

Політичні інститути та процеси

УДК 324

DOI <https://doi.org/10.5281/zenodo.19097898>

Засоби протидії інформаційним політичним маніпуляціям у європейських правилах щодо штучного інтелекту: можливості та проблеми запровадження в Україні

Дем'янюк Руслан Анатолійович,

аспірант кафедри політичних наук,

Навчально-наукового інституту права та політології,

Українського державного університету імені Михайла Драгоманова,

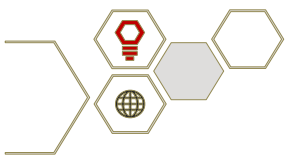
Київ, Україна, <https://orcid.org/0009-0000-6431-3397>

Прийнято: 04.03.2026 | Опубліковано: 18.03.2026

Анотація: У статті розглянуто проблеми і можливості адаптації та імплементації в Україні передбачених європейськими правилами щодо штучного інтелекту засобів протидії інформаційним політичним маніпуляціям.

Метою проведення дослідження є вивчення та аналіз можливостей і проблем адаптації та імплементації в Україні заходів протидії інформаційним політичним маніпуляціям у європейських правилах щодо штучного інтелекту. Адже протидія інформаційним політичним маніпуляціям з використанням штучного інтелекту створює нові виклики та завдання.

Штучний інтелект надає нові широкі можливості для політичних маніпуляцій. Масове генерування під час виборів або кризових ситуацій за допомогою штучного інтелекту фейкових новин, маніпулятивних наративів і пропаганди створює потужні можливості для негативного впливу на громадську думку. Європейським Союзом розпочато впровадження гармонізованих правил



щодо штучного інтелекту, які містять додаткові засоби протидії з дезінформацією та пропагандою.

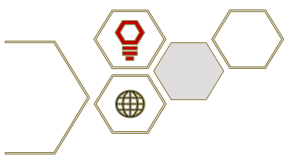
Актуальність теми полягає у необхідності дослідження таких норм для визначення можливостей їх адаптації та імплементації, особливо під час війни, адже інформаційні атаки, наразі вже з використанням штучного інтелекту, є частиною російської стратегії агресії проти України.

Висновками такого аналізу є визначення основних понять та термінів; характеристика протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту; встановлення та аналіз заходів протидії інформаційним політичним маніпуляціям у європейських правилах щодо штучного інтелекту; визначення можливостей та основних проблем у їх запровадженні в Україні; розроблення рекомендацій щодо адаптації кращих з них та подальшої їх імплементації.

За результатами системного аналізу визначено, що європейські правила щодо штучного інтелекту поєднують як правове регулювання так і етичні принципи та технологічну відповідальність, а тому імплементація кращих з них та комплексний підхід з розвитку інфомедіаграмотності мають стати основою для запобігання інформаційним маніпуляціям з використанням штучного інтелекту в Україні.

Запропоновано розробити, змінити та удосконалити механізми протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту в Україні з урахуванням європейських правил. У статті проаналізовано засоби протидії інформаційним політичним маніпуляціям у гармонізованих європейських правилах щодо штучного інтелекту, зокрема їх класифікацію за рівнем ризику для основоположних прав громадян.

Ключові слова: політичні маніпуляції, інформаційні політичні маніпуляції, штучний інтелект, політична дезінформація, AI Act, Digital Services Act, європейські правила щодо штучного інтелекту, протидія інформаційним політичним маніпуляціям з використанням штучного інтелекту.



Countering information-political manipulation within European artificial intelligence regulations: opportunities and challenges for implementation in Ukraine

Ruslan Demianiuk,

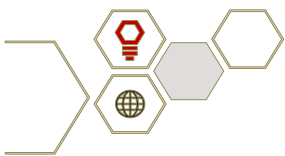
postgraduate student of the Department
of Political Science, Educational and Scientific Institute of Law and Political Science,
Ukrainian State University named after Mykhailo Drahomanov
Kyiv, Ukraine, <https://orcid.org/0009-0000-6431-3397>

Abstract: This article examines the problems and opportunities of adapting and implementing tools to counter information-political manipulation in Ukraine, as provided by European AI regulations.

The purpose of this research is to study and analyze the possibilities and problems of adapting and implementing European AI anti-manipulation measures in Ukraine. Countering such manipulation with the use of artificial intelligence, after all creates new challenges and tasks.

AI provides broad new opportunities for political manipulation. The mass generation of fake news, manipulative narratives, and propaganda during elections or crises using AI creates strong possibilities for a negative influence on public opinion. The European Union has started the process of implementation of harmonized rules on artificial intelligence (the AI Act), which includes additional measures to fight disinformation and propaganda.

The relevance of this topic is the necessity to study these rules to find ways for their adaptation and implementation, especially during the war. Informational attacks, now using artificial intelligence, are part of the Russian strategy of aggression against Ukraine.

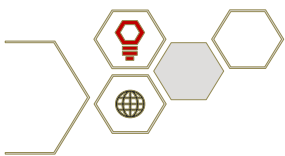


The results of the study include: defining the main concepts and terms; characterizing the counteraction to information-political manipulation using AI; analyzing specific measures in European AI regulations; identifying opportunities and main problems for their implementation in Ukraine; and developing recommendations for adapting best practices.

Based on the results of the systemic analysis, it is determined that European AI rules combine legal regulation with ethical principles and technological responsibility. Therefore, the implementation of these best practices and a complex approach to developing info-media literacy should be the basis for preventing AI-based information manipulation in Ukraine.

It is proposed to develop, change, and improve the mechanisms for countering AI-driven manipulation in Ukraine based on European rules. The article analyzes tools for countering manipulation in the harmonized European AI rules, particularly their classification by risk level for citizens' fundamental rights.

Keywords: political manipulation, information-political manipulation, artificial intelligence, political disinformation, AI Act, Digital Services Act, European rules on artificial intelligence, countering information-political manipulation using artificial intelligence.



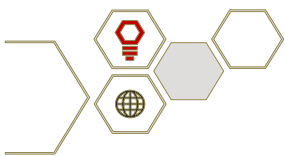
Постановка проблеми. Штучний інтелект надає нові можливості для створення та використання великої кількості удосконалених навчальних просторів для покращення процесу розвитку людей та їх груп. Проте ця інноваційна система надає потужні інструменти для маніпулятивних, експлуататорських та соціально-контрольних практик у політичній сфері, а наявні заходи запобігання стрімко стають не дієвими.

