збройні конфлікти змінили свої підходи та принципи, створюючи нові уявлення про це з юридичної точки зору. Розвиток цифрових технологій породжує нові загрози, пов’язані з кібервійнами, інформаційними операціями та атаками на критичну інфраструктуру. У таких умовах особливого значення набувають розвиток кібербезпеки, міжнародне співробітництво та впровадження сучасних засобів захисту інформації.

3. Отже, враховуючи європейський досвід, Україна має достатньо досвіду та ресурсів, щоб запровадити ризик-орієнтований підхід до регулювання систем розроблених на основі технології штучного інтелекту та забезпечити баланс між інноваціями і захистом прав людини.

Крім того, важливим завданням залишається розвиток цифрових прав громадян, зокрема права на приватність, захист персональних даних, доступ до інформації та безпечне використання цифрових сервісів.

ВИСНОВКИ

1. Проаналізовано поняття, ознаки та види інформаційних технологій у сучасному міжнародному праві. Сучасні інформаційні технології охоплюють широкий спектр технічних і програмних засобів, серед яких особливе значення мають комп'ютерні та мережеві технології, хмарні сервіси, великі дані, штучний інтелект, блокчейн та технології кібербезпеки.

Їх активне впровадження сприяє розвитку міжнародного співробітництва, цифрової економіки та глобального інформаційного суспільства. В зв’язку з цим використання новітніх інформаційних технологій породжує нові виклики для міжнародного права, пов'язані із захистом персональних даних, забезпеченням кібербезпеки, дотриманням прав людини та регулюванням діяльності штучного інтелекту.

Таким чином, у сучасному міжнародному праві інформаційні технології розглядаються не лише як інструмент, а й як самостійний об’єкт регулювання, що суттєво впливає на суверенітет держав, права людини та глобальну безпеку в цілому.

2. Досліджено становлення міжнародно-правового регулювання інформаційних технологій, яке пройшло довгий шлях характерний тим, що та нормативно-правова база законів, стандартів, яка була на початкових етапах сприяла більшому осмисленню щодо правового врегулювання даних питань в порівнянні з тими, що впроваджувалися на початковому етапі, забуваючи про важливість юридичної бази в цілому як галузі, яка повинна першочергово зосереджуватися на чітко визначених юридичних доктринах, а не на поверхневих судженнях, які не враховують практичну реалізацію таких норм.

3. З’ясовано принципи міжнародного права у сфері використання інформаційних технологій. Вони відіграють суттєву роль в міжнародно-правовому забезпеченні інформаційних технологій як галузі.

4. Встановлено роль ООН, Ради Європи, Європейського Союзу та інших міжнародних організацій у сфері інформаційних технологій. Вони сприяють співпраці між дослідниками, фахівцями та урядами для вирішення спільних викликів та використання можливостей, які надають інформаційні технології. Захист інтелектуальної власності в цифровій сфері є ключовим завданням для таких організацій, як Всесвітня організація інтелектуальної власності, що стимулює інновації.

5. Досліджено міжнародно-правовий захист персональних даних, приватності та цифрових прав людини. Динамічна система міжнародного нормативного забезпечення постійно адаптується до технологічних змін. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, GDPR та резолюції ООН є ключовими орієнтирами, але для ефективного захисту необхідна глобальна співпраця, посилення наглядових механізмів та підвищення правової грамотності.

6. Визначено, що міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинності є одним із ключових напрямів розвитку сучасного міжнародного права. Глобальна цифровізація суспільства потребує ефективних механізмів захисту приватності та персональної інформації.

Міжнародні стандарти, сформовані ООН, Радою Європи та Європейським Союзом, створюють основу для забезпечення балансу між технологічним розвитком і захистом прав людини. Подальший розвиток штучного інтелекту та цифрових технологій вимагатиме вдосконалення міжнародно-правових механізмів та поглиблення міжнародного співробітництва у сфері цифрових прав.

7. Проведено аналіз правового регулювання штучного інтелекту, великих даних та цифрових платформ у міжнародному праві. Міжнародно-правове забезпечення в сферах ШІ, Великих даних та цифрових платформ є динамічною областю, що вимагає уваги з боку правозахисників, державних органів і технологічних компаній. Створення ефективних правових

механізмів, які підтримують інновації та водночас захищають права людини, є нагальною потребою сучасності.

8. Проаналізовано інформаційні технології в умовах збройних конфліктів та загроз міжнародній безпеці, які стали одним із ключових факторів ролі сучасних збройних конфліктів та міжнародної безпеки, забезпечуючи ефективне управління військами, підтримують функціонування державних інституцій та створюють нові можливості для захисту національних інтересів.

Досвід України доводить, що інформаційні технології є не лише інструментом розвитку, а й важливим елементом обороноздатності держави та гарантією її стійкості перед сучасними викликами.

9. Досліджено перспективи вдосконалення міжнародно-правового регулювання інформаційних технологій в Україні та світі. Міжнародно-правове регулювання інформаційних технологій є однією з найдинамічніших галузей сучасного міжнародного права. Розвиток цифрових технологій потребує постійного вдосконалення правових механізмів, спрямованих на забезпечення кібербезпеки, захист персональних даних, регулювання продуктів розроблених на основі технології штучного інтелекту та гарантування цифрових прав людини.

Для України пріоритетними напрямами залишаються гармонізація законодавства з правом Європейського Союзу, розвиток системи кібербезпеки, впровадження сучасних стандартів захисту персональних даних та створення правових засад використання штучного інтелекту. Реалізація цих заходів сприятиме інтеграції України до європейського цифрового простору та зміцненню її позицій у глобальному інформаційному суспільстві.

10. Рекомендовано переглянути правові норми, які стосуються інформаційних технологій на національному та міжнародному рівнях, оскільки вони мають вагомі недоліки через зміни в розвитку та акцентних напрямках правовідносин в даній специфічній сфері. В зв’язку з цим також рекомендовано переглянути механізми міжнародного співробітництва організацій та держав і правове регулювання технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабенко Є.К. Основні аспекти поняття інформаційної системи інтернет. *XI Наукова-технічна конференція студентства та молоді «Світ інформації та телекомунікації»:* матеріали міжнар. конф., м.Київ, 19 лют. 2021 р. Київ, 2021. С. 24-26.
2. Бабенко Є.К. Вплив комп'ютерного дизайну та інформаційних технологій на освітній процес навчання в університетах *II Всеукраїнська науково-технічна конференція Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і освіти* : матеріали всеукр. наук.-практ. конф., м.Київ, 18 лист. 2024 р. Київ, 2024. С. 381-382.
3. Бабенко Є.К. Взаємодія Інтернет речей зі Штучним інтелектом на прикладі двох напрямків застосування *VII Міжнародна Науково-технічна конференція «Сучасний стан та перспективи розвитку IoT»*: матеріали міжнар. наук.-практ. конф., м.Київ, 15 квіт. 2025 р. Київ, 2025. С. 122-125.
4. Бабенко Є.К. Етичні норми використання штучного інтелекту в контексті бізнесу. *Міжнародна науково-практична конференція Синергія інновацій: політика, економіка та менеджмент в цифровому світі*: матеріали міжнар. наук.-практ. конф., м.Київ, 16 квіт. 2025 р. Київ, 2025. С. 324-327.
5. Бабенко Є.К. Когнітивна модель інформаційних технологій в застосуванні судової експертизи та питань викликів щодо кібербезпеки персональних даних. III Міжнародна науково-практична конференція «Інформаційні системи та технології: результати і перспективи» IST 2026: матеріали міжнарод. наук.-практ. конф., м.Київ, 10 бер. 2026р. Київ, 2026. С. 417-419.
6. Бабенко Є.К. Технологія блокчейн в управлінні у напрямку захисту

даних. *Міжнародна науково-практична конференція Синергія інновацій: політика, економіка та менеджмент в цифровому світі* : матеріали міжнар. наук.-практ. конф., м.Київ, 16 квіт. 2025 р. Київ, 2025. С. 209-211.

7. Бабенко Є.К. Сучасні виклики правового аспекту інформаційних технологій. *VIII Міжнародній науково-практичній конференції «Реалії та перспективи розбудови правової держави в Україні та світі»* : матеріали міжнар. наук.-практ. конф., м.Київ, 12-13 трав. 2025 р. Київ, 2025. С. 218-220.
8. Бабенко Є.К. Безпека персональних даних при використанні технологій Інтернету речей *VII Міжнародна Науково-технічна конференція «Сучасний стан та перспективи розвитку IoT»* : матеріали міжнар. наук.-практ. конф., м.Київ, 15 квіт. 2025 р. Київ, 2025. С. 257-259.
9. Бабенко Є.К. Застосування штучного інтелекту в розробці комп'ютерних ігор та як його використання впливає на розробників. *II Міжнародна науково-практична конференція Інформаційні системи та технології : результати і перспективи IST 2025* : матеріали міжнар. наук.-практ. конф., м.Київ, 5 бер. 2025 р. Київ, 2025. С. 301-302.
10. Бабенко Є.К., Бабенко К.М. Технологія IoT та її застосування в аналітиці даних *VII Міжнародна Науково-технічна конференція «Сучасний стан та перспективи розвитку IoT»*: матеріали міжнар. наук.-практ. конф., м.Київ, 15 квіт. 2025 р. Київ, 2025. С. 300-302.
11. Бабенко Є.К., Бабенко К.М. Штучний інтелект як інструмент в аналітиці даних. *II Всеукраїнська науково-технічна конференція Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і освіти* : матеріали всеукр. наук.-практ. конф., м.Київ, 18 лист. 2024 р. Київ, 2024. С. 153-155.
12. Бабенко Є.К., Бабенко К.М. Правові аспекти імплементації інформаційних систем в умовах євроінтеграції. *VIII Міжнародній науково-практичній конференції «Реалії та перспективи розбудови правової держави в Україні та світі»* : матеріали міжнар. наук.-практ.

