

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ**

Кафедра політології та публічного управління

На правах рукопису

ДРАНОВСЬКА АЛІНА ВАСИЛІВНА

**ЦИФРОВА ТРАНСФОРМАЦІЯ ДЕРЖАВНОГО УПРАВЛІННЯ
США: МОЖЛИВОСТІ, РИЗИКИ ТА ГЛОБАЛЬНІ ТЕНДЕНЦІЇ**

Спеціальність: 052 «Політологія»

Освітньо-професійна програма: «Політологія та державне управління»

Робота на здобуття освітнього ступеня «Бакалавр»

Науковий керівник:

ПАНИШКО ГАЛИНА ТАРАСІВНА,

кандидат історичних наук,

доцент

РЕКОМЕНДОВАНО ДО ЗАХИСТУ

Протокол №

засідання кафедри політології та
публічного управління

від

2025 р.

Завідувач кафедри

проф. Бусленко В. В.

ЛУЦЬК – 2025

АНОТАЦІЯ

Драновська Аліна Василівна. Цифрова трансформація державного управління США: можливості, ризики та глобальні тенденції – Кваліфікаційна наукова праця на правах рукопису. Робота на здобуття освітнього ступеня «Бакалавр». Спеціальність: 052 «Політологія». Освітньо-професійна програма: «Політологія та державне управління». – Волинський національний університет імені Лесі Українки, Луцьк, 2025.

У **Вступі** обґрунтовано актуальність теми цифровізації публічного управління, сформульовано мету, завдання, об'єкт і предмет дослідження, визначено методологічну базу й практичну значущість роботи.

Метою бакалаврської роботи є аналіз особливостей цифрової трансформації публічного управління у США, виявлення її можливостей і ризиків, а також порівняння глобальних моделей цифрового врядування.

Об'єктом дослідження є система публічного управління в умовах цифрової трансформації.

Предметом дослідження є зміст, передумови, ризики та перспективи цифрової трансформації державного управління в США.

У Розділі 1 «Теоретичні та концептуальні засади цифрової трансформації державного управління» розглядається еволюція поняття цифрового врядування, зміна управлінських парадигм, роль даних як нового субстрату державності, а також порівнюються глобальні моделі цифрової трансформації.

У Розділі 2 «Особливості та передумови цифрової трансформації державного управління в США» проаналізовано історичну динаміку цифрових ініціатив у США, нормативно-інституційні чинники, вплив технологій на сервісну архітектуру публічного управління та особливості впровадження інноваційних підходів до кібербезпеки, відкритих даних і державної платформенної логіки.

У Розділі 3 оцінено можливості та ризики цифрової трансформації у США, зокрема питання цифрової інклюзії, конфіденційності, етичного дизайну алгоритмів та перспективи розвитку публічного управління в умовах глобальної цифрової епохи.

У **Висновках** визначено цифрову трансформацію як стратегічний напрям модернізації американського врядування, підкреслено потребу в балансі між ефективністю, безпекою й етичністю цифрових рішень, а також окреслено рекомендації для імплементації успішних практик у вітчизняному контексті.

Ключові слова: цифрова трансформація, США, державне управління, цифрове врядування, публічні послуги, інклюзія, штучний інтелект, кібербезпека, відкриті дані, digital government.

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА КОНЦЕПТУАЛЬНІ ЗАСАДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ.....	8
1.1. Сутність цифрової трансформації в системі публічного управління...	8
1.2. Глобальні підходи та моделі цифрового врядування: порівняльний аналіз.....	13
РОЗДІЛ 2. ОСОБЛИВОСТІ ТА ПЕРЕДУМОВИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ В США.....	22
2.1. Еволюція цифрових ініціатив у державному секторі США	24
2.2. Інституційні, нормативні та технологічні чинники цифровізації публічного управління в США	33
РОЗДІЛ 3. МОЖЛИВОСТІ, РИЗИКИ ТА НАПРЯМИ РОЗВИТКУ ЦИФРОВОГО УПРАВЛІННЯ В КОНТЕКСТІ ГЛОБАЛЬНИХ ТЕНДЕНЦІЙ.....	46
3.1. Переваги та ризики цифрової трансформації державного управління США	46
3.2. Перспективи розвитку цифрового врядування в умовах глобальної цифрової епохи	54
ВИСНОВКИ.....	63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	66

ВСТУП

Актуальність теми. Процеси цифрової трансформації набули пріоритетного значення у сфері публічного управління, кардинально змінюючи взаємодію між державою, громадянами та бізнесом. У XXI столітті цифровізація стала не просто інструментом оптимізації адміністративних процедур, а стратегічним напрямом розвитку державності, що охоплює інституційну, нормативну, інфраструктурну й комунікаційну складову. Технології штучного інтелекту, автоматизація, блокчейн, хмарні сервіси та платформи відкритих даних формують нову архітектуру публічного управління - прозору, адаптивну, сервісну. У глобальному контексті цифрове врядування перетворюється на стандарт політичної легітимності, індикатор державної ефективності та чинник національної конкурентоспроможності. Для таких країн, як США, що перебувають у центрі світового технологічного прогресу, цифрова трансформація не лише сприяє модернізації управлінських процесів, а й виконує функцію м'якої сили в глобальній геополітичній конкуренції.

