

Фаєр Богдан Леонідович
здобувач ступеня вищої освіти магістр
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

Лазор Оксана Дмитрівна
доктор наук з державного управління, професор,
професор кафедри публічного управління та менеджменту
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

ЕЛЕКТРОННЕ ВРЯДУВАННЯ ТА ПУБЛІЧНА СЛУЖБА: ЗАРУБІЖНІ ПРАКТИКИ ЗАБЕЗПЕЧЕННЯ ПРОЗОРОСТІ ТА ЗАХИСТУ ДАНИХ

Електронне врядування (e-Government) стало ключовим інструментом модернізації публічних послуг у всьому світі. Воно передбачає використання інформаційно-комунікаційних технологій (ІКТ) для підвищення ефективності, доступності та прозорості публічного управління. У сучасних умовах глобалізації та цифровізації особливого значення набувають питання забезпечення прозорості діяльності органів влади та захисту персональних даних громадян. Зарубіжний досвід у цій сфері демонструє різноманітні підходи, які можуть слугувати прикладом для країн, що розвиваються, зокрема України. У цьому контексті аналіз практик таких країн, як Естонія, Південна Корея, Сінгапур та держави Європейського Союзу, дозволяє визначити ключові принципи та виклики, пов'язані з впровадженням електронного врядування.

Естонія заслужено вважається піонером у сфері електронного врядування, демонструючи, як цифрові технології можуть трансформувати публічного управління. Її модель базується на платформі X-Road — децентралізованій системі обміну даними, яка забезпечує інтеграцію державних реєстрів і послуг у реальному часі. Ця система дозволяє громадянам отримувати доступ до більшості державних послуг онлайн — від подання податкових декларацій до реєстрації бізнесу чи електронного голосування на виборах. Прозорість діяльності уряду досягається завдяки відкритим порталам, таким як "eesti.ee", де публікуються дані про державні витрати, законотворчі ініціативи та рішення місцевих органів влади. Кожен громадянин може відстежити, як використовуються бюджетні кошти, що значно знижує корупційні ризики та підвищує довіру до держави. Захист даних в Естонії забезпечується через впровадження передових технологій, зокрема KSI Blockchain, який гарантує цілісність інформації та унеможливорює її несанкціоновану зміну. Кожен громадянин отримує цифровий ідентифікатор у вигляді ID-картки або Mobile-ID, що дозволяє безпечно автентифікуватися в системі та підписувати документи онлайн. Принцип "одноразового введення даних" (Once-Only Principle) є ще одним

важливим елементом: інформація, надана державі, зберігається централізовано і не потребує повторного введення для різних установ, що мінімізує ризик витоку даних і спрощує взаємодію з урядом. Естонський підхід також включає активну просвітницьку роботу серед населення [1].

Південна Корея відома своєю розвиненою інфраструктурою ІКТ і високим рівнем проникнення інтернету, що стало основою для ефективного електронного врядування. Одним із ключових проєктів є система KONEPS (Korean Online E-Procurement System), яка забезпечує прозорість державних закупівель. Усі тендери проводяться онлайн, а інформація про контракти доступна громадськості, що зменшує корупційні ризики. Щодо захисту даних, Південна Корея впровадила суворі закони, такі як "Закон про захист персональних даних" (Personal Information Protection Act, PIPA), який регулює збір, обробку та використання інформації. Сінгапур інтегрує електронне врядування в концепцію "розумної нації" (Smart Nation), де технології використовуються для оптимізації публічних послуг і підвищення якості життя. Портал SingPass забезпечує єдиний доступ до всіх державних послуг, а програма відкритих даних (Open Data) дозволяє громадянам аналізувати інформацію про діяльність уряду, наприклад, статистику транспорту чи екології. Захист даних у Сінгапурі базується на комплексній системі кібербезпеки. Уряд активно співпрацює з приватним сектором для розробки рішень із шифрування та запобігання кібератакам. Законодавство, зокрема "Закон про кібербезпеку" (Cybersecurity Act), зобов'язує державні установи дотримуватися високих стандартів захисту інформації. Сінгапурський досвід показує, що прозорість і безпека можуть бути досягнуті через поєднання відкритості та жорсткого контролю за технологіями [2].

У країнах Європейського Союзу електронне врядування розвивається в рамках стратегії "Цифрового єдиного ринку" (Digital Single Market), спрямованої на уніфікацію цифрових послуг і підвищення їхньої доступності. Прозорість забезпечується через портали відкритих даних, такі як EU Open Data Portal, де публікуються звіти про бюджетні витрати, екологічні показники та діяльність інституцій ЄС. Наприклад, громадяни можуть ознайомитися з інформацією про розподіл фондів на регіональні проєкти чи моніторинг виконання директив. Водночас захист персональних даних регулюється Загальним регламентом із захисту даних (GDPR), який встановлює єдині стандарти для всіх країн-членів, гарантуючи безпеку інформації як у державному, так і в приватному секторах. країни, такі як Данія, використовують систему NemID — єдиний цифровий ключ для доступу до державних і банківських послуг, що спрощує бюрократичні процеси й одночасно підвищує безпеку [3].

Уроки з цих викликів включають кілька ключових моментів. По-перше, необхідні значні інвестиції в інфраструктуру — від розширення доступу до інтернету до створення надійних серверів. По-друге, країни повинні розробляти гнучке законодавство, яке адаптується до швидких технологічних змін, як це зроблено з GDPR у ЄС. По-третє, освіта громадян є критично

важливою: програми цифрової грамотності, подібні до естонських, можуть допомогти подолати бар'єри й залучити більше людей до електронного врядування. Нарешті, міжнародна співпраця, наприклад обмін досвідом через платформи ООН чи двосторонні угоди, сприяє поширенню найкращих практик [4].

Україна, перебуваючи на шляху цифровізації публічного управління, може взяти за основу низку зарубіжних практик для вдосконалення електронного врядування, підвищення прозорості та захисту даних. По-перше, естонська модель X-Road і принцип "одноразового введення даних" могли б значно спростити бюрократичні процеси в Україні. Впровадження подібної децентралізованої платформи дозволило б інтегрувати державні реєстри, усунути дублювання інформації та прискорити надання послуг через портал "Дія" [5]. Додатково, естонський досвід із e-Residency міг би стати основою для залучення іноземних інвесторів, пропонуючи їм доступ до українських цифрових сервісів. По-друге, Південна Корея демонструє, як прозорість у державних закупівлях через систему на кшталт KONEPS може знизити корупцію — ключову проблему України. Створення аналогічної платформи з відкритим доступом до тендерів і контрактів посилює контроль громадськості над витратами бюджету. Також корейський підхід до цифрової освіти громадян міг би допомогти Україні подолати низький рівень цифрової грамотності, особливо серед старшого населення, через спеціальні програми навчання. Для реалізації цих запозичень Україні потрібні інвестиції в інфраструктуру, реформа правової бази та просвітницька робота.

Список використаних джерел

1. X-Road e-Estonia. URL: <https://e-estonia.com/solutions/x-road-interoperability-services/x-road/>.
2. Regulation - 2016/679 - EN - gdpr - EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
3. Government Technology Agency of Singapore (GovTech). URL: <https://www.tech.gov.sg/>.
4. Digital government. OECD. URL: <https://www.oecd.org/en/topics/digital-government.html>.
5. Дія – Державні послуги онлайн. URL: <https://diia.gov.ua/>.