конф., м.Київ, 12-13 трав. 2025 р. Київ, 2025. С. 16-18.

13. Бабенко Є.К., Бабенко В.В. Інтеграція Європейських практик в митному регулюванні в Україні. *VIII Міжнародній науково-практичній конференції «Реалії та перспективи розбудови правової держави в Україні та світі»*: матеріали міжнар. наук.-практ. конф., м.Київ, 12-13 трав. 2025 р. Київ, 2025. С. 81-84.
14. Бабенко Є.К., Бабенко В.В., Бабенко К.М. Вплив технологічних процесів штучного інтелекту у сфері ІТ-консалтингу в Україні та в світі. *III Міжнародна науково-практична конференція «Інформаційні системи та технології: результати і перспективи» IST 2026*: матеріали міжнар. наук.-практ. конф., м.Київ, 10 бер. 2026 р. Київ. С.341-342.
15. Бабенко Є.К., Бабенко К.М. Штучний інтелект як новий інструмент в системах документообігу. *II Міжнародна науково-практична конференція Інформаційні системи та технології: результати і перспективи IST 2025* : матеріали міжнар. наук.-практ. конф., м.Київ, 5 бер. 2025 р. Київ, 2025. С. 303-304.
16. Tallinn Manual 3.0: Sovereignty and Attribution in 2025 Cyber Warfare. *Journal of Law and Cyber Warfare.* URL: https://www.jlcw.org/2025/07/22/tallinn-manual-3-0-sovereignty-and-attribution-in-2025-cyber-warfare/ (дата звернення: 01.05.2026).
17. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку). *Офіційний вісник Європейського Союзу.* 2019. L151.c.15
18. Про інформацію: Закон України від 02.10.1992 р. №.2657-XII. *Відомості Верховної Ради України*. 1992. №48. Ст.650.
19. Про електронні комунікації: Закон України від 16.12.2020 р. №1089-IX. *Офіційний вісник України*. 2021. №6. Ст.306.

20. Про кіберзлочинність: Конвенція від 23.11.2001 р. №994_575. *Офіційний вісник України.* 2007. №65. Ст.2535.
21. Бабенко К.М. Технології блокчейн та її застосування в системах електронного обліку. *Міжнародна науково-практична конференція Синергія інновацій: політика, економіка та менеджмент в цифровому світі* : матеріали міжнар. наук.-практ. конф., м.Київ, 16 квіт. 2025 р. Київ, 2025. С. 212-214.
22. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких, даних: Регламент Європейського Парламенту і Ради (ЄС) від 27.04.2016 р. № 984_008-16. *Офіційний вісник Європейського Союзу*. 2016. L 119.
23. Француз А.Й., Француз-Яковець Т.А., Баликіна Л.І. Конституційні права, свободи та обов'язки людини і громадянина: комплекс навч.-метод. Забезпечення дисципліни. Київ: Атіка, 2012. 204 с.
24. Конвенція «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981 р. *Офіційний вісник України.* 2011. №1. Ст. 85.
25. Регламент Європейського Парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27.04.2016р. *Офіційний вісник Європейського Союзу.* 2016. L199. 1 с.
26. Про захист персональних даних: Закон від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. №34. Ст. 481.
27. Mikitery and Paramilitary Activities in and against Nicaragua (Nicaragua v. States of America). *International Court of Justice.* URL: https://www.icj-cij.org/case/7 (дата звернення: 10.04.2026).
28. Regulation EU 2024/1689 of the European Parlament and of the Council of 13 June 2024 (Artificial Intelligence Act). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 17.05.2026).

29. Timeline of advancements in information and communication technology and cybersecurity. *NDL Digital Collections*. URL: https://dl.ndl.go.jp/view/download/digidepo_9104292_po_20140317.pdf?contentNo=1 (дата звернення: 01.02.2026).
30. Форманюк В.В. Поняття та критерії класифікацій агентств ЄС в інституціональному праві ЄС: Теоретичний аспект. *Держави та регіони. Серія: Право.* 2023. №2(80). С. 159-163 DOI: https://doi.org/10.32840/1813-338X-2023.2.28
31. Search all EU institutions and bodies *European Union*. URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies_en (дата звернення: 01.03.2026).
32. Деркач В.Г., Прокопович-Ткаченко Є.Д., Руденко Є.Г. Використання штучного інтелекту в судовому процесі України: Правові, етичні та процесуальні аспекти. *Юридичний науковий електронний журнал*. 2025. №3/2025. С. 460-464 DOI: https://doi.org/10.32782/2524-0374/2025-3/109
33. Цифрова ера правосуддя: роль ШІ у забезпеченні єдності судової практики в Україні. *Верховний Суд*. URL: https://court.gov.ua/storage/portal/supreme/prezentacii_2025/120_AI_uniformity_of_judicial_practice_bernaziuk.pdf (дата звернення: 02.03.2026).
34. Ера ШІ й роль верховних судів у цифровій трансформації. *Юридична Газета.* URL: https://yur-gazeta.com/publications/practice/sudova-praktika/era-shi-y-rol-verhovnih-sudiv-u-cifroviy-transformaciyi-pravosuddya.html (дата звернення: 03.03.2026).
35. Прохазка Г.А. Штучний інтелект в міжнародному праві. *Юридичний науковий електронний журнал.* 2023. №2. С.153-155. DOI: https://doi.org/10.32782/2524-0374/2022-2/33
36. Про захист фізичний осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЕС Європейського Парламенту та Ради від 24.10.1995 р. №95/26/ЄС. *Верховна Рада України Законодавство України.* URL: https://zakon.rada.gov.ua/laws/card/994_242

37. Tallinn Manual 2.0 on the International Law applicable to Cyber Operations. First edition. Michael N. Shmitt, Liis Vihul. Cambridge University Press. 2017. P.598.
38. Корольова В.В., Чорна В.О. Поняття та суть ІТ-права як галузі права. Legal Bulletin. 2025. №1(15). С.77-81 DOI: https://doi.org/10.31732/2708-339X-2025-15-A11
39. Про Національну програму інформатизації: Закон України від 01.12.2022 р. №.2807-IX. *Відомості Верховної Ради України*. 2023. №51. Ст.127.
40. Статут Організації Об'єднаних Націй від 26.06.1945 р. №995_010. *Офіційний вісник України*. 2025. №70. Ст.4849
41. Про захист цивільного населення під час війни: Женевська Конвенція від 12.08.1949 р. № 995_154. Офіційний вісник України. 2013. №27. Ст.942.
42. Що стосується захисту жертв міжнародних збройних конфліктів: Додатковий протокол до Женевської Конвенції (Протокол I) від 08.06.1977 р. №995_199. *Зібрання чинних міжнародних договорів України*.1990. №1. Ст.25
43. Case № 58170/13, 62322/14, 24960/15 Big Brother Watch and Others v. The United Kingdom. *HUDOC-European Court of Human Rihgts*. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-221054&filename=CASE%20OF%20BIG%20BROTHER%20WATCH%20AND%20OTHERS%20v.%20THE%20UNITED%20KINGDOM%20-%20%5BUkrainian%20Translation%5D%20summary%20by%20the%20Supreme%20Court%20of%20Ukraine.pdf (дата звернення: 01.02.2026).
44. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 9102014 та Директиви (ЄС) 2018/1972 та Директиви (ЄС) 2016/1148 (Директива NIS 2) від 14.12.2022 р. №2022/2555. *Офіційний вісник Європейського Союзу.* 2022. L333. С. 80
45. EU-U.S. Data Privacy Framework Principles Issued By The U.S. Department of Commerce. *Data Privacy Framework Program.* URL: https://privacyshield dev.blob.core.windows.net/publicsiteassets/Full%20Text_EUU.S.%20DPF.pd

f (дата звернення: 20.02.2026).

46. Case C-293/12 (2014) Digital Rights Ireland v Minister for Communicatons Marine and Natural Resources and Others. *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293 (дата звернення: 25.02.2026)
47. Case C-131/12 (2014) Google Spain and Google Inc.v AgenciaEspanola de Protecciode Datos (AEPD) and Mario Costeja Gonzalez. *EUR-Lex.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ013 (дата звернення: 22.02.2026).
48. On horizontal cybersecurity requirements for products with digital elements and amending and Directive (Cyber Resilience Act): Regulation (EU) of The European Parliament and of The Council in 20.11.2024 №. 2847. *Official Journal of the European Union*. 2024. L EN. URL: http://data.europa.eu/eli/reg/2024/2847/oj (дата звернення: 24.02.2026).
49. Case C-311/18 (2020) Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. *EUR-Lex.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311 (дата звернення: 29.02.2026).
50. Lessons from the first cyber war: How supporting Ukraine on the digital battlefield can help improve the Uk`s online resilience by David Kirichenko. *HJS. Centre for Russia and Eurasia studies*. 2024. P.40.
51. Проти транснаціональної організованої злочинності: Конвенція Організації Об'єднаних Націй від 15.11.2000 р. №995_789. *Офіційний вісник України*. 2006. №14. Ст.340.
52. Dita Aulia Salma, Fahlesa Munabari Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia. Deviance Jurnal Kriminologi. Volume 7 Nomor 1. 2023. P. 32-45 DOI: http://dx.doi.org/10.36080/djk.2412
53. African Union Convention on Cyber Security and Personal Data Protection. *African Union.* URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_

protection_e.pdf (дата звернення: 29.02.2026).