Цифровізація публічного управління в США має складну еволюційну динаміку, охоплюючи періоди адміністративної централізації, децентралізації та партнерства з приватним сектором. Її зміст зумовлений як внутрішніми соціально-економічними запитами, так і технологічними трендами, що генеруються ІТ-індустрією. У сучасних умовах зростає значення стратегій digital-first, відкритого коду, кібербезпеки, захисту персональних даних, а також забезпечення цифрової інклюзії. Національні цифрові платформи та ініціативи на зразок Data.gov, US Digital Service, FedRAMP стали прикладом інституціоналізованої цифрової трансформації, що охоплює усі рівні публічного управління. Водночас стрімкість цифрових змін породжує нові виклики - фрагментацію інфраструктур, нерівномірність доступу до цифрових послуг, ризики надмірної алгоритмізації рішень. Це актуалізує потребу у порівняльному

аналізі підходів до цифрового врядування, вивченні передумов, ризиків та перспектив трансформації публічного сектора США.

Огляд наукової літератури засвідчує, що цифрова трансформація публічного управління є предметом міждисциплінарного аналізу в політичній економії, інформаційних технологіях, адміністративному праві та соціології управління. У роботах Батракової Т.І. та Линовецької В.Ю. представлено засади цифрової економіки та її вплив на систему державного управління. Гражевська Н.І., Струтинська І.В., Олійник Д.І. та Левицька Н.О. аналізують зміни нормативно-правового середовища, індикатори цифровізації, понятійно-категоріальний апарат трансформації управління. У контексті США вивчаються цифрові стратегії та публічна дипломатія (Т. Alden, К. Chan, С. Bjola, R. Chhabra), цифрова дипломатія в соціальних мережах (Chen K.), інституційні підходи до цифрового уряду (Cigera X. та ін.), а також приклади адаптації ІТ-рішень до викликів пандемії (Bartolome G.). Разом з тим, залишається недостатньо розробленим системний аналіз саме американської моделі цифрового врядування у зв'язку з глобальними трендами трансформації державного сектору. Недостатньо узагальнені як стратегічні, так і нормативно-технологічні чинники, що забезпечили ефективність цифрової трансформації у США, що й зумовлює наукову доцільність дослідження.

Об'єктом дослідження є система публічного управління в умовах цифрової трансформації.

Предметом дослідження є зміст, передумови, ризики та перспективи цифрової трансформації державного управління в США.

Мета дослідження полягає в аналізі особливостей цифрової трансформації публічного управління у США, порівнянні глобальних моделей цифрового врядування, а також виявленні ризиків і напрямів подальшого розвитку державного управління в цифрову епоху.

Для досягнення поставленої мети передбачається розв'язати такі завдання:

- розкрити сутність цифрової трансформації у сфері публічного управління;

- порівняти глобальні моделі цифрового врядування та визначити їхні ключові характеристики;
- дослідити етапи розвитку цифрових ініціатив у державному секторі США;
- проаналізувати інституційні, нормативні та технологічні чинники цифровізації американського публічного управління;
- охарактеризувати переваги та ризики, пов'язані з цифровою трансформацією державного управління у США;
- визначити перспективи розвитку цифрового врядування в умовах глобальної цифрової епохи.

Методи дослідження. У процесі написання дипломної роботи було використано структурно-функціональний підхід до аналізу системи публічного управління в умовах цифровізації. Метод порівняльного аналізу застосовано для вивчення зарубіжних моделей цифрового врядування. Історико-ретроспективний підхід дозволив дослідити етапи еволюції цифрових ініціатив у США. Метод системного аналізу дав змогу визначити взаємозв'язки між інституційною побудовою управління та цифровими змінами, а логіко-аналітичний підхід – узагальнити ризики й перспективи цифрового управління в глобальному контексті.

