***Арделян Іван Сергійович****, аспірант*

*Київський університет культури, м.Київ*

***Науковий керівник: Гаврилюк Алла Михайлівна****,*

*Доктор наук з державного управління, професор,*

*Київський національний університет культури і мистецтв, м.Київ*

**ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ У ПУБЛІЧНОМУ АДМІНІСТРУВАННІ**

Багато різних аспектів соціального розвитку відіграють важливу роль у державному управлінні. Ці теми є важливими тенденціями з навколишнього середовища, такими як глобалізація та її проблеми, які характеризують інформаційну революцію сучасного суспільства. Чимало значної ролі у свою чергу також відіграє військовий конфлікт. Зважаючи на це, на даному етапі необхідно розглянути нові методи та стратегії управління, що відповідають сучасним вимогам. Одним із останніх інструментів управління є штучний інтелект та машинне навчання, на якому український уряд зосереджується у встановленні нової політики та стандартів в освіті.

Багато проектів штучного інтелекту цінують взаємодію між академічними, приватними та державними установами. Мережі, в яких працюють урядовці, та ефективне використання їх знань мають вирішальне значення для успіху та інновацій [3, с.84]. Однак цій співпраці заважають конфіденційність і безпека обміну інформацією, відмінності в розумінні доступної інформації та недостатня координація між організаціями. Це вкрай важливо з точки зору безпеки під час обміну інформацією, що становить питання цілісності інформаційного простору та потенційного ризику особистої інформації [1].

Це питання слід розглядати в контексті зростання політичної та економічної напруженості, наприклад конкуренції між Сполученими Штатами та Китаєм і військового конфлікту з Росією. Ці виклики включають цифрове шпигунство, збільшення інформації та цифрового втручання, а також залежність від іноземних технологій та інфраструктури [3, с.84].

Але попит на технічну автономію не обмежується Європою. Будь-яка країна, яка перебуває у політичному конфлікті з сусідніми країнами, ворогами чи навіть країнами-союзниками, може бути стурбована послугами, які надають ці країни. Ця залежність може поставити уряд під загрозу, оскільки супротивники чи конкуренти, інші країни, можуть отримати доступ до серверів, на яких надаються державні служби, або блокувати трафік між цими службами, громадянами та підприємствами. Технічні рішення щодо зменшення залежності від іноземних гравців та інфраструктури обговорюються протягом тривалого часу, включаючи можливе відокремлення національних кордонів від глобальної інфраструктури Інтернету.

Хоча концепція цифрового суверенітету набула популярності в багатьох країнах, вона корениться в геополітичній напруженості, яка існувала в історії. Деякі країни розвинули інфраструктуру політичного тиску ще до концепції суверенітету та незалежності, а інші нещодавно почали думати про свою інфраструктуру з геополітичної точки зору. Дискусії про цифровий суверенітет і стратегічну автономію, заочно, обертаються переважно навколо понять взаємозалежності, суверенітету та контролю, хоча також враховуються юридичні аспекти суверенітету.

Поняття цифрового суверенітету, включаючи різні терміни, такі як кіберсуверенітет, технологічний суверенітет, суверенітет даних і цифровий суверенітет, є відкритим полем, якому часто бракує чіткого визначення. Кіберсуверенітет, який широко використовується Росією та Китаєм, зосереджується на контролі внутрішньої інформації. Ці країни хочуть контролювати все те, що виходить і виїжджає з країни, віддаючи перевагу безпеці даних над безпекою в Інтернеті [4, с.420].

Дебати щодо цифрового суверенітету в Європі та Європейському Союзі почалися після викриття Едварда Сноудена, який виявив, що Європа стала жертвою кібершпигунства, і загострилися в останні роки. Сьогоднішні дискусії зосереджені на необхідності позиції Європи/ЄС у геоекономічній та геополітичній конкуренції між США та Китаєм, необхідності зменшити залежність від великих технологічних компаній та Інтернету, а також зменшити залежність від європейського насіння/європейських матеріалів і ключові матеріали ланцюга поставок, такі як напівпровідники [2]. Ці дискусії відбуваються в контексті геополітичної напруженості та зростання кіберактивності в Інтернеті, включаючи дезінформацію (втручання у вибори), вандалізм і кіберзлочинність. У цих дебатах часто обговорюється технологічний суверенітет і цифровий суверенітет, зокрема технологічний суверенітет, заснований на інструментах.

Аргументи щодо суверенітету та цілісності даних зазвичай базуються на ідеї контролю та захисту даних, які важливі як в економічній, так і в політичній сферах. У контексті використання штучного інтелекту в обробці інформації, яка перетинає кордони національної інформації, існує загроза суверенітету країни через пряме втручання в процес прийняття рішень у сфері державного управління та надання адміністративних послуг. Наприклад, такі країни, як Нідерланди, Україна та Тайвань, наполегливо докладають зусиль, щоб зберегти контроль над своєю інформацією, зберігаючи велику частину державного контролю в межах своїх кордонів. Оскільки уряди цих країн прагнуть консолідувати дані, вони також стикаються з занепокоєнням щодо великої кількості американських провайдерів, які отримують їхні послуги, що може вплинути на незалежність їхньої інфраструктури.