54. Римський Статут Міжнародного Кримінального Суду від 17.07.1998 р. №995_588. Відомості Верховної Ради України. 2025. №1-2. Ст.1
55. H.R. 1626 Consolidated Appropriations Act (Cloud Act). *Congress.Gov*. URL: https://www.congress.gov/bill/115th-congress/house-bill/1625/text (дата звернення: 30.02.2026).
56. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. *United Nations Office of Legal Affairs.* URL: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (дата звернення: 01.03.2026).
57. United States v/ Microsoft Corp., 584 U.S. (2018). *JUSTIA.* URL: https://supreme.justia.com/cases/federal/us/584/17-2/ (дата звернення: 10.03.2026).
58. Big Brother Watch v. United Kingdom. Open Society Justice Initiative. URL: https://www.justiceinitiative.org/litigation/big-brother-watch-v-united-kingdom (дата звернення: 02.03.2026).
59. United States v. Ulbricht. *Court Listener By Free Law.* URL: https://www.courtlistener.com/docket/4353251/united-states-v-ulbricht/ (дата звернення: 05.03.2026).
60. Хартія основоположних прав Європейського Союзу. *EUR-Lex Access to European Union law*: URL: https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX:12012P/TXT (дата звернення: 21.04.2026).
61. State v. Loomis. *JUSTIA U.S. Law.* URL: https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html (дата звернення: 06.03.2026).
62. The California Consumer Privacy Act of 2018. Spirion Protect What Matters Most. URL: https://www.spirion.com/wp-content/uploads/2020/07/Spirion_CCPA_v3.pdf (дата звернення: 05.05.2026).
63. Brazilian Civil Rights Framework for the Internet. *The national Congress.* URL: https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf (дата звернення: 10.05.2025)

64. Посібник з європейського права у сфері захисту персональних даних. *Уповноважений Верховної Ради України з прав людини.* URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/Data_Protection_Handbook_ukr%202020.pdf (дата звернення: 01.05.2026).
65. Про захист прав людини і основоположних свобод: Конвенція Ради Європи від 04.11.1950 р. №995_004. *Урядовий кур'єр*. 2010. № 215.
66. Про торгівельні аспекти прав інтелектуальної власності: Угода СОТ від 15.04.1994 р. № 981_018. Офіційний вісник України. 2010. № 84. Ст. 2989.
67. ДСТУ 5034:2008. Інформаційні технології. Терміни та визначення основних понять. Київ. ДП «УкрНДНЦ», 2008. 28 с.
68. Digital Services Act Regular EU 2022/2065. *EUR-Lex Access to European Union law*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065 (дата звернення: 14.05.2026).
69. Digital Market Act Regular EU 2022/1925. *EUR-Lex Access to European Union law*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925 (дата звернення: 14.05.2026).
70. ЮНЕСКО. Концепція інформаційного суспільства. URL: https://unesdoc.unesco.org/ark:/48223/pf0000124675 (дата звернення: 04.06.2026).
71. Recommendation on the Ethics of Artificial Intelligence. *UNESCO.* URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата звернення: 07.05.2026).
72. ILOVEYOU. *Вікіпедія Вільна енциклопедія.* URL: https://uk.wikipedia.org/wiki/ILOVEYOU (дата звернення: 07.06.2026).
73. Кібератаки під час російсько-грузинської війни. *Вікіпедія Вільна енциклопедія.* URL: https://uk.wikipedia.org/wiki/Кібератаки_під_час_російсько-грузинської_війни (дата звернення: 08.05.2026).
74. Stuxnet-перша цифрова зброя-вірус. *BBC.* URL: https://www.bbc.com/ukrainian/news/2011/02/110215_stuxnet_virus_oh (дата звернення: 09.05.2026).
75. Кібератака на енергетичні компанії України. *Вікіпедія Вільна енциклопедія.* URL: https://uk.wikipedia.org/wiki/Кібератака_на_енергетич

ні_компанії_України (дата звернення: 09.05.2026).

76. Petya. *Вікіпедія Вільна енциклопедія.* URL: https://uk.wikipedia.org/wiki/Petya (дата звернення: 07.05.2026).
77. NSA Report on Russian Spearphishing. *EMBED.* URL: https://embed.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing/#document/p1 (дата звернення: 07.05.2026).
78. International Humanitarian Law and The Growing Involvement of Civilians in Cyber Operations and Other Digital Activities During Armed Conflict. *ICRC.* URL: https://shop.icrc.org/download/ebook?sku=4895/002-ebook (дата звернення: 01.03.2026)
79. Secretary-General`s High-level Panel on Digital Cooperation. United Nations. URL: https://www.un.org/en/sg-digital-cooperation-panel (дата звернення: 02.03.2026).
80. Digital Governance. Council of Europe Portal. URL: https://www.coe.int/en/web/digital-governance/overview (дата звернення: 03.03.2026).
81. Цифрова стратегія ЄС. EU4Digital. URL: https://eufordigital.eu/uk/discover-eu/eu-digital-strategy/ (дата звернення: 04.03.2026).
82. About IFIP. *IFIP*. URL: https://www.ifip.org/about-ifip/ (дата звернення: 04.03.2026).
83. Про громадські і політичні права: Міжнародний пакт ООН від 16.12.1966 р. № 995_043. Верховна Рада України Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 04.03.2026).
84. About WIPO. *WIPO.* URL: https://www.wipo.int/en/web/about-wipo (дата звернення: 11.04.2026)
85. About The International Telecommunication Union (ITU). *ITU.* URL: https://www.itu.int/en/about/Pages/default.aspx (дата звернення: 11.04.2026)
86. About ISO. *ISO.* URL: https://www.iso.org/about (дата звернення: 12.04.02026).

87. Інститут інженерів з електротехніки та електроніки. *Вікіпедіа вільна енциклопедія.* URL: https://uk.wikipedia.org/wiki/Інститут_інженерів_з_електротехніки_та_електроніки (дата звернення: 14.04.2026)
88. About ICANN. *ICANN.* URL: https://www.icann.org/resources/pages/about-icann (дата звернення: 15.04.2026).
89. Загальна декларація прав людини ООН від 10.12.1948 р. №995_015. *Офіційний вісник України.* 2008. №93. Ст.3130
90. W3C re-launched as a public-interest non-profit organization. *World Wide Web Consortium*. URL: https://www.w3.org/press-releases/2023/w3c-le-launched/ (дата звернення: 18.04.2026).
91. Introduction to the IETF. *IETF*. URL: https://www.ietf.org/about/introduction/ (дата звернення: 20.04.2026).
92. Samuel D. Warren, Louis D. Brandeis The Right to Privacy (1890 p.). *Cornell Browers Computer Science*. URL: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (дата звернення: 07.05.2026)
93. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р. №994_687. Офіційний вісник України. 2010. № 45. Ст. 1920.
94. About FIRST. *FIRST.* URL: https://www.first.org/abou/ (дата звернення: 15.05.2026).
95. CERT Division. *Carnegie Mellon University.* URL: https://www.sei.cmu.edu/divisions/cert/ (дата звернення: 15.05.2026).
96. Global Digital Compact Revisions. *United Nations.* URL: https://www.un.org/en/summit-of-the-future/global-digital-compact (дата звернення: 16.05.2026).
97. Про громадські і політичні права: Міжнародний пакт ООН від 16.12.1966 р. № 995_043. *Верховна Рада України Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 17.05.2026).

98. Про запобігання злочину геноциду та покарання за нього: Конвенція ООН від 09.12.1948 р. №995_155. *Офіційний вісник України*. 2024. № 42. Ст. 2577.
99. Declarations on Principles of International Law Friendly Relations and Co-operation amoung states in Accordance with the charter of the United Nations. *UNHCR.* https://www.refworld.org/ites%2Fdefault%2Ffiles%2Flegacy-pdf%2Fen%2F1970-10%2F3dda1f104.pdf (дата звернення: 16.05.2026).
100. SDG Regulation and the Once-Only Technical System as key-players in the EU digital policy landscape. European Commission. URL: https://ec.europa.eu/digital-building-blocks/sites/spaces/OOTS/pages/774145239/SDG+Regulation+and+the+Once-Only+Technical+System+as+keyplayers+in+the+EU+digital+policy+landscape (дата звернення: 17.05.2026).
101. Informational self-determination. *Wikipedia.* URL: https://en.wikipedia.org/wiki/Informational_self-determination (дата звернення: 17.05.2026).