Структура роботи. Робота складається зі вступу, трьох розділів, шести підрозділів, висновків і списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА КОНЦЕПТУАЛЬНІ ЗАСАДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ

1.1. Сутність цифрової трансформації в системі публічного управління

Цифрова трансформація системи публічного управління - це феномен, що вийшов далеко за межі інформаційно-комунікаційних змін. Це радикальна мутація управлінської тканини, що охоплює не лише технічний аспект, а й інституційний код держави, політичну динаміку, ціннісні орієнтири, адміністративну етику, механізми соціального включення та саму логіку відносин між владою і суспільством. Йдеться про метаморфозу, в якій влада перестає існувати як монолітна структура й перетворюється на інтелектуальну інфраструктуру - гнучку, мережеву, реактивну, здатну постійно реконфігуруватися згідно з поточними викликами, інформаційними потоками й логікою алгоритмічного аналізу. Управління більше не розгортається у межах класичних адміністративно-правових систем - воно втілюється в технологічних рішеннях, у конструкції цифрових платформ, у поведінці машин, які в реальному часі опрацьовують величезні масиви даних, роблять попередню класифікацію подій, надають прогностні оцінки та формують готові моделі управлінської реакції. Розпорядження, що раніше спирались на статичну норму, тепер формуються динамічно, в середовищі розподіленої інформаційної дійсності, де центральною цінністю стає не повноваження, а об'єднаний - структурований, контекстуалізований, уніфікований - потік даних, який живить аналітичні центри прийняття рішень [14, с. 7].

Цей перехід не є лінійним, бо змінюється сам архетип державності: з інституційного на інформаційний. Якщо традиційна бюрократія мислилася через сталість форм, процедур і функціональних зон, то цифрова держава - це потік інтерфейсів, API-зв'язків, алгоритмів оцінювання, процедур самоадаптації. Вона не стільки адмініструє, скільки агрегує і моделює: не виконує накази згори вниз, а пропонує варіанти дій, що виростають із аналізу емпіричних показників. Така держава не має усталеного центру, бо вона функціонує як мережева екосистема

- платформа, яка організовує взаємодію між різними акторами: громадянами, бізнесом, неурядовими структурами, автоматизованими агентами. І в цьому середовищі класичне уявлення про вертикальну підпорядкованість втрачає сенс - набагато продуктивнішим стає поняття цифрової конвергенції, коли різні елементи системи перебувають у постійній взаємодії, утворюючи голографічну управлінську модель, що відображає цілісну картину функціонування соціуму. У цій системі держава вже не є єдиним джерелом рішень - вона забезпечує процес синхронізації між розподіленими джерелами знань, аналітики, алгоритмів [13, с. 4].

Технологічна зміна парадигми відображається у розриві між тим, як ми традиційно уявляємо державу, й тим, як вона функціонує в цифровій реальності. Стара модель - це статична, юридично оформлена структура. Нова - це техноорганізм, що постійно оновлюється, переписується, автоматично оптимізується. Програмний код замінює собою норму, а реєстри - документ. Те, що колись потребувало адміністративного акта, тепер відбувається автоматично: система виявляє подію, аналізує її значущість, генерує відповідну реакцію й документує дію в цифровому логі. При цьому цифрова архітектура держави вибудовується навколо принципів інтероперабельності, відкритості, контекстної обробки інформації та гнучкої модульності. Якщо раніше інформація збиралась з периферії та передавалась у центр для обробки, то сьогодні обробка відбувається децентралізовано, у точці доступу, у реальному часі, без потреби ручного втручання. Так формується середовище, у якому ухвалення рішень делегується автоматизованим системам, а людська роль переміщується з рівня операцій до рівня проєктування та нагляду за алгоритмами.

Цифрова трансформація також змінює інституційну логіку функціонування влади. Традиційні відомства, організовані за галузевим принципом, поступаються місцем платформам, які інтегрують функції навколо життєвих ситуацій громадян. Це означає, що державні сервіси перестають функціонувати ізольовано - вони формуються як частини єдиної цифрової траєкторії користувача. Людина не повинна знати, який орган відповідає за той

чи інший аспект її запиту - система сама формує логіку взаємодії, надаючи комплексний сервіс. У цьому сенсі управління більше не є актом контролю, а актом оркестрації - системного, точного узгодження між даними, сервісами, політиками та інституціями. Адміністративна функція трансформується в сервісну логіку - із акцентом на зручність, доступність, адаптивність, етичність алгоритмів. І водночас це породжує нові виклики - питання захисту персональних даних, прозорості процесів автоматизованого ухвалення рішень, ризику реплікації соціальних упереджень через алгоритмічні моделі. Тут управління набуває форми етичного дизайну, у якому кожен технічний компонент супроводжується нормативною рефлексією [5, с. 45].

