Інформаційне право

УДК 342.7:004.8:32(477)

DOI https://doi.org/10.5281/zenodo.18470007

Штучний інтелект у публічному управлінні: загрози та можливості для демократичної участі

Косілова О. І.,
д.ю.н., доцент, професор кафедри міжнародного права та права ЄС
Державний податковий університет, Україна,
https://orcid.org/0000-0002-5574-3771

Федірко І. П.,
кандидат філософських наук, доцент, доцент кафедри політології
Київського національного університету імені Тараса Шевченка,
Україна, https://orcid.org/0000-0003-4626-512X

Прийнято: 10.01.2026 | Опубліковано: 30.01.2026

Анотація. Мета. Стаття має на меті дослідити вплив впровадження технологій штучного інтелекту (ШІ) на реалізацію політичних прав і свобод людини і громадянина в умовах цифровізації державного управління в Україні. Автор аналізує потенційні переваги та ризики, що виникають на перетині технологічного прогресу, демократичного врядування та захисту прав людини.

Методи. У дослідженні застосовано міждисциплінарний підхід, який охоплює порівняльний аналіз, структурно-функціональний метод, нормативно-правовий аналіз, а також елементи прогностичного методу. Окрему увагу приділено аналізу чинного законодавства України,

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

європейських директив і міжнародних стандартів у сфері прав людини та цифрових технологій.

Результати. У статті виявлено, що хоча технології штучного інтелекту відкривають нові можливості для демократизації суспільства — наприклад, шляхом електронного голосування, цифрової участі громадян та автоматизації публічних сервісів — вони також несуть суттєві ризики. Серед них — порушення приватності, маніпулювання громадською думкою через мікротаргетинг, дискримінація, заснована на алгоритмічних упередженнях, та можливість авторитарного контролю над інформаційним простором. Проаналізовано практики різних країн (зокрема Естонії, США, Швейцарії), а також окреслено стан законодавства в Україні, зокрема у сфері кібербезпеки, захисту персональних даних та інформаційної політики.

Висновки. Автор приходить до висновку, що впровадження ШІ в політичну сферу вимагає чітких етичних і правових обмежень, забезпечення прозорості алгоритмів, незалежного моніторингу використання таких технологій у публічному управлінні, а також активного розвитку цифрової грамотності населення. Необхідним є формування національної стратегії етичного та безпечного застосування ШІ, гармонізація українського законодавства з європейськими стандартами, а також запровадження пілотних проєктів із використання ШІ в політичному процесі — за умови дотримання прав людини та принципів верховенства права.

Ключові слова: штучний інтелект, політичні права, свободи громадян, цифровізація, вибори, кібербезпека, алгоритмічна прозорість, цифрове врядування, дезінформація.

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

The impact of artificial intelligence on the realization of political rights and freedoms of the individual and citizen in Ukraine

Kosilova O. I.,
Doctor of Law, Associate Professor,
Professor at the Department of International Law and EU Law
State Tax University, Ukraine,
https://orcid.org/0000-0002-5574-3771

Fedirko I. P.,
PhD in Philosophy, Associate Professor,
Associate Professor at the Department of Political Science
Taras Shevchenko National University of Kyiv, Ukraine,
https://orcid.org/0000-0003-4626-512X

Abstract. **Purpose.** This article aims to explore the impact of the implementation of artificial intelligence (AI) technologies on the realization of political rights and freedoms of individuals and citizens within the context of Ukraine's digital transformation of public governance. The author analyzes the potential benefits and risks arising at the intersection of technological progress, democratic governance, and human rights protection.

Methods. The research applies an interdisciplinary approach, including comparative analysis, structural-functional method, legal-normative analysis, and elements of foresight methodology. Special attention is given to the analysis of current Ukrainian legislation, relevant European directives, and international human rights and digital governance standards.

