

Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019).

Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2024. № 2.

DOI: <http://doi.org/10.32702/2307-2156.2024.2.7>

УДК 351/354:005.5

Н. О. Максименцева,

д. ю. н., доцент, доцент кафедри парламентаризму,

ННІ публічного управління та адміністрування КНУ імені Тараса Шевченка

ORCID ID: <https://orcid.org/0000-0001-7774-1948>

М. Г. Максименцев,

д. ю. н., заступник директора,

«Юридичне бюро «Альмега»

ORCID ID: <https://orcid.org/0000-0002-1173-9113>

**ШТУЧНИЙ ІНТЕЛЕКТ У ПУБЛІЧНОМУ УПРАВЛІННІ: ПЕРЕВАГИ
ЦИФРОВИХ ТЕХНОЛОГІЙ ТА ЗАГРОЗИ СУВЕРЕННОМУ
ІНФОРМАЦІЙНОМУ ПРОСТОРУ**

N. Maksimentseva,

*Doctor of Law, Associate Professor, Associate Professor of the Department of
Parliamentarism, Scientific Institute of Public Administration and Civil Service of
Taras Shevchenko National University of Kyiv*

M. Maksimentsev,

Doctor of Law, Deputy Director,

“Legal Bureau “Almega”

**ARTIFICIAL INTELLIGENCE IN PUBLIC ADMINISTRATION:
ADVANTAGES OF DIGITAL TECHNOLOGIES AND THREATS TO THE
SOVEREIGN INFORMATION SPACE**

Завдяки аналізу поточного використання технологій штучного інтелекту в державному управлінні за допомогою настільних досліджень та інтерв'ю з експертами ця стаття досліджує можливості штучного інтелекту в уряді та те, як це впливає на створення суспільної цінності за допомогою технологій штучного інтелекту. Такі ідеї зацікавляють політиків і державних службовців і керівників, інформуючи їх про різні чинники, необхідні для створення суспільної цінності, зокрема з точки зору внутрішніх можливостей. Ця стаття містить додаткову інформацію та простір для майбутніх досліджень, щоб глибше охарактеризувати вплив цих факторів, щоб забезпечити позитивний внесок технологій штучного інтелекту в державне належне врядування, публічне управління, яке їх впроваджує.

Поряд із проблематикою штучного інтелекту в публічному секторі державної влади і публічних послуг, автор також досліджує, якою мірою державні послуги і сфера публічного управління та обслуговування громадян різних країн транскордонно покладаються на інфраструктуру за межами їх власної юрисдикції, які включають країни в Азії, включаючи Тайвань, Європу, зокрема Україну, і Сполучене Королівство (Великобританію), яке є активним у цьому відношенні. Поєднуючи різні методи, ми визначаємо, де і як розміщені домени, а також мережеві шляхи, якими йде трафік громадян до них. Ми розкриваємо різні стратегії та ступені автономії, а також складні компроміси між різними ризиками для технічної автономії і інформаційного суверенітету, деякі з яких можуть бути більшими, ніж ризики, пов'язані із залежністю від іноземних постачальників і загрози інформаційно – технологічному суверенітету. Це включає в себе транснаціональних провайдерів, які використовуються всіма країнами та є орендарями трафіку та серверів в тій самій мережі, а також трафік між громадянами та урядами, який регулярно передає дані через міжнародні кордони у процесі адміністрування послуг або виконання інформаційно – оперованих засобами штучного інтелекту (ШІ) функцій публічного управління, адміністрування та

належного врядування на забезпечення суспільного блага чи надання послуг соціуму.

By analyzing the current use of artificial intelligence technologies in government through desk research and expert interviews, this paper explores the possibilities of artificial intelligence in governance and how this affects the creation of public value through artificial intelligence technologies. Such ideas are of interest to politicians and civil servants and managers, informing them about the various factors necessary for the creation of public value, in particular from the point of view of internal capabilities. This paper provides additional information and scope for future research to further characterize the impact of these factors in order to ensure that AI technologies make a positive contribution to public good and good governance, the public administration that implements them.

Along with the issues of artificial intelligence in the public sector of government and public services, the author also examines the extent to which public services and the sphere of public administration and service to citizens of different countries cross-border rely on infrastructure beyond their own jurisdiction, which include countries in Asia, including Taiwan, Europe, in particular Ukraine, and the United Kingdom of Great Britain, which is proactive in this regard. By combining various methods, we determine where and how the domains are located, as well as the network paths through which citizens' traffic goes to them. We reveal different strategies and degrees of autonomy, as well as complex trade-offs between various risks to technical autonomy and information sovereignty, some of which may be greater than the risks associated with dependence on foreign suppliers and threats to information technology sovereignty. This includes transnational providers that are used by all countries and are tenants of traffic and servers in the same network, as well as traffic between citizens and governments that regularly transfer data across international borders in the process of administering services or performing information-operated means of artificial intelligence (AI) functions of public

management, administration and proper governance to ensure the public good or provide services to the society.

Ключові слова: *публічне управління, адміністрування, врядування, інформаційні технології, штучний інтелект, інформаційний (цифровий) суверенітет.*

Key words: *public management, administration, governance, information technologies, artificial intelligence, information (digital) sovereignty.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Багато тенденцій і факторів суспільного розвитку впливають на публічне управління.

Вони відіграють важливу роль як зовнішні процеси для публічного управління середовищем, наприклад глобалізація та її проблеми, які характеризують перехід сучасного суспільства на інформаційну стадію розвитку.

Відповідні зміни та нові виклики, безумовно вносить війна. Зважаючи на це, необхідно розглянути нові форми та стратегії управління, які можуть задовольнити поточні вимоги до управління.

У числі найновіших інструментів управління варто виділити популярний штучний інтелект (ШІ), якому приділяє увагу уряд України при формуванні стратегій, стандартів нової освіти. В нещодавньому офіційному опитуванні 2023 року українських освітян всі вчителі, які були опитані, знали про сервіси штучного інтелекту. Водночас сім із десяти людей користувалися принаймні одним із них протягом останніх півроку. Загалом 76% вчителів, які були опитані, хоча б раз використовували ШІ, і половина з них мала позитивний досвід взаємодії. Усі вчителі вважають, що в найближчі роки освіта та публічні сфери будуть змінені штучним інтелектом [1].

Важливо дослідити та вивчити роботу штучного інтелекту, особливо щодо можливих застосовувань у сфері публічного управління. Президент України назвав розвиток цифровізації в Україні однією з стратегічних цілей удосконалення та активного залучення до сфери публічного управління. Це важливе та актуальне питання, як він зазначив під час однієї з офіційних зустрічей з керівництвом, зокрема, Microsoft у США [2]. При цьому, розвиток інформаційних технологій повинен сприяти сталому розвитку суспільства не створюючи загроз безпеці і цифровому простору країн, його інформаційному суверенітету (digital sovereignty, eng.). Лише за кілька років проблема «цифрового суверенітету» стала важливою проблемою безпеки для урядів у всьому світі, що відображає зростаюче занепокоєння щодо ризиків безпеки, пов'язаних із державними послугами, які залежать від іноземних постачальників послуг цифрової інфраструктури та маршрутів передачі і зберігання інформації.

