14. Skyba, O. (2024). Instytutsiitsna stiikist derzhavy yak faktor yii staloho rozvytku ta ekonomichnoi bezpeky. Stalyi rozvytok ekonomiky, (3(50)), 256–261. https://doi.org/10.32782/2308-1988/2024-50-38

15. Steblianko, A. V., & Lisov, D. A. (2021). Biuro ekonomichnoi bezpeky yak subiekt zabezpechennia ekonomichnoi bezpeky. Nove ukrainske pravo, (6), 187–191. https://doi.org/10.51989/nul.2021.6.28

16. Cherneha, V. (2022). Vplyv podatkovoi polityky na investytsiinyi klimat krainy. Intelekt KhKhI, (3, 2022). https://doi.org/10.32782/2415-8801/2022-3.14

Vladyslav Pustovar,
doctoral student at the Educational and Research Institute of Law and Political Science,
Mykhailo Drahomanov Ukrainian State University

Political Stability as a Key Factor of Economic Security: an Institutional Approach

The article examines the stability and efficiency of the political system as one of the key factors of economic security of the state. In modern conditions, political stability is becoming the basis for the effective functioning of state institutions, making strategically important decisions and ensuring stable economic development. The author emphasizes that the stability of the political system is determined by a number of factors, including institutional stability, political legitimacy, socio-economic conditions, and the impact of external threats. These factors interact with each other, creating a basis for sustainable development and risk reduction.

One of the main aspects of political resilience is institutional stability, which implies the reliable operation of public authorities such as the parliament, government and judiciary. Stable and effective institutions ensure compliance with laws, transparency of decisions, and predictability of political processes, which strengthens citizens' trust in the government. The article notes that institutional stability is an important element in preventing crises that can destabilize the political system and have a negative impact on economic security. Political legitimacy, which is the public recognition of the legitimacy of the government, also plays an important role in ensuring stability. It is noted that public trust in the political system and government reduces the risk of social conflicts, thus contributing to a stable political environment. In addition, the legitimacy of the government largely depends on its ability to respond to the demands of society and ensure the implementation of economic and social programs, which contributes to the strengthening of economic security.

The article also discusses socio-economic factors that have a significant impact on the sustainability of the political system. Economic growth, equitable distribution of resources, and access to basic services such as healthcare and education reduce social tensions and promote political stability. On the other hand, economic crises, high unemployment and social inequality can become catalysts for protests and political unrest that threaten the stability of the state.

Keywords: *political stability, efficiency of the political system, economic security, institutional stability, political legitimacy.*

https://doi.org/10.31392/UDU-nc.series22.2024.36.08
УДК 327:070.1]:17

Олександр Гоманюк,
здобувач за спеціальністю 291 Міжнародні відносини,
суспільні комунікації та регіональні студії,
Волинський національний університет ім. Лесі Українки, м. Луцьк
ORCID: 0009-0001-7635-6519*; e-mail: alex.ua.man@gmail.com*

ПИТАННЯ ЕТИКИ ТА КОНФІДЕНЦІЙНОСТІ У ЦИФРОВИХ МІЖНАРОДНИХ КОМУНІКАЦІЯХ

У статті розглядаються проблеми конфіденційності даних та цифрових прав людини в сучасному глобальному середовищі, де інформаційні потоки перетинають кордони в реальному часі. Автор аналізує основні виклики для захисту персональних даних у міжнародних комунікаціях, звертаючи увагу на різноманітність правових підходів у різних країнах та ризики, пов'язані з обміном особистою інформацією. Поняття конфіденційності визначається як захист особистої інформації від несанкціонованого доступу, особливо в умовах, коли дані можуть бути передані через кордони з різними правовими стандартами. Стаття акцентує увагу на ролі великих корпорацій, таких як Google та Facebook, у збереженні й захисті даних користувачів, зважаючи на можливі загрози витоку або зловживання інформацією. Аналізуються заходи, які приймають держави, зокрема ЄС, для забезпечення захисту даних, проте глобальна природа інтернету створює проблеми у виконанні таких вимог. У контексті цифрових прав людини розглядаються аспекти права на приватність, свободу вираження поглядів, доступ до інформації та захист від цифрового стеження. Автор підкреслює, що ці права тісно пов'язані з базовими правами людини, проте сучасний розвиток технологій створює нові загрози. Зокрема, згадується випадок з Cambridge Analytica, який ілюструє можливість

використання персональних даних для маніпуляції громадською думкою. Порушується питання цифрового розриву, що обмежує доступ до інтернету значній частині населення, особливо у країнах, що розвиваються, і сприяє соціальній нерівності. Окремо розглянуто проблему цифрового стеження та можливість використання технологій, таких як розпізнавання облич, для дискримінації або порушення прав людини, як це відбувається у системі соціального кредиту в Китаї. Стаття також висвітлює питання етичного застосування штучного інтелекту та потребу в міжнародних стандартах для забезпечення прозорості, відповідальності та безпеки у використанні цифрових технологій.