ДОДАТКИ

Додаток А

Список Апробації до кваліфікаційної роботи

Міністерство освіти і науки України
Сумський державний педагогічний університет
імені А.С. Макаренка
Навчально-науковий інститут історії, права та міжнародних відносин
Кафедра права та публічного управління

ЗБІРНИК
НАУКОВИХ ПРАЦЬ

VIII Міжнародної науково-практичної конференції

РЕАЛІЇ ТА ПЕРСПЕКТИВИ
РОЗБУДОВИ ПРАВОВОЇ ДЕРЖАВИ
В УКРАЇНІ ТА СВІТІ

Суми

Матеріали VIII Міжнародної науково-практичної конференції (м. Рієка, 12-13.05.25)

Бабенко Єлизавета Костянтинівна,
студентка 1 курсу магістерського рівня Державного університету інформаційно-комунікаційних технологій та студентка 1 курсу магістерського рівня Київський університет права Національної академії наук України
Бабенко Костянтин Миколайович,
студент 3 курсу бакалаверського рівня Державного університету інформаційно-комунікаційних технологій

ПРАВОВІ АСПЕКТИ ІМПЛЕМЕНТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

В умовах сьогодення Україна приділяє значну увагу євроінтеграції, а разом з цим інформатизації процесів, прагнучи, в першу чергу, побороти бюрократизм, корупцію та створити максимально несприятливі умови для поширення колабораційної діяльності.

Загалом, поняття інформатизації, в загальному розумінні, достатньо широко розкривається в статті 1 Закону України «Про Національну програму інформатизації» і, по суті, означає «сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, технологічних та виробничих процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій» [1, ст.1].

Варто звернути увагу, що цьому Закону в Україні приділяється особлива увага з 1998 року. Програма періодично переглядається та контролюється її виконання. Кабінет Міністрів України щорічно звітує про стан інформатизації держави та про прогреси з розвитку інформаційних технологій і ресурсів.

Наприклад, відповідно до звіту за довоєнний період 2021 року Міністерство цифрової трансформації України активно продовжувало працювати над створенням цифрової держави, доволі впевнено рухаючись до режиму «без паперів» [2, с.1, 2].

Основна особливість цього режиму полягає в тому, що посадові особи державних органів в нашій країні не матимуть права вимагати паперові документи, якщо вся необхідна інформація вже міститься в державних електронних ресурсах. Зокрема, саме для цього в 2021 році був прийнятий досить конструктивний Закон «Про особливості надання публічних (електронних публічних послуг)», його ще називають «Законом про paperless» тобто «Законом без паперів» [3].

Війна не зупинила період євроінтеграції, а разом з ним інформатизації процесів, а навпаки Україна активніше продовжила впроваджувати нові програми та технології скоригувавши курс на кібербезпеку та кібергігієну, не забуваючи при цьому про чотири основних напрями: цифрове законо-

ЗМІСТ

СЕКЦІЯ 1.
ЄВРОІНТЕГРАЦІЙНІ СТУДІЇ ЯК ВЕКТОР РОЗБУДОВИ ДЕМОКРАТІЇ ТА ПРАВОВОЇ ДЕРЖАВИ 14
Агарков В.С.
Гармонізація української моделі регулювання підприємництва з європейськими практиками, правові та управлінські аспекти 14
Бабенко Є.К., Бабенко К.М.
Правові аспекти імплементації інформаційних систем в умовах євроінтеграції 16

Ходун Е.О.
Політика «контрольованої релігії» в СРСР: правова оболонка репресивних практик у контексті європейського право розуміння свободи совісті 76
Чмеленко В.В.
Консультативна психологічна допомога: особливості правового регулювання 78

СЕКЦІЯ 4.
АКТУАЛЬНІ ПРОБЛЕМИ ПУБЛІЧНОГО ПРАВА: ЄВРОПЕЙСЬКІ СТАНДАРТИ ТА НАЦІОНАЛЬНІ ПІДХОДИ 81
Бабенко Є.К., Бабенко В.В.
Інтеграція європейських практик в митному регулюванні в Україні 81

СЕКЦІЯ 4.

АКТУАЛЬНІ ПРОБЛЕМИ ПУБЛІЧНОГО ПРАВА: ЄВРОПЕЙСЬКІ СТАНДАРТИ ТА НАЦІОНАЛЬНІ ПІДХОДИ

Бабенко Єлизавета Костянтинівна,
студентка 1 курсу магістерського рівня Державного університету інформаційно-комунікаційних технологій та студентка 1 курсу магістерського рівня Київський університет права Національної академії наук України
Бабенко Валентина Володимирівна,
магістр права

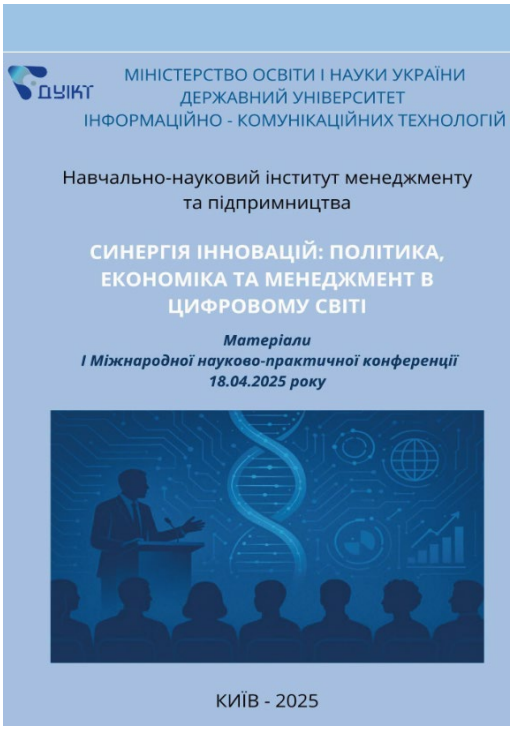
ІНТЕГРАЦІЯ ЄВРОПЕЙСЬКИХ ПРАКТИК В МИТНОМУ РЕГУЛЮВАННІ В УКРАЇНІ

В кожній країні одним з головних елементів будь-яких сфер, без яких складно уявити сьогоденний світ, можна вважати, митну діяльність на якій базуються імпортні та експортні дії з товаром. Крім того сам товар, наразі, відіграє важливу роль для розвитку будь-якої держави, збільшення її доходів та підвищення добробуту населення в цілому.

Прикладів в сьогоденних реаліях безліч, коли держава не може не експортувати або не імпортувати продукцію і, в основному, на це впливають правові елементи законодавства кожної країни окремо, де встановлюються свої правила, які іноді є ускладненими або не зрозумілим для представника кожної іншої країни і тут виникають різні спірні моменти, тому на території Європейського Союзу (надалі - ЄС) встановленні загальні правила, які поширюються на всіх членів-держав та учасників зовнішньоекономічної діяльності, які в силу обставин мають транспортувати свої товари через митну територію ЄС. Особливо гостро постало це питання, коли розпочалася цифровізація процесів, де впровадження інформаційних технологій в різні сфери суспільного та державного життя стало звичайним явищем і тут майже відразу почало виникати багато питань та непередбачуваних ситуацій.

Нині, держави, які бажають приєднатися до ЄС або суб'єкти господарювання яких мають наміри займатися зовнішньоекономічною діяльністю з суб'єктами господарювання Європейського Союзу та/або вести власний бізнес на території ЄС, для зручності співпраці, повинні впроваджувати в своїх країнах зміни до законодавства, які, в цілому, відповідатимуть правилам Європейського Союзу.

Україна достатньо давно має намір і бажання приєднатися і в подальшому співпрацювати з ЄС, в зв'язку з чим, вже тривалий період часу, все більше запроваджує в державі митні правила Європейського Союзу, наближаючи таким чином наше законодавство до практик ЄС, врегульовуючи це на законодавчому рівні і, в першу чергу, для полегшення подальшого ведення господарської діяльності в сфері зовнішньоекономічних торгових відносин.



СЕКЦІЯ 2

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН У ФІНАНСИ ТА УПРАВЛІННЯ

Бабенко Є. К.	Технологія блокчейн в управлінні у напрямку захисту даних	209

СЕКЦІЯ 6

ЦИФРОВА ЕТИКА ТА СОЦІАЛЬНА ВІДПОВІДАЛЬНІСТЬ БІЗНЕСУ

Альміз К. С.	Теоретичні питання інформаційно-комунікаційне забезпечення підприємств	322
Бабенко Є. К.	Етичні норми використання штучного інтелекту в контексті бізнесу	324

СЕКЦІЯ 2

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН У ФІНАНСИ ТА УПРАВЛІННЯ

ТЕХНОЛОГІЯ БЛОКЧЕЙН В УПРАВЛІННІ У НАПРЯМКУ ЗАХИСТУ ДАНИХ

Бабенко Єлизавета Костянтинівна
студентка 5 курсу, групи КНДМ-51
Державного університету інформаційно-комунікаційних технологій

Постановка проблеми. Розвиток технологій сприяє новим можливостям для впровадження їх в різні сфери суспільного життя: державних та приватних структур. Блокчейн відносно нова технологія, яка становить процес безпосередньої взаємодії різних елементів діяльності компанії. В свою чергу, дані є складовою будь-якого об'єкту, який оточує діяльність людини, що і є проблемою, в тому числі їх правомірності їх використання чи зберігання.

Мета дослідження. Дослідити технології блокчейну в компаніях в напрямку даних. Визначити ключові особливості, структуруючи на реальних прикладах застосування та виявлення проблеми.

Основні результати дослідження. Технологія Блокчейн, яка забезпечує складну, але ефективну складову будь-якої компанії для забезпечення децентралізованої структури даних, тому даний можна розуміти по-різному. Однак, сам термін пояснює процес, за яким відбувається процес з урахуванням особливості технології, яка формується за принципом покрокового лінійного формування надані доступу до різних типів даних компанії. Тому Блокчейн – інформаційна технологія спрямована на падання цифрової інформації. До прикладу можна привести водоспадний метод ведення проектів, який чудово може демонструвати принцип роботи Блокчейну.