Аналіз останніх досліджень і публікацій. Технології штучного інтелекту (ШІ) в публічному управлінні привертають все більше уваги через потенційні переваги, які вони можуть надати в покращенні діяльності уряду. Проте перетворення технологічних можливостей у конкретні суспільні цінності для установ сфери публічного управління все ще обмежені. Поява штучного інтелекту (ШІ) розглядається як нова зміна гри в секторі публічного управління та адміністрування. Очікування від штучного інтелекту стосуються використання інтелектуальних машин, щоб взяти на себе людські завдання та виконувати їх ефективніше та результативніше з відчутними результатами (Schiff, D. S., Schiff, K. J., Pierson, P) [3] та створювати суспільну цінність (Sun, T. Q., Medaglia, R.). Однак, створення суспільної цінності за допомогою технологій штучного інтелекту також вимагає від організацій запровадження додаткових змін, таких як організаційні чи культурні (Tangi, L., van Noordt, C., Rodriguez Müller A. P, [5] Misuraca, G. [6]), і ці зміни вимагають різноманітного набору ресурсів, від технологічних до людських і більше нематеріальних ресурсів, таких як відповідний набір навичок і

схильність до інновацій. Необхідні ресурси для впровадження штучного інтелекту називають можливостями штучного інтелекту, концептуалізованими та вимірними в попередніх дослідженнях (Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y., Niehaves, B. [7]). У вітчизняних джерелах ці питання вже були предметом дискусій у роботах О. В. Карпенко [8], Р. Р. Марутян [9], О. Сакаль, Ю.Л. Скляр, О.М. Ткаленко, А.О. Макаренко, О.В. Полоневич [10], В.М. Третьак, Ю. І. Тюрі [11] та ін.

Існують досить недосліджені, але прогресивні та більш технологічно детерміновані погляди на технологічні зміни, які припускають, що штучний інтелект буде суспільною зміною «сам по собі», нехтуючи інституційною динамікою, яка сприяє або перешкоджає розвитку його сприйняття (M.J. Ahn, Y.-C. Chen [12]) або ті, які стверджують, що штучний інтелект автоматично принесе користь (або шкоду) суспільству, не враховуючи складність соціально-технічної взаємодії штучного інтелекту та державних установ, за допомогою яких це відбувається (A. Sanina, A. Balashov, M. Rubtcova [13]). Ці погляди пропонують мінімальний контекст, який лише дає поверховий погляд на процес, ігноруючи внутрішні можливості організації, що призводить до низького використання технології (I.Mergel, H.Dickinson, J.Stenvall, M.Gasco [14]). Сьогодні штучний інтелект більше не можна вважати новою технологією, а радше набором більш зрілих технологій, які вже використовуються в кількох державних секторах публічного управління, а також у багатьох випадках вже випробуваний через пілотні проекти, яким не вдається розширити масштаби, обмежуючи вплив (R. Medaglia, I. Tangi [15]) штучного інтелекту на прогрес і розвиток публічного управління та не відповідають очікуванням щодо створення суспільної цінності. Ця відсутність ефекту в основному зумовлена контекстуальними, умовно – формальними застереженнями, міркуваннями безпеки, а не лише технологічними факторами (P. Mikalef, M. Gupta [16]).

Формування цілей (постановка завдання). Досі залишається багато невідомого про процеси розробки та реалізації ініціатив ШІ, які ШІ мають можливості для державних служб, і як це впливає на вибір щодо цього розвитку та результати таких ініціатив. Таким чином, це дослідження спрямоване на дослідження динаміки того, як різні компоненти можливостей ШІ впливають на розробку та розгортання ШІ в публічному управлінні. Крім того, це дослідження має на меті зрозуміти, що таке можливості штучного інтелекту, як їх можна отримати та як це сприяє створенню цінності за допомогою технологій ШІ в контексті урядування.

Виклад основного матеріалу. Враховуючи поточні та практичні дослідницькі зусилля, штучний інтелект розглядається як загальний термін для «спеціальної форми ІТ-систем, додатків або програмного забезпечення, які здатні виконувати завдання, які зазвичай потребують людського інтелекту» [17]. Часто ці системи базуються на методах машинного навчання, але не виключно. Це узгоджується з іншими дослідженнями штучного інтелекту в уряді для більш гнучкого визначення штучного інтелекту і включає різні технології та методології, які дозволяють комп'ютерам виконувати ці завдання, які зазвичай потребують людського інтелекту [18]. Сучасні дослідження штучного інтелекту не мають універсального визначення або підходу до того, що є чи не є штучним інтелектом, як це спостерігалось при дослідженні ШІ в урядуванні [19]. Хоча було зазначено про технічні відмінності між підходами ШІ та системами ШІ, така глибока класифікація не завжди необхідна для розуміння сприйняття та досвіду ШІ і може обмежити дослідження технологій, які самі державні служби вважають ШІ незалежно від того, чи ця функція визнана як ШІ всіма зацікавленими сторонами [20]. Однак такий гнучкий підхід до штучного інтелекту пов'язаний із труднощами, оскільки він може охоплювати занадто багато додатків і технологій, які, незважаючи на подібний загальний термін, помітно відрізняються одна від одної, потенційно вимагаючи різних компонентів і факторів, що створюють

суспільну цінність, але це все ще поле безрезультатних досліджень і науково – прикладного пошуку.

Загалом програми штучного інтелекту можуть потенційно підвищити ефективність і результативність надання адміністративних послуг і підтримувати прийняття урядових рішень шляхом імітації різних варіантів політики при виконанні функцій публічного управління. Дослідники вказали на потенціал покращення розробки політики за допомогою технологій штучного інтелекту, надаючи державним службовцям додаткову інформацію, отриману на основі даних [21], автоматизувати повсякденні завдання та процеси [22], покращити інформацію, що надається громадянам, зробити послуги більш персоналізованими і краще зрозуміти настрої та потреби громадян, наприклад, за допомогою аналізу даних із соціальних мереж. Однак більшість потенційних наслідків ШІ (позитивних чи негативних) ще належить підтвердити й оцінити на емпіричній основі. Це пов'язано з різними бар'єрами, з якими громадські організації стикаються в інноваціях, які включають кілька факторів, що походять від середовища, організаційного контексту, рівня інновацій, а також індивідуальних пов'язаних факторів, до певної міри унікальних у контексті державного сектора порівняно з приватним сектором. Дехто зауважує, що застосування ШІ в державному секторі може не відрізнятися від приватного сектору, як стверджують деякі ІТ-директори[23], і проблеми з отриманням користі від інновацій ШІ в організаціях приватного сектора подібні [24]. Інші дослідники вказують на помітні відмінності між державним і приватним секторами, наприклад потребу державного сектора максимізувати суспільну цінність, а не комерційну цінність, коли вони впроваджують технології ШІ, різниця у мотивації персоналу, цілях і намірах організації, наявності унікальних бар'єрів, що обмежують впровадження ШІ в державній службі, які вимагають спеціального аналізу, що пояснює, чому громадське сприйняття штучного інтелекту в державному секторі відбувається повільніше, ніж у приватному секторі [25]. Інші вказують на те, що очікування від громадян [26], а також вимоги до прозорості та зрозумілості

вищі порівняно з приватним сектором, як у функціонуванні самих систем штучного інтелекту, так і більшої прозорості інформації про те, як витрачаються державні ресурси, що створює різні вимоги щодо розгортання ШІ в адміністративних послугах та державній службі порівняно з організаціями приватного сектора. Таким чином, незважаючи на те, що деякі проблеми використання інновацій, зокрема технологій штучного інтелекту, можна порівняти як з приватним, так і з державним сектором, контекст, у якому працюють державні органи управління, є різним, і, отже, результати приватного сектору можуть не бути безпосередньо перенесені на сферу публічного управління без коригування цієї контекстуальної різниці.

Концепція можливостей штучного інтелекту була запроваджена, щоб краще визначити, які ресурси організації повинні придбати та розвивати, щоб отримати переваги від застосування технологій штучного інтелекту, зазначивши, що, незважаючи на велике хвилювання щодо технології, багато організацій стикаються з проблемами в отриманні підвищення продуктивності від їх використання. Можливості штучного інтелекту базуються на теорії ресурсів (RBV - Resource-Based Theory), теорії інноваційних можливостей і структурі технології, організації та середовища (TOE - Technology-Organisation-Environment). Погляд через призму теорії ресурсів (RBV) організацій підкреслює взаємодоповнюваність як ІТ-активів, так і можливостей з організаційними можливостями для досягнення підвищення ефективності [27]. Ця організаційна здатність виявляти, розробляти, тестувати, використовувати та інтегрувати інновації в організацію також була концептуалізована дослідженнями як інноваційна здатність, що включає різні ресурси та можливості, якими має володіти сфера публічного управління, щоб бути інноваційною, ризикувати та використовувати інновації для покращення своєї діяльності та створення суспільної цінності [28]. Ці організаційні фактори пояснюють, чому цей історичний прогрес електронного урядування є незбалансованим між органами державного управління, незважаючи на доступність цих технологій. Основна ідея цього підходу полягає в тому, що

ефективне використання та управління цими технологіями може призвести до створення цінності, а не технологія сама по собі. Наявність штучного інтелекту в державному управлінні не обов'язково має суспільну цінність, оскільки різні фактори можливостей відіграють роль у визначенні рішення щодо прийняти технології ШІ у застосування та визнання продуктивності ШІ.