Results. The article identifies that while AI technologies offer new opportunities for enhancing democratic processes—such as electronic voting, digital civic participation, and automation of public services—they also pose significant risks. These include violations of privacy, manipulation of public opinion through

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

microtargeting, discrimination based on algorithmic bias, and the potential for authoritarian control over the information space. The article analyzes relevant international practices (notably in Estonia, the United States, and Switzerland) and outlines the current state of Ukrainian legislation in the fields of cybersecurity, data protection, and information policy.

Conclusions. The study concludes that the integration of AI into the political domain requires clear ethical and legal safeguards, algorithmic transparency, independent oversight of AI applications in governance, and a strong emphasis on digital literacy among citizens. It is essential to develop a national strategy for the ethical and secure use of AI, harmonize Ukrainian legislation with European standards, and launch pilot projects for AI use in political processes—under strict compliance with human rights and the rule of law.

Keywords: artificial intelligence, political rights, civil liberties, digitalization, elections, cybersecurity, algorithmic transparency, digital governance, disinformation.

Постановка проблеми. У сучасному світі, що стрімко змінюється під впливом цифрових технологій, штучний інтелект (ШІ) активно проникає в політичну сферу. Це відкриває нові можливості для врядування, участі громадян, виборчих процесів і електронної демократії. Водночас використання ШІ супроводжується викликами, які впливають на реалізацію політичних прав і свобод.

Особливої актуальності це набуває для України, яка в умовах воєнного стану та цифрових реформ стикається з кібератаками, маніпуляціями в інформаційному просторі та недостатнім правовим регулюванням технологій. У таких обставинах важливо оцінити відповідність впровадження ШІ принципам демократії, прав людини та верховенства права.

Цифрова трансформація розширює зміст політичних прав: це не лише вибори, а й постійна цифрова взаємодія з владою. Запропонований

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

структурований підхід (технічні, правові, етичні, інституційні загрози) дозволяє комплексно аналізувати виклики цифрового середовища.

Отже, використання ШІ в політиці потребує глибокого аналізу його потенціалу й ризиків — від захисту персональних даних до забезпечення недискримінації та чесних виборів. Необхідно сформувати збалансований підхід, який дозволить одночасно впроваджувати інновації та гарантувати дотримання прав і свобод громадян.

Аналіз останніх досліджень і публікацій.

Упродовж останніх років спостерігається інтенсивне зростання академічного інтересу до впливу штучного інтелекту (ШІ) на демократичні процеси, політичні права та цифрове врядування. Сучасні дослідження демонструють як високий потенціал ШІ для оптимізації державного управління, так і суттєві ризики, пов’язані з порушенням прав людини, приватності та нерівного доступу до цифрових ресурсів.

Науковці, як-от Г. Прайс, С. Фенацці, Ів-Марі Дубле, акцентують увагу на потребі в етичному врегулюванні алгоритмів, прозорості в ухваленні рішень та запобіганні дискримінації. Ці праці формують основу для глобального дискурсу про ризики автоматизованого прийняття рішень у політичному просторі. Зокрема**, П. Таддео та Л. Флоріді** наголошують, що без належного контролю, ШІ може підривати демократичні інститути, особливо у сферах е-голосування та політичної реклами.

На практичному рівні, в Естонії, Швейцарії та США вже імплементовані ШІ-рішення в електронну демократію, що дає емпіричну базу для аналізу як переваг, так і викликів — таких як кіберзагрози чи алгоритмічна упередженість. У звітах Центру досліджень ЄС (2020–2023), зокрема в аналізах GDPR та Digital Services Act, окреслено критичну потребу у забезпеченні контролю за використанням персональних даних у виборчих процесах.

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

В українському контексті дослідження зосереджуються переважно на цифровізації та електронному врядуванні (С. Цяпа, І. Караваєв, А. Ярова, Є. Дорожко, С. Корнєєва), проте без глибокого аналізу впливу ШІ саме на реалізацію політичних прав — участі у виборах, доступу до достовірної інформації, рівності у політичній комунікації. Така аналітична прогалина особливо помітна на тлі глобального тренду інтеграції ШІ в політичне управління.

