ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД»
МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
Кафедра _____

КУРСОВА РОБОТА

з дисципліни: **«ІНФОРМАЦІЙНЕ ПРАВО»**

за темою: **«СПІВРОБІТНИЦТВО УКРАЇНИ З ІНШИМИ ДЕРЖАВАМИ ТА МІЖНАРОДНИМИ ОРГАНІЗАЦІЯМИ В МІЖНАРОДНІЙ ІНФОРМАЦІЙНІЙ СФЕРІ»**

Студента (ки): Носенко К.О.
курсу: 4
групи: ІН16-9-22-Б1П (4.0д)
Спеціальність: 081 Право
Керівник: доцент, к.ю.н. Лебедєв О.П.

Оцінка: _____
Національна шкала_____
Кількість балів: _____ ECTS _____

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

м. Чернігів 2026

ЗМІСТ

ВСТУП

Актуальність теми. У третій декаді XXI століття міжнародна інформаційна сфера перетворилася на провідну арену міждержавної взаємодії, де технологічний прогрес визначає рівень національного суверенітету та глобального впливу. Для України питання міжнародного співробітництва в інформаційній галузі набуло екзистенційного значення. В умовах триваючої відсічі збройній та гібридній агресії, інформаційний простір став не лише засобом комунікації, а й об’єктом критичного захисту, що потребує консолідації зусиль із міжнародними партнерами.

Актуальність дослідження зумовлена необхідністю правового забезпечення інтеграції України до Єдиного цифрового ринку ЄС (Digital Single Market) та поглиблення стратегічного партнерства з НАТО у сфері кібероборони. Поява нових викликів, пов’язаних із розвитком штучного інтелекту, квантових обчислень та масових дезінформаційних кампаній, вимагає від нашої держави не лише адаптації внутрішнього законодавства, а й активної участі у формуванні нових глобальних стандартів цифрової етики та інформаційної безпеки. Співпраця з ООН, Радою Європи, ЮНЕСКО та Міжнародним союзом електрозв’язку є ключовим інструментом утвердження України як суб’єкта, а не об’єкта міжнародного інформаційного права.

Об’єктом дослідження є сукупність міжнародно-правових відносин, що виникають між Україною, іноземними державами та міжнародними організаціями у процесі формування, захисту та використання глобального інформаційного простору.

Предметом дослідження є норми міжнародного та національного інформаційного права, двосторонні та багатосторонні договори, акти міжнародних організацій та стратегічні документи України, що регламентують міжнародне співробітництво в інформаційній сфері.

Метою курсової роботи є системний аналіз правових засад, механізмів та пріоритетних напрямів взаємодії України з міжнародними інституціями та окремими державами для зміцнення національної інформаційної безпеки та реалізації євроатлантичного вектору розвитку.

Для досягнення мети визначено такі **завдання**:

розкрити правову природу міжнародної інформаційної сфери як об'єкта регулювання;

проаналізувати систему міжнародно-правових актів у сфері інформації та кібербезпеки;

дослідити роль ООН та ЮНЕСКО у забезпеченні свободи інформації та дотримання цифрових прав;

визначити особливості взаємодії України з НАТО та ЄС у протидії гібридним загрозам;

оцінити перспективи адаптації українського законодавства до вимог цифрового права ЄС;

сформулювати пропозиції щодо посилення ролі України у міжнародних системах інформаційного врядування.

Методологічну основу дослідження становлять діалектичний метод пізнання, порівняльно-правовий метод (для зіставлення національних та міжнародних стандартів), системно-структурний підхід та метод прогнозування.

Наукова новизна роботи полягає у комплексному дослідженні правового статусу України як «цифрового щита» Європи, що не лише реципіює міжнародні норми, а й пропонує власні кейси правового регулювання інформаційної сфери в умовах воєнного стану та цифрової трансформації.

Практичне значення одержаних результатів курсового дослідження полягає у можливості їхнього прикладного застосування для зміцнення суб'єктності України в глобальному цифровому просторі. Сформульовані висновки та пропозиції можуть бути використані у наступних сферах:

У зовнішньополітичній діяльності: аналіз міжнародно-правових інструментів взаємодії з НАТО та ЄС може стати підґрунтям для розробки нових двосторонніх угод про кібербезпеку та обмін розвідувальною інформацією, а також для посилення позицій України в межах міжнародних робочих груп ООН з питань інформаційної безпеки.

У сфері державного управління: результати дослідження можуть бути враховані Міністерством цифрової трансформації та Міністерством закордонних справ України при реалізації стратегії «цифрової дипломатії» та впровадженні стандартів Digital Single Market (Єдиного цифрового ринку ЄС) у національну практику.

У законотворчій роботі: висновки щодо імплементації норм європейського цифрового права (зокрема Digital Services Act та AI Act) можуть бути використані профільними комітетами Верховної Ради України при підготовці законопроєктів про захист критичної інформаційної інфраструктури та регулювання штучного інтелекту.

