

5. Аграрна Україна: до та після незалежності. URL: <https://latifundist.com/spetsproekt/284-agrarnaya-ukraina-do-i-posle-nezavisimosti#>

6. Рекордний 2021. URL: <https://latifundist.com/spetsproekt/956-rekordnij-2021--bilshe-100-mln-t-vrozhayu-mozhemo-zvikati-do-sotki-chi-tse-vinyatok>

7. Сучасний стан сільського господарства в умовах військового стану в Україні. URL: [http://repositsc.nuczu.edu.ua/bitstream/123456789/17810/1/Zb%D1%96rnik%20NUCZU\\_2023\\_1\\_18.pdf#page=146](http://repositsc.nuczu.edu.ua/bitstream/123456789/17810/1/Zb%D1%96rnik%20NUCZU_2023_1_18.pdf#page=146)

8. Як війна трансформує АПК. URL: <https://mind.ua/publications/20245249-mind-intelligence-yak-vijna-transformue-apk>

---

**Роман ЛИСЕНКО**

*студент другого курсу освітньої програми  
«Суспільне і приватне врядування»,  
НаУКМА*

## **ВПЛИВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ НА НАДАННЯ ДЕРЖАВНИХ ПОСЛУГ**

*Ключові слова: цифрова трансформація, конфіденційність, безпека даних, державні послуги, ефективність.*

*Метою дослідження є розгляд впливу цифрової трансформації на надання державних послуг, аналіз викликів та бар'єрів у впровадженні цифрових технологій для надання державних послуг та визначення етичних та правових наслідків використання цифрових технологій у наданні державних послуг.*

### **Вплив цифрової трансформації на надання державних послуг: Аналіз якості, ефективності та доступності**

Цифрова трансформація докорінно змінила спосіб надання державних послуг. Вона дозволила урядам надавати громадянам послуги кращої якості, підвищити операційну ефективність і доступність. Ми розглянемо вплив цифрової трансформації на надання державних послуг, зосередившись на ключових сферах якості, ефективності та доступності.

Цифрова трансформація значно покращила якість надання державних послуг. Використовуючи цифрові технології, уряди можуть надавати громадянам більш персоналізовані та ефективні послуги. Наприклад,

онлайн-портали та додатки дозволяють громадянам отримати доступ до низки державних послуг, таких як подача податкових декларацій, оформлення паспортів та поновлення водійських прав, не виходячи з дому. Це позбавляє громадян необхідності фізично відвідувати державні установи, заощаджуючи їхній час і гроші.

Цифрові технології також дають можливість урядам збирати та аналізувати дані про надання послуг, що дозволяє їм визначати сфери, які потребують вдосконалення, та підвищувати якість своїх послуг. Наприклад, аналізуючи відгуки громадян, уряди можуть визначити сфери, в яких послуги не відповідають вимогам, і вжити заходів для їх покращення [2].

Цифрова трансформація також має значний вплив на ефективність надання державних послуг. Оцифровуючи та автоматизуючи процеси, уряди можуть скоротити час і ресурси, необхідні для надання послуг. Це не лише робить процес швидшим та ефективнішим, але й зменшує ймовірність помилок та підвищує точність [4].

Наприклад, оцифрування процесів реєстрації земельних ділянок скорочує час, необхідний для завершення транзакцій, зменшує потребу в паперовій документації та підвищує точність даних. Так само автоматизація процесів збору податків полегшує громадянам сплату податків, зменшує потребу в ручному втручанні та покращує збір надходжень.

Цифрова трансформація також зробила державні послуги більш доступними для громадян. Використовуючи цифрові технології, уряди можуть охопити громадян у віддалених і недостатньо обслуговуваних районах, які раніше мали проблеми з доступом до державних послуг. Це особливо важливо в країнах, що розвиваються, де доступ до державних послуг часто обмежений [5].

Наприклад, мобільні сервіси та кіоски надають громадянам доступ до низки державних послуг навіть у районах з обмеженим доступом до Інтернету. Це дає змогу громадянам отримати доступ до таких послуг, як охорона здоров'я, освіта та соціальне забезпечення, навіть якщо вони розташовані у віддалених районах.

### **Виклики та бар'єри у впровадженні цифрових технологій для надання державних послуг: Рішення та стратегії для державного сектору**

Цифрова революція принесла значні зміни в наше життя, в тому числі в спосіб взаємодії з державним сектором. Уряди в усьому світі інвестують значні кошти в цифрові технології, щоб надавати кращі державні послуги. Однак впровадження цифрових технологій у державному секторі є складним завданням, що супроводжується бар'єрами та перешкодами, які необхідно подолати. Ми розглянемо виклики та бар'єри у впровадженні

цифрових технологій для надання державних послуг, а також запропонуємо рішення та стратегії для державного сектору.