Недостатньо розробленими залишаються питання: правового статусу ШІ в політичних процесах; відповідальності за рішення, ухвалені системами ШІ; захисту від дезінформації, створеної алгоритмами.

Зазначимо, що у «Концепції розвитку ШІ в Україні» (2020) і «Стратегії інформаційної безпеки» (2021) ці аспекти задекларовані, однак без розгорнутої деталізації механізмів захисту політичних прав у цифровому середовищі. Наявні дослідження, переважно описові, потребують доповнення системним аналізом новітніх загроз — зокрема глибинних фейків (deepfakes), політичного мікротаргетингу, а також етичних аспектів алгоритмічного управління громадською думкою.

Таким чином, подальші дослідження в Україні мають зосередитись на:

- ✓ формуванні етично-правової рамки впровадження ШІ в політичні процеси;
- ✓ адаптації законодавства України до міжнародних стандартів (GDPR, Council of Europe AI guidelines);
- ✓ розробленні механізмів запобігання маніпуляціям політичною поведінкою через ШІ.

Формулювання цілей статті (постановка завдання)

Метою цієї статті є комплексне дослідження впливу впровадження технологій штучного інтелекту на реалізацію політичних прав і свобод людини і громадянина в Україні в умовах цифрової трансформації державного управління. Автор прагне проаналізувати як позитивний потенціал ШІ для

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

підвищення ефективності демократичних процесів, так і загрози, що постають перед політичними правами внаслідок його неконтрольованого або непрозорого застосування.

Виклад основного матеріалу дослідження. Процес цифровізації глибоко впливає на політичні права та свободи, створюючи як нові можливості для їх реалізації, так і значні виклики. Зокрема, це стосується захисту персональних даних, боротьби з дезінформацією, забезпечення кібербезпеки виборчих процесів та рівного доступу до політичної інформації. Штучний інтелект дозволяє практично повністю виключити людський фактор з процесів забезпечення захисту інформації та залишає лише допоміжні функції моніторингу та корекції.

У зв'язку з цим штучний інтелект є технологією майбутнього. Штучний інтелект та його технології відкривають нові горизонти в епоху цифровізації та розпочинають активно використовуються у цивільній та військовій сферах. За оцінками експертів, очікується, що завдяки впровадженню таких рішень зростання світової економіки у 2024 році дорівнюватиме $1 трлн [1, с.52].

З іншого боку, розвиток технологій ШІ обумовлює виникнення загроз правам і свободам громадян. Зокрема, загрозу становлять дезінформаційні кампанії з використанням ШІ (deepfakes, бот-мережі), що здатні маніпулювати політичною поведінкою громадян, а недостатній рівень інформаційної гігієни та державного реагування може призвести до ерозії легітимності демократичних процедур.

Розвиток технології ШІ призводить до зміни статусу людини в суспільстві, тому використання технології ШІ має поважати основні права та свободи людини та громадянина, особливо трудові права (оскільки існує «ефект заміщення»), й таким чином викликає появу соціальних проблем, та проблем пов'язаних з реалізацією окремих прав та свобод. У зв'язку з цим застосування технологій ШІ в соціально-економічній та управлінських сферах має бути зважене та контрольоване громадськістю та органами державної