У сфері національної безпеки: розроблені рекомендації щодо правових механізмів протидії гібридним загрозам та дезінформації мають практичну цінність для діяльності Центру протидії дезінформації та РНБО України в контексті захисту суверенітету в інформаційній сфері.

У навчальному процесі: матеріали курсової роботи можуть бути використані при викладанні дисциплін «Інформаційне право», «Міжнародне публічне право», «Право міжнародних організацій» та спецкурсів із кіберправа для студентів юридичних спеціальностей.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПРАВОВІ ЗАСАДИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА В ІНФОРМАЦІЙНІЙ СФЕРІ

1.1. Поняття, принципи та правова природа міжнародної інформаційної сфери як об’єкта правового регулювання.

Міжнародна інформаційна сфера в сучасній доктрині інформаційного права розглядається як складна, багаторівнева система глобальних суспільних відносин, що виникають у процесі створення, збирання, обробки, зберігання та транскордонного поширення інформації. Це глобальний комунікаційний простір, який не обмежується національними кордонами та охоплює сукупність інформаційних інфраструктур, суб’єктів міжнародного права, а також технологічних протоколів, що забезпечують функціонування всесвітньої мережі. Поняття міжнародної інформаційної сфери як об’єкта правового регулювання включає не лише технічну складову (мережі та канали зв’язку), а й змістовну (контент, знання, культурні цінності) та регуляторну (міжнародні стандарти, договори, регламенти) компоненти. Правова природа цієї сфери є гібридною, оскільки вона поєднує норми публічного міжнародного права, що регулюють відносини між державами (інформаційний суверенітет, кібербезпека), та норми приватного права, які визначають умови транскордонної електронної комерції та захисту інтелектуальної власності [2].

Правова природа міжнародної інформаційної сфери характеризується екстеріторіальністю, високою динамічністю та складністю ідентифікації юрисдикції. Оскільки інформаційні потоки є нематеріальними та миттєвими, класичні правові інститути, засновані на територіальному принципі, зазнають трансформації. У 2026 році доктрина наголошує на переході від суто державного контролю до багатосторонньої моделі управління (multistakeholder model), де суб'єктами виступають не лише держави, а й міжнародні організації (ООН, МСЕ), транснаціональні корпорації та громадянське суспільство. Об’єктом регулювання тут виступає не сама інформація як статичний ресурс, а

саме процес інформаційного обміну, що має стратегічне значення для глобальної безпеки та сталого розвитку [4]. Такий підхід дозволяє розглядати міжнародну інформаційну сферу як спільне надбання людства, що потребує узгоджених правових режимів захисту від кіберзагроз та цифрової дискримінації [6].

Принципи міжнародного інформаційного права становлять фундамент правового регулювання цієї сфери. До загальновизнаних принципів належать: принцип вільного потоку інформації та ідей (free flow of information), що є базовим для демократичного суспільства; принцип інформаційного суверенітету держави, який дає право нації самостійно визначати свою інформаційну політику в межах кордонів; та принцип міжнародного співробітництва у сфері використання інформаційно-комунікаційних технологій. Окремо виділяють принципи пропорційності та необхідності при обмеженні доступу до інформації, принцип невтручання у внутрішні справи через інформаційний вплив (протидія дезінформації), а також принцип забезпечення безпеки глобальної критичної інфраструктури. У 2026 році особливої ваги набув принцип цифрової солідарності, що передбачає допомогу державам у подоланні «цифрового розриву» та захисті від транскордонних кібератак [3].

Система правового регулювання в цій сфері включає міжнародні конвенції (наприклад, Будапештську конвенцію про кіберзлочинність), двосторонні договори, а також акти «м’якого права» (резолюції ООН, стандарти ISO). Особливу роль відіграють регіональні стандарти, зокрема Регламенти ЄС (GDPR, DSA, DMA), які завдяки ефекту «Брюсселя» стають глобальними орієнтирами. Правове регулювання міжнародної інформаційної сфери спрямоване на досягнення балансу між безпековими інтересами держав та правами людини на приватність і вільне вираження поглядів. Це створює передумови для формування глобального цифрового порядку, де право домінує

над технологічним хаосом, забезпечуючи стабільність міжнародних комунікацій [5].

1.2. Система міжнародно-правових актів у сфері інформаційного обміну, кібербезпеки та захисту персональних даних.