Однією з суттєвих проблем у впровадженні цифрових технологій для надання державних послуг є брак цифрової грамотності серед громадян. Цифрові технології вимагають від людей певного рівня цифрових навичок для їх ефективного використання. Багато громадян, особливо в громадах з недостатнім рівнем обслуговування, не мають необхідних навичок, щоб орієнтуватися в цифрових послугах. Як наслідок, вони можуть не мати доступу до основних державних послуг, таких як охорона здоров'я чи освіта, які доступні лише онлайн [1]. Уряди повинні інвестувати в програми цифрової грамотності, які навчають громадян, як використовувати цифрові технології для доступу до державних послуг [6].

Ще однією перешкодою для впровадження цифрових технологій у державному секторі є цифровий розрив. Цифровий розрив – це розрив між тими, хто має доступ до цифрових технологій, і тими, хто його не має. Цей розрив може бути зумовлений такими факторами, як географія, дохід або освіта [1]. Уряди повинні вжити заходів для подолання цифрового розриву, надаючи доступ до цифрових технологій громадам, які не мають достатнього рівня обслуговування. Цього можна досягти за допомогою таких ініціатив, як надання безкоштовного або дешевого доступу до Інтернету, розповсюдження цифрових пристроїв серед недостатньо охоплених громад та інвестування в інфраструктуру для покращення інтернет-зв'язку.

Конфіденційність і безпека даних також є значними перешкодами на шляху впровадження цифрових технологій для надання державних послуг. Уряди повинні забезпечити захист даних громадян і недопущення порушення їхнього приватного життя. Цього можна досягти шляхом впровадження надійних законів про захист даних, забезпечення безпеки та шифрування цифрових технологій, а також надання громадянам можливості відмовитися від збору даних [6]. Крім того, уряди повинні забезпечити наявність необхідних ресурсів для виявлення та ефективного реагування на кіберзагрози.

Ще однією проблемою впровадження цифрових технологій у державному секторі є відсутність інтеграції між різними системами. Уряди часто використовують кілька систем для надання державних послуг, і ці системи можуть неефективно взаємодіяти одна з одною [1]. Це може призвести до неефективності та помилок, що ускладнює доступ громадян до державних послуг. Уряди повинні забезпечити інтеграцію цифрових систем для надання громадянам безперешкодного користувацького досвіду. Цього можна досягти, інвестуючи в рамки та стандарти інтероперабельності, які гарантують, що різні системи можуть взаємодіяти одна з одною.

Вивчаючи досвід Канади, визначено, що значним викликом у впровадженні цифрових технологій для надання державних послуг є опір змінам, оскільки чимало людей неохоче впроваджувати нові технології. Тому уряд повинен інформувати своїх громадян про переваги цифрових технологій та забезпечувати зручність цифрових послуг для користувачів [7].

### **Етичні та правові наслідки використання цифрових технологій у наданні державних послуг: Рамки для конфіденційності, безпеки та підзвітності**

У сучасному світі цифрові технології зробили революцію у сфері надання державних послуг. Цифрові технології дозволили урядам надавати послуги громадянам швидко та ефективно. Однак, зі збільшенням використання цифрових технологій у наданні публічних послуг виникають етичні та правові наслідки, які необхідно враховувати. Етичні та правові наслідки використання цифрових технологій у наданні державних послуг включають конфіденційність, безпеку та підзвітність.

Недоторканність приватного життя є основоположним правом кожного громадянина. З використанням цифрових технологій уряди збирають і зберігають особисту інформацію громадян. Ця інформація включає імена, адреси, номери телефонів та інші персональні дані. Збір і зберігання цих даних викликає занепокоєння щодо недоторканності приватного життя. Уряди повинні забезпечити, щоб особиста інформація громадян збиралася і зберігалася таким чином, щоб захистити їхнє приватне життя. Уряди повинні запровадити механізми, які захищають приватність громадян, гарантуючи, що їхня особиста інформація не буде передана стороннім особам.

Безпека є ще одним етичним і правовим наслідком використання цифрових технологій у наданні державних послуг. Уряди повинні забезпечити захист особистої інформації громадян. Використання цифрових технологій означає, що існує ризик кібератак, які можуть скомпрометувати особисту інформацію громадян [4]. Уряди повинні запровадити механізми, які гарантують безпеку персональних даних громадян. Цього можна досягти за допомогою технологій шифрування та інших заходів безпеки, які захищають особисту інформацію громадян від кібератак.

Для вирішення етичних і правових наслідків використання цифрових технологій у наданні державних послуг необхідно створити основи для захисту приватності, безпеки та підзвітності. Ці рамки повинні забезпечити захист приватного життя громадян, безпеку їхньої особистої інформації та підзвітність урядів за свої дії. Ці рамки можуть бути досягнуті за

допомогою законодавства та нормативно-правових актів, які регулюють використання цифрових технологій у наданні публічних послуг [3].