Використання штучного інтелекту для інформаційних політичних маніпуляцій істотно посилюють і без того серйозну загрозу. Масове генерування під час виборів або кризових ситуацій за допомогою штучного інтелекту фейкових новин, маніпулятивних наративів і пропаганди створює потужні можливості для негативного впливу на громадську думку.

Європейським Союзом розроблено та з лютого 2025 вже розпочато впровадження (окремих положень) гармонізованих правил щодо штучного інтелекту, які містять додаткові засоби протидії з дезінформацією та пропагандою. Необхідність дослідження таких практик для визначення можливостей їх адаптації та імплементації є особливо актуальною в умовах війни, адже інформаційні атаки, наразі вже з використанням штучного інтелекту, є частиною російської стратегії агресії проти України.

Зловживання у використанні штучного інтелекту суперечать цінностям Європейського Союзу, а тому опрацювання засобів протидії інформаційним політичним маніпуляціям, передбачених гармонізованими правилами щодо штучного інтелекту, допоможе Україні, яка прагне до членства у зазначеному об'єднанні, створити удосконалені інструменти.

Розробка удосконалених систем навчання, з урахуванням широкого застосування штучного інтелекту, визначенням навичок та знань, які повинні адаптуватися до майбутніх потреб, насамперед тих з них, які стануть дієвими запобіжниками політичним маніпуляціям з використанням штучного інтелекту.

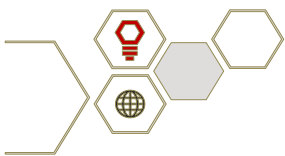


Аналіз причин і спрямування політичних повідомлень згенерованих під час виборів або кризових ситуацій за допомогою штучного інтелекту є важливим для розкриття напрямів розвитку сучасних «інфократії», «цифрократії» та стрімкої зміни політичного представництва й управління за цифрової інформаційно-комунікаційної доби.

«Сучасна політична практика доводить, що штучний інтелект функціонує як політичний модератор, який не лише детермінує зміст інформаційного простору, а й впливає на стратегічне конструювання суспільних уявлень. Інтенсифікація алгоритмічного втручання у політичні процеси вимагає комплексного аналізу, здатного віднайти баланс між технологічним прогресом й збереженням демократичної легітимності інформаційного середовища» [1, с. 101].

Розкриття механізму нових чи удосконалених політико-маніпулятивних методів і прийомів набуває актуальності в контексті відстоювання українського національного інформаційного простору від інформаційної агресії, активної пропаганди країни-окупанта генерованої за допомогою штучного інтелекту. Набуття нових знань може бути одним із дієвих засобів протидії шкідливому впливу зазначеним проявам інформаційних політичних маніпуляцій з використанням штучного інтелекту та сприятиме формуванню комунікаційної спроможності громадянського суспільства запобігати таким викликам.

Аналіз останніх досліджень і публікацій. Дослідженню штучного інтелекту присвячені праці таких науковців, як У. Петерс, Н. Ферг'юсон, Е. Бернейз, І. Бубнов, М. Шевчук, В. Виздрик, О. Мельник, М. Лазарович, Т. Гончарук-Чолач, О. Докаш, а ролі і значення політичних маніпуляцій – А. Міхненко, М. Месюк, В. Корольчук та інших. Протидія інформаційним політичним маніпуляціям та дезінформації є предметом аналізу багатьох зарубіжних дослідників [19]. Попри це процес їх аналізу постійно ускладнюється.



Виділення невирішених раніше частин загальної проблеми.

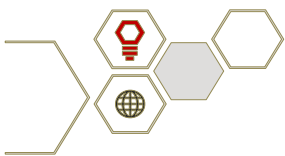
Зосередимося на спробах сформулювати рекомендації щодо удосконалення механізмів протидії в Україні інформаційним політичним маніпуляціям з використанням ШІ з урахуванням удосконалених європейських правил, тобто питаннях, які не повною мірою були висвітлені до цього часу.

Формулювання цілей статті (постановка завдання). Вивчення проблематики на шляху пристосування та запровадження в Україні заходів протидії інформаційним політичним маніпуляціям у європейських правилах щодо штучного інтелекту є метою цієї статті.

Серед завдань статті необхідно виокремити:

- визначення основних понять і термінів проблеми;
- характеристику протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту;
- з'ясування важливості ефективної протидії інформаційним політичним маніпуляціям із застосуванням ШІ;
- аналіз заходів протидії інформаційним політичним маніпуляціям у європейських правилах щодо штучного інтелекту та можливостей і основних проблем у їх запровадженні в Україні;
- розроблення рекомендацій щодо адаптації окремих з них для їх подальшої імплементації.

Методи дослідження застосовані у статті, охоплюють теоретичний аналіз наукової літератури, спрямованої на дослідження штучного інтелекту, заходів протидії дезінформації у європейських правилах щодо штучного інтелекту, а також емпіричного вивчення заходів протидії інформаційним політичним маніпуляціям у європейських правилах щодо штучного інтелекту. За допомогою порівняльного методу та методу політичного аналізу, а також узагальнення окреслено можливості та проблеми у запровадженні в Україні заходів протидії інформаційним політичним маніпуляціям у європейських правилах щодо штучного інтелекту.



Методологія дослідження запобігання політичним маніпуляціям з використанням штучного інтелекту спрямована на виявлення способів дезінформації, оцінку їх впливу та розробку механізмів протидії та поєднує якісні і кількісні підходи.

Виклад основного матеріалу дослідження.

«Штучний інтелект (ШІ) – це сімейство інтенсивних цифрових технологій, що сприяє широкому спектру економічних, екологічних та соціальних переваг у всьому спектрі галузей промисловості та соціальної діяльності. Завдяки покращенню прогнозування, оптимізації операцій та розподілу ресурсів, а також персоналізації цифрових рішень, доступних для окремих осіб та організацій, використання ШІ може забезпечити ключові конкурентні переваги для підприємств та підтримувати соціально та екологічно корисні результати» [12, п. 4].

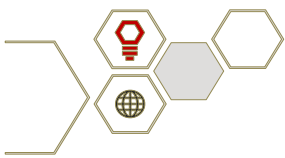
«Штучний інтелект, функціонуючи в межах кібернетично орієнтованих механізмів дискурсивної регуляції, не лише реорганізує парадигмальні засади політичної комунікації, а й спричиняє багатовекторну модуляцію когнітивних алгоритмів соціальної перцепції» [21].

Механізми створення, поширення та сприйняття інформації істотно трансформовано внаслідок стрімкого розвитку штучного інтелекту (ШІ).