 ISSN: 3041-2110

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

влади. У зв'язку з цим постає питання про правове регулювання цих процесів в Україні, де національне законодавство має адаптуватися до викликів цифрової епохи. Інтеграція України до європейської спільноти, зокрема до Ради Європи засвідчила прийняття Україною низки міжнародно-правових зобов’язань, насамперед, – повага та захист до прав людини. Серед зобов’язань, взятих перед Радою Європи, визначальною є ратифікація Україною Конвенції про захист прав людини та основоположних свобод у 1997 році [2] та пов’язану з нею визнання юрисдикції Європейського суду з прав людини. Питання, пов'язані з використанням штучного інтелекту (далі ШІ), повинні регулюватися відповідно до норм міжнародних договорів і конвенцій, ратифікованих більшістю європейських держав. Зокрема, відповідно до спеціалізованих міжнародних угод у сфері розвитку ШІ: Конвенції Ради Європи про кіберзлочинність, також відомої як Будапештська конвенція [3]; Європейська етична хартія щодо використання штучного інтелекту в судових системах та їхньому середовищі, Загальний регламент захисту даних[4].

Зростання обсягів обробки персональних даних створює серйозні загрози для політичних прав і свобод. Сучасні технології дають змогу збирати великі масиви інформації про громадян, зокрема їхні політичні уподобання, що активно використовується для мікротаргетингу під час виборчих кампаній. Це може впливати на політичний вибір громадян і спотворювати демократичні процеси. Відомим прикладом є скандал із Cambridge Analytica, коли дані мільйонів користувачів Facebook були використані для маніпуляцій у США та Великій Британії.

Недостатній захист персональних даних підвищує ризики витоків і зловживань. Тому одним з основних викликів цифровізації є забезпечення їхньої безпеки та недопущення несанкціонованого використання. Окрім цього, цифрові технології можуть використовуватися для обмеження політичних

 ISSN: 3041-2110

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

прав — наприклад, через цензуру або закони про кібербезпеку, які іноді застосовують для придушення свободи слова.

Наприклад, у таких країнах, як Китай або росія, цифрові технології використовуються для блокування опозиційних сайтів, соціальних мереж або платформ, де громадяни можуть висловлювати критику влади. Це обмеження загрожує принципам демократичного суспільства та сприяє створенню авторитарних режимів, які використовують цифрові інструменти для контролю над населенням.

Згідно із положеннями чинного законодавства штучний інтелект – організована сукупність інформаційних технологій, із застосуванням яких можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [1, с.57].

Попри очевидні переваги використання ШІ, необхідно враховувати і потенційні загрози для прав і свобод людини. Ще у 2012 році філософ Х'ю Прайс у статті «Штучний інтелект: чи зможемо ми утримати його в коробці?» наголошував на необхідності сприймати ШІ як реальну загрозу, а не наукову фантастику. Він підкреслював, що штучний інтелект, на відміну від людини, не має еволюційної мотивації поділяти людські цінності — як-от любов, щастя чи навіть виживання. Машини можуть бути просто байдужими до людства, що потенційно призведе до катастрофічних наслідків [6].

Використання штучного інтелекту ставить під загрозу низку прав людини, закріплених у міжнародних документах, зокрема право на приватність, свободу вираження поглядів, недискримінацію, свободу пересування, чесні вибори та справедливий суд. Україна активно долучається до правового врегулювання ШІ, прагнучи інтегруватися у глобальний ринок

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

інновацій і використовує досвід таких країн, як Естонія, на шляху до створення «електронної держави». У 2020 році було схвалено Концепцію розвитку ШІ, що передбачає його впровадження в ключові сектори — економіку, публічне управління, кібербезпеку, правосуддя тощо. Мета документа — підвищити ефективність управління та задовольнити права громадян шляхом розвитку конкурентоспроможної цифрової економіки [7].

Концепція розвитку ШІ приділяє особливу увагу сфері кібербезпеки. Законодавство України визначає захист комунікаційних, інформаційних і технологічних систем, зокрема критичної інфраструктури, як пріоритет під час розвитку ШІ. Тривалий час в Україні не існувало чіткого правового регулювання інформаційної та кібербезпеки. Першим кроком у цьому напрямі став законопроєкт «Про засади інформаційної безпеки України» [8]. Основною вимогою є надійний захист персональних даних, їх обробка за згодою особи, з правом на доступ і виправлення інформації.