ЕТИЧНІ НОРМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОНТЕКСТІ БІЗНЕСУ

Бабенко Єлизавета Костянтинівна
студентка 5 курсу, групи КНДМ-51
Державного університету інформаційно-комунікаційних технологій

Постановка проблеми. Цифрова трансформація продовжує розвиватися, втручаючись в різні напрямки формуючи свої правила та проблеми. Тому наразі постає багато питань в напрямку цифрової етики, яка є невід'ємною частиною в будь-якій складовій на прикладі бізнес процесу, який охоплюється різними аспектами даного процесу. Ця тема є актуальною, адже відсутність етичних норм сприяє вільному безконтрольному використанні штучного інтелекту та може призвести до непередбачуваних наслідків.

Мета дослідження. Дослідити етичні норми використання штучного інтелекту на прикладі декількох компаній та визначити їх значимість і доцільність.

Основні результати дослідження. Етичні норми використання штучного інтелекту є складним поняттям, охоплюючи багато компонентів та нюансів при його впроваджені в різних середовищах особливо, наразі, це стосується напрямку бізнесу. Різні джерела висвітлюють ряд компонентів, як формують загальну картину. Складатися з прозорості, підзвітності, тобто основні моменти, які повинні захищати становлення суспільством та державою моральних норм в напрямку роботи людини від повного замінювання її технологіями. Всі зазначені компоненти повинні забезпечувати безпеку, але нажаль багато міжнародних та Українських компаній нехтують цим, беручи до уваги багато плюсів використання технологій (штучного інтелекту), особливо зі сторони фінансової складової, яка є головною при прийняті рішення: чи наймати працівника чи замінити його на технологію, яка може виконувати навіть більше дій ніж людина.

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка
Факультет інформаційних технологій
Кафедра інформаційних систем та технологій

SCIIST
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY SCIENTIFIC CONFERENCE

3-я Міжнародна науково-практична конференція

«ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ: РЕЗУЛЬТАТИ І ПЕРСПЕКТИВИ»
(IST 2026)

10 березня 2026 р.

Proceedings 3rd International scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2026), March 10, 2026 - K.: FIT TSNUK, 2026.

92. PHYSICS-INFORMED GRAPH NEURAL NETWORKS FOR AGRO-RESOURCE MONITORING AND RECOVERY PREDICTION Kristina Silvanovych, Olena Hrynova 330
93. THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DIGITAL DESIGN PROCESSES: AI AS A TOOL, NOT A REPLACEMENT Anastasiia Slobodina, Mykola Kostikov 335
94. ВИЯВЛЕННЯ PROMPT-ІН'ЄКЦІЙ У ВЕЛИКИХ МОВНИХ МОДЕЛЯХ МЕТОДАМИ СЕМАНТИЧНОГО АНАЛІЗУ Володимир Ахрамович, Володимир Санченко 337
95. ВПЛИВ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ IT-КОНСАЛТИНГУ В УКРАЇНІ ТА В СВІТІ Єлизавета Бабенко, Валентина Бабенко, Костянтин Бабенко 341

Матеріали 3-ої Міжнародної науково-практичної конференції "ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ: РЕЗУЛЬТАТИ І ПЕРСПЕКТИВИ", 10 березня 2026 р. – К.: ФІТ КНУТШ, 2026 р.

КОНТЕЙНЕРИЗОВАНОГО INFERENCE Даниіл Фуркало, Володимир Петрівський 385
109. ДОСЛІДЖЕННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ПРОГНОЗУВАННЯ ПОПИТУ НА МОЛОЧНУ ПРОДУКЦІЮ Катерина Чорнобай, Сергій Грибков 388
110. ЖАНРОВА КЛАСИФІКАЦІЯ МУЗИЧНИХ КОМПОЗИЦІЙ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ Антон Шаповалов, Ганна Красовська 391
111. ПРОГРАМНА СИСТЕМА ФОРМУВАННЯ НАВЧАЛЬНИХ НАБОРІВ ДАНИХ ДЛЯ СТРУКТУРНОЇ СЕГМЕНТАЦІЇ МУЗИЧНИХ СИГНАЛІВ Дар'я Шкуратовська, Анастасія Ніколаєнко 393
112. СТОХАСТИЧНЕ МОДЕЛЮВАННЯ ФІНАНСОВИХ ЧАСОВИХ РЯДІВ: ВІД ГЕОМЕТРИЧНОГО БРОУНІВСЬКОГО РУХУ ДО НЕЙРОННОЇ ДИФУЗІЙНО-СТРИБКОВОЇ МОДЕЛІ Юрій Юрченко, Олександр Заковортний 397
Section Cognitive modeling and knowledge engineering 402
Секція Когнітивне моделювання та інженерія знань 402
113. ABOUT ONE RECOMMENDATION MODEL FOR DATA PREDICTION BASED ON FUZZY LOGIC Eugene Ivokhin, Glib Shelyakin 403
114. CONSIDERING PSYCHOLOGICAL CHARACTERISTICS OF STUDENTS FOR ADAPTIVE E-LEARNING Mykola Kostikov, Vladlen Lisnevskyi 405
115. IDENTIFYING RESEARCHERS' SCIENTIFIC AREAS BASED ON PUBLICATION CLUSTERING Alisher Shaimuran 408
116. ОСОБЛИВОСТІ ТА ПРОБЛЕМАТИКА ВИКОРИСТАННЯ ГЕОІНФОРМАЦІЙНИХ ДАНИХ ПРИ ПЛАНУВАННІ ГУМАНІТАРНОГО РОЗМІНУВАННЯ В УКРАЇНІ Дмитро Аеров 414
117. КОГНІТИВНА МОДЕЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАСТОСУВАННІ СУДОВОЇ ЕКСПЕРТИЗИ ТА ПИТАНЬ ВИКЛИКІВ ЩОДО КІБЕРБЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ Єлизавета Бабенко 417

Proceedings 3rd International scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2026), March 10, 2026 - K.: FIT TSNUK, 2026.

ВПЛИВ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ IT-КОНСАЛТИНГУ В УКРАЇНІ ТА В СВІТІ

Єлизавета Бабенко, Валентина Бабенко, Костянтин Бабенко

Анотація. В даній тезі досліджено та розглянуто теоретичну і практичну складову впливу технологічного процесу штучного інтелекту в сфері консалтингу в Україні та в світі. З тенденцією розвитку впроваджень різних технологічних рішень, одним з них консалтинг сприяв змінам. Здійснено порівняльний аналіз технологічних процесів штучного інтелекту в сфері IT-консалтингу між Україною та зарубіжними країнами.

Ключові слова: IT-консалтинг, штучний інтелект, інформаційні технології.

I. ВСТУП

Інноваційні підходи до формування сфери консалтингу в різних країнах розвивається завдяки зовнішнім та внутрішнім факторам, які змінюють звичайні процеси суспільної діяльності. З такими підходами сфера консалтингу розвинулася з різних напрямків створюючи нові сектори взаємодії. Одне з них сприяло виникненню IT-консалтингу, який продовжує розвиватися та вдосконалюватися при впровадженні різних IT технологій. Штучний інтелект, як один з технологічних рішень, які збільшили спектр можливостей в сфері консалтингу.

Однак, можливості такого впровадження має суперечливі моменти такого впровадження, які стверджують про наявність проблематики та сприяли технологічним процесам впровадження штучного інтелекту в сферу консалтингу. Підтвердження цього спостерігається і в інших сферах діяльності.

II. ДАНІ ТА МЕТОДИ

Обрані дані та методики задіяні для формування дослідження, які зазначають важливість тематики, демонструючи проблематику та враховують особливості: документація та дослідження в сфері інформаційних технологій та консалтингу, а саме наукові праці, щодо опису технічної складової технології та її особливості з практичного впровадження; інші дослідження (практичні кейси, статистика та публічні медіа дані), які мають дотичні елементи проаналізованого об'єкту.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Результати дослідження демонструють виклики та проблематику сьогодення, які впливають на сферу консалтингу в Україні та в світі через впровадження технологічних рішень. Консалтинг неоднозначний термін, який на базисі розуміється, як послуга з передачі інформації, яку варто поділити на такі види послуг:

1) Теоретичні: аудит, планування, моніторинг.
2) Практичні розробка, тестування, перенесення інфраструктури.

Такий розподіл послуг аргументується особливістю консалтингу, в якому сформований різний спектр діяльності залежно від напрямку. Технологія, як ключовий об'єкт дослідження сприяє змінам звичайних процесів, які можуть впливати як з позитивної так і з негативної сторони. Базисні IT технології вже залучені до звичайних процесів діяльності (наприклад хмарні сховища, системи безпеки, тощо). Однак головним викликом такого впливу технологічного впровадження може сприяти на сторону щодо таких принципів: прозорість, відкритість, доступність та безпека даних [1].

Proceedings 3rd International scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2026), March 10, 2026 - K.: FIT TSNUK, 2026.