Ключові слова: *конфіденційність, захист персональних даних, етика, цифрові права людини, кібербезпека, штучний інтелект (ШІ).*

Вступ. Дотримання етики та конфіденційності у цифрових міжнародних комунікаціях є ключовим аспектом із багатьох причин. Порушення етичних норм і приватності може значно нашкодити репутації та іміджу учасників комунікації, їх організацій. У багатьох країнах існують закони, що регулюють збереження конфіденційності та етичні норми в інтернет-комунікаціях. Порушення цих законів може мати юридичні наслідки. Цифрові комунікації часто передбачають обмін особистою інформацією. Збереження конфіденційності допомагає захистити особисті дані від несанкціонованого доступу та зловживань. Дотримання етичних норм сприяє підтримці професійної етики та створює здорове середовище для співпраці, довіри, що є критичним у бізнесі, політиці та міжнародних відносинах. Незаконне використання інформації, яка була отримана шляхом порушення конфіденційності, може призвести до кіберзлочинності, такої як шахрайство, крадіжка особистих даних тощо. Дотримання етики та конфіденційності є основними принципами в сучасних цифрових комунікаціях, сприяючи безпеці, довірі та ефективності у міжнародних взаємодіях. Сучасний світ, у якому цифрові технології відіграють вирішальну роль у міжнародних комунікаціях, стикається усе частіше з новими викликами в питаннях етики та конфіденційності. Інформаційні технології стали основою для міжнародної торгівлі, дипломатії, освітніх і культурних обмінів, але з цим зростають ризики щодо збереження конфіденційності даних, використання технологій в етичних межах і захисту прав людини в онлайн-середовищі. Розглянемо основні аспекти цих викликів, їх вплив на міжнародні комунікації.

Аналіз останніх досліджень і публікацій. Питання етики та конфіденційності у цифрових міжнародних комунікаціях досліджують багато науковців з різних галузей, зокрема з права, інформаційної безпеки, політології, етики та соціальних наук. Філософ, один із провідних дослідників етики інформаційних технологій, відомий роботами у сфері інформаційної етики та цифрової конфіденційності Л. Флоріді досліджує проблеми приватності, етики цифрових даних, вплив інформаційних технологій на суспільство (Floridi, 2014, Floridi, 2019, Floridi, 2023). Соціолог, авторка книги «*Епоха спостережницького капіталізму»* (*«The Age of Surveillance Capitalism»*) Ш. Зубофф аналізує, як великі технологічні компанії збирають і використовують персональні дані, в т.ч. етичні виклики, пов'язані з цим процесом (Zuboff, 2019). Дослідниця у галузі етики та технологій, яка працює над питаннями конфіденційності та безпеки у цифровому світі, Г. Ніссенбаум розробила концепцію *«контекстуальної доброчесності» («contextual integrity»*), що акцентує: захист конфіденційності залежить від того, в якому контексті використовується інформація (Nissenbaum, 2009; Brunton, Nissenbaum, 2015). Експерт у сфері конфіденційності, засновник Центру інформаційної приватності (Center for Information Privacy) М. Ротенберг займався питаннями регулювання та прав на приватність у цифровому світі (Rotenberg, 2006 Rotenberg 2007, Rotenberg 2010, Rotenberg 2020). Науковець в галузі комп'ютерної етики Д. Джонсон досліджує етичні питання, пов'язані з комп'ютерними системами та конфіденційністю. Вона фокусується на тому, як технологічні зміни впливають на особисті права і свободи (Johnson, 2020; Johnson, 2021). Засновник руху вільного програмного забезпечення Р. Столлман також піднімає питання конфіденційності та етики у цифрових комунікаціях, зокрема щодо прав користувачів на контроль над своїми даними (Stallman, 2023).

Українські науковці досліджують digital етикет і комунікації, їхній розвиток і сучасні тенденції, зокрема аналізується природа та функції digital етикету як форми поведінкової культури у віртуальному просторі, а також як одного зі способів реалізації особистої свободи

самовираження з повагою до інтересів інших (Андрійченко, Близнюк, Майстренко, 2021). Предметне поле для таких досліджень у рамках сучасних політичних наук розвивають напрацювання щодо інформаційно-аналітичної діяльності як частини політичної культури та міжнародної безпекової політики (Шуляк, 2020), стосовно політико-правового врегулювання суспільних відносин під час використання інформаційних і комунікативних можливостей інтернет-мережі (Шайгородський, 2022), з питань сучасних викликів застосування штучного інтелекту в політичному житті та публічному управління (Cholyshkina, Karnaukh, Volianiuk, 2024). Викликає інтерес і дослідження щодо ведення зовнішньополітичної діяльності з використанням новітніх технологій на просторах Всесвітньої мережі Інтернет. Автори зазначають, що вплив комунікаційних процесів на міжнародній арені та розвиток інформаційно-комунікаційних технологій в політичній сфері, котрі призвели до необхідності використання оновлених засобів ведення зовнішньої політики, є обґрунтованими (Шелемба, Симчера, 2020). В Україні досліджують і роль цифрової дипломатії в контексті публічної дипломатії, а також її значення в політичній діяльності; підкреслюють, що сучасне суспільство неможливо уявити без соціальних мереж як обміну інформацією та обговорення актуальних тем. Для більшості людей користування соціальними мережами є звичним явищем, а для дипломатів, політиків це не лише засіб спілкування з широкою аудиторією, але й можливість зрозуміти суспільні настрої в країні їхнього перебування. Цифровий простір дозволяє відстежувати реакцію громадськості на дії влади та використовувати його для впливу на громадську думку, формування позитивного іміджу своєї країни за кордоном (Мірошниченко, Федорова, 2022). Ці дослідники зробили вагомий внесок у розвиток розуміння етичних і конфіденційних аспектів цифрових комунікацій на глобальному рівні, але питання етики та конфіденційності у цифрових міжнародних комунікаціях в Україні є мало дослідженим, тому вважаємо цю тему актуальною для наукової розвідки.