Наприклад, дослідження використання чат-ботів показало, що значний тиск навколишнього середовища може призвести до рішення використовувати технології чат-ботів на початку, але продуктивність цих чат-ботів значно відрізняється залежно від рівня економічного розвитку та організаційної готовності організації. Концепція включення чат-ботів у державні організації також враховує додаткову організаційну роботу, необхідну для підтримки високої ефективності технології, наприклад, необхідність призначення нових посад для роботи та навчання з технологією чат-ботів, а також перегляд його ефективності як «організаційного агента» [29]. Навіть одна й та сама система штучного інтелекту, яка використовується в різних організаціях, може мати різний ефект через організаційний контекст і середовище, які вона використовує. Для того, щоб мати можливість розгортати управлінські рішення застосування штучного інтелекту, які покращують якість і ефективність організації, необхідні внутрішні компетенції, які виходять за рамки простої мотивації використовувати технології штучного інтелекту. Інші дослідження наголошують на тому, що технології штучного інтелекту потрібні для того, щоб отримати користь від технологій штучного інтелекту, і разом із тим й для успішної подальшої розробки більш досконалого штучного інтелекту [30], а також інтегрувати їх в організацію на більш масштабній системній основі.

Більшість проектів ШІ сильно покладаються на внутрішню та зовнішню співпрацю між академічними, приватними та іншими, державними службами. Мережі, в яких працює державне управління, і те, як публічне управління використовує досвід цих мереж, мають вирішальне значення для

започаткування та успіху багатьох інновацій [31], вимагаючи від організації можливості співпрацювати з різними учасниками. Однак така співпраця не є простою, оскільки конфіденційність і безпека під час обміну даними, відсутність розуміння того, які дані потрібні та доступні, неузгодженість між організаціями та відсутність взаємодії з боку влади обмежують таку співпрацю, тим більше що питання безпеки при обміні даними ставить під сумнів стійкість суверенітету інформаційного простору і загрозу стороннього впливу на дані та розпорядження чутливою інформацією ззовні.

Це слід розглядати в контексті зростання геополітичної та геоекономічної напруги, як-от конкуренція між США та Китаєм і політична напруга з Росією. Проблеми різноманітні та включають цифрове шпигунство (американське, російське та китайське), відхід від конкуренції між Китаєм і США, збільшення інформаційних операцій і цифрового втручання, а також залежність від іноземних технологій, інфраструктури та сировини, як от, наприклад, Президентка Єврокомісії (ЄС) Комісії Урсула фон дер Ляєн (2019) підкреслила важливість суверенітету, кібернетичної конкурентоздатності ЄС і стратегічної автономії як ключових елементів стабільності і розвитку ЄС, пообіцявши «все необхідне» для забезпечення глобальної конкурентоспроможності Європи; Фон дер Ляєн також прагнула сприяти розвитку європейських стартапів, надаючи відкритий доступ до європейських суперкомп'ютерів для тих, хто розробляє штучний інтелект, водночас рекламуючи закон про штучний інтелект, розроблений в рамках ініціативи ЄС, як глобальний стандарт — навіть до завершення роботи над ним [32]. Проте прагнення до технічної незалежності не обмежується лише Європою. Будь-яка країна, яка стикається з геополітичною напруженістю з сусідами, антагоністами чи навіть союзниками, може турбуватися про свою залежність від послуг, що надаються в цих країнах. Ця залежність наражає уряди на ризики з точки зору того, що супротивники чи конкуренти — інші держави — отримують доступ до хостів, які запускають державні служби, або перехоплюють трафік між цими службами, громадянами та бізнесом. Технічні

рішення для зменшення залежності від іноземних суб'єктів та інфраструктур – або навіть для простої демаркації національних кордонів у глобальній інфраструктурі Інтернету – обговорюються протягом тривалого часу. Нещодавні дослідження показали, що спеціалізовані урядові структури можуть змінити маршрутизацію та потоки даних відповідно до національних уподобань, якщо вони готові вкласти в це політичну волю і ресурси. Наприклад, Росія фактично відокремила Крим від української маршрутизації та вбудувала його в російські мережі та маршрутизацію, зробивши Крим «відокремленим» з точки зору потоків цифрових даних [33]. Питання, чи роблять ці види технологічного втручання частини Інтернету більш суверенними і – що ще важливіше – сприяють більшій незалежності та зниженню вразливості до зовнішнього втручання? Країни розглядають інтеграцію своєї цифрової економіки та державних систем у глобальну мережу Інтернет як потенційний ризик, який дедалі частіше виражається мовою цифрового суверенітету та стратегічної автономії. Дебати щодо цифрового суверенітету є широкими. Хоча концепція цифрового суверенітету є новим модним словом у багатьох країнах, вона пов'язана з геополітичною напруженістю, яка існує в усі часи. Деякі країни розвивали свою інфраструктуру в умовах геополітичного тиску задовго до того, як концепція цифрового суверенітету та стратегічної автономії стала помітною, тоді як інші країни лише нещодавно повернулися до геополітичного погляду на свою інфраструктуру. Суверенітет є водночас наріжним каменем міжнародного (правового) порядку, а також досить невловимою концепцією. Стівен Краснер назвав суверенітет «організованим лицемірством», щоб показати, що сильні держави часто формують відповідно до своїх потреб податливу концепцію [34]. Суверенітет має правові та інституційні конотації як на внутрішньому, так і на міжнародному рівнях. Макс Вебер у трактаті «Політика як покликання» [35] визначив (суверенну) державу як монополію на законне застосування насильства. У міжнародному плані міжнародна система держав побудована на правовому суверенітеті та нормах невтручання у справи іншої

держави, що іноді називають Вестфальським суверенітетом. Ці концепції обертаються навколо прав і обов'язків або повноважень, які держава має в силу того, що вона є міжнародно визнаною суверенною державою. Краснер також вводить поняття «суверенітету взаємозалежності», що означає «здатність уряду контролювати будь-які транскордонні переміщення (ідей, товарів, людей)». Це важливе поняття контролю протиставляється повноваженням, коли йдеться про суверенітет (Краснер каже): «влада передбачає взаємно визнане право суб'єкта брати участь у певних видах діяльності (...) контроль може бути досягнутий просто шляхом застосування грубої сили без взаємного визнання авторитету взагалі». Дебати про цифровий суверенітет і стратегічну автономію, здається, розв'язуються здебільшого навколо поняття взаємозалежності, суверенітету та контролю, хоча також є певні відтінки юридичного суверенітету. Цифровий суверенітет – або його численні зміни, такі як кіберсуверенітет, технологічний суверенітет, суверенітет даних і цифрова стратегічна автономія – це широке поле, якому часто бракує точних визначень. Кіберсуверенітет здебільшого використовується Росією та Китаєм і зосереджений на контролі над національною цифровою [36] інформаційною сферою [37].