Все більше політична комунікація залежить від автоматизованих систем аналізу даних, таргетованої реклами та генеративних моделей, здатних створювати переконливий, але маніпулятивний контент. Такі фактори формують нові загрози для демократичних процесів, зокрема виборів, формування громадської думки та реалізації свободи волевиявлення.

Разом з великим потенціалом, розвиток штучного інтелекту, закладає підґрунття і для політичних маніпуляцій.

Потреба детального вивчення інформаційних політичних маніпуляцій з використанням штучного інтелекту, передусім зумовлена, посиленням під час війни, загроз поширення оманливої інформації.



В минулих поглядах масового суспільства маніпулятивна політична комунікація, через призму наукових робіт (передусім політологічних та психологічних) проглядається як міцно утверджена цілісна система.

Водночас за допомогою технологій, політичні маніпуляції, перетворюються на домінуючі фактори політичного процесу.

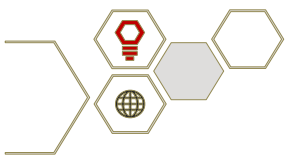
В. Корольчук справедливо вважає, що «маніпуляція – це прихований вплив, факт якого не повинен бути усвідомлений об'єктом маніпуляції. Для досягнення успіху маніпуляція має залишатися непомітною. Успіх маніпуляції гарантовано, коли маніпульована особа вірить, що все, що робиться, є природнім і невідворотним. Для маніпуляції потрібна фальшива дійсність, у якій її присутність не буде відчуватися» [7, с. 219].

«Для політичних досліджень важливо вивчати наслідки застосування подібних технік у ширшому статистичному обсязі: «природа маніпуляції полягає в подвійному впливові – поряд з відкритим повідомленням маніпулятор посиляє адресату «закодований» сигнал, сподіваючись на те, що цей сигнал розбудить ті образи у свідомості адресата, які йому потрібні» [7, с. 219].

«Роль і значення маніпуляції стали усвідомлюватися в результаті широкого використання політичних технологій і завдяки вивченню так званого «масового суспільства» і «масової свідомості» [9, с. 7].

На тлі швидких та радикальних цифрових перетворень, удосконалюється і визначення маніпуляції у сфері політичної комунікації.

Одже цілісна система заснована на високому рівні доступності інформації та високих технологіях у цій сфері, що складається з організаційних, ідеологічних та психологічних заходів, які спрямовані на приховану зміну масової свідомості, з метою стимулювання суспільних настроїв та громадської активності у потрібному маніпуляторіві напрямі у процесі здобуття, утримання і використання політичної влади є сучасним відображенням інформаційних політичних маніпуляцій.

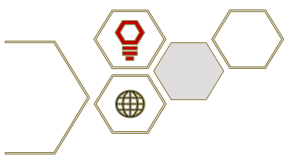


«Одним із основних інструментів, що використовує ІІІ у політичних маніпуляціях, є персоналізація контенту, зокрема через соціальні мережі. Алгоритми аналізують поведінку користувачів, їх інтереси, історію пошуків і вподобань, що дозволяє створювати рекламу та повідомлення, які максимально відповідатимуть індивідуальним переконанням виборців. Така таргетована комунікація стає дедалі ефективнішою, адже вона не просто інформує, а й формує емоційні зв'язки та поглиблює розрив між різними групами виборців, підвищуючи ризик поляризації суспільства. Завдяки цьому ІІІ дозволяє не лише впливати на електоральні вподобання, але й створювати нові форми політичних маніпуляцій, таких як автоматизоване створення контенту чи навіть фальсифікація новин» [8, с. 132, 13, с. 496].

Боти, які генерують і поширюють дезінформацію, стають важливими інструментами для політичних сил, що намагаються вплинути на громадську думку або дискредитувати опонентів. Маючи можливість створювати численні фальшиві облікові записи в соцмережах і розповсюджувати маніпулятивний контент, ІІІ здатен значно змінити політичну ситуацію, не залишаючи слідів.

«Ці технології мають значний вплив на виборчі кампанії та загалом на політичну культуру. Традиційні методи виборчих кампаній, такі як дебати, прес-конференції чи публічні виступи, стають менш важливими, оскільки частина електорального процесу тепер переміщується у цифрове середовище.

І це не просто зміна формату взаємодії з виборцями, а й глибока трансформація самої суті виборчої культури, де особисті уподобання та емоції важать більше за інтелектуальні або логічні аргументи» [8, с. 132, 2, с. 128].



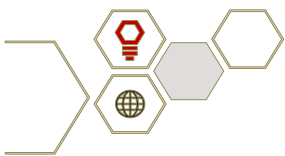
«Штучний інтелект може автоматизувати кіберзагрози і зробити їх складнішими і масштабнішими. Наприклад, хакери можуть використовувати алгоритми машинного навчання для адаптації систем безпеки, виявлення їхніх вразливостей і створення шкідливого програмного забезпечення, що обходить традиційні методи захисту. Крім того, штучний інтелект може аналізувати поведінку користувачів і виявляти найбільш вразливі елементи системи, що дає змогу проводити цілеспрямовані атаки» [14, с. 160–166].

«Особливу небезпеку становлять технології глибокого підроблення на основі штучного інтелекту, які можна використовувати для створення реалістичних підробок відео та аудіозаписів з метою поширення дезінформації, маніпулювання громадською думкою та дискредитації політичних лідерів. Вони можуть бути використані для створення реалістичних підробок зображень і звуку з метою поширення дезінформації, маніпулювання громадською думкою та дискредитації політичних лідерів. Це підриває довіру до інформації і може мати серйозні наслідки» [5, с. 196–202].

Генерування за допомогою ШІ фейкових новин, маніпулятивних наративів та пропаганди негативно впливає на громадську думку, особливо під час виборів або кризових ситуацій. Технології генеративного штучного інтелекту надали можливості для здешевлення, пришвидшення та масштабування створення переконливої дезінформації, що посилює негативний вплив на сучасний політичний ландшафт.

Такі удосконалені за допомогою ШІ можливості для політичного впливу, як системи аналізу великих масивів даних, алгоритми машинного навчання, генеративні моделі та інші, не лише посилюють загрози інформаційній безпеці, але створюють нові загрози демократії.

Відтак протидія інформаційним політичним маніпуляціям з використанням штучного інтелекту з стає одним із найпріоритетніших завдань на сучасному етапі розвитку.



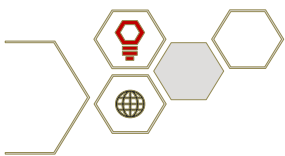
«Залежно від обставин щодо його конкретного застосування, використання та рівня технологічного розвитку, ШІ може створювати ризики та завдавати шкоди суспільним інтересам і основоположним правам, що захищаються законодавством Союзу. Така шкода може бути матеріальною або нематеріальною, включаючи фізичну, психологічну, соціальну чи економічну шкоду» [12, п. 5].

