

4. Концепція розвитку штучного інтелекту в Україні: Схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 22.04.2026).

5. Куйбіда В. С., Карпенко О. В. Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України. Державне управління*. 2018. № 1. С. 5–10.

6. Попович Т. П. Право особи на захист персональних даних в Інтернеті: теоретико-правові аспекти. *Аналітично-порівняльне правознавство*. 2021. № 2. С. 51–54. DOI <https://doi.org/10.24144/2788-6018.2021.02.9>.

7. Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року: Схвалено розпорядженням Кабінету Міністрів України від 17 листопада 2021 р. № 1467 (в редакції розпорядження Кабінету Міністрів України від 13 травня 2025 р. № 464-р). URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text> (дата звернення: 22.04.2026).

8. Царенко І. О., Красножон Н. С. Електронне урядування як інструмент посилення конкурентоспроможності країни. *Ефективна економіка*. 2020. № 8. DOI: 10.32702/2307-2105-2020.8.74.

Швидюк С. М.,

кандидат політичних наук, доцент,
Чернівецький національний університет
імені Юрія Федьковича

ПРОБЛЕМА ТІНЬОВОГО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ УПРАВЛІННІ В УКРАЇНІ

Однією з актуальних проблем сучасного етапу розвитку публічного управління є масштабна трансформація, зумовлена імплементацією технологій штучного інтелекту (ШІ). Незважаючи на те, що цей процес частково охоплюється офіційними державними стратегіями цифровізації та прозорими процедурами закупівель, поза їхніми межами формується складна неконтрольована реальність, яка у науковому дискурсі концептуалізується як екосистема «тіньового штучного інтелекту» (Shadow AI) або BYOAI (Bring Your Own AI) [7]. Варто відзначити, що сутність зазначеного феномену зво-

диться до стихійного та нерегламентованого застосування публічними службовцями загальнодоступних генеративних нейромереж із метою оптимізації щоденних адміністративних завдань [8, р. 70]. Аналіз статистичних показників свідчить, що станом на початок 2026 року 49% інтернет-користувачів в Україні застосовують ШІ; при цьому, зокрема, 23% респондентів інтегрують генеративні моделі безпосередньо у власні професійні процеси [3]. Найбільш стрімке поширення спостерігається серед професійно зайнятих осіб із вищою освітою, що безпосередньо відповідає демографічному профілю публічних службовців.

По суті, відбувся парадигмальний перехід від тіньових інформаційних технологій (ІТ) до тіньового ШІ. По-перше, якщо на попередніх етапах розвитку проблематика обмежувалася переважно інфраструктурою зберігання даних (використання особистих накопичувачів чи хмарних сервісів), то на сучасному етапі спостерігається тенденція, за якої службовець безпосередньо делегує алгоритмам виконання власних когнітивних функцій, що неминуче призводить до масштабного соціотехнічного збою в системі публічного управління. З огляду на це генерується складний комплекс критичних загроз, серед яких виокремлюються: компрометація масивів інформації та пряме порушення чинного законодавства про захист персональних даних, алгоритмічна упередженість (наслідком якої є генерація хибних, юридично нікчемних управлінських рішень), а також юридична розмитість, що спричиняє руйнацію фундаментального принципу підзвітності. Водночас системним наслідком цього явища стає ерозія інституційної пам'яті, спровокована поступовою деградацією фахових аналітичних навичок управлінського персоналу.

Проведений нами емпіричний аналіз масиву даних державних закупівель, акумульованих в електронній системі Prozorro протягом 2024–2026 років, дозволив підтвердити гіпотезу стосовно того, що масове поширення явища тіньового ШІ безпосередньо каталізується глибокою структурною асиметрією. По-друге, досліджено, що на макрорівні центральні органи влади активно розбудовують інфраструктуру «Суверенної фабрики ШІ» [4] та імплементують національну велику мовну модель «Сяйво», тоді як передові інституції (наприклад, Національний банк України) здійснюють закупівлю безпечних корпоративних ліцензій рівня Enterprise [6]. Натомість на мікрорівні фіксується діаметрально протилежна ситуація: понад 95% муніципалітетів функціонують в умовах інституційного вакууму, не здійснивши жодної закупівлі безпечних технологічних рішень для працівників.

Ще одним непрямим свідченням проникнення інструментів ШІ в роботу публічних службовців є низка програм підвищення кваліфікації, погоджених з НАДС і представлених на офіційному «Порталі управління знаннями». Серед затверджених курсів: «Штучний інтелект у роботі публічного службовця», «Основи штучного інтелекту для публічного службовця» [7], «Штучний інтелект: нові можливості в роботі державного службовця», «Застосування штучного інтелекту: функціонал та особливості», «Штучний інтелект в професіоналізації публічної служби», «Можливості використання цифрових технологій та штучного інтелекту в діяльності публічного службовця» [5]. Наявність такого масиву освітніх ініціатив підтверджує, що публічні службовці масово та цілеспрямовано навчаються застосовувати алгоритми для своїх завдань. Проте виникає парадокс: оскільки на мікрорівні (як доводить аналіз Prozorro) держава не забезпечує їх легальними корпоративними ліцензіями, усі здобуті на цих офіційних курсах навички службовці змушені реалізовувати через власні персональні акаунти у публічних чат-ботах, генеруючи той самий неконтрольований тіньовий ШІ.