Ці країни, віддаючи перевагу мові інформаційної безпеки над кібербезпекою, хочуть (абсолютного) контролю над тим, яка інформація надходить і циркулює у внутрішніх цифрових дебатах. Пов'язана дискусія про «кібер-Вестфалію» та питання про те, чи можна міжнародну державну систему накласти на глобальний Інтернет. Ці дебати частково технічного характеру, тобто чи можна це зробити, але здебільшого політичного характеру, тобто чи потрібно це робити. Ці дебати пов'язані з територіальним виміром суверенітету та, зрештою, ставлять питання, чи можна кіберпростір «обмежувати» кордонами суверенних держав. Оскільки більшість технологічних перекладів цієї ідеї потребуватимуть змін у маршрутизації та трафіку даних, багато хто побоюється, що (спроба) зміни меж призведе до фрагментації Інтернету [38]. Більшість цих понять суверенітету зосереджені

навколо поняття контролю над передачею та зберіганням даних, а деякі навіть контролю над самою інформацією). Дебати про цифровий суверенітет у Європі та ЄС почалося після викривних заяв Сноудена, яке виявило вразливість Європи до кібершпигунства, і посилилося в останні роки [39]. Основними складовими нинішніх дебатів є: потреба в автономній Європі/ЄС позиції щодо геоекономічної та геополітичної конкуренції між США та Китаєм, потреби зменшити залежність від великих технологічних корпорацій і платформ, а також потреби зменшити Європейську/ЄС залежність від сировини та життєво важливих елементів цифрового ланцюжка поставок, таких як напівпровідники. Ці дебати відбуваються на тлі зростання геополітичної напруженості та посилення державних кібероперацій у кіберпросторі, починаючи від дезінформації та (виборчого) втручання, через саботаж і закінчуючи складним кібершпигунством. У цих дебатах технологічний суверенітет і цифровий суверенітет часто знаходяться на одному рівні, при цьому технологічний суверенітет трохи більше схиляється до апаратного забезпечення. Стратегічна автономія, термін, запозичений із геостратегічної/військової сфери, часто зображується як умова для суверенітету. Суверенітет даних зазвичай розглядається як підмножина цифрового суверенітету та має елементи державного суверенітету та особистого суверенітету. Якщо віддавати частину владних повноважень інструментам ШІ, який використовує дані, які поза межами інформаційного суверенітету, то через ШІ фактично опосередковано створюється і загроза державному суверенітету. Через трафік можливе стороннє втручання в генерування засобами ШІ тих чи інших рішень і дій в публічному управлінні та при наданні адміністративних послуг.

На державному рівні мова йде про збереження контролю над даними як з економічних міркувань — як сировини для економіки даних — так і з політичних міркувань — збереження контролю над чутливими та конфіденційними даними, такими як державні дані та комунікації. Політичне також поширюється на особисте, оскільки суверенітет даних іноді включає

поняття конфіденційності та захисту даних, які захищені в ЄС, як основні права через GDPR (Загальний регламент захисту даних, GDPR; Регламент (ЄС) 2016/679) [40]. Контроль над доменами, лише частина цього суверенного ланцюжка.

Для прикладу, Нідерланди, Україна та Тайвань, понад 90% усіх державних доменів розміщені всередині країни. Уряд Сполученого Королівства (Великобританія) розміщує трохи більше 75% своїх доменів усередині країни, тоді як Пакистан має більшу кількість державних доменів, розміщених за межами своїх кордонів, ніж усередині країни, при цьому найбільша частка після самого Пакистану проживає в США. домени розподіляються між хостинг-провайдерами. Для Індії та Тайваню це централізовано, причому уряд Тайваню розміщує понад 82% їхніх доменів за допомогою єдиного постачальника, власної урядової мережі GSNET (Мережа державних послуг). Провідний індійський провайдер, Національний центр інформатики, також є державною організацією та розміщує 65% державних доменів Індії. Натомість найбільші провайдери для України та Нідерландів хостять менше третини або чверті, відповідно, усіх доменів. Є низка невеликих провайдерів, що розміщують державні домени для Нідерландів, України та Великобританії. У всіх країнах ми знаходимо державні послуги, розміщені у провайдерів США. Примітно, що для Великобританії 6 з топ-10 провайдерів є американськими компаніями, включно з топ-3. Ми знаходимо американських хостинг-провайдерів у топ-10 усіх країн, крім України. Однак навіть в Україні США все ще мають найбільшу частку українських державних доменів після самої України. Незважаючи на тривалий конфлікт між Україною та Росією, який триває з 2013 року, є, що сайти продовжують працювати на російській інфраструктурі, так це веб-сайт кримського парламенту, але зараз він не працює. Хоча сайт зник, DNS-записи домену все ще вказують на IP-адреси, оголошені CrelCom, кримським інтернет-провайдером. Класифікація цих адрес як «російських» базується на даних, відображених у базі даних адрес RIPE NCC на даний момент, і ці дані були змінені на «російські» з

«українських» між 2013 і 2014 роками [41]. Для Нідерландів, країни-члена ЄС, національні та керівні в ЄС принципи роблять загалом небажаним розміщення державних веб-сайтів за межами ЄС. Однак не всі домени є однаково чутливими.

Висновки. Технології штучного інтелекту (ШІ) продовжують розігрівати інтерес багатьох органів публічного управління завдяки технологічній майстерності та прогресу останнього десятиліття. Однак перетворення технологічних можливостей, які надає технологія, на конкретну бізнес-цінність для компаній і суспільну цінність від державних адміністрацій, які використовують цю технологію для покращення своєї діяльності, було обмеженим. Одним із важливих факторів, що перешкоджають прогресу у впровадженні технологій ШІ в публічному управлінні, є відсутність можливостей ШІ в організації. Хоча, ймовірно, це часто розглядається як організаційний, технічний досвід у розробці ШІ, наприклад, наявність адекватних спеціалістів із обробки даних, які знають, як розгортати алгоритми машинного навчання, можливості ШІ розуміються ширше. Він включає різні технічні та нетехнічні компоненти, якими повинні володіти державні адміністрації, щоб ефективно розробляти та використовувати технології ШІ. Це дослідження додає нові ідеї в цьому напрямку, зосереджуючись на сферах публічного управління, які вважаються відносно зрілими у сфері ШІ у своїх країнах. Дослідження покладається на обмежений спектр кількох прикладів. Набуття можливостей штучного інтелекту, а також взаємодоповнюваність і взаємодія між різними компонентами державних адміністрацій, які ще не використовують технології ШІ, можуть дати різні результати. Крім того, як зазначалося, поточне розгортання технологій штучного інтелекту в публічному управлінні знаходиться на ранній, але умовно зрілій стадії. Цілком може статися, що деякі з підкреслених проблем, могли бути вже подолані або виявлені заново в міру розвитку галузі. Водночас якісний характер дослідження доповнює та підсилює існуючі кількісні дослідження можливостей ШІ. Іншим критерієм аналізу, оскільки дослідження вивчає

кілька компонентів можливостей штучного інтелекту, є внесок у продуктивність організації та створення вартості за допомогою технологій штучного інтелекту. Під час детальнішого вивчення концепцій і компонентів можливостей штучного інтелекту було виявлено кілька підкомпонентів і проблем, які не можна було розглянути настільки глибоко, як хотілося б у цьому дослідженні. Однак це залишає багато можливостей для майбутніх досліджень, щоб вивчити конкретні проблеми, пов'язані з набуттям можливостей ШІ різними способами. Крім того, штучний інтелект і можливості ШІ розглядаються цілісно, охоплюючи низку різних технологій, які є штучним інтелектом дослідниками сферами публічної служби, які їх розгортають. Ми проаналізували державні домени для низки країн, які мають складні відносини з сусідами або союзниками: Індії, Нідерландів, Пакистану, Тайваню, України та Сполученого Королівства. Ми визначаємо, де і як розміщені домени, а також мережеві шляхи, якими йде до них трафік громадян. Ми знайшли дуже різні стратегії в шести країнах, що відображає їх реакцію на геополітичне середовище. У той час як деякі уряди зберігають більше суверенітету, ніж інші, жоден не може претендувати на справжню автономію, тоді як деякі навіть залежать від інфраструктури, розміщеної у мережі інтернет геополітичними конкурентами. Ми не повинні ототожнювати територіальність з автономією. Існують складні компроміси між різними ризиками та залежностями. За деяких умов, таких як загроза вторгнення або відсутність національних можливостей для захисту цифрової інфраструктури, уряд може краще захистити свій суверенітет, покладаючись на дружніх і потужних іноземних постачальників. Дискусія про те, чи бажано прагнення до більшого цифрового суверенітету чи автономії, все ще триває. Держави повинні вирішити, як вони хочуть управляти цими ризиками порівняно з перевагами, які надають цифрові технології для сприяння належному врядуванню, ефективному високотехнологічному державному управлінню та потенціалу ефективних у часі та економічності послуг, які несе штучний

інтелект, оскільки він доступний для застосування у масштабах і потребах на розсуд кожної окремої державної влади.