Метою дослідження є вивчення інструментів захисту персональних даних у цифрових комунікаціях на міжнародному рівні, зокрема в умовах різних юридичних та етичних стандартів між країнами. Це оцінка впливу різних міжнародних законів і регуляцій, таких як GDPR (General Data Protection Regulation), на захист даних; аналіз загроз для конфіденційності користувачів у глобальному цифровому середовищі; аналіз етичних стандартів для забезпечення захисту конфіденційності та цифрових прав у міжнародних комунікаціях; дослідження впливу штучного інтелекту та автоматизованих систем на персональні дані та конфіденційність користувачів.

Методи дослідження, які використані для вивчення конфіденційності та етичних питань в міжнародних цифрових комунікаціях: контент-аналіз – вивчення наявних міжнародних законів, правил і політик щодо конфіденційності даних (наприклад, GDPR); аналіз контенту соціальних медіа, щоб визначити, як особиста інформація використовується або передається; порівняння міжнародних правових рамок у різних країнах, таких як ЄС, США, Китай, щоб зрозуміти різницю у законодавчому підході до конфіденційності даних; кейс-стаді – вивчення конкретних випадків порушення конфіденційності або використання даних, як у випадку Cambridge Analytica, для детального аналізу наслідків і виявлення вразливостей у системах захисту; порівняльний аналіз – порівняння політик конфіденційності у різних країнах, щоб зрозуміти, як відмінності в культурах і правових нормах впливають на захист особистих даних.

Результати та дискусії. У світі, де обмін інформацією між країнами відбувається в реальному часі, зберігання й захист персональних даних стають важливими питаннями. Кожна цифрова взаємодія – від реєстрації у соціальних мережах до міжнародних транзакцій – передбачає збирання великої кількості особистої інформації. Проблема конфіденційності загострюється у міжнародних комунікаціях, адже дані користувачів можуть бути передані через кордони, де закони щодо захисту конфіденційної інформації можуть відрізнятися.

Конфіденційність – це принцип, який передбачає захист особистої інформації від несанкціонованого доступу або розголошення. Вона охоплює збереження та захист даних, які можуть бути приватними або чутливими, щоб вони не потрапили до сторонніх осіб або

організацій без згоди власника. Конфіденційність важлива у багатьох сферах, зокрема в політичній, медичній, юридичній, бізнесовій, цифровій. У контексті цифрових комунікацій конфіденційність означає захист персональних даних користувачів інтернету, які можуть бути зібрані, передані або використані третіми сторонами. Це також передбачає забезпечення того, що тільки уповноважені особи мають доступ до таких даних, і що вони не будуть використані для шкідливих цілей без відома та згоди користувача (Bukaty, 2019).

Міжнародні корпорації, такі як Google, Facebook або Amazon, мають доступ до особистих даних мільярдів людей, що створює ризики неправомірного використання інформації або витоку даних. Багато держав приймають закони для регулювання цього питання, наприклад, Європейський Союз встановлює суворі правила щодо обробки персональних даних. Однак глобальна природа інтернету означає, що зобов'язання щодо конфіденційності часто не збігаються між країнами, створюючи ризики для користувачів.

Збираючи дані, організації повинні діяти відповідно до етичних стандартів. Прозорість і згода користувачів на збір інформації є центральними принципами етичного використання даних. У міжнародних комунікаціях це питання ускладнюється через різницю в культурних і юридичних стандартах. Що є прийнятним з етичної точки зору в одній країні, може бути неприпустимим в іншій. Це важливе питання: як створити універсальні етичні стандарти для захисту конфіденційності в глобальному цифровому середовищі (Бем, Городиський, 2021).

В епоху стрімкого розвитку цифрових технологій, коли інформаційні потоки перетинають кордони в реальному часі, виникає необхідність переосмислення традиційних прав людини в новому контексті. Поняття цифрових прав людини охоплює право на приватність, свободу вираження поглядів, доступ до інформації, а також захист від дискримінації та цифрового стеження. Ці права стають невід'ємною частиною демократичного суспільства, де технології впливають на кожен аспект життя людини.

Цифрові права мають тісний зв'язок з базовими правами людини, що закріплені у міжнародних документах, таких як Загальна декларація прав людини ООН або Європейська конвенція з прав людини. Проте розвиток інтернету, соціальних мереж і технологій штучного інтелекту створив нові загрози для цих прав. Термін «цифрові права» був запроваджений для того, щоб позначити специфічні права, які пов'язані з використанням інтернету та цифрових технологій. Це право на конфіденційність, свободу слова, право на доступ до інформації, а також захист від цензури та контролю з боку урядів або корпорацій.

Одним із центральних питань цифрових прав є право на приватність**.** У цифровому світі люди щоденно передають величезні обсяги персональних даних – від пошукових запитів до фінансових транзакцій. Ці дані можуть бути використані корпораціями для цілей таргетованої реклами або політичних кампаній, як це сталося у справі Cambridge Analytica, коли дані мільйонів користувачів Facebook використовувалися для маніпуляції виборами. Приватність також стає об'єктом порушення з боку держав. Наприклад, у деяких країнах активно використовуються технології для стеження за громадянами та збору особистої інформації без їхньої згоди. Це викликає занепокоєння у світової спільноти, адже така практика може призводити до порушення основоположних прав людини. Захист приватності вимагає прийняття міжнародних законів, які гарантують збереження конфіденційної інформації та забороняють її несанкціоноване використання. Одним із прикладів такого регулювання є GDPR – загальноєвропейський закон про захист даних, який встановлює високі стандарти конфіденційності (Kuner, Bygrave, Docksey, Dreschler, 2020; Ukrow, 2018).