Указом Президента №685/2021 введено в дію Стратегію інформаційної безпеки, яка визначає основні терміни, загрози та виклики у цій сфері [9]. Стратегія наголошує на ризиках, пов’язаних із низьким рівнем інформаційної культури та медіаграмотності, що робить суспільство вразливим до деструктивних інформаційних впливів, зокрема під час воєнного стану. Саме тому критично важливим є розвиток навичок аналізу інформації та доступ до перевірених джерел.

На нашу думку, технології ШІ повинні насамперед захищати право людини на гідність — базове й фундаментальне право, порушення якого означає посягання на всі інші права. ШІ трансформує структуру правовідносин, створюючи модель «людина-машина», що зумовлює потребу у врегулюванні правового статусу інтелектуальних систем, відповідальності за їхні дії, а також захисту прав інтелектуальної власності, створеної роботами. Інтеграція ШІ має бути безпечною для людини, з урахуванням кожного з основоположних прав і особливо — права на гідність. Однією з найбільших

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

проблем є порушення конфіденційності та втручання в приватне життя в цифровому середовищі.

З огляду на різний рівень соціально-економічного розвитку країн, важливо розробити універсальні правила використання ШІ з урахуванням принципу непорушності прав людини. Основні права є невідчужуваними та можуть обмежуватись лише в особливому порядку. Преамбула до Конвенції зазначає, що права найкраще реалізуються в умовах ефективної політичної демократії. Зокрема, ст. 3 Протоколу № 1 гарантує право голосу та участі у вільних виборах на основі загального виборчого права [10].

Відповідно до статті 25 Міжнародного пакту про громадянські та політичні права, кожен громадянин має право без дискримінації брати участь у державних справах. Європейський суд з прав людини наголошує, що регулярні вибори є основою демократії та мають супроводжуватися свободою вираження, рівним ставленням до виборців та правом бути обраним.

Запровадження електронного голосування в Україні відкриває нові можливості для участі громадян у виборах та референдумах. ШІ може сприяти автоматизації реєстрації, підрахунку голосів, моніторингу порушень та інформуванню виборців. Такі технології вже активно застосовуються в США, Канаді, Бразилії, Індії, Естонії, Південній Кореї. У Великобританії, Німеччині, Франції, Іспанії, Португалії, Італії, Норвегії, Швейцарії, Казахстані, Японії, Китаї проводяться експерименти з його використання [11]

Закон України «Про всеукраїнський референдум» вже передбачає можливість е-голосування (ст. 6, 13, 23) [14], однак для впровадження необхідні підзаконні акти, технічний регламент та ефективні механізми забезпечення прозорості, безпеки та доступності цього процесу.

Україна лише розпочинає впровадження електронного голосування, поки що без належної законодавчої бази. Проєкт постанови, поданий нардепом О.І. Тищенком, залишається нереалізованим. Із 2002 року в ЦВК функціонує система «Вибори» для оперативного визначення результатів. Міністерство

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

цифрової трансформації запустило пілотний проєкт Smart-ID ПриватБанку — електронний підпис на SIM-карті, що наближає до е-голосування, але не гарантує достатнього захисту.

До основних ризиків е-голосування належать: можливість фальсифікацій через втручання в систему; ризик витоку даних і порушення таємниці голосування; недовіра до прозорості та надійності технологій; високий ризик кібератак, особливо в умовах війни.

З 2015 року в Україні діє система «електронних звернень» — інструмент електронної демократії, що дозволяє подання скарг, пропозицій і петицій. Відповідно до Закону України «Про звернення громадян» [19], електронна петиція — форма колективного звернення. Перша успішна петиція стосувалась права на захист. У процесі було виявлено використання ботів для накрутки підписів. У 2018 році за допомогою електронних платформ було проведено понад 1000 консультацій [21].

На сьогодні петиції можна подавати через сайти Президента, Верховної Ради, Кабміну та місцевих рад.