КОГНІТИВНА МОДЕЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАСТОСУВАННІ СУДОВОЇ ЕКСПЕРТИЗИ ТА ПИТАНЬ ВИКЛИКІВ ЩОДО КІБЕРБЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

Єлизавета Бабенко

Анотація. В даній тезі досліджено та розглянута теоретична і практична складова когнітивної моделі, як частини інформаційних технологій зі застосуванням в сфері судової експертизи та питань викликів щодо кібербезпеки персональних даних. Тенденція впровадження інформаційних технологій, де когнітивні технології моделювання, обчислень та оцінки при якому формується експертиза. Приведено можливі приклади методів технології штучного інтелекту в судовій експертизі. Здійснено порівняльний аналіз практичного використання в Україні та у світі.

Ключові слова: когнітивні інформаційні технології, судова експертиза, кібербезпека, персональні дані, штучний інтелект.

I. ВСТУП

Інформаційні технології продовжують впроваджуватися в різні напрямки суспільства створюючи нові можливості для розвитку суспільства. Відповідно цього Україна активно впроваджує різні інформаційні технології в державні установи, а саме особливу увагу надає впровадженню штучного інтелекту. Однак, постає питання доцільності та питань безпеки таких впроваджень, адже дослідження демонструють відповідні виклики навіть на даних етапах зазначають не тільки дослідники в своїх наукових роботах, але й в різних медіа просторах, закликаючи звертати увагу на даний об'єкт зокрема в питаннях об'єктивності таких результатів досліджень. Судова експертиза та загалом експертні висновки є однією з тих видів державної діяльності, які ще не почали офіційно/публічно використовувати когнітивні моделі, а саме когнітивні обчислення штучного інтелекту, але звертаючи увагу на різні нормативні документи та стратегії розвитку можна зробити припущення, що після завершення пріоритетних напрямків можуть перейти і до інших.

II. ДАНІ ТА МЕТОДИ

Основні дані зазначають важливість тематики демонструючи проблематику. В дослідженні враховуються дані та метрики з трьох напрямків, які є підгрунтям дослідження і формують загальний огляд теоретичної та практичної складової (Для більш точніших даних було проаналізовано українські та зарубіжні джерела):

– Інформаційно-технологічна документація та дослідження, а саме наукові праці, щодо опису технічної складової технології та його особливості з практичного впровадження;
– Нормативна база відповідного законодавства в сфері судової експертизи, в яких зазначена специфіка досліджуваного об'єкту;
– Інші дослідження (практичні кейси, статистика та публічні медіа дані), які мають дотичні елементи проаналізованого об'єкту;
– Застосовані методи дослідження: було використано збирання даних та подальший їх аналіз для формування дослідження.

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка
Факультет інформаційних технологій
Кафедра інформаційних систем та технологій

SCIIST
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY SCIENTIFIC CONFERENCE

2-а Міжнародна науково-практична конференція

«ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ: РЕЗУЛЬТАТИ І ПЕРСПЕКТИВИ»
(IST 2025)

5 березня 2025 р.

84. DATA-DRIVEN APPROACHES FOR RISK MANAGEMENT IN MARITIME ROUTE OPTIMIZATION USING CLOUD AND DISTRIBUTED SYSTEMS Pavlo Kalenyk, Volodymyr Vychuzhanin 288
85. LOSSLESS IMAGE COMPRESSION BASED ON AUTOENCODER NEURAL NETWORKS Oleksandr Kis, Gennadiy Kis, Olga Polonevych, Kamila Storchak 291
86. LEVERAGING AI FOR AGRICULTURAL LAND MONITORING AND RECLAMATION Kristina Silvanovych, Olena Hrynova 295
87. RECOGNIZING A PERSON'S EMOTIONAL STATE IN IMAGES Vladyslav Synhaivskyi, Volodymyr Druzhynin 298
88. ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В РОЗРОБЦІ КОМП'ЮТЕРНИХ ІГОР ТА ЯК ЙОГО ВИКОРИСТАННЯ ВПЛИВАЄ НА РОЗРОБНИКІВ Єлизавета Бабенко 301
89. ШТУЧНИЙ ІНТЕЛЕКТ ЯК НОВИЙ ІНСТРУМЕНТ В СИСТЕМАХ ДОКУМЕНТООБІГУ Єлизавета Бабенко, Костянтин Бабенко 303

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В РОЗРОБЦІ КОМП'ЮТЕРНИХ ІГОР ТА ЯК ЙОГО ВИКОРИСТАННЯ ВПЛИВАЄ НА РОЗРОБНИКІВ

Єлизавета Бабенко

Анотація. У тезі досліджено та розглянуто нюанси і особливості застосування штучного інтелекту в розробці комп'ютерних ігор та його використання зі сторони розробників. Приведено приклади застосування штучного інтелекту в комп'ютерних іграх. Визначено основні складові процесу розробки продукту. Проаналізовано нюанси та складності у виборі і впровадженні штучного інтелекту за ту чи іншу функціональну складову кінцевого IT продукту.

Ключові слова: штучний інтелект; комп'ютерні ігри; комп'ютерні відеоігри; розробка; вплив використання ШІ на розробників

I. ВСТУП

На сьогоднішній момент існує багато можливостей та технологій за допомогою, яких створюються комп'ютерні ігри для різних видів графіки. З розвитком технологій потреба в зацікавленості потенційних користувачів стає складнішою з кожним новим етапом. З популяризацією штучного інтелекту та його розвитку дозволили впровадити та реалізувати нові можливості, які в свою чергу ускладнили розробникам підтримку робото спроможності готової відеогри.

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Створення відеоігор є складною та трудомісткою реалізацією цікавого геплею. Для залучення більшої аудиторії гравців потрібно задіяти більш складніші технології: VR (віртуальну, змішану, повну реальність), штучний інтелект, захват руху (motion capture), тощо. Ці технології потребують більше часу, більшого місця на пристрої, тобто, враховуючи програмне та апаратне забезпечення для реалізації запланованого функціоналу кінцевого продукту. При розробці будь-якого IT продукту окрім програмної складової реалізації також на початковому етапі враховуються багато факторів для формування повної концепції. Тому потрібно врахувати наступні складові процеси розробки продукту в будь-якій сфері IT:

Технічні міркування: полягає в розумінні впровадженої технології враховуючи програмну та апаратну складову з її максимальними можливостями, які вона надає для коректного впровадження та функціонування технології.

Методологічні розробки: здійснити конкретний опис процесу створення кінцевого продукту у вигляді готової комп'ютерної гри;

Візуальна концепція: є головним елементом в IT продукту так, як користувач першим кроком взаємодії з продуктом спостерігає. Також візуальна складова потрібна для визначення типу використаної графіки для тої чи іншого стилю та посилу гри;

Інструменти та рамки розробки: додаткові можливості для полегшення розробки продукту. Наприклад: Unity ML-Agents Tookit (для застосування різних методів навчання штучного інтелекту для розробки відповідної графіки візуальної частини продукту), Unreal Engine з Blueprints AI System (движок розробки відеоігор з ШІ), Godot Engine з AI API (движок з підтримкою AI), Tensor Flow Py Torch (бібліотеки для складних задач штучного інтелекту генеруючи контенту та машинного навчання), AI Behavior Tookit (використовують для встановлення поведінки NPS в ігровому процесі відповідно до змінених сценаріїв) тощо.

ШТУЧНИЙ ІНТЕЛЕКТ ЯК НОВИЙ ІНСТРУМЕНТ В СИСТЕМАХ ДОКУМЕНТООБІГУ

Єлизавета Бабенко, Костянтин Бабенко

Анотація. В даній тезі досліджено та розглянута теоретична складова штучного інтелекту, як новий інструмент в системах документообігу. Проаналізовано компоненти та складові принципу використання штучного інтелекту в контексті документообігу та самого документу. Також приведено сучасний приклад програмного кінцевого IT продукту, який можна використовувати для широкого кола сфер діяльності таких як підприємство або організації.

Ключові слова: штучний інтелект; документ; документообіг; система.

I. ВСТУП

Наразі впровадження штучного інтелекту в документообіг та в його систему автоматизовує багато процесів, на які людина може витратити значно більше часу. На думку багатьох людей технологія використання штучного інтелекту є чудовим інноваційним, швидким помічником для реалізації конкретної поставленої задачі та для зменшення витрат на робочу силу. Але чи насправді нам вони потрібні в даній сфері застосування? Чи насправді нам потрібно оптимізовувати робочий процес за допомогою штучного інтелекту.

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Як і будь-яка технологія Штучний інтелект, перш за все, являє собою набір нюансів та проблем, які на певному шляху можуть як вдосконалювати так і набувати все більше не потрібного функціоналу, породжуючи, таким чином, додаткові виклики для фахівців з програмування і паралельно виникають додаткові витрати для споживачів, а саме: на тестування, впровадження, навчання персоналу. Однак, розглядаючи можливості, які надає штучний інтелект варто згадати наступні, а саме: генерація контенту, структуризація контенту, діалоговий сервер, тощо.

Загалом, Штучний інтелект проник в наше повсякденне та професійне життя швидким та бурхливим напливом. Він здійснює напівавтоматичний процес документообігу, допомагає оптимізовувати та пришвидшити процеси, обробляти дані, в тому числі великі обсяги інформації і, таким чином, впливає на оперативність та якість прийняття рішень, як в бізнес сфері так і в політичній.

В цілому, документообіг – процес руху документів в організації/підприємстві. Наразі більше використовують електронний документообігу (більш розповсюдженим є електронний документообіг).