Література

1. Результати всеукраїнського дослідження про перспективи ші в загальній середній освіті. Міністерство освіти і науки України, (2023), Опубліковано 20 грудня 2023 року, available at: <https://mon.gov.ua/ua/news/rezultati-vseukrayinskogo-doslidzhennya-pro-perspektivi-shi-v-zagalnij-serednij-osviti> (accessed 22 January 2024).
2. Володимир Зеленський зустрівся з президентом корпорації Microsoft, (2021), 22 вересня 2021 року, available at: <https://www.president.gov.ua/news/volodimir-zelenskij-zustrivsvya-z-prezidentom-korporaciyi-mic-70761> (accessed 22 January 2024).
3. Schiff, D. S., Schiff, K. J., & Pierson, P, (2021), “Assessing public value failure in government adoption of artificial intelligence”, *Public Administration*, April, pp. 1–21, available at: <https://doi.org/10.1111/padm.12742> https://www.researchgate.net/publication/351111444_Assessing_Public_Value_Failure_in_Government_Adoption_of_Artificial_Intelligence (accessed 22 January 2024).
4. Sun, T. Q., & Medaglia, R., (2019), “Mapping the challenges of artificial intelligence in the public sector: Evidence from public healthcare”. *Government Information Quarterly*, 36 (2), pp. 368–383, available at: <https://doi.org/10.1016/j.giq.2018.09.008> . https://research-api.cbs.dk/ws/portalfiles/portal/58401014/rony_medaglia_et_al_mapping_the_challenges_acceptedmanuscript.pdf (accessed 22 January 2024).
5. 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, available at: <https://doi.org/10.1145/3598469.3598516> (accessed 22 January 2024).

6. van Noordt, C., & Misuraca, G., (2020), “Evaluating the impact of artificial intelligence technologies in public services: Towards an assessment framework. In Y. Charalabidis, M. A. Cunha, & D. Sarantis (Eds.)”, *International conference on theory and practice of electronic governance (ICEGOV 2020)*, pp. 8–16, available at: https://www.researchgate.net/publication/345015726_Evaluating_the_impact_of_artificial_intelligence_technologies_in_public_services_towards_an_assessment_framework (accessed 22 January 2024).

7. Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y., Niehaves, B., (2021), “Enabling AI capabilities in government agencies: A study of determinants for European municipalities”, *Government Information Quarterly*, 39 (February), Article 101596. <https://doi.org/10.1016/j.giq.2021.101596> (accessed 22 January 2024).

8. Карпенко О. В., (2021), “Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти”, *Державне управління: удосконалення та розвиток*, №10, 18.10.2021, available at: http://www.dy.nayka.com.ua/pdf/10_2021/4.pdf (accessed 22 January 2024).

9. Марутян Р.Р., (2018), “Інформаційні технології інтелектуального управління у публічно-управлінській практиці: зарубіжний та вітчизняний досвід”, *Вісник Національного університету цивільного захисту України*, 2018, № 2, сс. 146–153, available at: http://nbuv.gov.ua/j-pdf/VNUCZUDU_2018_2_22.pdf (accessed 22 January 2024).

10. Ткаленко О.М., Макаренко А.О., Полоневич О.В., (2021), “Інтелектуальні технології та системи штучного інтелекту для підтримки прийняття рішень”, *Телекомунікаційні та інформаційні технології*, 2019, № 2. С. 53–59, available at: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vduikt_2019_2_9.pdf (accessed 22 January 2024).

11. Тюрюк Ю.І. “Деякі аспекти побудови нормативної бази адміністративно-правового регулювання діяльності зі створення, впровадження та використання штучного інтелекту в Україні”, *JURIS EUROPAENSIS SCIENTIA*, 2022, №5, сс. 25-28, available at: http://jes.nuoua.od.ua/archive/5_2022/5.pdf (accessed 22 January 2024).
12. Ahn, M. J., & Chen, Y.-C., (2022), “Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government”, *Government Information Quarterly*, 39(2), Article 101664, available at: <https://doi.org/10.1016/j.giq.2021.101664> . <https://www.sciencedirect.com/science/article/abs/pii/S0740624X21001003?via%3Dihub> (accessed 22 January 2024).
13. Sanina, A., Balashov, A., & Rubtcova, M., (2021), “The socio-economic efficiency of digital government transformation”, *International Journal of Public Administration*, 00(00), pp.1–12, available at: <https://doi.org/10.1080/01900692.2021.1988637> (accessed 22 January 2024).
14. Mergel, I., Dickinson, H., Stenvall, J., & Gasco, M., (2023), “Implementing AI in the public sector”, *Public Management Review*, 00(00), pp.1–13, available at: <https://doi.org/10.1080/14719037.2023.2231950> (accessed 22 January 2024).
15. Medaglia, R., & Tangi, L., (2022), “The adoption of artificial intelligence in the public sector in Europe: Drivers, features, and impacts”, Vol. 1, Issue 1. *Icegov 2022. Association for Computing Machinery*, available at: <https://doi.org/10.1145/3560107.3560110> (accessed 22 January 2024).
16. Mikalef, P., & Gupta, M., (2021), “Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance”. *Information & Management*, 58(3), Article 103434, available at: <https://doi.org/10.1016/j.im.2021.103434> . <https://www.sciencedirect.com/science/article/pii/S0378720621000082?via%3Dihub> (accessed 22 January 2024).

17. Tangi, L., van Noordt, C., Combetto, M., Gattwinkel, D., Pign, & Pignatelli, F., (2022), AIwatch European landscape on the use of artificial intelligence by the public sector, available at: <https://doi.org/10.2760/39336> . <https://op.europa.eu/en/publication-detail/-/publication/7ed5aa59-dca1-11ec-a534-01aa75ed71a1/language-en> (accessed 22 January 2024).

18. Madan, R., & Ashok, M., (2023), “AI adoption and diffusion in public administration: A systematic literature review and future research agenda”, *Government Information Quarterly*, 101774, available at: <https://doi.org/10.1016/j.giq.2022.101774> . <https://www.sciencedirect.com/science/article/pii/S0740624X22001101?via%3Dihub> (accessed 22 January 2024).

19. Sienkiewicz-Małyjurek, K., (2023), “Whether AI adoption challenges matter for public managers? The case of polish cities”, *Government Information Quarterly*, March, 101828, available at: <https://doi.org/10.1016/j.giq.2023.101828> . <https://www.sciencedirect.com/science/article/abs/pii/S0740624X2300028X?via%3Dihub> (accessed 22 January 2024).

20. Gesk, T. S., & Leyer, M., (2022), “Artificial intelligence in public services: When and why citizens accept its usage”, *Government Information Quarterly*, 39(3), Article 101704, available at: <https://doi.org/10.1016/j.giq.2022.101704> . <https://www.sciencedirect.com/science/article/pii/S0740624X22000375?via%3Dihub> (accessed 22 January 2024).

21. Veale, M., & Brass, I., (2019), “Administration by algorithm? Public management meets public sector machine learning. Algorithmic Regulation”, pp.1–30, available at: <https://doi.org/10.31235/OSF.IO/MWHNB> , available at: <https://osf.io/preprints/socarxiv/mwhnb> (accessed 22 January 2024).

22. Ranerup, A., & Henriksen, H. Z., (2022), “Digital discretion: Unpacking human and technological Agency in Automated Decision Making in Sweden’s social services”, *Social Science Computer Review*, 40(2), pp.445–461. <https://doi.org/10.1177/0894439320980434> , available at:

<https://journals.sagepub.com/doi/10.1177/0894439320980434> (accessed 22 January 2024).