Свобода вираження поглядів є фундаментальним правом людини, яке має новий вимір у цифрову епоху. Соціальні мережі, блоги та інші онлайн-платформи дозволяють вільно висловлювати думку, обмінюватися інформацією з великою аудиторією. Проте це право часто обмежується цензурою або контролем над інформаційними потоками з боку урядів або компаній. У деяких країнах свобода слова в інтернеті жорстко контролюється, а доступ до певних вебсайтів блокується, що ставить під загрозу демократичні принципи. Наприклад, Китай активно використовує систему «Великого китайського фаєрвола», яка обмежує доступ до багатьох західних сайтів, зокрема й Google та Facebook. Такі дії викликають міжнародні

суперечки щодо порушення цифрових прав громадян (Нагнічук, 2015). Великий китайський фаєрвол (Great Firewall of China) – це комплексна система інтернет-цензури та контролю, яку застосовує уряд Китаю для обмеження доступу до певних вебсайтів і сервісів за межами країни, а також для моніторингу інтернет-активності користувачів. Офіційно це частина більшої ініціативи під назвою «Золотий щит» (Golden Shield Project), яка спрямована на захист національної безпеки та забезпечення соціальної стабільності. Окрім того, зростає загроза дезінформації та маніпуляцій у цифрових середовищах. Поширення фейкових новин, дезінформаційних кампаній і маніпулятивних алгоритмів впливає на громадську думку, підриває демократичні процеси та створює нерівні умови для користувачів.

У сучасному світі інтернет стає не просто інструментом комунікації, а й важливим фактором для соціальної, економічної та політичної участі. Тому право на доступ до інтернету розглядається як важлива частина цифрових прав людини. Організація Об'єднаних Націй у своїх резолюціях визнає доступ до інтернету одним із основних прав, адже воно дозволяє людям отримувати інформацію, навчатися, вести бізнес і брати участь у громадському житті. Однак у світі досі існує значний розрив у доступі до інтернету між різними країнами та соціальними групами. Більше ніж 40% населення планети не мають доступу до глобальної мережі, що обмежує їхні можливості для розвитку та соціальної інтеграції. Цей цифровий розрив може стати джерелом нових форм нерівності та дискримінації (Гронь, Погореленко, 2018).

Одним із найсерйозніших порушень цифрових прав є цифрове стеження**.** Уряди та компанії можуть використовувати цифрові технології для відстеження поведінки громадян в інтернеті, зокрема пошукові запити, місцезнаходження, комунікації. Це викликає серйозні побоювання щодо порушення прав людини та вторгнення в приватне життя. Такі технології як розпізнавання облич, обробка великих обсягів даних можуть використовуватися для дискримінації та порушення прав. Наприклад, в Китаї активно використовується система соціального кредиту, де поведінка громадян оцінюється за допомогою цифрових алгоритмів, що можуть впливати на доступ до послуг, кредитів або навіть пересування (Сопілко, 2013).

На міжнародному рівні питання захисту цифрових прав стають дедалі важливішими. Організації як ООН, Європейський Союз та громадські ініціативи активно працюють над розробкою стандартів і законодавства для забезпечення захисту прав людини в цифровому просторі. Проте цифрові права залишаються предметом постійних дебатів, оскільки технології продовжують розвиватися. Важливим кроком до захисту прав людини в інтернеті є розвиток глобальної правової бази та механізмів захисту, що забезпечують прозорість, відповідальність та етичне використання цифрових технологій (Кравчук, 2013).

Серед викликів у сфері конфіденційності відсутність універсального міжнародного законодавства з регулювання захисту даних у глобальних комунікаціях. У різних країнах існують різні правові підходи до конфіденційної інформації, це може створювати проблеми для багатонаціональних компаній і користувачів. Наприклад, вимоги ЄС (GDPR) можуть бути зовсім іншими, ніж законодавство у США або Китаї. Необхідна глобальна співпраця, яка б сприяла гармонізації правових стандартів. Міжнародні організації, як ООН або ЄС, повинні відігравати активну роль у розробці загальних стандартів конфіденційності, щоб забезпечити надійніший захист даних у глобальному масштабі.

Важливою складовою сучасних цифрових комунікацій є використання штучного інтелекту. ШІ дозволяє обробляти величезні обсяги даних і приймати автоматизовані рішення, що може сприяти прискоренню міжнародної комунікації та обміну інформацією. Проте використання ШІ також ставить серйозні етичні питання. Насамперед, мова йде про прозорість алгоритмів та їхню справедливість. Як ШІ обробляє інформацію і чи не порушує він права людини під час прийняття рішень? Наприклад, використання ШІ для прогнозування поведінки користувачів або для автоматизації процесів у дипломатії може призвести до необ'єктивних висновків або навіть до політичних маніпуляцій.

Штучний інтелект – це галузь комп'ютерної науки, яка займається створенням машин і програм, здатних виконувати завдання, що зазвичай вимагають людського інтелекту. Це

навчання, розпізнавання мови, візуальне сприйняття, прийняття рішень, розв'язання проблем. Основною метою ШІ є моделювання та автоматизація інтелектуальних процесів (аналітика, розуміння контексту, планування, навіть креативність). Існує кілька підходів до ШІ: слабкий ШІ (або вузький ШІ) – спеціалізується на виконанні одного завдання, наприклад, розпізнаванні зображень або голосу; сильний ШІ – це система, яка здатна до універсальної інтелектуальної діяльності, подібної до людського мислення. Ці системи могли б виконувати будь-яке завдання, яке здатна виконати людина. ШІ активно застосовується в різних сферах: охороні здоров'я, фінансах, транспорті, маркетингу, освіті та інших (Нагнічук, 2015).