Система міжнародно-правових актів у сфері інформаційного обміну, кібербезпеки та захисту персональних даних у 2026 році являє собою багаторівневу структуру, що поєднує універсальні інструменти ООН, регіональні стандарти (зокрема ЄС та Ради Європи) та акти спеціалізованих інституцій. В основі регулювання інформаційного обміну лежать положення Загальної декларації прав людини та Міжнародного пакту про цивільні і політичні права, які закріплюють фундаментальне право на вільне збирання та поширення інформації незалежно від державних кордонів. Проте сучасна доктрина наголошує на тому, що ці права не є абсолютними та можуть бути обмежені в інтересах національної безпеки, що набуло особливої гостроти у зв’язку з поширенням транскордонної дезінформації та використанням інформаційних технологій для ведення гібридних воєн [3]. Ключовим документом у цій сфері залишається Окінавська хартія глобального інформаційного суспільства та Декларація принципів Всесвітнього саміту з питань інформаційного суспільства (WSIS), які визначають стратегічні напрями подолання цифрового розриву та створення інклюзивного цифрового простору [1].

Сфера кібербезпеки регулюється системою актів, що спрямовані на криміналізацію протиправних діянь у цифровій сфері та встановлення стандартів відповідальної поведінки держав у кіберпросторі. Центральне місце тут посідає Конвенція про кіберзлочинність (Будапештська конвенція) 2001 року з її додатковими протоколами, що забезпечує правову базу для міжнародного співробітництва у розслідуванні злочинів, пов’язаних із

комп’ютерними даними та системами. На глобальному рівні діють доповіді Групи урядових експертів ООН (GGE) та Робочої групи відкритого складу (OEWG), які формулюють норми відповідальної поведінки держав, спрямовані на запобігання конфліктам у кіберпросторі та захист критичної інфраструктури [5]. Важливою частиною цієї системи є також стандарти ISO/IEC 27000, які, хоч і належать до актів «м’якого права», фактично визначають техніко-юридичний режим безпеки інформаційних послуг на глобальному ринку [2].

Захист персональних даних у міжнародному праві базується на принципах недоторканності приватного життя та інформаційного самовизначення. Провідну роль відіграє Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+) та її оновлена версія, що враховує виклики епохи Big Data та штучного інтелекту. Найбільш впливовим регуляторним інструментом є Загальний регламент про захист даних (GDPR) Європейського Союзу, який завдяки механізму екстеріторіальності встановив золотий стандарт приватності для всього світу. У 2026 році до цієї системи додалися норми Digital Services Act (DSA) та AI Act, що регулюють відповідальність платформ за профілювання користувачів та прозорість алгоритмів [4]. Таким чином, міжнародно-правова база еволюціонує від захисту фізичних носіїв інформації до гарантування цифрової гідності особи в умовах тотальної алгоритмізації суспільних процесів [6].

1.3. Суб’єкти міжнародного інформаційного співробітництва: роль держав та роль міжнародних міжурядових організацій.

Суб’єкти міжнародного інформаційного співробітництва у 2026 році становлять розгалужену систему, де ключова роль традиційно належить державам як первинним суб’єктам міжнародного права, проте функціональне лідерство все частіше переходить до міжнародних міжурядових організацій. Роль держав у цій сфері є фундаментальною, оскільки вони виступають

гарантами інформаційного суверенітету та основними розробниками національних стратегій кібербезпеки. Саме держави формують правовий режим транскордонних інформаційних потоків, укладають двосторонні та багатосторонні договори, а також несуть відповідальність за поведінку в кіберпросторі. У сучасних умовах доктрина інформаційного права підкреслює перехід держав від моделі «жорсткого контролю» до ролі регулятора, що забезпечує баланс між національною безпекою та дотриманням прав людини на приватність і вільне вираження поглядів [2]. Держави також є основними суб'єктами, що протидіють глобальним кіберзагрозам та дезінформаційним кампаніям, використовуючи механізми дипломатичного та правового тиску [5].

Міжнародні міжурядові організації (ММО) виконують роль координаційних центрів та майданчиків для встановлення глобальних техніко-юридичних стандартів. Особливе місце посідає Організація Об'єднаних Націй (ООН), яка через діяльність Групи урядових експертів (GGE) та Робочої групи відкритого складу (OEWG) формулює норми відповідальної поведінки держав у цифровому середовищі [1]. Спеціалізовані установи ООН, такі як Міжнародний союз електрозв'язку (МСЕ), відіграють критичну роль у розподілі частотного ресурсу та розробці технічних стандартів (ITU), що забезпечують сумісність національних інформаційних систем. ЮНЕСКО, своєю чергою, зосереджується на етичних аспектах використання штучного інтелекту, захисті свободи слова та подоланні цифрового розриву між розвиненими країнами та країнами, що розвиваються. Регіональні організації, як-от Європейський Союз та Рада Європи, стають «нормативними лідерами», чиї регламенти (GDPR, DSA, AI Act) фактично набувають статусу глобальних стандартів завдяки механізму екстеріторіальності [4].