23. Criado, J. I., & Ode Zarate-Alcarazo, L., (2022), “Technological frames, CIOs, and artificial intelligence in public administration: A socio-cognitive exploratory study in Spanish local governments”, *Government Information Quarterly*, 39(3), Article 101688, available at: <https://doi.org/10.1016/j.giq.2022.101688> .
<https://www.sciencedirect.com/science/article/pii/S0740624X22000211?via%3Dihub> (accessed 22 January 2024).

24. Shollo, A., Hopf, K., Thiess, T., & Müller, O., (2022), “Shifting ML value creation mechanisms: A process model of ML value creation”, *Journal of Strategic Information Systems*, 31(3), Article 101734, available at: <https://doi.org/10.1016/j.jsis.2022.101734> .
<https://www.sciencedirect.com/science/article/pii/S0963868722000300?via%3Dihub> (accessed 22 January 2024).

25. Zuiderwijk, A., Chen, Y.-C., & Salem, F., (2021), “Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda”, *Government Information Quarterly*, 38(March), Article 101577, available at: <https://doi.org/10.1016/j.giq.2021.101577> .
<https://www.sciencedirect.com/science/article/pii/S0740624X21000137?via%3Dihub> (accessed 22 January 2024).

26. Gaozhao, D., Wright, J. E., & Gainey, M. K., (2023), “Bureaucrat or artificial intelligence: people’s preferences and perceptions of government service”, *Public Management Review*, pp.1–28, available at: <https://doi.org/10.1080/14719037.2022.2160488> (accessed 22 January 2024).

27. Wade, M., & Hulland, J., (2004), “The resource-based view and information systems research: Review, extension, and suggestions for future research”, *MIS Quarterly: Management Information Systems*, 28(1), pp. 107–142, available at: https://www.researchgate.net/publication/220260051_The_Resource-

Based View and Information Systems Research Review Extension and Suggestions for Future Research (accessed 22 January 2024).

28. Lewis, J. M., Ricard, L. M., & Klijn, E. H., (2018), “How innovation drivers, networking and leadership shape public sector innovation capacity”, *International Review of Administrative Sciences*, 84(2), pp. 288–307, available at: <https://doi.org/10.1177/0020852317694085> .
<https://journals.sagepub.com/doi/10.1177/0020852317694085> (accessed 22 January 2024).

29. Maragno, G., Tangi, L., Gastaldi, L., & Benedetti, M., (2022), “AI as an organizational agent to nurture: Effectively introducing chatbots in public entities”, *Public Management Review*, pp. 1–31, available at: <https://doi.org/10.1080/14719037.2022.2063935> .
<https://re.public.polimi.it/retrieve/e95d70a3-75db-42c1-b239-1c80038ad2e6/AI%20as%20an%20organizational%20agent%20to%20nurture%20effectively%20introducing%20chatbots%20in%20public%20entities.pdf> (accessed 22 January 2024).

30. Neumann, O., Guirguis, K., & Steiner, R., (2022), “Exploring artificial intelligence adoption in public organizations: A comparative case study”, *Public Management Review*, pp. 1–27, available at: <https://doi.org/10.1080/14719037.2022.2048685> .
<https://www.tandfonline.com/doi/full/10.1080/14719037.2022.2048685> (accessed 22 January 2024).

31. Cordella, A., & Hesse, J., (2015), “E-government in the making: An actor networkperspective. Transforming Government: People”, *Process and Policy*, 9(1), pp.104–125, available at: <https://doi.org/10.1108/TG-02-2014-0006> .
https://www.researchgate.net/publication/276926940_E-government_in_the_Making_An_Actor_Network_Perspective (accessed 22 January 2024).

32. Jörn Fleck, (2023), “Reading between the lines of Ursula von der Leyen’s ambitious vision for the EU. Atlantic Council”, *New Atlanticist*, September

14, 2023, available at: <https://www.atlanticcouncil.org/blogs/new-atlanticist/reading-between-the-lines-of-ursula-von-der-leyens-ambitious-vision-for-the-eu/> (accessed 22 January 2024).

33. Douzet, F., Petiniaud, L., Salamatian, L., Limonier, K., Salamatian, K., & Alchus, T., (2020), “Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis”, *2020 12th international conference on cyber conflict (CyCon)*, pp. 157–182, available at: <https://doi.org/10.23919/CyCon49761.2020.9131726> .
https://d1wqtxts1xzle7.cloudfront.net/63394899/CyCon_2020_9_Douzet_Petiniaud_Salamatian_Limonier_Salamatian_Alchus20200522-63843-xu4f81-libre.pdf?1590152602=&response-content-disposition=inline%3B+filename%3DMeasuring_the_Fragmentation_of_the_Inter.pdf&Expires=1706379427&Signature=A0SRqAZIXUKMWh43x4j~Znl8rZs8A~fPpMwDHI96uERNIji3D8j3FVdp6CyfHyp5YXmmII1IYhEl7bcgSB90twlagQm9C5e8h2dpzr8CBMZm~nTh27yYxASilgsNdDEa1CpE6Jtv3AHovSsCE3S5C1D1zOQWc0BxaCMKDjBcbpuNgITWEnQpKjHMUx1pN0qqEjstgfxpuVxjaI-3JG3k443iLF9bIdquK~7pZtbCbH4md5WKIU62JezKcMvuANUbeIeyXrAdx2WDF9iSM6fudffnNRbaTaK~oF8X6vTzU0Kr5BG-TZTVZfR0g2DdV3LJxtdEChS2TRKBYpleo6JmEQ_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (accessed 22 January 2024).

34. Krasner, S. D., (1999), *Sovereignty: Organized hypocrisy*, Princeton, Princeton University Press. B. Jansen et al, available at: <https://archive.org/details/sovereigntyorgan0000kras> (accessed 22 January 2024).

35. Weber, M., (2004), *The vocation lectures. “Science as a vocation” and “Politics as a vocation”*, Indianapolis: Hackett Publishing Company, available at: https://ia800107.us.archive.org/26/items/max_weber_the_vocation_lectures_scienc_e/Max%20Weber%2C%20David%20S.%20Owen%2C%20Tracy%20B.%20Strong%2C%20Rodney%20Livingstone-The%20Vocation%20Lectures_%20Science%20As%20a%20Vocation%2C%20Politics%20As%20a%20Vocation%20%282004%29.pdf (accessed 22 January 2024).

36. Creemers, R., (2020), China's conception of cyber sovereignty: rhetoric and realization, In D. Broeders, & B. van den Berg (Eds.), *Governing cyberspace: Behaviour, power and diplomacy*, London: Rowman & Littlefield, available at: <https://dx.doi.org/10.2139/ssrn.3532421> .
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532421 (accessed 22 January 2024).
37. Kurowska, X., (2020), What does Russia want in cyber diplomacy? A primer, In D. Broeders, & B. van den Berg (Eds.), *Governing cyberspace: behaviour, power and diplomacy*, London: Rowman & Littlefield, pp. 85 – 106, available at: https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf (accessed 22 January 2024).
38. Mueller, M., (2017), *Will the Internet fragment? Sovereignty, globalization and cyberspace*, John Wiley & Sons, available at: <https://ijoc.org/index.php/ijoc/article/viewFile/8202/2198> (accessed 22 January 2024).
39. Broeders, D., Cristiano, F., & Kaminska, M., (2023), “In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions”, *JCMS: Journal of Common Market Studies*, 61(5), pp. 1123–1431, available at: <https://doi.org/10.1111/jcms.13462> .
<https://onlinelibrary.wiley.com/doi/10.1111/jcms.13462> (accessed 22 January 2024).
40. Регламент Європейського Парламенту і Ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), Переклад, (2016), available at: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (accessed 22 January 2024).
41. RIPE Network Coordination Centre, RIPEstat, Historical WHOIS, (2023), available at: <https://stat.ripe.net/widget/historical->

[whois?pk_vid=fac55c350f3d8fa31607272904a2e27b#w.resource=80.245.112.0/20](https://mon.gov.ua/ua/news/rezultati-vseukrayinskogo-doslidzhennya-pro-perspektivi-shi-v-zagalnij-serednij-osviti)
<https://www.president.gov.ua/news/volodimir-zelenskij-zustrivsvya-z-prezidentom-korporaciyi-mic-70761> (accessed 22 January 2024).