Попередження політичного маніпулювання з використанням ШІ у потребує невідкладного пошуку нових методик та удосконалення існуючих, зокрема шляхом дослідження можливостей удосконалення грамотності у цій сфері та системного нормативного регулювання самих технологій та шляхів їх розповсюдження, а не просто цензури контенту.

Водночас існуючі методи перевірки фактів (фактчекінгу) є недостатніми, коли мова йде про алгоритмічні операції впливу. Тому Європейським Союзом, спираючись на цінності верховенства права, прав людини та прозорості, розроблено систему правил, спрямованих на протидію інформаційним політичним маніпуляціям з використанням ШІ.

Серед загроз інформаційній безпеці варто виділити:

- маніпуляція людьми з використанням ШІ;
- створення шкідливого програмного забезпечення за допомогою ШІ;
- формування та поширення з використанням ШІ оманливих повідомлень, зокрема дезінформації у політичній сфері;
- перевантаження за допомогою ШІ системи запитами для унеможливлення доступу до ресурсів;
- кібертероризм та несанкціонований доступ.



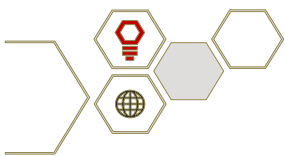
Слід відзначити, що штучний інтелект значно підвищив ефективність маніпулятивних практик шляхом алгоритмічного підсилення радикального або маніпулятивного контенту в соцмережах, автоматизованого створення фейкових новин і політичних наративів, пришвидшення їх поширення та масштабування, мікротаргетингу політичної реклами на основі персональних даних, використання дипфейк-відео та аудіо, що імітують реальних політиків, бот-мереж та тролів з елементами ШІ. Інформація, у цифрову епоху, відіграє ключову роль у формуванні демократичних процесів, політичної свідомості і соціальних наративів. Однак кількість та складність інформаційних маніпуляцій і дезінформації зростає, особливо з розвитком генеративних моделей штучного інтелекту (ШІ), здатних автоматично створювати тексти, зображення, відео та аудіо контент, що вводять в оману мільйони користувачів.

Наведені чинники створюють реальні загрози для свободи формування політичної думки та чесності виборів, а відтак довіри до демократичних інститутів.

«Не всі шкідливі публікації в соціальних мережах є повністю помилковими. Вони можуть містити певну істину, бути незначною мірою оманливими або поза контекстом, або можуть стосуватися проблемних, суперечливих питань, які не обов'язково кваліфікуються як неминуче небезпечні. Встановити походження конкретних фрагментів дезінформації може бути надзвичайно складно» [19].

В контексті України насамперед війна та безпекові кризи є ідеальними умовами для створення та поширення за допомогою штучного інтелекту дезінформації та політичних інформаційних маніпуляцій.

«Дезінформація може замінити складні або заплутані політичні явища редукованими історіями «добра проти зла» і «нас проти них».



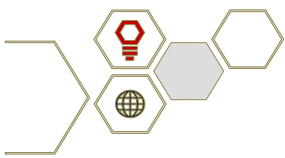
Ці епістемологічні ярлики, які знецінюють комплексний аналіз і часто виключають критичну перевірку своїх припущень і уподобань, посилюються в ехо-камерах соціальних медіа, які підсилюють таку думку. Крім того, ефективні дезінформаційні кампанії посилюють ці упередження, щоб створити політичні розбіжності всередині групи / поза групою. Дослідження показують, що користувачі соціальних мереж набагато частіше діляться неперевіреними історіями, ніж розміщують виправлення, коли історії були показані помилковими або маніпульованими» [19].

«Напрями спроможностей оперативно та ефективно встановлювати та розвивати взаємовідносини між політичними суб'єктами будуть відрізнятися залежно від контексту, але вони викликають сильну громадську реакцію і сформульовані, щоб резонувати між такими сферами як політична ідеологія або партія, етнічна приналежність, раса, релігія. Невизначені політичні результати, які залежать від громадської підтримки, особливо схильні до дезінформації та інформаційних маніпуляцій» [19].

«Швидкі темпи розвитку соціальних медіа та технологічної культури, пов'язані з її зростанням, прискорюють і поширення дезінформації. «Стратегія максимального залучення» сприяє поширенню інформації в публічній сфері з невеликою повагою до критичного розслідування або здорового скептицизму» [19].

Штучний інтелект як удосконалена технологія надає нові можливості безкарно генерувати та поширювати дезінформацію, завдяки анонімності у інформаційному просторі, спрощенню доступності інформації та прискоренню процесів її обміну.

З метою протидії зазначеним негативним факторам Європейський Союз (ЄС) розробив комплекс правил, спрямованих на протидію цим загрозам, інтегруючи інструменти регулювання ШІ в ширшу систему багаторівневих механізмів боротьби з маніпуляціями в інформаційному просторі.



«З огляду на значний вплив, який штучний інтелект може мати на суспільство, та необхідність зміцнення довіри, життєво важливо, щоб штучний інтелект та його регуляторна база розвивалися відповідно до цінностей Союзу, закріплених у статті 2 Договору про Європейський Союз (ДЄС), основних прав і свобод, закріплених у Договорах, та, відповідно до статті 6 ДЄС, у Хартії. Як передумову, штучний інтелект має бути людиноцентричною технологією. Він має служити інструментом для людей, з кінцевою метою підвищення добробуту людства» [12, п. 6].

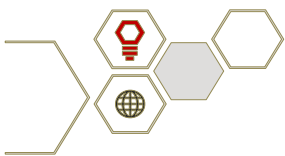
Серед правових і етичних принципів, на яких базується Європейський підхід до регулювання ШІ слід виділити:

- демократичний контроль над цифровими технологіями;
- прозорість алгоритмів;
- відповідальність розробників і користувачів ШІ;
- недискримінація та повага до прав людини;
- захист свободи слова.

Для забезпечення послідовного та високого рівня захисту суспільних інтересів щодо здоров'я, безпеки та основних прав слід встановити спільні правила для систем штучного інтелекту з високим рівнем ризику.

«Ці правила повинні відповідати Хартії, бути недискримінаційними та відповідати зобов'язанням Союзу в галузі міжнародної торгівлі. Вони також повинні враховувати Європейську декларацію про цифрові права та принципи цифрового десятиліття та етичні рекомендації щодо надійного штучного інтелекту, розроблені Експертною групою високого рівня з питань штучного інтелекту (AI HLEG)» [12, п. 7].