Технологія машинного навчання продовжує цікавити багато державних установ через стрімкий розвиток за останні кілька десятиліть. Однак трансформація технологій у відчутні переваги для компаній і суспільства завдяки вдосконаленню корпоративного управління є обмеженою. Однією з головних перешкод для впровадження їх використання в державному секторі є брак процесорних потужностей.

Це означає не тільки наявність технічних навичок у розробці штучного інтелекту, таких як навички обробки даних і машинного навчання, але й загальне розуміння технологій і методів, необхідних для впровадження штучного інтелекту в державному управлінні. [3, с.85].

Хоча деякі держави зберігають більший суверенітет, ніж інші, жодна не може претендувати на повну незалежність, оскільки деякі покладаються на інфраструктуру, контрольовану політичними силами, з якими вони конкурують через Інтернет. Важливо розрізняти регіон і автономію, оскільки існує складний компроміс між ризиком і страхуванням. Через обставини, такі як загроза нападу або недостатній національний захист цифрової інфраструктури, уряди можуть вирішити захистити свій суверенітет, покладаючись на дружні та потужні іноземні продукти.

Використання власних алгоритмів і моделей машинного навчання дозволяє країні зменшити залежність від іноземних технологій і постачальників. Це особливо важливо в умовах глобальної конкуренції та кібервійн, коли технологічна автономія стає ключовим фактором національної безпеки.

Крім того, машинне навчання допомагає забезпечити кращий контроль над національними даними. Замість передачі даних до закордонних компаній, які можуть підпадати під юрисдикцію інших держав, уряди можуть використовувати власні технології для обробки і зберігання інформації. Це не лише підвищує безпеку, але й забезпечує дотримання національних стандартів і регуляцій щодо конфіденційності та захисту даних.

Наочним прикладом для нас, авжеж, буде сфера захисту інформаційного простору від дезінформації та пропаганди. Алгоритми машинного начання можуть аналізувати медійний контент, виявляючи фейкові новини та маніпулятивні матеріали, що дозволяє ефективніше протидіяти інформаційним атакам. Це особливо важливо в сучасному світі, де інформаційна безпека стає невід'ємною частиною національної безпеки.

Дискусія про те, боремося ми за більший цифровий суверенітет чи незалежність, триває. Країни повинні визначити свій підхід до цих ризиків у контексті переваг, які надають цифрові технології для кращого державного управління, потужного технологічного потенціалу та здатності надавати ефективні та економічно ефективні послуги. Важливо враховувати, що використання штучного інтелекту може відрізнятися залежно від потенціалу та можливостей кожної країни [3, с.82].

Отже, перспективи використання машинного навчання у публічному адмініструванні показують, що його впровадження може значно підвищити ефективність рішень у цій сфері. Автоматизація процесів за допомогою алгоритмів машинного навчання дозволяє здійснювати аналіз великої кількості даних швидко та точно, що сприяє зниженню витрат часу та ресурсів.

Також важливим є вдосконалення якості прийняття рішень завдяки здатності алгоритмів виявляти складні взаємозв'язки в даних, що можуть залишатися непоміченими людським аналізом. Це сприяє більш обґрунтованому прийняттю рішень та знижує ймовірність помилок через людський фактор.

Однак, існують виклики, пов'язані з етичними аспектами та конфіденційністю даних, які потребують уважного врахування та розробки відповідних заходів захисту. Впровадження машинного навчання потребує не лише технічної, але й правової та організаційної підготовки для забезпечення безпеки та ефективного використання цих технологій.

Таким чином, машинне навчання представляє значний потенціал для трансформації публічного адміністрування, забезпечуючи покращення у прийнятті рішень та оптимізації адміністративних процесів. Проте, успішна імплементація вимагає комплексного підходу до управління даними, захисту конфіденційності та вирішення етичних питань.

**Список використаних джерел:**

1. Результати всеукраїнського дослідження про перспективи ШІ в загальній середній освіті. Міністерство освіти і науки України, (2023), Опубліковано 20 грудня 2023 року, Режим доступу: https://mon.gov.ua/news/rezultati-vseukrainskogo-doslidzhennya-pro-perspektivi-shi-v-zagalniy-seredniy-osviti (Дата звернення: 04.07.2024).

2. Володимир Зеленський зустрівся з президентом корпорації Microsoft, (2021), 22 вересня 2021 року, Режим доступу: https://www.president.gov.ua/news/volodimir-zelenskij-zustrivsya-z-prezidentomkorporaciyi-mic-70761 (Дата звернення: 04.07.2024).

3. Терещенко В.М., Бугайов А.Д. Алгоритми машинного навчання у контексті великих даних. Штучний інтелект, 3, 2018. С. 80–86. Режим доступу: http://dspace.nbuv.gov.ua/handle/123456789/162446 (Дата звернення: 04.07.2024).

4. Tangi, L., van Noordt, C., & Rodriguez Müller, A. P., (2023), “The challenges of AI implementation in the public sector. An in-depth case studies analysis”, Proceedings of the 24th annual international conference on digital government research, pp. 414–422, Режим доступу: https://doi.org/10.1145/3598469.3598516 (Дата звернення: 04.07.2024).