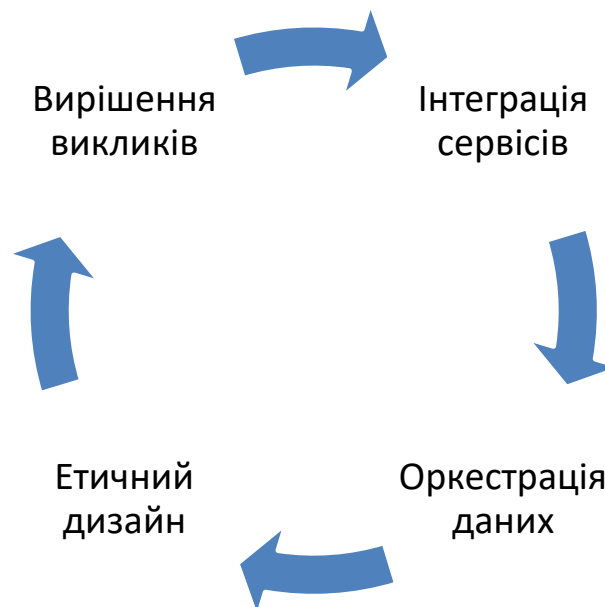


Рис. 1.1 Цикл цифрової трансформації в управлінні

Дані як адміністративний субстрат - це не метафора, а нова управлінська онтологія. Усі державні функції починають вибудовуватись навколо логіки даних. Але це не просто накопичення інформації, а її осмислена, структурована обробка у режимі потокового аналізу. Це вимагає створення цифрових близнюків інституцій - точних моделей, які імітують функціонування державних структур у реальному часі й дають змогу експериментувати з управлінськими сценаріями без ризику для реального середовища. Дані тут виступають як операційна матерія державності - вони визначають пріоритети політик,

формують бюджетну логіку, задають параметри безпеки, зумовлюють вибір технологій і моделі взаємодії з громадянами. Якщо раніше бюрократія володіла файлами, то сьогодні вона володіє потоками - безперервним обігом інформації, що синхронізує державу з реальністю. Цей потік не можна зупинити - він постійно оновлюється, перетікає між системами, структурується в режимі реального часу, слугує матеріалом для машинного навчання, із нього видобуваються інсайти, які формують нову політичну логіку [12, с. 5].

Таблиця 1.1

Цифрова онтологія державного управління: від потоків даних до цифрової легітимності

Категорія	Опис трансформації	Функціональний ефект	Вплив на громадянина
Дані як субстрат	Дані = операційна матерія держави	Основа для політик, безпеки, бюджету	Очікування прозорості, захист персональних даних
Цифровий двійник інституцій	Імітація структури та процесів у цифровому середовищі	Моделювання рішень без ризику для реальності	Менше помилок, гнучкіші сервіси
Потоки замість файлів	Безперервний обмін інформацією між системами	Синхронізація функцій, автоматизація управління	Сервісна швидкість, відсутність дублювання
Машинне навчання в управлінні	Аналіз потоків у реальному часі	Прогнозування, адаптивні політики	Персоналізовані рішення, адаптація до поведінки
Цифрова легітимність	Визнання держави через її цифрову ефективність	Заміна бюрократичного авторитету на інтерфейсну довіру	Гарантія захищеності, доступність сервісу
Цифрова справедливість	Доступність, гуманність і контроль за логікою рішень	Рівний доступ, системна етика	Можливість перевірити, як і чому прийняте рішення

І в цій логіці цифрове управління не лише оптимізує процеси - воно створює нову форму легітимності. Громадянин очікує не просто швидкої відповіді, а передбачуваної поведінки системи. Довіра формується через досвід взаємодії - через зрозумілий інтерфейс, через прозорі алгоритми, через можливість контролю за власними даними, через доступ до цифрових прав.

Держава повинна не лише надавати послугу, а давати людині впевненість, що її дані захищені, що рішення приймаються чесно, що вона може побачити логіку цих рішень. Тому трансформація - це не лише про цифрові сервіси, а про формування цифрової справедливості - коли доступ, ефективність, прозорість і гуманність стають не риторикою, а операційними стандартами. Така держава вже не є абстрактною інституцією - вона живе в додатку, в браузері, у смартфоні, в біометричних даних, у цифровому профілі людини. І саме тут відбувається найглибша зміна: держава більше не десть - вона всюди, вона поруч, вона в коді, у сигналі, у запиті [8, с. 3].