Європейські правила щодо ШІ за рівнем ризику для основоположних прав громадян класифіковано на

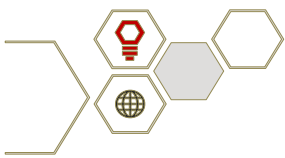


- заборонені (Акт про ШІ забороняє його використання ШІ для когнітивного маніпулювання поведінкою, а саме технологій з використанням методів, які експлуатують вразливості певних груп для суттєвого викривлення їхньої політичної волі).
- високоризикові (призначений для впливу на результати виборів або поведінку виборців у межах політичних кампаній, ШІ віднесений до категорії високого ризику, що зобов'язує розробників гарантувати «людський контроль» над алгоритмами.
- вимоги до прозорості (обов'язок маркування контенту, чітке поінформування користувачів про їх взаємодію із ШІ або якщо аудіо-та відеоконтент (дипфейки) є штучно створеними).

Для протидії політичним маніпуляціям Європейськими правилами щодо ШІ передбачено:

- пряму заборону систем ШІ, що здійснюють маніпулятивний або підсвідомий вплив на поведінку людей;
- класифікація систем ШІ за рівнем ризику;
- вимога прозорості для генеративного ШІ (позначення контенту, створеного ШІ);
- жорсткі вимоги до систем ШІ, що можуть впливати на демократичні процеси.

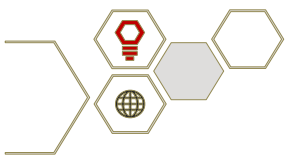
Таким чином, необхідна правова база Союзу, яка встановлює гармонізовані правила щодо ШІ, для сприяння розвитку, використанню та впровадженню ШІ на внутрішньому ринку, що водночас відповідає високому рівню захисту суспільних інтересів, таких як здоров'я та безпека, а також захисту основних прав, включаючи демократію, верховенство права та охорону навколишнього середовища, визнаних та захищених законодавством Союзу.



Для досягнення цієї мети слід встановити правила, що регулюють розміщення на ринку, введення в експлуатацію та використання певних систем ІІІ, тим самим забезпечуючи безперебійне функціонування внутрішнього ринку та дозволяючи цим системам користуватися принципом вільного руху товарів і послуг.

«Окрім численних корисних застосувань штучного інтелекту, його також можна використовувати зловживаючи, надаючи нові та потужні інструменти для маніпулятивних, експлуаторських та соціально-контрольних практик. Такі практики є особливо шкідливими та зловживальними і повинні бути заборонені, оскільки вони суперечать цінностям Союзу, таким як повага до людської гідності, свобода, рівність, демократія та верховенство права, а також основоположним правам, закріпленим у Хартії, включаючи право на недискримінацію, на захист даних та на приватне життя, а також права дитини» [12, п. 28].

«Ці правила повинні бути чіткими та надійними у захисті основних прав, підтримувати нові інноваційні рішення, створюючи європейську екосистему державних та приватних суб'єктів, які створюють системи ІІІ відповідно до цінностей Союзу та розкривають потенціал цифрової трансформації в усіх регіонах Союзу. Встановлюючи ці правила, а також заходи на підтримку інновацій з особливим акцентом на малі та середні підприємства (МСП), включаючи стартапи, цей Регламент підтримує мету просування європейського людиноцентричного підходу до штучного інтелекту та є світовим лідером у розробці безпечного, надійного та етичного штучного інтелекту, як зазначено Європейською Радою, а також забезпечує захист етичних принципів, як цього спеціально вимагає Європейський парламент» [12, п. 8].



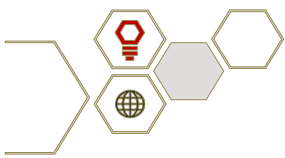
До основних європейських правил протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту варто віднести:

1. Artificial Intelligence Act (AI Act) 2020/1828 (Закон про штучний інтелект), зі змінами внесеними Регламентом Європейського Парламенту та Ради (ЄС) 2024/1689 від 13 червня 2024 року [12]. Artificial Intelligence Act (AI Act) — був першим масштабним регламентом щодо штучного інтелекту, що визначив правові межі для розробки, розповсюдження й використання систем ШІ в ЄС. Зазначені норми набули чинності 1 серпня 2024 року, проте їх запровадження розтерміновано залежно від категорій ризику технологій. Їх основою є збереження балансу між досягненням мети щодо зменшення ризиків для прав людини, демократичних процесів, пов'язаних з використанням ШІ, та не створенням перешкод для інновацій. Ці правила містять класифікацію ШІ за рівнями ризику та передбачають вимоги щодо управління такими ризиками, прозорості та звітності.

Варто відзначити, що AI Act містить пряму заборону використання ШІ для експлуатації вразливостей певних груп населення або маніпуляції поведінкою користувачів. Зокрема, під заборонаю системи, що використовують «маніпулятивні чи оманливі техніки», метою яких є змусити людину ухвалити рішення, яке вона би не ухвалила самостійно. Також заборони поширюються і на загрози інформаційним процесам різними формами маніпуляцій (deepfake відео/аудіо, автоматизовані фейки), що можуть бути використані у політичних кампаніях чи суспільних дискусіях. «Якщо Закон про ШІ загалом класифікує дипфейки як «обмежений ризик», то його Додаток III 8 (b) розглядає системи ШІ, що використовуються для впливу на вибори, референдум або поведінку голосування фізичних осіб, як високий ризик.

Основні його положення:

- відповідно до статті 52 (3) творці, розробники та користувачі технологій deepfake повинні розкривати будь-який контент, створений ШІ. Це



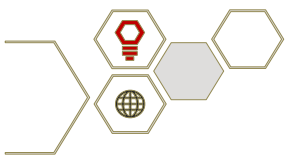
має на меті приборкати помилкову дезінформацію та забезпечити обізнаність аудиторії про штучний контент;

- класифікація та знак ідентифікації глибоких підробок. У контекстах, які суттєво впливають на права людей або суспільство (наприклад, політичні маніпуляції, наклеп), дідфейки можуть бути класифіковані як високоризикові;
- відстежуваність/підзвітність у створенні та поширенні дідфейків: записи процесів і даних, які використовуються для створення дідфейків, щоб відстежувати їх походження;
- зловмисне використання дідфейків, наприклад, у соціальному скорингу або для незаконного стеження, класифікуються як неприйнятний ризик і заборонені» [16, р. 9–10].