Штучний інтелект, в свою чергу, – «напрямок комп'ютерних наук, який здійснює автоматизацію та «імітацію» машиною або за допомогою відповідної програми розумової діяльності людини» [1, с.49]. Наразі можна поділити технологію ШІ застосовну для документообігу на два напрямки:

повноцінні програми або платформи, які користувач може одразу використовувати без допоміжних дій. Яскравим прикладом застосування штучного інтелекту в програмному забезпеченні для документообігу та роботи з документами – Google Document Artificial Intelligence, за допомогою якого можна обробляти неструктуровано подану інформацію [2].

сторонні IT продукти, які виступають незамінним помічником для загального користування в будь-яких сферах діяльності і підходять як для створення контенту так і перефразовування вже готового набору тексту. В цьому разі ШІ видає готовий результат у вигляді структурованого готового документу за тою тематикою, якою його запитували.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

VI ВСЕУКРАЇНСЬКА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ
«СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ IOT»
15 квітня 2025 року
Збірник тез

м. Київ

Бабенко Єлизавета Костянтинівна
студентка 5 курсу, групи КНДМ-51
Державного університету
інформаційно-комунікаційних технологій

ВЗАЄМОДІЯ ІНТЕРНЕТ РЕЧЕЙ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ НА ПРИКЛАДІ ДВОХ НАПРЯМКІВ ЗАСТОСУВАННЯ

В тезі розглянуто взаємодія Інтернет речей (IoT) зі Штучним інтелектом на прикладі двох різних напрямків застосування, як самостійні сфери, враховуючи їх особливості при реалізації в інформаційних продуктах. Також проаналізовано майбутні перспективи взаємодії даних технології та виявлено позитивні та негативні сторони впровадження даної взаємодії, які є суттєвими недоліками в майбутньому та можуть вплинути на виникнення низки проблем і в інших сферах.

Постановка задачі

Наразі різні види технологій мають взаємодію між собою, створюючи нові можливості та вдосконалюючи одна одну. Однак не всі зараз технології використовуються один з одним. Такими є технології Інтернету речей та Штучний інтелект. В загальному розумінні та принципах технологія, як кожна окрема складова інформаційних технологій зрозуміла, але якщо їх поєднати, який результат можна отримати в різних напрямках та сферах застосування.

Мета дослідження

Дослідити взаємодію технології Інтернету речей зі Штучним інтелектом на прикладі двох напрямків з урахуванням їх особливостей та нюансів.

Результати дослідження

На сьогоднішній день немає наглядного прикладу застосування IoT технологій та Штучного інтелекту, але якщо розглядати дану взаємодію в майбутній перспективі, то можна зазначити цікаву взаємодію, яка може відігравати ключову роль не тільки з точки зору привернення уваги користувачів, але й для розробників, які зможуть зробити процес вдосконалення та оновлення своїх програм без великої кількості витраченого часу в деяких моментах. Однак потрібно виокремити і негативну сторону такої взаємодії в надмірній кількості, а саме таким чином буде сприяти недостатній кількості даних, що може призвести до точки, коли розробники будуть свідомо не надавати можливість заборони використання їхніх даних задля отримання невистачаючої інформації.

IoT є технологією за допомогою, якої можна автоматизувати простий процес, спрошуючи собі життя за конкретним алгоритмом зазначених чи встановлених дій, а Штучний інтелект є процес безпосередньої імітації машиною розумову діяльність людини [1, с.49].

Бабенко Єлизавета Костянтинівна
студентка 5 курсу, групи КНДМ-51
Державного університету
інформаційно-комунікаційних технологій

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

В тезі досліджено прогалини щодо безпеки персональних даних, які обробляються програмними рішеннями робленими на основі технології Інтернет речей (IoT). В цілому, можна зазначити, що вони є непомітними нам одразу. Теза спрямована розкрити особливості принципу безпеки при використанні технології в програмних продуктах обробки персональних даних. Проаналізовано реальні приклади проблем при застосуванні приладів користувачами.

Постановка задачі

Наразі в еру інформаційних технологій та повної цифровізації проявляється тенденція важливості безпеки даних. Тому наразі йде проблема в загальному характері про використання персональних даних, яку можна розглядати безпосередньо з двох напрямків захисту безпеки, а саме зі сторони програмної реалізації та зі законодавчої. Однак, при будь-якому використані Інтернету речей відбуваються збирання персональних даних тієї особи, яка володіє та користується нею. Людина безпосередньо є персональними даними, які формують її як окремий об'єкт, який технологія чи система може розрізнити. Ось тут і виникає проблема безпосередньої безпеки таких даних, які інколи людина несвідомо надає технології право доступу, які надалі будуть використовуватися та збиратися.

Мета дослідження

Дослідити безпосередню безпеку персональних даних при використанні технологій IoT та виявити прогалини в системах безпеки з урахування виявлених недоліків девайсів та IT продуктів.

Результати дослідження

Кожен стикався з моментом, коли потрібно надати дозвіл до своїх персональних даних для доступу використання додатку чи програми. Особливо цей момент відчувається помітно в програмах для використання IoT технологій, а саме смарт годинниках, розумному будинку, розумному місті, впровадження безпосередньо в автомобілі, тощо.

В законодавчому аспекті як і в Україні та інших державах можна бачити регулюючі документи, які на перший погляд нібито здійснюють безпеку, але це

Бабенко Єлизавета Костянтинівна
студентка 5 курсу, групи КНДМ-51
Державного університету
інформаційно-комунікаційних технологій

Бабенко Костянтин Миколайович
студент 3 курсу, групи АЗД-31
Державного університету
інформаційно-комунікаційних технологій

ТЕХНОЛОГІЯ IoT ТА ЇЇ ЗАСТОСУВАННЯ В АНАЛІТИЦІ ДАНИХ

У даній тезі розглянуто сутність та зміст технології IoT та типові особливості її застосування для аналізу даних та формування баз даних зі значним обсягом інформації. Досліджено теоретичну складову та наведено декілька прикладів щодо застосування технології Інтернет речей як практичного рішення сьогодення. Виокремлено проблему застосування даної технології при зборі персональних даних.

Постановка задачі

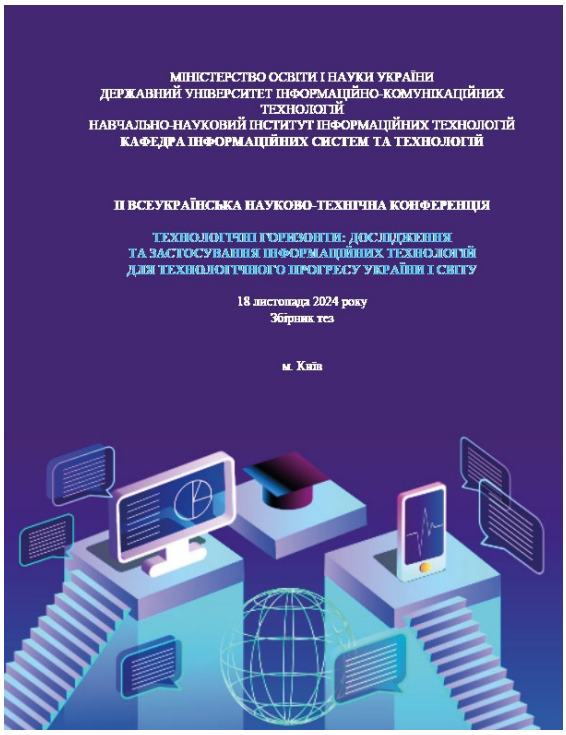
Технології розвиваються шаленими темпами і карантин та досить таки тривала війна в Україні не стали перешкодою для їх впровадження як бізнесом, державою чи простими громадянами. Нині технологія Інтернет речей вважається чи не однією з найпопулярніших технологій, яка спрямована на оптимізацію процесів, що нас оточують. Однак, найчастіше нові можливості породжують нові виклики. Актуальність даної теми суттєво зростає, адже автоматизація процесів збору, аналізу чи обміну інформації в сучасних умовах не синхронізуються з дотриманням законодавства про захист персональних даних. Дана теза спрямована на дослідження особливостей застосування технології IoT в аналітиці даних в умовах сьогодення.

Мета дослідження

Визначити сутність та зміст технології IoT та дослідити певні особливості її застосування в аналітиці даних. Окреслити проблему застосування технології Інтернет речей при зборі персональних даних.

Результати дослідження

В загальному розуміння технологія IoT або технологія Інтернет речей являє собою «сукупність взаємопов'язаних фізичних пристроїв із вбудованими датчиками, виконавчими пристроями та програмним забезпеченням, що утворюють або входять до складу мережі» [1].



Бабенко Єлизавета Костянтинівна
студентка 5 курсу, групи КНДМ-51
Державний університет інформаційно-комунікаційних технологій
Бабенко Костянтин Миколайович
студент 3 курсу, групи АЗД-31
Державний університет інформаційно-комунікаційних технологій

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНТРУМЕНТ В АНАЛІТИЦІ ДАНИХ

Постановка задачі. Штучний інтелект як технологія сучасності з кожним днем все більше захоплює сфер суспільного життя. Наразі складно назвати галузь, яку, в цілому, могла оминути технологія штучного інтелекту. В цілому, на перший погляд, автоматизація здатна оптимізувати досить таки багато процесів, на які людина витратила б значну частину часу. Нині аналіз даних є важливою опцією для будь-якої установи, підприємства, організації чи просто звичайної людини. Інформаційна війна в Україні не збавляє обертів і породжує все нові виклики, тому немає жодних сумнівів в актуальності даної теми. Дана теза спрямована на дослідження питань пов'язаних з застосуванням штучного інтелекту як технології, яка здатна обробляти великі обсяги інформації, при цьому структуруючи дані та перетворюючи їх на корисну інформацію, яка оптимізує процеси прийняття рішень в цілому.