Співвідношення ролей держав та ММО характеризується синергією: держави делегують організаціям частину своїх повноважень для вирішення транскордонних проблем, які неможливо розв'язати на національному рівні (наприклад, управління кореневими серверами Інтернету або протидія

глобальним кіберзлочинам). Водночас ММО забезпечують легітимізацію міжнародних стандартів та надають експертну підтримку країнам у процесі гармонізації законодавства. У 2026 році спостерігається тенденція до посилення ролі ММО у сфері «цифрової дипломатії», де вони виступають медіаторами у конфліктах щодо використання кіберзброї та маніпулювання інформаційним простором [3]. Таким чином, міжнародне інформаційне співробітництво еволюціонує від міжурядових консультацій до створення глобальної системи колективної цифрової безпеки, де держави та міжнародні інституції діють як єдиний правовий механізм [6].

РОЗДІЛ 2. МЕХАНІЗМИ ТА НАПРЯМИ ВЗАЄМОДІЇ УКРАЇНИ З МІЖНАРОДНИМИ ІНСТИТУЦІЯМИ У ЦИФРОВУ ЕПОХУ

2.1. Співробітництво України з Організацією Об’єднаних Націй та ЮНЕСКО у сфері свободи слова та інформаційної етики.

Співробітництво України з Організацією Об’єднаних Націй (ООН) та її спеціалізованою установою ЮНЕСКО у сфері свободи слова та інформаційної етики у 2026 році набуло стратегічного значення, перетворившись із формального дотримання міжнародних стандартів на активну фазу захисту національного інформаційного простору в умовах глобальних гібридних загроз. Основу цієї взаємодії складає реалізація положень Загальної декларації прав людини та Міжнародного пакту про цивільні і політичні права, де Україна виступає не лише як реципієнт рекомендацій, а й як держава-донор унікального досвіду протидії масштабним дезінформаційним кампаніям [7]. В межах Генеральної Асамблеї ООН Україна ініціює резолюції, спрямовані на захист журналістів у зонах конфліктів та засудження використання інформаційних технологій для підриву суверенітету держав. Правовий аспект цієї співпраці базується на міжнародно-правовому визнанні права на доступ до об'єктивної інформації як невід’ємної складової безпеки людини [3].

Особлива роль у цьому процесі належить ЮНЕСКО як головній міжурядовій організації, відповідальній за промоцію свободи вираження поглядів та розвиток медіаграмотності. Співробітництво України з ЮНЕСКО здійснюється через Міжнародну програму розвитку комунікації (IPDC), яка спрямована на підтримку незалежних медіа та розвиток етичних стандартів журналістики. У 2026 році пріоритетним напрямом стала імплементація «Рекомендації ЮНЕСКО щодо етики штучного інтелекту», що вимагає від України розробки національних етичних фільтрів для запобігання алгоритмічній дискримінації та маніпулюванню свідомістю громадян через соціальні мережі [4]. ЮНЕСКО також надає технічну та методологічну

допомогу в оцінці збитків, завданих медіаінфраструктурі України, та сприяє створенню безпечних умов для роботи репортерів через надання засобів захисту та проведення тренінгів із цифрової безпеки [6].

Інформаційна етика в контексті співпраці з ООН розглядається як інструмент забезпечення «інформаційної гігієни» та відповідального використання цифрових ресурсів. Україна бере активну участь у розробці Глобального цифрового договору (Global Digital Compact), який має на меті встановити єдині етичні правила для технологічних гігантів, зокрема щодо прозорості модерації контенту та захисту дітей у цифровому середовищі [5]. Доктрина інформаційного права України 2026 року акцентує увагу на тому, що свобода слова не є абсолютною і має закінчуватися там, де починається мова ворожнечі або заклики до насильства, що повністю корелюється з останніми звітами Спеціального доповідача ООН з питань свободи думки та вираження поглядів [2]. Таким чином, взаємодія з ООН та ЮНЕСКО дозволяє Україні не лише зберігати демократичні стандарти в умовах війни, а й формувати нову глобальну архітектуру інформаційної безпеки, засновану на пріоритеті прав людини та етичному використанні інновацій [4].

2.2. Стратегічне партнерство з НАТО та структурами ЄС у галузі протидії гібридним загрозам та дезінформації.

Стратегічне партнерство України з НАТО та структурами Європейського Союзу у 2026 році трансформувалося у цілісну систему колективної інтелектуальної та технологічної оборони, де протидія гібридним загрозам розглядається як критичний елемент національної та регіональної безпеки. Взаємодія з Альянсом базується на положеннях Дорожньої карти Партнерства зі стратегічних комунікацій та активній участі України в роботі Центру передового досвіду НАТО з питань стратегічних комунікацій (StratCom COE) у Ризі та Центру передового досвіду НАТО з кібероборони (CCDCOE) у

Таллінні. Це партнерство передбачає не лише обмін розвідувальними даними про активність ворожих ботоферм та хакерських угруповань, а й спільну розробку доктринальних документів, що визначають правовий режим реагування на «сірі» загрози, які формально не підпадають під дію ст. 5 Північноатлантичного договору, але системно підривають стійкість демократичних інститутів [3]. Правова природа цього партнерства змістилася від консультативної підтримки до операційної сумісності, де українські фахівці інтегровані в європейську мережу раннього попередження про гібридні атаки [5].