Основною темою застосування штучного інтелекту є питання етики, довіри та надійності, що відображено в основних документах ЄС, таких як Recommendation of the Council on Artificial Intelligence (OECD) (OECD, 2019) та Ethics Guidelines for Trustworthy AI (High-Level Expert, 2019a; High-Level Expert, 2019b). Такий підхід сприяє формуванню ключових принципів, які мають пріоритетне значення для всіх міжнародних і національних нормативно-правових документів, а також документів, що стосуються прав людини, захисту споживачів, персональних даних, інтелектуальної власності, відповідального бізнесу та конкуренції. Згідно з Recommendation of the Council on Artificial Intelligence (OECD, 2019) відповідальне управління надійним ШІ має базуватися на таких ключових принципах:

- інклюзивне зростання, сталий розвиток і добробут (підтримка людського потенціалу та креативності, залучення недостатньо представлених груп населення, зменшення соціальної, економічної та гендерної нерівності, а також захист природного середовища);
- людиноцентричні цінності та справедливість (дотримання верховенства права, прав людини, демократичних цінностей, в т.ч. свободу, гідність, рівність, конфіденційність та недискримінацію);
- прозорість та зрозумілість (надання достатньої інформації для розуміння систем ШІ, зокрема щодо взаємодії з ними, можливості оскарження результатів, отриманих від ШІ);
- надійність, безпека та захист (забезпечення безпечного функціонування систем ШІ, управління ризиками протягом усього їх життєвого циклу, включаючи захист даних та конфіденційність);
- відповідальність і підзвітність (користувачі ШІ повинні нести відповідальність за дотримання цих принципів) (Драч, Петроє, Бородієнко, та ін., 2023).

Одним із викликів для забезпечення етики і конфіденційності в міжнародних цифрових комунікаціях є необхідність глобальної співпраці. Окремі країни можуть мати свої власні закони та стандарти, але вони не завжди узгоджуються з глобальними вимогами. Необхідність міжнародних угод і регуляторних механізмів є ключовим елементом для створення безпечного й етичного цифрового простору. Міжнародні форуми, такі як G7, G20, ООН, ЄС, стають платформами для обговорення цих питань і розробки міжнародних норм, які забезпечують конфіденційність й етичні стандарти у цифрових комунікаціях.

Глобальна співпраця та регулювання штучного інтелекту стали ключовими питаннями через стрімкий розвиток технологій, що змінюють різні аспекти життя – від економіки до національної безпеки. ШІ пропонує великі можливості для покращення людського добробуту, але водночас несе значні ризики, зокрема пов'язані з конфіденційністю, етикою, безпекою та нерівністю. Тому міжнародна співпраця і регулювання стають важливими для забезпечення збалансованого використання цих технологій. Глобальна природа ШІ вимагає міжнародної координації та об'єднання зусиль для вирішення викликів, які виходять за межі окремих країн. Технології ШІ розробляються та використовуються по всьому світу, і їх вплив на суспільство може бути транснаціональним. Наприклад, алгоритми для обробки даних або автоматизації можуть бути розроблені в одній країні, але використовуватися в іншій, створюючи нові загрози для прав людини, безпеки, економічної стабільності. Спільні виклики, які вимагають міжнародної співпраці:

- захист конфіденційності та персональних даних;
- протидія дезінформації та маніпуляціям у політичній та соціальній сферах;
- забезпечення етичного використання ШІ у сфері працевлаштування та освіти;

– управління ризиками, пов'язаними з автономними системами (наприклад, військовими роботами чи автомобілями).

Ефективне регулювання ШІ вимагає встановлення міжнародних стандартів і норм для захисту прав людини, а також забезпечення прозорості та відповідальності технологій. Низка країн і міжнародних організацій уже роблять кроки в цьому напрямку. Європейський Союз став одним із піонерів у розробці законодавства щодо ШІ. Пропонований Акт про штучний інтелект (AI Act) ставить собі за мету регулювати використання високоризикових ШІ систем, зокрема в сферах охорони здоров'я, транспорту, правосуддя. Цей акт про вимоги до прозорості алгоритмів, відповідальності за помилки і дотримання етичних стандартів. У ЮНЕСКО приділяють увагу розробкам рекомендацій і міжнародних стандартів етичного використання ШІ. У 2021 році ЮНЕСКО ухвалила перший глобальний документ – Рекомендації з етичного використання ШІ, де закладені принципи, що мають на меті зменшити ризики, пов'язані з дискримінацією та порушенням прав людини. G7 та G20 обговорюють розробку глобальних принципів і підходів до регулювання ШІ. Вони закликають до підвищення прозорості, етичної відповідальності та розвитку інклюзивних ШІ технологій, щоб не допускати цифрової нерівності.

Сучасні підходи до регулювання ШІ ґрунтуються на кількох принципах:

– Прозорість – ШІ системи мають бути доступними для аналізу. Користувачі повинні знати, як алгоритми приймають рішення, мати можливість оскаржувати результати.

– Безпека – технології ШІ повинні бути перевірені і нести відповідальність за можливі помилки чи збої. Це особливо актуально для медичних і автономних систем.

– Етичність – використання ШІ має відповідати етичним нормам, щоб уникнути дискримінації, расизму, гендерної нерівності або упередженості в алгоритмах.