У правовому полі ЄС як інструменти протидії інформаційним маніпуляціям, передбачено маркування ШІ-контенту та прозорість (обов'язкове сповіщення користувача про те, що він взаємодіє з ШІ-системою, маркування контенту, створеного або зміненого ШІ), що має за мету зменшення ризиків введення в оману та зміцнення довіри громадян до цифрового середовища.

Набрання чинності AI Act можна розділити на чотири етапи:

- початок дії заборон для систем із неприйнятним ризиком (з 02.02.2025);
- введення зобов'язань для моделей ШІ загального призначення (GPAI) та створення державами національних компетентних органів (з 02.08.2025);
- старт виконання вимог нового закону більшістю високоризикових систем (з 02.08.2026);
- введення зобов'язань для окремих категорій "вбудованих" високоризикових систем (з 02.08.2027).



Водночас ЄС в окреслені у зазначених вище правилах строки не спромігся розробити та затвердити технічні стандарти під зазначені вище регуляції, без яких виконання зобов'язань на практиці буде неможливим.

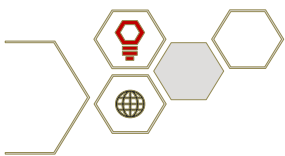
2. Digital Services Act (DSA) встановлює вимоги до великих інтернет-платформ щодо модерації, прозорості політик і доступу дослідників до даних, що також є критично важливим для протидії масовим маніпуляціям. Цей підхід дає системну правову відповідь, де AI Act зосереджується на ШІ-системах, а DSA — на екосистемі інтернет-контенту загалом.

«Так, Європейським цифровим актом (Digital Services Act, DSA) та Законом про цифрові ринки (Digital Markets Act, DMA) на технологічні компанії покладено обов'язки щодо видалення фейкової інформації, забезпечення прозорості алгоритмів, захисту користувачів від маніпулятивного контенту, впровадження механізмів швидкого реагування на інформаційні атаки, а також застосування, за невиконання таких правил, істотних штрафів» [17, 18].

Згідно з DSA, всі посередники зобов'язані боротися з незаконним контентом, таким як терористичний контент і мова ненависті [17].

«В 2024 році прийнято керівні принципи для постачальників VLOP та VLOSE з рекомендованим пом'якшенням ризиків для доброчесності виборців. Конкретні заходи щодо пом'якшення наслідків, пов'язаних з генеративним ШІ (штучним інтелектом), включали чітке маркування вмісту, такого як ШІ-згенерований або маніпульований текст» [15].

- «Окрім регуляторних діалогів з VLOPs та VLOSEs, при Європейській раді з цифрових послуг була створена спеціальна робоча група для обміну досвідом та національних органів влади з виборчих питань» [16, р. 7–8]. «ТТРА (Регламент про прозорість та таргетування політичної реклами) обмежує методи націлювання та доставки; підвищує захист персональних даних в інтернет-політичній рекламі; забороняє профілювання



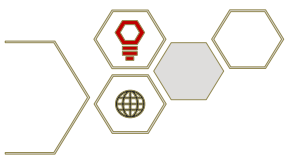
(використання спеціальних категорій даних, таких як расове або етнічне походження користувачів і політична думка); забороняє організаціям, які не є членами ЄС, фінансувати політичну рекламу в ЄС за три місяці до виборів або референдуму» [16, р. 9].

Запровадженню в Україні європейських правил протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту може посприяти як значний інтерес громадськості до інфомедіаграмотності та тісна співпраця з ЄС у сфері цифрової безпеки.

Доцільно узагальнити напрацювання ЄС у здійсненні супротиву інформаційним політичним маніпуляціям з використанням штучного інтелекту з метою розроблення рекомендацій щодо адаптації найкращих з них та вивчення можливостей їх запровадження в Україні.

В цьому контексті необхідно дослідити баланс між громадянськими свободами, захистом цивільного населення та національною безпекою.

Наразі в Україні відсутній закон, який би належним чином регламентував важливі аспекти функціонування штучного інтелекту. Для подолання такої нормативної прогалини у такій важливій сфері протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту розпорядженням Кабінету Міністрів України від 09.05.2025 за № 457-р. затверджено «план заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки» [11].

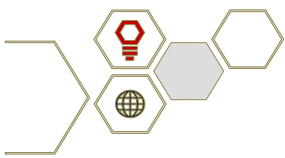


Зазначена Концепція передбачає розроблення та ухвалення законопроекту щодо правового врегулювання у сфері розвитку штучного інтелекту. Водночас варто не повторити неділки ЄС і забезпечити своєчасне розроблення та затвердження технічних стандартів під зазначені вище регуляції. Також наявна потреба в розробленні методичних рекомендацій щодо використання технологій штучного інтелекту у сфері вищої освіти, забезпечення доступу до освіти за освітньо-професійними програмами, зокрема в галузі інформаційних технологій, штучного інтелекту, аналізу інформації.

«В даному контексті варто зазначити, що технологічна, або цифрова грамотність (яка разом інформаційною грамотністю та медіа грамотністю є складовими частинами інфомедійної грамотності) передбачає вміння користуватись сучасними інформаційними технологіями та програмним забезпеченням із урахуванням усіх можливостей, що надає інформаційний прогрес» [3].

Впровадження освітніх програм щодо цифрової грамотності, як важливого елемента інфомедійної грамотності, для удосконалення навичок узагальнення інформації, а також направлених на розвиток критичного мислення, на моє переконання, повинно стати ключовою процедурою. Залучення інфомедіаграмотності до шкільної та університетської освіти, підвищення підтримки ініціатив із підвищення інформаційної обізнаності, як позитивні практики ЄС, є актуальними для запровадження в Україні. Важливим елементом є також швидке реагування на дезінформаційні кампанії, шляхом здійснення належної державної комунікації.

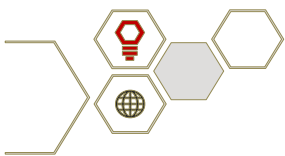
На перший погляд швидке та системне удосконалення інфомедійної грамотності шляхом впровадження високоефективної цифрової освіти і може стати тим дієвим запобіжником політичним маніпуляціям в інформаційному суспільстві, з широкими та надзвичайними можливостями.



Водночас при розробці методичних рекомендацій щодо використання технологій штучного інтелекту в сфері освіти варто врахувати, що на шляху швидкого покращення вміння знаходити, аналізувати, використовувати інформацію, а також вміння отримувати доступ до медіа, аналізувати контент, оцінювати медіаповідомлення, а також створювати контент для самовираження та спілкування і тим більше удосконалення вміння користуватись сучасними інформаційними технологіями та програмним забезпеченням, виникають проблеми як фінансово-економічного так і психологічного характеру.