Співпраця з Європейським Союзом у галузі протидії дезінформації у 2026 році фокусується на імплементації норм Кодексу практики щодо дезінформації та Регламенту про цифрові послуги (DSA). Головним інституційним партнером України виступає робоча група EEAS East StratCom Task Force, яка оперує проєктом EUvsDisinfo. В межах цього співробітництва Україна приєдналася до Європейської обсерваторії цифрових медіа (EDMO), що дозволяє здійснювати транскордонний фактчекінг та ідентифікувати координовану неавтентичну поведінку в соціальних мережах на ранніх стадіях. Юридичний аспект взаємодії з ЄС включає гармонізацію українського законодавства про медіа та рекламу з європейськими стандартами прозорості фінансування контенту, що є ключовим інструментом боротьби з прихованим іноземним впливом (malign foreign influence) [4]. Важливу роль відіграє також Європейський центр з протидії гібридним загрозам (Hybrid CoE), де Україна спільно з партнерами тестує правові моделі атрибуції кібератак та інформаційних операцій [2].

Особливістю стратегічного партнерства у 2026 році є акцент на «когнітивну стійкість» суспільства. Спільно з НАТО та ЄС Україна впроваджує довгострокові програми з медіаграмотності та критичного мислення, які розглядаються не просто як освітні проєкти, а як елемент цивільної оборони в інформаційній сфері. Доктрина інформаційного права України акцентує на тому, що протидія гібридним загрозам потребує створення «кільця безпеки»

навколо державних реєстрів та критичної інфраструктури, що реалізується через спільні з ЄС проєкти з кіберзахисту, такі як PESCO (Постійне структуроване співробітництво). Таким чином, стратегічне партнерство дозволяє Україні використовувати передові технологічні рішення Заходу (зокрема AI-моніторинг контенту), водночас надаючи партнерам унікальні кейси протидії реальним гібридним операціям, що робить український досвід невід'ємною частиною глобальної архітектури інформаційної безпеки [10].

2.3. Взаємодія з Міжнародним союзом електрозв'язку та Радою Європи щодо впровадження стандартів штучного інтелекту.

Взаємодія України з Міжнародним союзом електрозв'язку (МСЕ) та Радою Європи (РЄ) у 2026 році становить фундаментальну основу для розбудови національної правової бази штучного інтелекту (ШІ), що базується на принципах людиноцентричності, безпеки та дотримання прав людини. Співпраця з МСЕ як спеціалізованою установою ООН зосереджена на техніко-технологічному аспекті стандартизації ШІ. Україна активно бере участь у глобальній ініціативі «AI for Good», яка сприяє використанню алгоритмів для досягнення цілей сталого розвитку. Правовий аспект цієї взаємодії реалізується через імплементацію технічних стандартів МСЕ (серія ITU-T), що визначають вимоги до архітектури нейромереж, якості вхідних даних та сумісності систем ШІ з критичною інформаційною інфраструктурою [2]. У межах МСЕ Україна також залучена до розробки глобальних етичних рамок, які мають запобігати використанню ШІ для кібератак на цивільні об'єкти, що є критично важливим в умовах ведення сучасної високотехнологічної війни [5].

На відміну від технічного підходу МСЕ, взаємодія з Радою Європи спрямована на правове забезпечення захисту демократії та фундаментальних свобод від потенційних загроз алгоритмізації. Ключовим інструментом цієї співпраці є імплементація положень Рамкової конвенції Ради Європи про

штучний інтелект, прав людини, демократії та верховенства права (2024 р.), яка стала першим міжнародним юридично обов'язковим договором у цій сфері. Україна як підписант Конвенції зобов'язалася впровадити механізми оцінки ризиків для систем ШІ, що використовуються в державному управлінні, правосудді та правоохоронній діяльності [13]. Це партнерство передбачає створення системи незалежного нагляду за алгоритмічними рішеннями, що дозволяє громадянам оскаржувати упереджені або дискримінаційні вердикти ШІ, забезпечуючи право на «людське втручання» в автоматизовані процеси [4].

Специфіка взаємодії з РЄ також включає адаптацію Рекомендацій Комітету Міністрів Ради Європи щодо ролі ШІ в медіа та сфері правосуддя. У 2026 році українські суди та органи прокуратури почали використовувати елементи «цифрового помічника» на базі ШІ, правовий режим якого був розроблений за методичної підтримки Європейської комісії з питань ефективності правосуддя (CEPEJ). Співпраця з МСЕ та РЄ дозволяє Україні уникнути «правового вакууму» у сфері інновацій, інтегруючи вітчизняний ІТ-сектор у глобальну систему довіри. Доктрина інформаційного права України наголошує, що така дворівнева взаємодія (технічна з МСЕ та ціннісна з РЄ) створює «цифровий щит», який дозволяє впроваджувати найсучасніші технології без ризику порушення конституційних прав громадян та національної безпеки [3]. Таким чином, Україна не лише споживає стандарти, а й стає майданчиком для апробації міжнародних норм у складних умовах, формуючи унікальний кейс відповідального використання ШІ [6].