– Захист персональних даних – ШІ системи, які збирають і обробляють персональні дані, повинні діяти відповідно до законів про захист інформації, таких як GDPR у Європі.

– Відповідальність – розробники та користувачі ШІ мають нести відповідальність за наслідки використання цих систем. Негативні наслідки повинні бути компенсовані, а технології мають перевірятися на можливі ризики перед впровадженням.

Попри прогрес у регулюванні ШІ, існують значні виклики, пов’язані з узгодженням підходів між різними країнами та організаціями. Одним із таких викликів є національні інтереси та конкуренція. Різні країни, зокрема США та Китай, розвивають ШІ з різними пріоритетами. Це може призводити до того, що міжнародної угоди щодо регулювання ШІ важко досягти через економічні та геополітичні протиріччя. Викликом є і постійний розвиток технологій. Оскільки ШІ швидко еволюціонує, законодавство часто не встигає за цими змінами. Це вимагає більш динамічних механізмів регулювання та міжнародного моніторингу. У майбутньому глобальна співпраця у регулюванні ШІ стане ще необхіднішою. Розвиток штучного інтелекту надає великі можливості для покращення життя людей, але ці можливості потрібно реалізовувати етично та відповідально. Потрібен активний діалог між урядами, приватними компаніями, науковими установами та громадськістю, щоб розробити загальноприйняті стандарти та принципи, які забезпечуватимуть використання ШІ.

Висновки. Цифрові міжнародні комунікації відкривають великі можливості для розвитку глобальних зв'язків, обміну інформацією та співпраці. Проте разом з цими перевагами постають серйозні виклики в сфері етики та конфіденційності. Важливість захисту персональних даних, забезпечення етичного використання інформаційних технологій і глобальна співпраця у питаннях регулювання цифрового простору стають основними завданнями сучасного суспільства. Право на приватність і захист даних є важливою частиною сучасних прав людини. В ООН, Європейському Союзі та багатьох інших міжнародних організаціях дедалі більше уваги приділяється цифровим правам, зокрема праву на захист персональних даних, свободу слова та доступ до інформації. З одного боку, цифрові технології надають нові можливості для вираження думок і доступу до знань. З іншого боку, ці ж технології можуть використовуватися для порушення прав людини, наприклад, через державне стеження, цензуру або контроль над інформаційними

потоками. Використання технологій для стеження за громадянами в деяких країнах ставить під загрозу фундаментальні права людини, що створює напругу в міжнародних відносинах. Глобальна співпраця та регулювання штучного інтелекту є вирішальними для мінімізації ризиків і максимізації вигод від використання цієї технології. Міжнародні організації та національні уряди повинні спільно працювати над розробкою ефективних і гнучких правових механізмів, які будуть враховувати як етичні питання, так і технічні виклики, що виникають із розвитком ШІ. Тільки через співпрацю та обмін досвідом можна забезпечити, щоб штучний інтелект служив на благо всього людства, а не тільки окремих інтересів.

Використані джерела:

1. Bennett, C. J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United State Itaca, NY : Cornell University Press.
2. Brunton, F., Nissenbaum, H. (2015). Obfuscation: A User's Guide for Privacy and Protest. Cambridge, MA: MIT Press.
3. Bukaty, P. (2019). The California Consumer Privacy Act (CCPA) : an implementation guide. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing.
4. Cholyshkina, O, Karnaukh, A, Volianiuk, O, Ostapenko, M, Holishevska, A. (2024). Public participation and innovative technologies: the role of artificial intelligence in public administration and sustainable development. Salud, Ciencia y Tecnología - Serie de Conferencias [Internet]. 30 [cited 2024 Aug. 12]; 3:974. Available from: https://conferencias.saludcyt.ar/index.php/sctconf/article/view/974
5. Finlyson, D., Moore M., (2019). Data protection in legal practice : the Infolegal guide to GDPR and the Data Protection Act 2018. London: Infolegal.
6. Floridi, L. (2019). The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford University Press . https://doi.org/10.1093/oso/9780198833635.001.0001
7. Floridi, L. (2023). The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford University Press. https://doi.org/10.1093/oso/9780198883098.001.0001
8. Floridi, L. (2014). The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press.
9. High-Level Expert Group on Artificial Intelligence. (2019a, April 8). A definition f AI: Main capabilities and scientific disciplines. European Commission. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines
10. High-Level Expert Group on Artificial Intelligence. (2019b, April 8). Ethics guidelines for trustworthy AI. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
11. Johnson, D. G. (2020), Engineering Ethics: Contemporary and Eduring Debates, Yale University Press, New Haven and London. ISBN: 978-0-300-20924-2
12. Johnson, D. G. (2021). Computer ethics. Upper Saddle River, NJ: Prentice Hall.
13. Kuner, C., Bygrave L.A., Docksey, C.A., Dreschler L. (2020). The EU General Data Protection Regulation (GDPR): a commentary. Oxford: Oxford University Press.
14. Nissenbaum, H.(2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.
15. OECD. (2019, May 22). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
16. Rotenberg M. (2006). Privacy and Human Rights: An International Survey of Privacy Laws and Developments. EPIC.
17. Rotenberg, M. (2007). Information Privacy Law. Aspen Publishing.
18. Rotenberg, M. (2010). Litigation Under the Federal Open Government Laws. EPIC.
19. Rotenberg, M. (2020). Other books include The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments. EPIC.
20. Stallman, R. (2023). GNU C Language Introduction and Reference Manual. GNU.
21. Ukrow, J. (2018). Practitioner's Corner · Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108. European data protection law review. Vol. 4, No. 2. Pp. 239–247.
22. Zuboff, Sh. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books. p. 22. ISBN 978-1-78125-685-5.
23. Андрійченко, Ж., Близнюк, Т., Майстренко, О. (2021). Digital етикет та комунікації: тенденції та вимоги сьогодення. *Економіка та суспільство*, (34). https://doi.org/10.32782/2524-0072/2021-34-24.
24. Бем, М., Городиський І. (2021). Захист персональних даних: правове регулювання та практичні аспекти : науково-практичний посібник. Захист персональних даних: правове регулювання та практичні аспекти (coe.int)
25. Гронь, О., Погореленко А. (2018). Проблеми захисту персональних даних у контексті сучасної комунікації. Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство. Вип. 19(1). С. 102–108.