Мета дослідження. Дослідити штучний інтелект як новий інструмент в аналітиці даних.

Результати дослідження. Під поняттям дані слід розуміти «інформацію, що одержується у процесі чуттєвого пізнання і ще не піддана переробці і узагальненню абстрактно-логічним мисленням людини» [1, с.19]. Такі дані вважаються лише так званою «сировиною» для створення інформації. При цьому інформація це вже «дані, зібрані і систематизовані в придатну для використання форму» [1, с.19].

Функціонально аналіз даних є важливим для будь-якої сфери суспільного життя, будь-то бізнес, медицина чи політика. Нині рух інформації навколо нас відбувається безперервно. Загалом, джерелом даних можуть виступати як системи електронного документообігу так і звичайні буклети, візитні картки чи інтернет-ресурси. Крім відкритих даних слід додатково згадати про персональні дані, як про інформацію з обмеженим доступом.

На ринку можна знайти достатньо професійних інструментів, призначених для аналізу даних. Всі вони направлені на допомогу та можуть візуалізувати, відстежувати та аналізувати дані, але частіше за все їх можливості обмежені

Бабенко Єлизавета Костянтинівна, студентка 5 курсу,
Державний університет інформаційно-комунікаційних технологій, Київ
Бабенко Костянтин Миколайович, студент 3 курсу,
Державний університет інформаційно-комунікаційних технологій, Київ

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНТРУМЕНТ РОБОТИ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Постановка задачі. Україна вже тривалий час позиціонує себе як цифрова держава. Держава, для якої війна не є перешкодою розробляти та впроваджувати нові технології. Штучний інтелект вважається однією з таким технологій, яка не стоїть на місці, а з кожним днем все глибше проникає в різні сфери суспільного життя. Однак, нові можливості породжують нові питання та нові випробування, тому немає жодних сумнівів в актуальності даної теми. Ця теза спрямована на дослідження викликів пов'язаних з застосуванням штучного інтелекту як новітньої технології в системах електронного документообігу в умовах сьогодення, враховуючи виклики які випали на долю українського народу.

Мета дослідження. Дослідити штучний інтелект як інструмент роботи систем електронного документообігу.

Результати дослідження. Під поняттям штучний інтелект слід розуміти «напрям комп'ютерних наук, який здійснює автоматизацію та «імітацію» машиною або за допомогою відповідної програми розумової діяльності людини. Також здійснює низку функцій таких, як: розпізнавання голосу, ідентифікація людини (сканер обличчя/відбитків пальців, чудовим прикладом є сканер обличчя/відбитків пальців для розблокування телефону), визначення емоції, написання текстів, створення музики та генерування зображень» [1, с.49].

Системою електронного документообігу, в свою чергу, слід вважати окрім апаратного та програмного забезпечення і сам електронний документообіг з усіма його життєвими циклами, пов'язаними зі створенням, редагуванням, обробкою й зберіганням електронних документів. В цілому, вже станом на 2013 рік в Україні працювало орієнтовно близько 50 різних систем електронного документообігу. Загалом, відповідно до даних порталу «Дія», станом на початок 2022 року, громадяни нашої держави вже мали можливість скористатися більше ніж 70 електронними послугами. Цифровізація й надалі набирає обертів і до 2024 року програма інформатизації зобов'язала Мінцифри до 100 відсотків публічних послуг перевести в цифровий формат [2, с. 3].

З однієї сторони, впровадження штучного інтелекту, наприклад, в державний проект (портал чи застосунок) «Дія», здавалося б неабияк полегшує роботу сервісу. Звісно, це доволі практично, коли чат-бот цілодобово може відповісти на питання користувачів та, поглянувши на цей технологічний інструмент, в цілому стає зрозуміло, що жоден програмний продукт не здатен

Бабенко Єлизавета Костянтинівна
студентка 5 курсу, групи КНДМ-51
Державний університет інформаційно-комунікаційних технологій

ВПЛИВ КОМП'ЮТЕРНОГО ДИЗАЙНУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ОСВІТНІЙ ПРОЦЕС НАВЧАННЯ В УНІВЕРСИТЕТАХ

Постановка задачі. З розвитком технологій постає питання з новими підходами до навчального процесу, його оптимізації та до сьогоденних студентів. Зацікавити студента своєю дисципліною має на меті кожен викладач, застосовуючи різні методи та способи, в тому числі новітні технології, тому ця тема є доволі актуальною. Дана теза висвітлює вплив інформаційних технологій, зокрема комп'ютерного дизайну та його складових, на освітній процес його позитивні та негативні впливи на здобувачів.

Мета дослідження. Проаналізувати вплив застосування комп'ютерного дизайну на освітній процес навчання в університетах.

Результати дослідження. Навчальний процес є головною складовою для успішного формування майбутнього спеціаліста. Для цього подача матеріалів в навчальному процесі є головною складовою в освіті.

Комп'ютерний дизайн є «створення візуального так званого «зовнішнього» вигляду за допомогою відповідних комп'ютерних технологій (IT) багатогранним та неоднозначним визначенням з урахуванням того, що даний термін включає в себе багато складових таких, як: графіка, анімація, відеоігри, тощо» і має свої особливості [1, с.21].

Однією з інноваційних технологій можна виділити віртуальну реальність та його види такі, як змішана та доповнена віртуальна реальність, які допоможуть більш точно та цікаво подати матеріал для слухачів. Звісно це дороге задоволення і не всі навчальні заклади зможуть впровадити це з урахуванням фінансових та фізичних можливостей облаштувати аудиторію хоча б для однієї дисципліни так, що б вистачило обладнання на всю групу та викладача.

Іншою технологією, як зазначає стратегія розвитку вищої освіти в Україні на 2021-2031 роки можна виділити відносно популярну технологію, а саме технології штучного інтелекту. Штучний інтелект є швидким методом поліпшенням освітнього процесу навчання як для викладачів при створенні візуалізації матеріалів, так і для студентів при виконанні домашніх завдань. З низки непоганих інструментів можна виділити наступні: Undetectable AI та Google Document AI для створення з неструктурованого тексту структурований;


PROMETHEUS
СЕРТИФІКАТ
Видано 31.10.2024
Бабенко Єлизавета Костянтинівна
Академічна доброчесність: онлайн-курс для викладачів
AcademIQ


СЕРТИФІКАТ № J4U/OS25/9
підтверджує, що
Бабенко Єлизавета
Директор ННІ права СумДУ Анатолій ЮЛІШ
Академічна координаторка освітнього проєкту «Доступ до правосуддя: кращі практики ЄС для України» Ольга ШПАГІР


СЕРТИФІКАТ № J4U/P25/13
підтверджує, що
Бабенко Єлизавета Костянтинівна
Академічна координаторка освітнього проєкту «Доступ до правосуддя: кращі практики ЄС для України» Ольга ШПАГІР


PROMETHEUS
СЕРТИФІКАТ
Видано 29.05.2025
Бабенко Єлизавета Костянтинівна
Наукова комунікація в цифрову епоху.


Міністерство освіти і науки України
Сумський державний педагогічний університет імені А.С. Макаренка
Навчально-науковий інститут історії, права та міжнародних відносин
Кафедра права та публічного управління
СЕРТИФІКАТ
Бабенко Єлизавета Костянтинівна
учасник VIII Міжнародної науково-практичної конференції
РЕАЛІЇ ТА ПЕРСПЕКТИВИ РОЗБУДОВИ ПРАВОВОЇ ДЕРЖАВИ В УКРАЇНІ ТА СВІТІ
Серія ННІІПМВ № 1805
Загальна кількість академічних годин - 12
Ректор Юрій ЛЯННОЙ
12-13 травня 2025
Ріка (Хорватія)


СЕРТИФІКАТ № J4U/T25/46
підтверджує, що
Бабенко Єлизавета Костянтинівна
Академічна координаторка освітнього проєкту «Доступ до правосуддя: кращі практики ЄС для України» Ольга ШПАГІР
Керівниця юридичної клініки ННІ права СумДУ Людмила РУДЕНКО


Clarivate
Web of Science Academy Certificate
Yelyzaveta Babenko
An Introduction to Ethical Publishing Behavior on 6/2/2025


ДИПЛОМ
ЛАУРЕАТА
Бабенко Єлизавета


Clarivate
СЕРТИФІКАТ
Yelyzaveta Babenko
Як написати наукову роботу (2): публікаційний процес


Навчально-науковий інститут менеджменту та підприємництва
Сертифікат
цей сертифікат підтверджує, що
Бабенко Єлизавета
брав (-ла) участь у І міжнародній науково-практичній конференції
Синергія інновацій: політика, економіка та менеджмент в цифровому світі, м.Київ, 18 квітня 2025 року
0,2 кредиту ЄКТС
Директор навчально-наукового інституту менеджменту та підприємництва Світлана ПЕТРОВСЬКА


СЕРТИФІКАТ
підтверджує, що
Бабенко Єлизавета
пройшов(ла) навчання за програмою Школи для студентства «Права людини під час війни: міжнародне гуманітарне право та міжнародне право захисту прав людини» (онлайн)
обсяг 12 годин(и)
Виконавчий директор УГСПЛ Олександр Павліченко