«Чим складнішою стає реальність і діяльність, тим менше людей нею займаються» [20].

«Успіх та можливості високих технологій у політичних справах великою мірою залежать від сформованості й розвиненості демократичного політичного режиму. Демократизація передбачає розвиток відкритого суспільства та відкритої держави, поглиблення міжнародної співпраці і глобального співробітництва з одночасним розвитком і зміцненням безпекових інститутів, спроможних захистити вразливі ніші цього політичного режиму. Нове покоління технологій, як і багато попередніх, однаково мають як соціально деструктивний, так і консолідуючий потенціал. Результати їх застосування залежать від існуючого політичного режиму, встановлених політичних правил гри, традицій у відносинах «влада-суспільство», розвитку освіти і науки, а також від міжнародної політичної кон'юнктури» [4, с. 91].



Вкрай важливим є також розроблення рекомендацій з кібербезпеки, які передбачатимуть пропозиції з використання технологій штучного інтелекту, зокрема щодо захисту моделей машинного навчання від несанкціонованого втручання в роботу, проведення оцінки стану захищеності інформаційно-комунікаційних систем, які використовують штучний інтелект для виявлення та протидії кіберзагрозам, забезпечення прийняття міжнародних стандартів у сфері розвитку штучного інтелекту як національних стандартів.

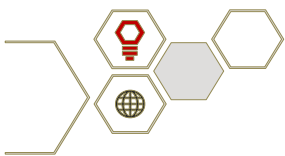
Тут слід зауважити, що насамперед в Україні передусім необхідно орієнтуватися на європейські стандарти у цій сфері, які до цього часу ще не набрали чинності. Тому їх аналіз та можливості запровадження в Україні можуть бути предметом подальшого перспективного дослідження.

Насамперед, важливими є опрацювання технічних стандартів під зазначені регуляції питань визначення та класифікації дідфейків та щодо віднесення систем ШІ, які використовуються для впливу на вибори, референдум, голосування фізичних осіб або маніпулювання поведінкою до високо ризикованих, а також заборону зловмисного використання дідфейків у соціальному скорингу або для незаконного стеження.

Варто також приділити належну увагу інсплементатії в Україні питань застосування в ШІ в діяльності правоохоронних та судових органів

Якщо система штучного інтелекту не навчена на високоякісних даних, не відповідає належним вимогам щодо її продуктивності, точності чи надійності, або не є належним чином розробленою та протестованою перед виведенням на ринок чи іншим введенням в експлуатацію, вона може виділяти людей дискримінаційним або іншим неправильним чи несправедливим чином.

Крім того, здійснення важливих процесуальних основних прав, таких як право на ефективний засіб правового захисту та на справедливий суд, а також право на захист та презумпція невинуватості, може бути ускладнене, зокрема, якщо такі системи штучного інтелекту не є достатньо прозорими, поясненьними та задокументованими.

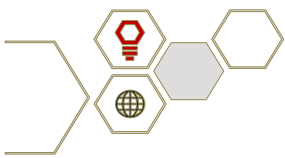


Тому доцільно класифікувати як високоризикові, оскільки їх використання дозволено відповідним законодавством Союзу та національним законодавством, низку систем штучного інтелекту, призначених для використання в контексті правоохоронних органів, де точність, надійність та прозорість особливо важливі для уникнення негативного впливу, збереження довіри громадськості та забезпечення підзвітності та ефективного відшкодування. Використання інструментів штучного інтелекту правоохоронними та іншими відповідними органами не повинно ставати фактором нерівності чи виключення.

«Не слід ігнорувати вплив використання інструментів штучного інтелекту на права підозрюваних на захист, зокрема, складність отримання змістовної інформації про функціонування цих систем та, як наслідок, складність оскарження їхніх результатів у суді, зокрема фізичними особами, щодо яких ведеться розслідування» [12, п. 59].

Важливими аспектами є тісна співпраця з ЄС у сфері цифрової безпеки та зацікавленість суспільства у інфомедіаграмотності.

Проблемою імплементації європейських правил щодо ШІ, як важливого знаряддя протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту є брак фінансів та кадрового забезпечення, який напряду пов'язаний з тривалою війною. Протидія викликам щодо використання ШІ у політичній сфері породжує проблему її не завжди обґрунтованого використання державою як засобу пригнічення політичної конкуренції та спотворення права на волевиявлення.



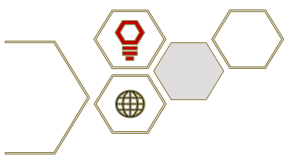
Як відзначає Р. Дудник: «Технологічний розвиток створює нові можливості та виклики, такі як кібербезпека та захист особистих даних. Інтеграція з міжнародним співтовариством розширює можливості розвитку правової системи України та підвищує її якість та ефективність. Глобалізація та інтеграція впливають на систему права України. Збереження національної ідентичності, гармонізація стандартів та адаптація до нових викликів є ключовими аспектами цього впливу» [6, с. 91].

Нетралізація нових інструментів політичних маніпуляцій з використанням ШІ, у цьому сенсі, є ключовим етапом у гармонізації правової системи України з відповідними європейськими правилами у цій сфері.

Впровадження таких перетворень створює реальні ризики для демократії, адже вони можуть пригнічувати політичну конкуренцію, формувати підвалини для політичної цензури.

Висновки. За підсумками проведеного дослідження необхідно зазначити, що новітні європейські правила щодо штучного інтелекту є системною відповіддю на загрози інформаційних політичних маніпуляцій із використанням штучного інтелекту. Згадані правила становлять комплекс додаткових узгоджених заходів стримування дезінформації, пропаганди з використанням згаданої інноваційної системи, вони поєднують як правове регулювання так і етичні принципи та технологічну відповідальність, що надасть можливість ЄС зберігати баланс між інноваціями та захистом демократії.

Європейський підхід до регулювання штучного інтелекту ґрунтується на ідеї, що технологічний розвиток має відбуватися в межах чітких правових рамок і відповідати фундаментальним цінностям ЄС. Саме тому ключову роль у протидії інформаційним політичним маніпуляціям відіграють нормативно-правові акти, які встановлюють обмеження, вимоги прозорості та механізми відповідальності для суб'єктів, що використовують ШІ.