В сучасній реальності цифрової багатовекторності держава перестає бути уособленням централізованого джерела інформації й єдиного адміністративного ядра - вона втрачає монополію на продукування, володіння і структурування даних, що довгий час були основою її регуляторної та політичної легітимності. Цей процес не є наслідком політичної кризи чи юридичного обмеження повноважень - його породжує інфраструктурна зміна самого інформаційного середовища. Сьогодні дані генеруються не лише державними установами - а радше навпаки, переважна частина соціально релевантної інформації виникає внаслідок діяльності приватних технологічних платформ, користувачів, сенсорних систем, мобільних додатків, краудсорсингових сервісів, а також автоматизованих аналітичних модулів. В умовах відкритих API, напівавтономних цифрових агентів і розгалужених комунікаційних хабів відбувається розмивання колишніх меж між державним і недержавним, між інформаційною структурою та політичною інституцією. Держава більше не може забезпечити вертикальне домінування у сфері даних - вона змушена перетворюватися на координатора, фасилітатора, модератора інформаційного середовища, вибудовуючи взаємодію в межах складної екосистеми даних, у якій різні суб'єкти мають власну аналітичну, оперативну і навіть нормативну спроможність. Управління набуває рис конфігураційного процесу - воно розгортається як політика даних, орієнтована не на централізовану обробку, а на

забезпечення умов циркуляції, верифікації, агрегування й алгоритмізації інформації, створеної у множинних точках соціального поля [6, с. 8].

Розгортання цифрової трансформації в цій динаміці вимагає також переосмислення інституційної форми публічної влади. Йдеться не про заміну бюрократії на інший адміністративний каркас, а про її поступове переформатування у гібридну, емульсивну організацію, в якій цифрові ланки й алгоритмічні модулі функціонують одночасно з традиційними структурами правового врядування. Цей організаційний сплав не піддається класичній ієрархічній логіці - він не будується за принципом «верх-низ», не підкоряється жорстким схемам делегування, а діє через логіку гнучких зв'язків, тимчасових конфігурацій, хмарних зв'язків і сервісної інфраструктури. У таких умовах зникає звичне протиставлення «реального» та «віртуального» - натомість формується поліструктурна система, в якій цифрові сервіси, автоматизовані панелі керування, біометричні модулі, машинно-зчитувані формати документів і навіть штучно згенеровані рішення стають складовими частинами публічного управління. Зрештою, ми отримуємо не оновлену версію класичної адміністрації, а постбюрократичну форму організації, яка функціонує не на основі правової інфраструктури, а на основі архітектури взаємодії - багатошарової, мережевої, змістово гнучкої, сервісно адаптованої до динаміки запитів громадян.

Цей новий формат змінює не лише структуру інституції, а й саму природу влади. Якщо раніше вона втілювалась у здатності видавати накази, затверджувати процедури й контролювати виконання, то тепер вона проявляється як спроможність управляти складністю: зшивати розподілені потоки даних, організовувати ефективну цифрову логістику, забезпечувати точкову регуляцію на базі алгоритмів реального часу, координувати взаємодію автономних цифрових агентів. Система, що виникає в цьому процесі, є неоднорідною, змінною, часто нелінійною. Вона вже не функціонує через стандартизовані регламенти, а через цифрові середовища, у яких інтеграція процесів відбувається не шляхом підпорядкування, а шляхом взаємної інтероперабельності. В цьому полягає головна відмінність нового

управлінського ландшафту - дані, сервіси, інтерфейси, ідентифікатори, блокчейн-записи й машинне навчання починають формувати елементи операційної влади, здатної діяти незалежно від традиційного правового мандата. Так з'являється потреба в нових етичних конструкціях - у гарантіях того, що алгоритми не лише ефективні, а й справедливі, прозорі, підконтрольні [4, с. 51].

Цифрова трансформація створює умови для глибокого зрушення у способі соціального залучення громадян до управління. Якщо раніше участь була переважно формальною - через петиції, звернення, участь у виборах або обмежене консультування - то тепер вона набуває оперативного характеру. У режимі реального часу громадянин може впливати на формування рішень, подавати дані, брати участь у краудсорсингових процесах розробки нормативних моделей, перевіряти логіку прийнятих дій. Такий формат можна позначити як інтерактивну легітимність - коли влада не лише делегується, а постійно підтверджується в режимі цифрового зворотного зв'язку. Це ставить публічне управління перед завданням підтримувати не лише якісну цифрову інфраструктуру, а й цифрову грамотність населення, забезпечення інклюзивності, доступності, захисту приватності та рівного доступу до цифрових послуг. У цій системі громадянин не лише адресат рішень - він елемент аналітичної мережі, постачальник даних, джерело інтерпретацій, співавтор алгоритмів. Держава, відповідно, має не лише моніторити, а й слухати, не лише передбачати, а й питати, не лише регламентувати, а й навчати.