Однією з основ для забезпечення конфіденційності, безпеки та підзвітності є Загальний регламент про захист даних (General Data Protection Regulation, GDPR) [8]. GDPR – це регламент, запроваджений Європейським Союзом для захисту приватного життя громадян. GDPR регулює збір та обробку персональних даних організаціями. Регламент вимагає, щоб організації отримували згоду від громадян перед тим, як збирати та обробляти їхні персональні дані. GDPR також зобов'язує організації впроваджувати заходи безпеки, які захищають персональні дані громадян від кібератак. Крім того, регламент вимагає від організацій бути прозорими у використанні персональних даних громадян.

Ще однією основою для забезпечення конфіденційності, безпеки та підзвітності є стандарт ISO/IEC 27001 [9]. Стандарт ISO/IEC 27001 – це стандарт, який забезпечує основу для управління інформаційною безпекою. Стандарт вимагає від організацій впроваджувати заходи безпеки, які захищають їхні інформаційні активи від кібератак. Крім того, стандарт вимагає від організацій впровадження системи моніторингу та вдосконалення системи управління інформаційною безпекою.

**Висновки.** Хоча цифрова трансформація покращила доступність державних послуг, існують побоювання, що вона може виключити певні групи громадян, які не володіють необхідними цифровими навичками або не мають доступу до технологій. Щоб вирішити цю проблему, уряди повинні інвестувати в програми цифрової грамотності та надавати доступ до технологій громадам, які не отримують належних послуг.

Впровадження цифрових технологій для надання державних послуг пов'язане зі значними викликами та бар'єрами, які необхідно подолати. Ці виклики включають відсутність цифрової грамотності, цифровий розрив, конфіденційність і безпеку даних, відсутність інтеграції між системами та опір змінам. Для подолання цих викликів уряди повинні інвестувати в програми цифрової грамотності, долати цифровий розрив, забезпечувати конфіденційність і безпеку даних, інтегрувати цифрові системи та інвестувати в стратегії управління змінами. Таким чином, уряди зможуть надавати кращі державні послуги, які відповідатимуть потребам та очікуванням громадян.

Насамкінець, не можна ігнорувати етичні та правові наслідки використання цифрових технологій у наданні державних послуг. Впроваджуючи вказані в дослідженні рамки, уряди можуть гарантувати, що переваги цифрових технологій у наданні державних послуг реалізуються без шкоди для приватності громадян.

### Список використаних джерел

1. Daub M., Domeyer A., Abdulkader Lamaa, and Renz F. Digital Public Services: How to Achieve Fast Transformation at Scale. URL: <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/digital-public-services-how-to-achieve-fast-transformation-at-scale#/>
  2. Eggers, W. D., Hurst S. Delivering the digital state: What if state government services worked like Amazon? *Deloitte Insights*. November 14, 2017
  3. 2023–2026 Data Strategy for the Federal Public Service. URL: <https://www.canada.ca/en/treasury-board-secretariat/corporate/reports/2023-2026-data-strategy.html>
  4. Osborne S. P., Cucciniello M., Nasi G. et al. Digital transformation, artificial intelligence and effective public services: challenges and opportunities. URL: <https://doi.org/10.1007/s43508-022-00058-7>
  5. O'Mahony J. et al. Rethinking the digital dividend: Government needs to deliver better citizen digital experiences, Adobe and Deloitte, 2019.
  7. Canada's Digital Ambition 2022. URL: <https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/canada-digital-ambition.html>
  8. General Data Protection Regulation. URL: <https://gdpr-info.eu>
  9. ISO/IEC 2700 стандарт. URL: <https://www.iso.org/standard/27001>
- 

**Сергій ЛИТВИНЕНКО**

*студент першого курсу освітньої програми  
«Суспільне і приватне врядування»,  
НаУКМА*

### **ПРОБЛЕМИ РОЗВИТКУ МЕДИЧНОЇ СФЕРИ В УМОВАХ COVID-19 ТА ВІЙНИ**

*Ключові слова: система охорони здоров'я, здоров'я нації, тривалість життя, медична реформа, медичні послуги, COVID-19, війна.*

*Мета дослідження – визначити тенденції функціонування медичної сфери України в умовах COVID-19 та війни.*

Національна політика у сфері охорони здоров'я є одним з ключових аспектів суспільного життя та благополуччя громадян. Протягом останніх 13 років, від 2010 до 2023 року, ця сфера пройшла значні зміни та виклики, які вимагають уваги та аналізу. У цьому звіті я пропоную оглянути