Звертаючи увагу на наявні нормативно-правові кроки з боку держави, з'ясовано, що вони демонструють небезпечну регуляторну дихотомію. Поради з відповідального використання ШІ в публічному управлінні від Мінцифри спільно з НАДС та Вищою школою публічного управління зосереджуються переважно на аспектах кібергігієни і, зокрема, пропонують: «публічному службовцю під час роботи з персональними даними необхідно ретельно оцінювати всі ризики, пов'язані із застосуванням ШІ» [2, с. 11], що перекладає тягар відповідальності на кінцевого користувача без забезпечення відповідною організаційною альтернативою на місцях.

Разом з тим, суворі вимоги Державної служби спеціального зв'язку та захисту інформації України (ДССЗІ), які стосуються параметрів диференційованої конфіденційності та федеративного навчання, зосереджені на математичному захисті макроінфраструктури [1], що залишає цілком відкритим питання повсякденної поведінкової практики службовців та врегулювання явища BYOAI.

Таким чином, для подолання виявленого інституційного розриву та відновлення алгоритмічної підзвітності в системі публічного управління, пропонується імплементація наступних практичних кроків:

Централізована легалізація. Забезпечення працівників органів публічного управління на місцях доступом до безпечних інструментів ШІ. З огля-

ду на те, що захищений контур національної мовної моделі «Сяйво» ще перебуває на етапі розробки, як проміжне, але надійне рішення видається доцільним здійснення централізованої закупівлі корпоративних ліцензій рівня Enterprise на провідні ШІ-інструменти. Ліцензійні умови таких підписок суворо гарантують конфіденційність та містять категоричну заборону на використання завантажених корпоративних даних для подальшого навчання моделей, що дозволить ефективно усунути наявний технологічний дефіцит без ризику витоку службової інформації.

Перехід до керованого дозволу. Впровадження жорсткої нормативної політики ШІ на робочому місці, яка передбачатиме чітке розмежування між дозволеним структуруванням виключно публічних даних та категоричною заборобою на введення до систем персональної чи іншої чутливої інформації.

Алгоритмічна прозорість. Передбачає формування відкритих місцевих реєстрів алгоритмів та регулярний аудит готовності інституцій до інтеграції ШІ з урахуванням передового європейського досвіду. Це, у свою чергу, стимулюватиме територіальні громади до виділення бюджетних асигнувань на легальні цифрові інструменти, а також даватиме змогу чітко бачити, які саме функції делегуються алгоритмам, і контролювати додержання принципу human on the loop.

Отже, ми вважаємо, що проблема тіньового застосування генеративних нейромереж у публічному секторі потребує системного переосмислення, а забезпечення інституційної безпеки неможливе без подолання структурної асиметрії та впровадження прозорих механізмів алгоритмічного управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наказ Адміністрації Держспецзв'язку від 23.02.2026 № 154 «Про затвердження Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту». *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-23-02-2026-154-pro-zatverdzhennya-rekomendacii-z-kiberzakhistu-informaciino-komunikacii-nikh-sistem-yaki-vikoristovuyut-tehnologiyi-shtuchnogo-intelektu> (дата звернення: 16.04.2026).

2. Поради з відповідального використання штучного інтелекту публічними службовцями. Березень 2025. Міністерство цифрової трансформації; НАДС; Вища школа публічного управління. 45 с. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Porady_z_vykorystannya_AI.pdf (дата звернення: 16.04.2026).

3. Семенюта І., Данькова Н. Кількість користувачів ШІ в Україні за рік зросла на 21 %, – дослідження «Детектора медіа». *ms.detector.media*. 13.03.2026. URL: <https://ms.detector.media/mediadoslidzhennya/post/39013/2026-03-13-kilkist-korystuvachiv-shi-v-ukraini-za-rik-zroslo-na-21-doslidzhennya-detektora-media/> (дата звернення: 16.04.2026).
4. Комплекс програмно-апаратних засобів «Суверенна фабрика штучного інтелекту». *Prozorro*. URL: <https://prozorro.gov.ua/uk/tender/UA-2025-08-07-011497-a> (дата звернення: 16.04.2026).
5. Можливості використання цифрових технологій та штучного інтелекту в діяльності публічного службовця. *Портал управління знаннями*. URL: <https://pdp.nacs.gov.ua/courses/mozhlyvosti-vykorystannia-tsyfrovykh-tekhnologii-ta-shtuchnoho-intelektu-v-diialnosti-publichnoho-sluzhbovtsia> (дата звернення: 16.04.2026).
6. Програмна продукція для впровадження технологій та сервісів на основі штучного інтелекту – 48517000–5. *Prozorro*. URL: <https://prozorro.gov.ua/uk/tender/UA-2025-03-13-014418-a> (дата звернення: 16.04.2026).
7. Anthuvan T., Prabhuram S., Raju G. et al. Bring Your Own Ai (BYOAI) in the Workplace: Patterns, Pitfalls, and the Byoai-GovTM Framework for Behavior-Aware Governance. *Lex localis – Journal of Local Self-Government*. 2025. Vol. 23, No. S6. P. 2693–2716. DOI: <https://doi.org/10.52152/mmrgh422>.
8. Tangi L., Rodriguez Müller A. P., Combetto M. A Silent Partner: The Shadow Presence of Generative Artificial Intelligence in Public Administrations. *Electronic Participation: 17th IFIP WG 8.5 International Conference, ePart 2025, Krems, Austria, August 31 – September 4, 2025, Proceedings*. Cham : Springer, 2026. P. 69–86. DOI: https://doi.org/10.1007/978-3-032-02515-9_5.