На сучасному етапі розвитку цифрових технологій немає простого пояснення того, що таке ШІ, якщо припустити, що він тлумачиться як термін, який використовується для опису машин, які виконують людські когнітивні функції, такі як навчання, розуміння, міркування або взаємодія, оскільки її можна розглядати і як предмет інформатики, і як правову категорію, зокрема, об’єкт цивільного права. Не менш важливими для правового обговорення є питання прийняття рішень ШІ та настання юридичної відповідальності за шкоду, заподіяну ШІ, а також права інтелектуальної власності на твори як інтелектуальну власність, створені за участю штучного інтелекту.

Виникнення загроз правам людини в тій чи іншій формі при використанні ШІ потребує пошуку шляхів подолання ризиків і загроз правам людини та належного функціонування правозахисного та правовідновлювального механізму. Важливо не перебільшувати переваги ШІ,

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

збалансувати переваги технологій ШІ, такі як точність і швидкість прийняття рішень, і етичність і емпатію, якості, якими може володіти лише людина при прийнятті рішень. Тому ми підтримуємо точку зору, що остаточне право прийняття рішень має належати виключно людині, яка перевіряє та контролює роботу ШІ. Однак впровадження ШІ у політичну сферу супроводжується низкою ризиків. Одним із найбільш значущих є маніпуляція громадською думкою. Завдяки алгоритмам таргетування, ШІ може використовуватися для створення персоналізованої політичної реклами, яка впливає на електоральні настрої. Особливе занепокоєння викликають технології створення глибоких фейків, які здатні поширювати дезінформацію, підриваючи довіру до демократичних інститутів. Іншим важливим викликом є забезпечення рівності у використанні ШІ. Алгоритмічна дискримінація, що виникає внаслідок вбудованих упереджень у моделях штучного інтелекту, може призводити до нерівного ставлення до окремих соціальних груп, порушуючи принцип рівності політичних прав.

Питання приватності також є актуальним у контексті застосування ШІ. Збір і аналіз персональних даних виборців викликає занепокоєння щодо їх безпеки та можливого зловживання інформацією. Особливо це важливо в умовах воєнного стану, коли забезпечення кібербезпеки набуває критичного значення. Використання ШІ може допомогти захистити виборчу інфраструктуру від кіберзагроз, але водночас потребує ретельного регулювання. Україна має значний потенціал для впровадження ШІ у політичні процеси. Зокрема, доцільно створити незалежні моніторингові органи для забезпечення прозорості використання технологій, розробити освітні програми для підвищення цифрової грамотності громадян та запровадити пілотні проекти електронного голосування для громадян за кордоном. Це дозволить зміцнити довіру громадян до демократичних процедур і забезпечити їхню більшу участь у політичному житті (див. таблиця 1).

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Таблиця1.

Застосування ШІ у публічному управлінні

Сфера застосування ШІ	**Політичне право**	**Основні ризики**	**Механізми захисту**
Електронні вибори та адміністрування виборів	Право обирати і бути обраним	Маніпуляції результатами, кібератаки, втручання в алгоритми підрахунку	Аудит алгоритмів, кіберзахист, міжнародні стандарти спостереження
Цифрові платформи політичної участі	Право на участь в управлінні державними справами	Алгоритмічне викривлення порядку денного, боти	Прозорість алгоритмів, модерація, незалежний нагляд
Політична онлайн-реклама	Свобода політичного волевиявлення	Мікротаргетинг, маніпуляція свідомістю	Обмеження таргетингу, публічні реєстри реклами
Аналітичні системи прийняття рішень	Право на рівний доступ до публічної служби	Алгоритмічна упередженість	Людський контроль, антидискримінаційні тести
Інформаційна безпека держави	Право на достовірну інформацію	Дезінформація, deepfakes	Фактчекінг, AI-детекція фейків, медіаграмотність

Джерело: власна розробка авторів (Косілова О. І., Федірко І. П.)