РОЗДІЛ 3. ПРАВОВІ АСПЕКТИ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ В МІЖНАРОДНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

3.1. Адаптація національного інформаційного законодавства до вимог цифрового права Європейського Союзу (Single Digital Market).

Адаптація національного інформаційного законодавства України до вимог цифрового права Європейського Союзу у 2026 році перейшла від стадії фрагментарного запозичення окремих норм до етапу повної інтеграції у Єдиний цифровий ринок (Single Digital Market). Цей процес є фундаментальною передумовою для вільного руху цифрових послуг, капіталу та даних між Україною та країнами-членами ЄС, що вимагає не лише формального перекладу директив, а й глибокої структурної перебудови правової системи. Центральне місце в цій адаптації посідає імплементація «цифрового пакету» ЄС, який включає Регламент про цифрові послуги (DSA) та Регламент про цифрові ринки (DMA). Правова природа цих актів спрямована на створення безпечного та конкурентного онлайн-середовища, де захист фундаментальних прав користувачів поєднується з жорсткими вимогами до прозорості алгоритмів великих технологічних платформ [4]. Для України це означає модернізацію Закону «Про медіа» та розробку спеціалізованого законодавства про відповідальність провайдерів проміжних послуг, що дозволяє вітчизняним IT-компаніям працювати за єдиними європейськими правилами без додаткових юридичних бар’єрів [3].

Важливим вектором адаптації є гармонізація режиму охорони персональних даних із стандартами GDPR. У 2026 році українське законодавство остаточно закріпило екстеріторіальний принцип захисту приватності та право на портативність даних, що є критичним для транскордонного надання фінансових та медичних послуг. Окрім цього, інтеграція у Single Digital Market передбачає впровадження норм Регламенту

eIDAS, що забезпечує взаємне визнання кваліфікованих електронних довірчих послуг. Це дозволяє українським підприємцям укладати юридично значущі контракти з європейськими партнерами в автоматизованому режимі, використовуючи «Дія.Підпис», що відповідає найвищим стандартам безпеки ЄС [2]. Особлива увага приділяється адаптації до AI Act — першого у світі всеосяжного закону про штучний інтелект, який класифікує системи ШІ за рівнем ризику та встановлює жорсткі вимоги до систем із «високим ризиком», що використовуються в критичній інфраструктурі та державному управлінні [15].

Виклики адаптації в умовах 2026 року пов’язані із необхідністю збереження балансу між жорсткою безпековою політикою України як держави, що перебуває у стані оборони, та ліберальними цінностями вільного інформаційного обміну, притаманними Єдиному цифровому ринку. Доктрина інформаційного права наголошує, що Україна не просто копіює європейські норми, а створює унікальний прецедент «стійкої цифровізації», де висока швидкість впровадження послуг (екосистема «Дія») поєднується із посиленим кіберзахистом [5]. Адаптація до Single Digital Market також включає розвиток законодавства про хмарні послуги та відкриті дані, що сприяє розвитку інноваційного підприємництва та залученню інвестицій у цифрову інфраструктуру. Таким чином, формування сумісного з ЄС цифрового правового простору є не лише вимогою Угоди про асоціацію, а й стратегічним інструментом економічного відновлення та посилення технологічного суверенітету України у глобальному світі [6].

3.2. Міжнародно-правові гарантії захисту критичної інформаційної інфраструктури України в умовах воєнного стану.

Міжнародно-правові гарантії захисту критичної інформаційної інфраструктури (КІІ) України в умовах воєнного стану у 2026 році становлять

унікальну систему, що поєднує класичні норми міжнародного гуманітарного права (МГП) із новітніми стандартами кібербезпеки та колективної цифрової оборони. Правова природа захисту КІІ базується на принципі розрізнення, закріпленому в Додатковому протоколі І до Женевських конвенцій, згідно з яким об’єкти, що забезпечують життєдіяльність цивільного населення (енергомережі, системи водопостачання, державні цифрові реєстри), не можуть бути ціллю атак, включно з кібероперaціями [16]. У сучасній доктрині інформаційного права наголошується, що руйнівний вплив на програмне забезпечення КІІ прирівнюється до кінетичного нападу, якщо його наслідки призводять до фізичного руйнування або загибелі людей, що активує механізми міжнародно-правової відповідальності агресора [3]. Україна в умовах воєнного стану активно використовує Талліннський посібник 3.0 (Tallinn Manual) як авторитетне джерело тлумачення норм міжнародного права стосовно кібервійни, що дозволяє юридично кваліфікувати атаки на КІІ як воєнні злочини [5].