Водночас варто враховувати, що цифрова трансформація не створює ідеального середовища - вона є джерелом нових загроз, викликів, зон турбулентності. Йдеться про кібербезпеку, втрату автономності систем через надмірну алгоритмізацію, загрозу надмірного спостереження, репродукцію структурної дискримінації в рамках машинного навчання. Тут виникає потреба не лише в інституційному контролі, а й у формуванні цифрової етики - набору принципів, які регламентують допустимість тих чи інших технологічних практик, балансують ефективність з гуманістичними цінностями, обмежують вторгнення в приватність. Усе це актуалізує новий вимір управлінського

мислення - нормативний дизайн алгоритмів, прозорість процесів автоматизованого прийняття рішень, можливість людського втручання, захист цифрових прав. І саме тут проявляється глибина трансформації: публічне управління перестає бути винятково політичним або юридичним феноменом - воно стає техно-політичним режимом взаємодії між державою, даними, інфраструктурою та суспільством [17, с. 4].

Загалом, втрата монополії на інформацію й виникнення емульсійних організаційних форм не є кризовим викликом для публічного управління - це нова реальність, яка потребує зовсім іншої граматики влади. Тепер держава має навчитися функціонувати в середовищі невизначеності, розподіленої суб'єктності, інтероперабельних архітектур і постійно оновлюваних технологічних умов. Вона повинна стати водночас платформою, медіатором, інноватором, цифровим гарантом, правовим експертом і соціальним фасилітатором. Саме така держава здатна відповідати на виклики постіндустріальної, інформаційно-поточної цивілізації, де управління - це вже не про контроль, а про взаємозв'язок. Не про вертикаль, а про резонанс. Не про владу, а про інтелектуальну співучасть. І тому цифрова трансформація - це не етап, не інструмент, не модернізація. Це нова філософія державності.

1.2. Глобальні підходи та моделі цифрового врядування: порівняльний аналіз

У сучасному глобалізованому управлінському ландшафті цифрове врядування постає як багаторівнева система з різними архітектурними рішеннями, що обумовлені політичними традиціями, економічною структурою, технонауковим потенціалом і культурною специфікою кожної країни. З-поміж багатьох моделей, які постали у відповідь на цифровий виклик XXI століття, найвиразніше виокремлюються два антагоністичні - але водночас взаємодоповнюючі - типи: централізовані державоцентричні системи та

децентралізовані, сервісно-орієнтовані платформи з високим рівнем участі приватного сектору. Кожна з них формує власну архітектуру управлінських процесів, власну логіку обробки даних, свій масштаб відповідальності й глибину алгоритмічного впливу на публічну політику. В умовах глобального техно-інституційного зсуву ці моделі вже не розглядаються як національні інновації - вони функціонують як еталони, до яких орієнтуються транснаціональні актори, уряди країн, міжнародні організації та корпоративні цифрові гравці. І якщо розглядати їх не як завершені системи, а як інституційно-технологічні траєкторії, стає можливим виявити глибші структурні принципи, що лежать в основі цифрової державності [7, с. 30].

Модель Естонії є репрезентативною формою цифрового централізму, що при цьому не обмежує гнучкість функціонування, а навпаки - забезпечує її через стандартизацію архітектури. Побудована на основі системи X-Road, естонська цифрова інфраструктура поєднує усі публічні реєстри, забезпечуючи транзакційне управління в режимі майже повної автоматизації. Кожен орган - лише вузол у системі, але всі дані перебувають у загальному доступі в межах чітко прописаних протоколів. Це забезпечує максимальну інтероперабельність і цілісність інформаційного простору. Громадяни мають уніфіковану цифрову ідентичність, яка дає доступ до більш як 99% публічних сервісів - від реєстрації компанії (що займає в середньому 18 хвилин) до електронного голосування на виборах. Система е-документів, е-підпису, е-податків і навіть е-резиденства формує не лише сервісну логіку, а й транснаціональну проекцію естонського врядування, яке вже давно вийшло за межі фізичного суверенітету. Цифрова держава тут не лише регулює, а й експортує свою модель, виступаючи як архітектор глобальної цифрової довіри [19, с. 6].

Сінгапур же демонструє іншу версію централізму - високотехнологічну, авторитарно ефективну, з елементами кібернетичного планування. Його архітектура «Smart Nation» базується на жорсткому державному контролі за цифровою екосистемою, в якій уряд не лише розпорядник, а й творець інфраструктури. Централізований хмарний сервіс GovTech забезпечує

інтеграцію понад 160 цифрових послуг, модулів штучного інтелекту та аналітичних систем в єдиний функціональний простір. Ключовим компонентом є система SingPass - цифровий ідентифікатор, пов'язаний із біометричними даними, який забезпечує доступ до всіх державних платформ. Аналітична платформа Smart Nation Sensor Platform (SNSP) дозволяє в режимі реального часу зчитувати мільйони параметрів із сенсорів у міському середовищі - від транспортних потоків до якості повітря - і на основі цих даних автоматично коригувати політики. Такий рівень централізації дозволяє забезпечити оперативність, безпеку, передбачуваність, але водночас формує серйозні виклики з точки зору приватності, прозорості алгоритмів і контролю за автоматизованими рішеннями.