Висновки. Підсумовуючи, ШІ є потужним інструментом для модернізації політичних процесів, підвищення прозорості виборчих процедур та забезпечення ефективності демократичних інститутів. Проте його використання вимагає чітких правових рамок та етичного підходу. Забезпечення прав людини, приватності та прозорості є ключовими принципами, які повинні лягти в основу інтеграції ШІ у політичну сферу. Належне регулювання та активна взаємодія з міжнародними партнерами сприятимуть збереженню демократичних цінностей і довіри громадян до державних інституцій.

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

На нашу думку, необхідно створити глобальне (обов'язкове) міжнародне законодавство щодо розробки та впровадження штучного інтелекту, зокрема для запобігання його нелегальному, тобто нецивілізаційному, використанню. Крім того, уряди та компанії, які використовують технологію штучного інтелекту, повинні знати про недосконаліть даних, на яких базується ця технологія, і подбати про запобігання дискримінації та порушенням прав людини. В Україні необхідно врегулювати діяльність у сфері ШІ, відповідно до міжнародних стандартів захисту прав людини, розробити власну національну стратегію формування засад етичного, соціального та нормативного застосування ШІ. Держава має створити такі умови, за яких розвиток ШІ не матиме негативного впливу на національну безпеку та дотримання Україною своїх зобов'язань за міжнародними договорами та угодами.

Закон України «Про захист персональних даних» хоча й забезпечує базові вимоги щодо обробки та зберігання даних, але не враховує специфіку сучасної цифровізації. Зокрема, відсутність чітких регуляцій щодо використання персональних даних під час політичних кампаній (мікротаргетинг, аналіз даних громадян) створює можливості для зловживань, подібних до випадку Cambridge Analytica. Важливо вдосконалити механізми захисту персональних даних, взявши за основу міжнародні стандарти, такі як GDPR, і створити чіткі правила використання політичними суб'єктами персональних даних виборців.

Попри існування Закону «Про основні засади забезпечення кібербезпеки», рівень захисту виборчої інфраструктури залишається недостатнім. Кібератаки на Центральну виборчу комісію під час виборів свідчать про необхідність посилення захисних заходів та впровадження сучасних технологічних рішень. Додатково, українське законодавство поки не пропонує належного захисту для цифрових платформ, які використовуються в

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

політичних кампаніях, а також не забезпечує чіткого регулювання кіберзагроз у межах виборчого процесу.

Одним із найбільших викликів є боротьба з дезінформацією, яка може підривати політичні процеси та впливати на виборчі результати. Законодавство щодо дезінформації в Україні перебуває на стадії розробки, але ініціативи, такі як законопроєкт «Про дезінформацію», викликали значні суперечки. Важливо знайти баланс між забезпеченням свободи слова та боротьбою з фейковими новинами, створивши механізми відповідальності за поширення дезінформації без порушення демократичних прав громадян.

Законодавство України недостатньо враховує сучасні цифрові виклики, пов'язані з політичними правами, особливо у контексті онлайн-комунікацій, цифрових платформ і соціальних мереж. Виборчі кампанії активно використовують інтернет-ресурси, проте їхній вплив на політичні процеси поки не врегульований належним чином. Наприклад, відсутні чіткі механізми контролю за використанням політичної реклами у соціальних мережах. Хоча Україна робить кроки до інтеграції міжнародних стандартів у своє законодавство (зокрема, через адаптацію до GDPR), все ще існують значні прогалини у гармонізації з міжнародними вимогами. Це стосується як захисту персональних даних, так і забезпечення прав на приватність у цифровому просторі. Аналіз українського законодавства показав, що в умовах стрімкої цифровізації існують певні прогалини, які потребують вдосконалення. Серед найбільших викликів — захист персональних даних під час виборів, протидія дезінформації та забезпечення кібербезпеки критичної інфраструктури. Пропоновані зміни до виборчого кодексу, законів "Про захист персональних даних", "Про звернення громадян", "Про інформацію" та "Про основні засади забезпечення кібербезпеки" покликані забезпечити ефективний захист політичних прав і свобод громадян в умовах цифровізації. Важливо також забезпечити належну імплементацію цих норм на практиці та посилити контроль за їхнім дотриманням.