References

1. Ministry of Education and Science of Ukraine, (2023), “The results of the all-Ukrainian study on the prospects of education in general secondary education”, available at: <https://mon.gov.ua/ua/news/rezultati-vseukrayinskogo-doslidzhennya-pro-perspektivi-shi-v-zagalnij-serednij-osviti> (accessed 22 January 2024).
2. President of Ukraine (2021), “Volodymyr Zelenskyi met with the President of Microsoft Corporation”, available at: <https://www.president.gov.ua/news/volodimir-zelenskij-zustrivsvya-z-prezidentom-korporaciyi-mic-70761> (accessed 22 January 2024).
3. Schiff, D. S., Schiff, K. J., & Pierson, P, (2021), “Assessing public value failure in government adoption of artificial intelligence”, *Public Administration*, April, pp. 1–21, available at: https://www.researchgate.net/publication/351111444_Assessing_Public_Value_Failure_in_Government_Adoption_of_Artificial_Intelligence (accessed 22 January 2024). <https://doi.org/10.1111/padm.12742>
4. Sun, T. Q., & Medaglia, R., (2019), “Mapping the challenges of artificial intelligence in the public sector: Evidence from public healthcare”. *Government Information Quarterly*, vol. 36 (2), pp. 368–383, available at: https://research-api.cbs.dk/ws/portalfiles/portal/58401014/rony_medaglia_et_al_mapping_the_challenges_acceptedmanuscript.pdf (accessed 22 January 2024). <https://doi.org/10.1016/j.giq.2018.09.008>
5. 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. <https://doi.org/10.1145/3598469.3598516>
6. van Noordt, C., & Misuraca, G., (2020), “Evaluating the impact of artificial intelligence technologies in public services: Towards an assessment framework”,

International conference on theory and practice of electronic governance (ICEGOV 2020), pp. 8–16, available at: https://www.researchgate.net/publication/345015726_Evaluating_the_impact_of_artificial_intelligence_technologies_in_public_services_towards_an_assessment_framework (accessed 22 January 2024).

7. Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y. and Niehaves, B. , (2021), “Enabling AI capabilities in government agencies: A study of determinants for European municipalities”, *Government Information Quarterly*, vol.39 (February), Article 101596. <https://doi.org/10.1016/j.giq.2021.101596>

8. Karpenko, O. V., (2021), “Artificial intelligence as a tool of public management of socio-economic development: smart infrastructure, digital systems of business analytics and transfers”, *Public administration: improvement and development*, vol.10, available at: http://www.dy.nayka.com.ua/pdf/10_2021/4.pdf (accessed 22 January 2024).

9. Marutyanyan R.R., (2018), “Information technologies of intellectual management in public management practice: foreign and domestic experience”, *Bulletin of the National University of Civil Defense of Ukraine*, 2018, vol. 2, pp. 146–153, available at: http://nbuv.gov.ua/j-pdf/VNUCZUDU_2018_2_22.pdf (accessed 22 January 2024).

10. Tkalenko O.M., Makarenko A.O., Polonevych O.V., (2019), “Intelligent technologies and artificial intelligence systems for decision support”, *Telecommunications and information technologies*, vol. 2. pp. 53–59, available at: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vduikt_2019_2_9.pdf (accessed 22 January 2024).

11. Tyurya, Yu.I. (2022), “Some aspects of building a regulatory framework for administrative and legal regulation of activities related to the creation, implementation and use of artificial intelligence in Ukraine”, *JURIS EUROPENSIS*

SCIENTIA, vol.5, pp. 25-28, available at:
http://jes.nuoua.od.ua/archive/5_2022/5.pdf (accessed 22 January 2024).

12. Ahn, M. J., & Chen, Y.-C., (2022), “Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government”, *Government Information Quarterly*, vol. 39(2), Article 101664, available at: <https://doi.org/10.1016/j.giq.2021.101664> .
<https://www.sciencedirect.com/science/article/abs/pii/S0740624X21001003?via%3Dihub> (accessed 22 January 2024).

13. Sanina, A., Balashov, A., & Rubtcova, M., (2021), “The socio-economic efficiency of digital government transformation”, *International Journal of Public Administration*, pp.1–12. <https://doi.org/10.1080/01900692.2021.1988637>

14. Mergel, I., Dickinson, H., Stenvall, J., & Gasco, M., (2023), “Implementing AI in the publicsector”, *Public Management Review*, pp.1–13. <https://doi.org/10.1080/14719037.2023.2231950>

15. Medaglia, R., & Tangi, L., (2022), “The adoption of artificial intelligence in the public sector in Europe: Drivers, features, and impacts”, *ICEGOV '22: Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, Vol. 1, Issue 1, Association for Computing Machinery, <https://doi.org/10.1145/3560107.3560110>

16. Mikalef, P., & Gupta, M., (2021), “Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance”. *Information & Management*, vol. 58(3), Article 103434, available at: <https://www.sciencedirect.com/science/article/pii/S0378720621000082?via%3Dihub> (accessed 22 January 2024). <https://doi.org/10.1016/j.im.2021.103434>

17. Tangi, L., van Noordt, C., Combetto, M., Gattwinkel, D., Pign, & Pignatelli, F., (2022), “AIwatch European landscape on the use of artificial intelligence by the public sector”, available at: <https://doi.org/10.2760/39336> .
<https://op.europa.eu/en/publication-detail/-/publication/7ed5aa59-dca1-11ec-a534-01aa75ed71a1/language-en> (accessed 22 January 2024).

18. Madan, R., & Ashok, M., (2023), "AI adoption and diffusion in public administration: A systematic literature review and future research agenda", *Government Information Quarterly*, 101774, available at: <https://www.sciencedirect.com/science/article/pii/S0740624X22001101?via%3Dihub> (accessed 22 January 2024). <https://doi.org/10.1016/j.giq.2022.101774>
19. Sienkiewicz-Małyjurek, K., (2023), "Whether AI adoption challenges matter for public managers? The case of Polish cities", *Government Information Quarterly*, March, 101828, available at: <https://www.sciencedirect.com/science/article/abs/pii/S0740624X2300028X?via%3Dihub> (accessed 22 January 2024). <https://doi.org/10.1016/j.giq.2023.101828>.
20. Gesk, T. S., & Leyer, M., (2022), "Artificial intelligence in public services: When and why citizens accept its usage", *Government Information Quarterly*, vol. 39(3), Article 101704, available at: <https://www.sciencedirect.com/science/article/pii/S0740624X22000375?via%3Dihub> (accessed 22 January 2024). <https://doi.org/10.1016/j.giq.2022.101704>.
21. Veale, M., & Brass, I., (2019), "Administration by algorithm? Public management meets public sector machine learning. Algorithmic Regulation", pp.1–30, available at: <https://osf.io/preprints/socarxiv/mwhnb> (accessed 22 January 2024). <https://doi.org/10.31235/OSF.IO/MWHNB>
22. Ranerup, A., & Henriksen, H. Z., (2022), "Digital discretion: Unpacking human and technological Agency in Automated Decision Making in Sweden's social services", *Social Science Computer Review*, vol. 40(2), pp.445–461. available at: <https://journals.sagepub.com/doi/10.1177/0894439320980434> (accessed 22 January 2024). <https://doi.org/10.1177/0894439320980434>
23. Criado, J. I., & Ode Zarate-Alcarazo, L., (2022), "Technological frames, CIOs, and artificial intelligence in public administration: A socio-cognitive exploratory study in Spanish local governments", *Government Information Quarterly*, vol. 39(3), Article 101688, available at: <https://www.sciencedirect.com/science/article/pii/S0740624X22000211?via%3Dihub> (accessed 22 January 2024). <https://doi.org/10.1016/j.giq.2022.101688>.