Важливим рівнем гарантій є стратегічне партнерство з НАТО та ЄС, яке трансформувалося з консультативного у прикладний безпековий механізм. Приєднання України до Об’єднаного центру передових технологій з кібероборони НАТО (CCDCOE) та інтеграція в систему PESCO (Permanent Structured Cooperation) створили правове поле для спільного відбиття атак на КІІ в режимі реального часу. Міжнародні гарантії також підкріплюються двосторонніми угодами з безпеки (Security Commitments), укладеними з провідними країнами світу впродовж 2024–2025 років, які окремим пунктом передбачають технологічну допомогу та спільне розслідування кіберінцидентів [4]. Окрім того, Директива ЄС про мережеву та інформаційну безпеку (NIS 2 Directive), норми якої Україна імплементує в національне законодавство, встановлює транскордонні стандарти стійкості, що зобов’язують міжнародних провайдерів хмарних послуг забезпечувати особливий режим захисту українських державних даних, розміщених на їхніх потужностях [17].

[Image showing the interaction between National Defense and International Cyber Law]

Особливе місце в системі гарантій посідає міжнародно-правова атрибуція кібератак — юридичний процес встановлення відповідальності держави-агресора за дії підконтрольних їй хакерських угруповань. Україна спільно з партнерами з Європейського Союзу використовує «Кібердипломатичний інструментарій» (Cyber Diplomacy Toolbox), що дозволяє накладати міжнародні санкції на суб'єктів, причетних до дестабілізації КІІ. У 2026 році доктрина інформаційного права України підкреслює, що захист КІІ виходить за межі суто технічних заходів і стає частиною «цифрового суверенітету», де міжнародні гарантії виступають стримуючим фактором проти ескалації кіберконфлікту [6]. Таким чином, міжнародне право в умовах воєнного стану еволюціонує від пасивних заборон до активних механізмів колективної цифрової стійкості (cyber resilience), що забезпечує безперервність функціонування держави навіть під тиском постійних технологічних загроз [2].

3.3. Перспективи створення глобальної системи цифрової безпеки та місце України у світовій архітектурі інформаційного врядування.

Перспективи створення глобальної системи цифрової безпеки у 2026 році визначаються переходом від фрагментарних національних стратегій до формування цілісної архітектури «колективного кіберзахисту», де ключовим елементом є не лише технічна стійкість, а й міжнародно-правова визначеність дій у цифровому просторі. Глобальна система цифрової безпеки базується на імплементації норм відповідальної поведінки держав, розроблених у межах ООН (GGE та OEWG), та впровадженні механізмів миттєвої атрибуції кібератак. Правова природа цієї системи передбачає створення транскордонних протоколів реагування на інциденти, що загрожують критичній інфраструктурі, та гармонізацію кримінального законодавства щодо кіберзлочинності на базі

оновленої Будапештської конвенції [5]. Основною перспективою розвитку є перехід до моделі «нульової довіри» (Zero Trust) на міждержавному рівні, де безпека гарантується не лише політичними деклараціями, а й автоматизованими системами верифікації інформаційних потоків та спільним використанням штучного інтелекту для виявлення аномалій у мережах [3].

Місце України у світовій архітектурі інформаційного врядування 2026 року є унікальним та визначальним, оскільки держава перетворилася з реципієнта допомоги на «нормативного інноватора» та провідного експерта з протидії гібридним загрозам. Завдяки успішному досвіду функціонування екосистеми «Дія» та стійкості державних реєстрів в умовах повномасштабної війни, Україна пропонує світу модель «цифрової фортеці», де висока швидкість надання послуг поєднується з безпрецедентним рівнем кіберзахисту [4]. Україна активно інтегрована в структури НАТО та ЄС, зокрема через участь у роботі Об’єднаного центру передового досвіду з кібероборони (CCDCOE), де українські кейси лягають в основу нових міжнародних стандартів захисту КІІ. Доктрина інформаційного права України наголошує, що наше місце в глобальному врядуванні визначається здатністю експортувати не лише ІТ-рішення, а й правові моделі захисту цифрового суверенітету в умовах екзистенційних загроз [2].

Майбутнє глобального інформаційного врядування передбачає посилення ролі «цифрової дипломатії» та створення міжнародних судів або арбітражів для вирішення спорів у кіберпросторі. Україна ініціює створення Глобального цифрового щита — ініціативи, що передбачає об'єднання зусиль демократичних країн для захисту від інформаційної агресії та алгоритмічного маніпулювання [6]. Важливим аспектом є участь України у розробці Глобального цифрового договору (Global Digital Compact) під егідою ООН, де вітчизняні фахівці відстоюють принципи прозорості платформ та відповідальності за поширення воєнної пропаганди. Отже, Україна у 2026 році де-факто є лабораторією майбутнього цифрового порядку, де відпрацьовуються правові механізми

захисту демократії від цифрового авторитаризму, що робить її невід'ємним та авторитетним суб'єктом світової архітектури врядування [5].