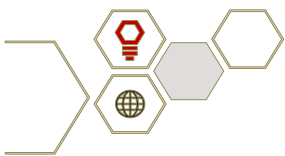
Європейська модель демонструє прагнення не заборонити інновації, а спрямувати їхній розвиток у русло, сумісне з демократичними цінностями та захистом прав людини. Запровадженню в Україні європейських правил протидії інформаційним політичним маніпуляціям з використанням штучного інтелекту може посприяти як значний інтерес громадськості до інфомедіаграмотності та тісна співпраця з ЄС у сфері цифрової безпеки, так і реалізація Концепції розвитку штучного інтелекту в Україні.

Однак для цього необхідно забезпечити розроблення та ухвалення національного законодавства щодо штучного інтелекту, підготовку та впровадження методики використання штучного інтелекту на всіх рівнях освіти, запровадження інструкцій з кібербезпеки з пропозиціями щодо захисту моделей машинного навчання від несанкціонованого втручання в роботу. А також прийняття міжнародних стандартів у сфері розвитку штучного інтелекту як національних стандартів.

Розвиток інфомедійної (зокрема цифрової) грамотності на всіх освітніх рівнях, підвищення підтримки суспільних проектів із підвищення поінформованості, розробки відповідних адаптивних систем навчання для впровадження удосконаленої цифрової освіти має стати основою для запобігання інформаційним маніпуляціям в Україні з використанням штучного інтелекту.

Критично важливим збереження європейської концепції цінностей для того, щоб регламентовані в Україні заходи запобігання інформаційним політичним маніпуляціям з використанням штучного інтелекту містили дієві запобіжники викликам для політичної конкуренції та свободи вибору.

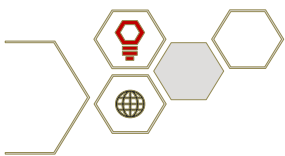
Таким чином захистити демократію та результативно протидіяти інформаційним ризикам може надати змогу лише обдуманий та упорядкований підхід дозволить Україні.



Простір для подальших досліджень тематики вбачається у детальнішому узагальненні наслідків запровадження в Україні технічних стандартів ЄС (які перебувають ще у стадії розробки та затвердження) під окремі елементи європейських правил протидії інформаційним маніпуляціям з використанням штучного інтелекту, створенні настанов щодо їх подальшого пристосування та покращення з метою побудови впорядкованої та дієвої системи.

Список використаних джерел

1. Бубнов І. В. Штучний інтелект як фактор політичного впливу в медійній сфері, 2025. DOI <https://doi.org/10.32782/app.v75.2025.14>.
2. Бернейз Е. Л. Пропаганда. К.: Сварог, 2023. 128 с.
3. Бути медіаграмотним: десять необхідних компетентностей <https://ms.detector.media/mediaosvita/post/18961/2017-05-24-buty-mediagramotnym-desyat-neobkhdnykh-kompetentnostey/>.
4. Волянчук О. Я. Політична реальність і доповнена реальність: особливості сумісності // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін [Відп. ред. О.В.Бабкіна]. Випуск 26: збірник наукових праць. К.: Вид-во НПУ імені М. П. Драгоманова, 2019. 86-93 с.
5. Виздрик В. С., Мельник О.М. Інформаційна безпека в Україні. *Grail of Science*. № 24. 2023. 196–202 с.
6. Дудник Р. М. Система права та правова система України в добу глобалістики (інтеграції). *Науковий вісник Ужгородського Національного Університету*. 2023. DOI <https://doi.org/10.24144/2307-3322.2023.79.1.6>.
7. Корольчук В. В. Маніпуляція з кримінологічної точки зору як один із засобів учинення злочинів. *Юридична психологія та педагогіка*, 1, 2013. 219 с.



8. Лазарович М. В., Гончарук-Чолач Т. В., Докаш О. Ю., Штучний інтелект у політичних маніпуляціях та трансформація виборчої культури. *Науковий журнал «Політікус». Політична культура та ідеологія*. Випуск 1. 2025. 131–135 с.

9. Міхненко А. М., Месюк М. П. Владні інститути та громадянське суспільство: діалог чи маніпуляція суспільною свідомістю? *Вісник Національної академії державного управління при Президентові України*, 2, 2009. 5–12 с.

10. Медійна та інформаційна грамотність кожного і для всіх// <https://pon.org.ua/novyny/8281-medyna-ta-nformacynagramotnst-kozhnogo-dlya-vsh.html>.

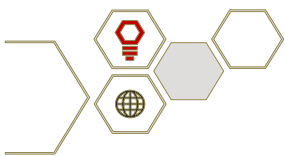
11. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки, затверджений розпорядженням Кабінету Міністрів України від 09.05.2025 за № 457-р. <https://zakon.rada.gov.ua/go/l545004>.

12. Регламент Європейського Парламенту та Ради (ЄС) 2024/1689 від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту та вносить зміни до Регламентів (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 та (ЄС) 2019/2144 та Директив 2014/90/ЄС, (ЄС) 2016/797 та (ЄС) 2020/1828 (Закон про штучний інтелект). <http://data.europa.eu/eli/reg/2024/1689/oj>.

13. Ферг'юсон Н. Приреченість: політика і катастрофи. Пер. Катерини Диса. К.: Наш Формат, 2022. 496 с.

14. Шевчук М. О. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2024. 160–166 с. DOI <https://doi.org/10.32782/2408-9257-2024-6-25>.

15. Artificial Intelligence Act. 2024. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.



16. Bentzen N., Chahri S. Members' Research Service PE 762.416. Online information manipulation and information integrity EPRS| European Parliamentary Research Service. 2024. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI\(2024\)_762416_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI(2024)_762416_EN.pdf).

17. Digital Services Act (DSA)|Updates, Compliance. 2022. <https://www.eu-digital-services-act.com/>.

18. Digital Markets Act, DMA. 2022. https://digital-markets-act.ec.europa.eu/index_en.

19. Hook K., Verdeja E. Social Media Misinformation and the Prevention of Political Instability and Mass Atrocities. 2022. <https://www.stimson.org/2022/social-media-misinformation-and-the-prevention-of-political-instability-and-mass-atrocities/>.

20. Measuring the Information Society Report 2018. Volume 1. URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx>.

21. Peters U. Algorithmic political bias in artificial intelligence systems. *Philosophy & Technology*. 2022. T. 35, № 2. URL: <https://link.springer.com/content/pdf/10.1007/s13347-022-00512-8.pdf>.

22. Policy Department for External Relations Directorate General for External Policies of the Union PE. 2021. The impact of disinformation on democratic processes and human rights in the world European Parliament coordinator. [https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU\(2021\)653635](https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653635).