24. Shollo, A., Hopf, K., Thiess, T., & Müller, O., (2022), “Shifting ML value creation mechanisms: A process model of ML value creation”, *Journal of Strategic Information Systems*, vol. 31(3), Article 101734, available at: <https://www.sciencedirect.com/science/article/pii/S0963868722000300?via%3Dihub> (accessed 22 January 2024). <https://doi.org/10.1016/j.jsis.2022.101734> .
25. Zuiderwijk, A., Chen, Y.-C., & Salem, F., (2021), “Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda”, *Government Information Quarterly*, vol. 38(March), Article 101577, available at: <https://www.sciencedirect.com/science/article/pii/S0740624X21000137?via%3Dihub> (accessed 22 January 2024). <https://doi.org/10.1016/j.giq.2021.101577> .
26. Gaozhao, D., Wright, J. E., & Gainey, M. K., (2023), “Bureaucrat or artificial intelligence: people’s preferences and perceptions of government service”, *Public Management Review*, pp.1–28. <https://doi.org/10.1080/14719037.2022.2160488>
27. Wade, M., & Hulland, J., (2004), “The resource-based view and information systems research: Review, extension, and suggestions for future research”, *MIS Quarterly: Management Information Systems*, vol. 28(1), pp. 107–142, available at: https://www.researchgate.net/publication/220260051_The_Resource-Based_View_and_Information_Systems_Research_Review_Extension_and_Suggestions_for_Future_Research (accessed 22 January 2024).
28. Lewis, J. M., Ricard, L. M., & Klijn, E. H., (2018), “How innovation drivers, networking and leadership shape public sector innovation capacity”, *International Review of Administrative Sciences*, vol. 84(2), pp. 288–307, available at: <https://journals.sagepub.com/doi/10.1177/0020852317694085> (accessed 22 January 2024). <https://doi.org/10.1177/0020852317694085> .
29. Maragno, G., Tangi, L., Gastaldi, L., & Benedetti, M., (2022), “AI as an organizational agent to nurture: Effectively introducing chatbots in public entities”, *Public Management Review*, pp. 1–31, available at: <https://re.public.polimi.it/retrieve/e95d70a3-75db-42c1-b239-1c80038ad2e6/AI%20as%20an%20organizational%20agent%20to%20nurture%20>

effectively%20introducing%20chatbots%20in%20public%20entities.pdf (accessed 22 January 2024). <https://doi.org/10.1080/14719037.2022.2063935> .

30. Neumann, O., Guirguis, K., & Steiner, R., (2022), “Exploring artificial intelligence adoption in public organizations: A comparative case study”, *Public Management Review*, pp. 1–27, available at: <https://www.tandfonline.com/doi/full/10.1080/14719037.2022.2048685> (accessed 22 January 2024). <https://doi.org/10.1080/14719037.2022.2048685> .

31. Cordella, A., & Hesse, J., (2015), “E-government in the making: An actor networkperspective. Transforming Government: People”, *Process and Policy*, vol. 9(1), pp.104–125, available at: https://www.researchgate.net/publication/276926940_E-government_in_the_Making_An_Actor_Network_Perspective (accessed 22 January 2024). <https://doi.org/10.1108/TG-02-2014-0006> .

32. Fleck, J. (2023), “Reading between the lines of Ursula von der Leyen’s ambitious vision for the EU. Atlantic Council”, *New Atlanticist*, available at: <https://www.atlanticcouncil.org/blogs/new-atlanticist/reading-between-the-lines-of-ursula-von-der-leyens-ambitious-vision-for-the-eu/> (accessed 22 January 2024).

33. Douzet, F., Pétiniaud, L., Salamatian, L., Limonier, K., Salamatian, K., & Alchus, T., (2020), “Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis”, 12th international conference on cyber conflict (CyCon), pp. 157–182, available at: https://d1wqtxts1xzle7.cloudfront.net/63394899/CyCon_2020_9_Douzet_Petinaud_Salamatian_Limonier_Salamatian_Alchus20200522-63843-xu4f81-libre.pdf?1590152602=&response-content-disposition=inline%3B+filename%3DMeasuring_the_Fragmentation_of_the_Inter.pdf&Expires=1706379427&Signature=A0SRqAZIXUKMWh43x4j~Znl8rZs8A~fPpMwDHI96uERNIJI3D8j3FVdp6CyfHyp5YXmmII1IYhEl7bcgSB90twlagQm9C5e8h2dpzr8CBMZm~nTh27yYxASilgsNdDEa1CpE6Jtv3AHovSsCE3S5C1D1zOQWc0BxaCMKDjBcbpuNgITWEnQpKjHMUx1pN0qqEjstgfxpuVxjaI-3JG3k443iLF9bIdquK~7pZtbCbH4md5WKIU62JezKcMvuANUbeIeyXrAdx2W

- DF9iSM6fudffnNRbaTaK~oF8X6vTzU0Kr5BG-TZTVZfR0g2DdV3LJxtdEChS2TRKBYpleo6JmEQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (accessed 22 January 2024). <https://doi.org/10.23919/CyCon49761.2020.9131726> .
34. Krasner, S. D., (1999), *Sovereignty: Organized hypocrisy*, Princeton University Press, Princeton, available at: <https://archive.org/details/sovereigntyorgan0000kras> (accessed 22 January 2024).
35. Weber, M., (2004), *The vocation lectures. "Science as a vocation" and "Politics as a vocation"*, Hackett Publishing Company, Indianapolis, available at: [https://ia800107.us.archive.org/26/items/max_weber_the_vocation_lectures_scienc_e/Max%20Weber%2C%20David%20S.%20Owen%2C%20Tracy%20B.%20Stron g%2C%20Rodney%20Livingstone-The%20Vocation%20Lectures_%20Science%20As%20a%20Vocation%2C%20Po litics%20As%20a%20Vocation%20%282004%29.pdf](https://ia800107.us.archive.org/26/items/max_weber_the_vocation_lectures_scienc_e/Max%20Weber%2C%20David%20S.%20Owen%2C%20Tracy%20B.%20Strong%2C%20Rodney%20Livingstone-The%20Vocation%20Lectures_%20Science%20As%20a%20Vocation%2C%20Po litics%20As%20a%20Vocation%20%282004%29.pdf) (accessed 22 January 2024).
36. Creemers, R., (2020), "China's conception of cyber sovereignty: rhetoric and realization", *Governing cyberspace: Behaviour, power and diplomacy*, Rowman & Littlefield, London, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532421 (accessed 22 January 2024). <https://dx.doi.org/10.2139/ssrn.3532421>
37. Kurowska, X., (2020), "What does Russia want in cyber diplomacy? A primer", *Governing cyberspace: behaviour, power and diplomacy*, Rowman & Littlefield, London, pp. 85 – 106, available at: https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf (accessed 22 January 2024).
38. Mueller, M., (2017), *Will the Internet fragment? Sovereignty, globalization and cyberspace*, John Wiley & Sons, available at: <https://ijoc.org/index.php/ijoc/article/viewFile/8202/2198> (accessed 22 January 2024).
39. Broeders, D., Cristiano, F., & Kaminska, M., (2023), "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its

Geopolitical Ambitions”, *JCMS: Journal of Common Market Studies*, vol. 61(5), pp. 1123–1431, available at: <https://onlinelibrary.wiley.com/doi/10.1111/jcms.13462> (accessed 22 January 2024). <https://doi.org/10.1111/jcms.13462> .

40. European Parliament and Council of the European Union (2016), “Regulation of the European Parliament and of the EU Council 2016/679 of April 27, 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data, and on the repeal of Directive 95/46/EC (General Data Protection Regulation)”, available at: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (accessed 22 January 2024).

41. RIPE Network Coordination Centre, RIPEstat, Historical WHOIS, (2023), available at: https://stat.ripe.net/widget/historical-whois?pk_vid=fac55c350f3d8fa31607272904a2e27b#w.resource=80.245.112.0/20&w.time=2013-04-04T05:57:03 (accessed 22 January 2024).

Стаття надійшла до редакції 07.02.2024 р.