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Список використаних джерел

1. Цяпа С. М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах. Інформація і право. № 2(37)/2021. DOI: https://doi.org/10.37750/2616-6798.2021.2(37).238336. С. 51–59.

2. Про захист прав людини і основоположних свобод: Конвенція РЄ від 1950 р.: Закон України від 17.07.1997 № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 02.11.2025).

3. Конвенція про кіберзлочинність. Ратифікація від 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 09.12.2025).

4. Що таке GDPR? Новий закон ЄС про захист даних. GDPR.eu, 2020. URL: https://gdpr.eu/what-is-gdpr/ (дата звернення: 05.08.2025).

5. Дубле Ів-Марі. Дезінформація та виборчі кампанії / пер. укр. мовою за підтримки проєкту Ради Європи «Підтримка прозорості, інклюзивності та чесності виборчої практики в Україні». Страсбург: Рада Європи, 2020. 33 с.

6. Прайс Г., Таллінн Дж. Штучний інтелект – чи можемо ми тримати його в коробці? URL: https://theconversation.com/artificial-intelligence-can-we-keep-it-in-the-box-8541 (дата звернення: 05.06.2025).

7. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 10.10.2025).

8. Про засади інформаційної безпеки України: проєкт Закону України від 28.05.2014. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123 (дата звернення: 10.12.2025).

9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 10.10.2025).

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

10. Протокол до Конвенції про захист прав людини і основоположних свобод від 20 березня 1952 р. URL: https://zakon.rada.gov.ua/laws/show/994_535#Text (дата звернення: 19.06.2023).

11. Електронні виборчі системи: процедури голосування та матеріальні засоби. Міжнародний досвід. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28966.pdf (дата звернення: 17.10.2025).

12. Караваєв І. Онлайн-вибори в Україні: реалії та перспективи. Юридична газета онлайн. 28 травня 2020. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/vibori-onlayn-v-ukrayini-realiyi-ta-perspektivi.html (дата звернення: 02.11.2025).

13. Ярова А. Електронні вибори в Естонії: досвід для України. Сутність та перспективи впровадження електронної демократії в Україні: матеріали міжнар. наук. конф. Вінниця: ВНТУ, 2017. URL: https://conferences.vntu.edu.ua/index.php/e-democracy/e-democracy2016/paper/viewFile/1694/1384 (дата звернення: 19.10.2025).

14. Про всеукраїнський референдум: Закон України № 1135-IX від 26.01.2021. URL: https://zakon.rada.gov.ua/laws/show/1135-20#Text (дата звернення: 19.12.2025).

15. Бюлетень Центральної виборчої комісії. № 3(27). 2013. URL: https://www.cvk.gov.ua/wp-content/uploads/2020/05/2013_3_visnik_title.cvk_.pdf (дата звернення: 02.11.2025).

16. Савчук О. Електронні виборчі системи: процедури голосування та логістика: міжнародний досвід. Інформаційний довідник. Європейський інформаційно-дослідницький центр, 2016. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28966.pdf (дата звернення: 02.11.2025).

17. Фенацці С. Швейцарська пряма демократія в епоху цифрових технологій. URL: https://www.swissinfo.ch (дата звернення: 02.11.2025).

 ISSN: 3041-2110

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

18. Про звернення громадян: Закон України від 02.10.1996 № 393/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text (дата звернення: 02.11.2025).

19. Дорожко Є. Електронні петиції в Україні. Громадський простір. URL: https://www.prostir.ua/?library=elektronni-petytsiji-v-ukrajini (дата звернення: 02.11.2025).

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license