26. Драч, І., Петроє, О., Бородієнко, О., Регейло, І., Базелюк, О., Базелюк, Н., Слободянюк, О. (2023). Використання штучного інтелекту у вищій освіті. *International Scientific Journal of Universities and Leadership*, (15), 66-82. https://doi.org/10.31874/2520-6702-2023-15-66-82

27. Кравчук, М. М. (2013). Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. Наукові записки Інституту законодавства Верховної Ради України. № 3. С. 123–126.

28. Мірошниченко, Т., & Федорова, Г. (2022). Цифрова дипломатія як сучасний комунікаційний інструмент міжнародних відносин. *Науково-теоретичний альманах Грані*, 24(12), 58-65. https://doi.org/10.15421/1721119

29. Нагнічук, О. І. (2015). Співвідношення права на свободу вираження щодо публічних осіб та права на повагу до приватного та сімейного життя публічних осіб у практиці Європейського суду з прав людини. Наукові записки НаУКМА. Юридичні науки. Т. 168. С. 72–77

30. Сопілко, І. М. (2013). Генезис змісту категорії «персональні дані». Юридичний вісник. Повітряне і космічне право. № 4. С. 62–66.

31. Шайгородський, Ю. (2022). Масмедіа як суспільно-політичний інститут: структура і функції. *Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін*, *22*(31), 26–34. https://doi.org/10.31392/NPU-nc.series22.2022.31.03

32. Шелемба, М. та Симчера, М. (2020). Цифрові комунікації та тренди в Україні: напрацювання, виклики та можливості. *Політукус,* 6, 104-109. https://doi.org/10.24195/2414- 9616.2020-6.17

33. Шуляк, А., (2020). Інформаційно-аналітична діяльність у міжнародних відносинах: навч. посіб. 2-е вид., перероб. і доп. Луцьк : Вежа-друк. 274 с.

References:

1. Bennett, C. J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United State Itaca, NY : Cornell University Press.

2. Brunton, F., Nissenbaum, H. (2015). Obfuscation: A User's Guide for Privacy and Protest. Cambridge, MA: MIT Press. ISBN 9780262029735.

3. Bukaty, P. (2019). The California Consumer Privacy Act (CCPA): an implementation guide. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing.

4. Cholyshkina, O, Karnaukh, A, Volianiuk, O, Ostapenko, M, Holishevska, A. (2024). Public participation and innovative technologies: the role of artificial intelligence in public administration and sustainable development. Salud, Ciencia y Tecnología - Serie de Conferencias [Internet]. 30 [cited 2024 Aug. 12]; 3:974. Available from: https://conferencias.saludcyt.ar/index.php/sctconf/article/view/974

5. Finlyson, D., Moore M. (2019). Data protection in legal practice : the Infolegal guide to GDPR and the Data Protection Act 2018. London: Infolegal.

6. Floridi, L. (2019). The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford University Press. URL: https://doi.org/10.1093/oso/9780198833635.001.0001

7. Floridi, L. (2023). The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford University Press. URL: https://doi.org/10.1093/oso/9780198883098.001.0001

8. Floridi, L. (2014). The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press.

9. High-Level Expert Group on Artificial Intelligence. (2019a, April 8). A definition f AI: Main capabilities and scientific disciplines. European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

10. High-Level Expert Group on Artificial Intelligence. (2019b, April 8). Ethics guidelines for trustworthy AI. European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

11. Johnson, D. G. (2020), Engineering Ethics: Contemporary and Eduring Debates, Yale University Press, New Haven and London. ISBN: 978-0-300-20924-2

12. Johnson, D. G. (2021). Computer ethics. Upper Saddle River, NJ: Prentice Hall.

13. Kuner, C., Bygrave, L.A., Docksey, C.A., Dreschler, L. (2020). The EU General Data Protection Regulation (GDPR): a commentary. Oxford: Oxford University Press.

14. Nissenbaum, H.(2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press. ISBN 9780804772891.

15. OECD. (2019, May 22). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

16. Rotenberg, M. (2006). Privacy and Human Rights: An International Survey of Privacy Laws and Developments. EPIC.

17. Rotenberg, M. (2007). Information Privacy Law. Aspen Publishing.

18. Rotenberg, M. (2010). Litigation Under the Federal Open Government Laws. EPIC.

19. Rotenberg, M. (2020). Other books include The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments. EPIC.

20. Stallman, R. (2023). GNU C Language Introduction and Reference Manual. GNU.

21. Ukrow, J. (2018). Practitioner's Corner · Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108. European data protection law review. Vol. 4, No. 2. Pp. 239–247.