Таблиця 1.2

Компоненти та наслідки цифрового централізму в моделі «Smart Nation»
Сінгапуру

Компонент / аспект	Технологічна реалізація	Функціональна роль	Переваги для держави
Цифрова платформа GovTech	Єдиний державний хмарний сервіс	Інтеграція понад 160 цифрових послуг	Оперативність, масштабованість, контроль
Система SingPass	Цифровий ID з біометрією	Доступ до держсервісів, ідентифікація особи	Спрощення процедур, безпека доступу
Сенсорна мережа SNSP	Мільйони сенсорів у міському середовищі	Збір даних про трафік, повітря, енергоспоживання тощо	Прогнозування, автоматизоване регулювання
Централізоване управління даними	Аналітичні модулі, AI, Big Data	Формування державних політик у реальному часі	Передбачуваність і адаптивність управління
Авторитарна цифрова модель	Державний контроль за всією цифровою екосистемою	Уряд як розпорядник, координатор і розробник інфраструктури	Висока ефективність, стабільність
Кібернетичне планування	Автоматизоване коригування рішень на основі даних	Гнучка адаптація до змін у середовищі	Мінімізація людського фактора, зниження ризиків помилок

На противагу цим підходам функціонує американська модель децентралізованого цифрового врядування, що базується на публічно-приватному партнерстві, відкритих платформах, модульному сервісному дизайні та технологічному плюралізмі. Замість створення єдиної централізованої системи, в США функціонує множинність цифрових ініціатив на різних рівнях - федеральному, штатному, муніципальному. Сервіси розробляються переважно приватними підрядниками - такими як Palantir, Salesforce, Google Public Sector або Accenture Federal Services - що створює величезну гнучкість у реагуванні, але водночас породжує фрагментованість, нерівномірність і слабкий рівень інтероперабельності. При цьому держава зберігає стратегічний контроль над критичними компонентами - такими як системи кібербезпеки, цифрової ідентичності (Login.gov) і національної хмарної інфраструктури FedRAMP. Платформи типу Data.gov, OpenGov, USAFacts забезпечують відкритість урядових даних для громадян, дослідників, журналістів, що сприяє розвитку civic tech, аналітики, інновацій. Американська модель демонструє приклад врядування як екосистеми, в якій функції розподілені між державними й недержавними суб'єктами, а сам процес управління формується через цифрову колаборацію [1, с. 6].

Англійська модель багато в чому подібна до американської, але має чіткішу інституційну рамку. Урядове бюро Government Digital Service (GDS), створене у 2011 році, стало каталізатором цифрового переформатування британського уряду. Через портал GOV.UK забезпечено доступ до понад 3000 сервісів, об'єднаних у єдиному інтерфейсі з уніфікованою навігацією, структурою й візуальним дизайном. Цифрові трансформації відбуваються за принципами service design, user-centered thinking та agile governance. GDS не лише координує цифрові проєкти - воно створює стандарти, кодекс дизайну, API-рекомендації, документацію для розробників, методики тестування та моніторингу якості сервісів. Водночас децентралізований характер британської політичної системи, автономія міністерств і агенцій формують певні обмеження у впровадженні єдиної цифрової архітектури. Ризик фрагментації тут частково

компенсується за рахунок відкритого коду, спільнот civic developers і наукових лабораторій, які активно взаємодіють із публічними платформами. Застосування хмарних технологій (AWS, Azure), системної інтеграції з NHS Digital, DVLA, HMRC показує, що навіть у децентралізованій моделі можлива висока ступінь когерентності - за умови стандартизації, публічного контролю й відкритості коду [11, с. 26].

Якщо порівнювати ці підходи, то естонська й сінгапурська моделі орієнтовані на повну державну інкорпорацію цифрової інфраструктури - тут держава одночасно розробник, власник і гарант цифрових сервісів. У США й Великій Британії навпаки - держава стає платформою для інновацій приватного сектору, модератором процесів, інституційним фасилітатором, але не завжди власником. У першому випадку перевага - в стабільності, безпеці, тотальній інтероперабельності. У другому - у швидкості, гнучкості, масштабованості. Проте централізація створює ризики авторитарної консервованості, а децентралізація - ризики розпорошеності, втрати контролю, комерціалізації публічної функції. Відтак, на глобальному рівні формується тенденція до гібридизації: країни дедалі частіше поєднують елементи обох моделей - створюють державне ядро з критичних компонентів (ідентифікація, безпека, дані), але водночас відкривають інфраструктуру для гнучкої взаємодії з ринком, громадянським суспільством, інноваційними середовищами.