ВИСНОВКИ

Результатом системного аналізу правових засад та механізмів співробітництва України з міжнародними суб’єктами в інформаційній сфері стали наступні висновки, що відображають сучасну архітектуру міжнародного інформаційного права:

Доведено, що міжнародна інформаційна сфера у 2026 році остаточно трансформувалася у простір глобальної конкуренції, де правове регулювання зміщується від суто технічних стандартів до формування етичних та безпекових норм (цифрова гуманістика). Україна в цій системі координат посідає унікальне місце суб'єкта, який не лише імплементує міжнародні норми, а й виступає донором безпекового досвіду в питаннях протидії гібридним загрозам. Правова природа міжнародної інформаційної сфери сьогодні визначається балансом між принципом суверенітету держави над власним цифровим простором та транскордонним характером сучасних інформаційних потоків.

Встановлено, що стратегічне співробітництво України з ЄС та НАТО вийшло на рівень повної функціональної інтеграції. Адаптація вітчизняного законодавства до стандартів Єдиного цифрового ринку (Digital Single Market) та впровадження норм Акта про цифрові послуги (DSA) дозволили Україні стати частиною європейського правового поля. Взаємодія з Альянсом у межах Об’єднаного центру передових технологій з кібероборони (CCDCOE) забезпечила нормативну базу для захисту критичної інфраструктури, що є визначальним фактором збереження державної стійкості в умовах воєнного стану.

Виявлено, що роль міжнародних організацій (ООН, ЮНЕСКО, РЄ) у регулюванні інформаційної сфери зміщується в бік створення глобальних запобіжників проти зловживання штучним інтелектом та алгоритмами дезінформації. Для України пріоритетним напрямом співпраці з цими інституціями є закріплення на міжнародному рівні юридичної відповідальності

держав за кібератаки та інформаційний тероризм. Концепція «цифрового щита», яку реалізує Україна, потребує подальшої кодифікації у межах нових багатосторонніх договорів під егідою ООН.

Перспективи подальшого співробітництва полягають у переході до моделі «випереджального правового регулювання». Україна має потенціал стати ініціатором створення Міжнародного агентства з цифрової безпеки або аналогічної структури, що координуватиме стандарти захисту даних у реальному часі. Резюмуючи, міжнародне співробітництво в інформаційній сфері для України є не лише інструментом євроінтеграції, а й ключовим правовим механізмом забезпечення національної безпеки та утвердження статусу високотехнологічної держави в новій архітектурі світового ладу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Декларація принципів «Побудова інформаційного суспільства — глобальне завдання у новому тисячолітті» (WSIS). URL: https://www.itu.int/net/wsis/docs/geneva/official/dop.html

2. Арістова І. В. Інформаційне право: підручник. Київ: Юрінком Інтер, 2024. 352 с.

3. Костицький В. В. Теорія інформаційного права: монографія. Київ: Наукова думка, 2023. 280 с.

4. Марущак А. І. Правове регулювання цифрових послуг в умовах євроінтеграції України. Право і суспільство. 2025. № 2. С. 115–122.

5. Бєляков К. І. Міжнародне інформаційне право: навчальний посібник. Київ: КНТ, 2025. 248 с.

6. Кохановська О. В. Цивільно-правові аспекти захисту інформаційних прав в Україні. Київ: Академіка, 2024. 312 с.

7. Статут Організації Об’єднаних Націй : міжнародний документ від 26 червня 1945 р. // Офіційний сайт Організація Об’єднаних Націй.

8. Статут ЮНЕСКО (Конституція ЮНЕСКО) : міжнародний документ від 16 листопада 1945 р. // Офіційний сайт ЮНЕСКО.

9. Рекомендація про етику штучного інтелекту ЮНЕСКО. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381115_ukr

10. Ліпкан В. А. Стратегічні комунікації: словник-довідник. Київ: Магістр-XXI сторіччя, 2024. 456 с.

11. Спільна декларація про співробітництво між ЄС та НАТО. URL: https://www.nato.int/cps/en/natohq/official_texts_210549.htm

12. Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права (CET № 225).

13. Стратегія розвитку штучного інтелекту в Україні до 2030 року [Електронний ресурс] / Міністерство цифрової трансформації України. – Режим доступу: https://thedigital.gov.ua

14. Угода про асоціацію між Україною та Європейським Союзом від 27.06.2014 р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_011

15. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту (Artificial Intelligence Act).

16. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I).

17. Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки в межах Союзу (Директива NIS 2).

18. Глобальний цифровий договір ООН (Global Digital Compact). Проєкт та декларації 2024-2026 рр.

19. Tallinn Manual 3.0 on the International Law Applicable to Cyber Operations (Draft analysis 2025/2026).