22. Zuboff, Sh. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books. p. 22. ISBN 978-1-78125-685-5.

23. Andriichenko, Zh., Blyzniuk, T., Maistrenko, O. (2021). Digital etyket ta komunikatsii: tendentsii ta vymohy sohodennia [Digital etiquette and communications: Trends and demands of today]. Ekonomika ta suspilstvo, (34). https://doi.org/10.32782/2524-0072/2021-34-24.

24. Bem, M., Horodyskyi I. (2021). Zakhyst personalnykh danykh: pravove rehuliuvannia ta praktychni aspekty: naukovo-praktychnyi posibnyk [*Protection of Personal Data: Legal Regulation and Practical Aspects: Scientific and Practical Guide*]. Zakhyst personalnykh danykh: pravove rehuliuvannia ta praktychni aspekty (coe.int)

25. Hron, O., Pohorelenko, A. (2018). Problemy zakhystu personalnykh danykh u konteksti suchasnoi komunikatsii [*Issues of Personal Data Protection in the Context of Modern Communication*]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia : Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo. Vyp. 19(1). S. 102–108.

26. Drach, I., Petroie, O., Borodiienko, O., Reheilo, I., Bazeliuk, O., Bazeliuk, N., Slobodianiuk, O. (2023). Vykorystannia shtuchnoho intelektu u vyshchii osviti [*The Use of Artificial Intelligence in Higher Education*]. International Scientific Journal of Universities and Leadership, (15), 66-82. URL: https://doi.org/10.31874/2520-6702-2023-15-66-82

27. Kravchuk, M. M. (2013). Mizhnarodnyi dosvid pravovoho rehuliuvannia zakhystu personalnykh danykh v merezhi Internet [*International Experience in Legal Regulation of Personal Data Protection on the Internet*]. Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy. № 3. S. 123–126.

28. Miroshnychenko, T., & Fedorova, H. (2022). Tsyfrova dyplomatiia yak suchasnyi komunikatsiinyi instrument mizhnarodnykh vidnosyn [Digital diplomacy as a modern communication tool in international relations]. Naukovo-teoretychnyi almanakh Hrani, 24(12), 58-65. https://doi.org/10.15421/1721119

29. Nahnichuk, O. I. (2015). Spivvidnoshennia prava na svobodu vyrazhennia shchodo publichnykh osib ta prava na povahu do pryvatnoho ta simeinoho zhyttia publichnykh osib u praktytsi Yevropeiskoho cudu z prav liudyny [*Correlation between the Right to Freedom of Expression Regarding Public Figures and the Right to Respect for Private and Family Life of Public Figures in the Case Law of the European Court of Human Rights*. *Scientific Notes of NaUKMA*]. Naukovi zapysky NaUKMA. Yurydychni nauky. T. 168. S. 72–77

30. Sopilko, I. M. (2013). Henezys zmistu katehorii «personalni dani» [*Genesis of the Content of the "Personal Data" Category*]. Yurydychnyi visnyk. Povitriane i kosmichne pravo. № 4. S. 62–66.

31. Shaigorodskyi, Yu. (2022). Masmedia yak suspilno-politychnyi instytut: struktura i funktsii. Naukovyi chasopys UDU imeni Mykhaila Dragomanova. Seriia 22. Politychni nauky ta metodyka vykladannia sotsialno-politychnykh dystsyplin, 22(31), 26–34. https://doi.org/10.31392/NPU-nc.series22.2022.31.03

32. Shelemba, M. ta Symchera, M. (2020). Tsyfrovi komunikatsii ta trendy v Ukraini: napratsiuvannia, vyklyky ta mozhlyvosti [Digital communications and trends in Ukraine: Developments, challenges, and opportunities]. Politukus, 6, 104-109. https://doi.org/10.24195/2414- 9616.2020-6.17

33. Shuliak, A. (2020). Informatsiino-analitychna diialnist u mizhnarodnykh vidnosynakh: navch. posib. 2-e vyd., pererob. i dop. Lutsk : Vezha-druk. 274 s.

Oleksandr Homaniuk,
Candidate in the specialty 291 International Relations,
Public Communications and Regional Studies,
Lesya Ukrainka Volyn National University, Lutsk

Ethics and Confidentiality Issues in Digital International Communications

The article examines data privacy and digital human rights issues in today's global environment, where information flows across borders in real time. The author analyzes key challenges for personal data protection in international communications, focusing on the diversity of legal approaches in different countries and the risks associated with personal information sharing. Privacy is defined as the protection of personal data from unauthorized access, especially in contexts where data may cross borders with varying legal standards. The article highlights the role of large corporations, such as Google and Facebook, in safeguarding and protecting user data, given the potential threats of data breaches or misuse. It examines measures taken by governments, particularly within the EU, to ensure data protection, though the global nature of the internet presents obstacles to enforcing such requirements. In the context of digital human rights, aspects such as the right to privacy, freedom of expression, access to information, and protection from digital surveillance are discussed. The author emphasizes that these rights are closely linked to basic human rights, yet the current advancement of technology creates new threats. The Cambridge Analytica case is cited as an example of how personal data can be used to manipulate public opinion. The article raises the issue of the digital divide, which limits internet access for a large portion of the population, especially in developing countries, contributing to social inequality. The problem of digital surveillance and the potential for technology, such as facial recognition, to be used for discrimination or human rights violations is also addressed, with mention of China's social credit system as an example. Finally, the article explores the ethical application of artificial intelligence and the need for international standards to ensure transparency, accountability, and security in the use of digital technologies.

Keywords: *confidentiality, personal data protection, ethics, digital human rights, cybersecurity, artificial intelligence (AI).*