В спектрі глобальних моделей цифрового врядування, що демонструють різні шляхи еволюції публічного управління, особливе місце займають так звані громадоцентричні та адаптивні гібридні системи, в основі яких лежить не лише техно-інституційна логіка, а передусім - антропоцентричне бачення держави як сервісного середовища. У таких моделях держава не обмежується функціональним адмініструванням - вона стає архітектором життєвого досвіду громадянина, платформою, яка реагує на його індивідуальні потреби, підтримує персоналізовані траєкторії, формує умови для прозорості й етичної взаємодії. На відміну від традиційних централізованих або ринково-орієнтованих систем, що зосереджуються на контролі, оптимізації або конкурентоспроможності, ці моделі

прагнуть до інституційної емпатії - до створення державного середовища, яке живе в режимі реального часу, не нав'язує уніфікованих сценаріїв, а підлаштовується під динаміку життя людини. У цьому підході основним об'єктом управління стає не сектор, не адміністративна одиниця, а життєва ситуація - подія, яка об'єднує множину сервісів, установ, нормативів і даних у єдину, когерентну траєкторію взаємодії. Таким чином, управління починає моделюватися не вертикаллю повноважень, а горизонталлю життєвих кейсів - як народження дитини, зміна місця проживання, відкриття бізнесу, догляд за особою з інвалідністю або втрата роботи. Саме навколо таких ситуацій і конструюється архітектура громадоцентричних систем [3, с. 7].

Канада є одним із провідних прикладів такої моделі. Через платформу Canada.ca держава надає громадянам доступ до персоналізованих цифрових сервісів, які адаптуються до конкретного життєвого контексту користувача. Тут застосовується принцип one-stop-life-event, що передбачає інтеграцію адміністративних дій з різних інституцій в єдиний логічний ланцюг, орієнтований на комфорт громадянина. Так, при втраті роботи особа отримує на одному цифровому екрані інформацію про виплати, можливості перекваліфікації, податкові пільги, варіанти страхування, доступ до кар'єрних консультацій і навіть підтримку ментального здоров'я. Систему побудовано на використанні Smart Client Portals - інтелектуальних особистих кабінетів, які формуються на основі поведінкових патернів, історії запитів, інтеграції з іншими державними платформами (Service Canada, CRA, Employment and Social Development Canada). Ці інтерфейси не просто інформують - вони передбачають дії, надають рекомендації, автоматично заповнюють документи, повідомляють про зміни. Алгоритми машинного навчання, зокрема на базі IBM Watson, використовуються для семантичного аналізу запитів користувачів, щоб покращити точність відповіді, уникати повторів і створювати умовно-індивідуальні сценарії обслуговування. Держава тут функціонує як інтуїтивна платформа, яка не нав'язує свій порядок денний, а спирається на реальний досвід людини як головний індикатор управлінської реакції.

Нова Зеландія йде ще далі в персоналізації. У межах програми SmartStart держава створила інтегровану цифрову траєкторію для майбутніх батьків, яка об'єднує понад 30 сервісів - від реєстрації народження й оформлення допомог до вибору лікаря, садочка, отримання податкових пільг. Алгоритми персоналізації враховують час події, географічне розташування, мову користувача, індивідуальні медичні параметри. Система працює на основі принципів “tell-us-once” і “life-journey thinking”, що означає - громадянин вводить інформацію лише один раз, а держава далі самостійно розподіляє її між потрібними структурами. Такий підхід забезпечує не лише економію часу, а й відчуття цілісної взаємодії з державою. Головне - що громадянин не мусить знати, яка інституція за що відповідає. Інфраструктура побудована за логікою “micro-services containerization” - тобто сервісна архітектура подрібнена на незалежні модулі, які можуть швидко оновлюватись, масштабуватись або замінюватись без зупинки всієї системи. Така модель не тільки покращує стабільність, а й дозволяє тестувати нові функції без ризику для основного ядра [15, с. 6].



Рис. 1.2 Цикл персоналізованих державних послуг в межах програми SmartStart

З іншого боку, адаптивно-гібридні моделі, на відміну від повноцінних громадоцентричних систем, базуються на ідеї стратегічної гнучкості: держава

задає загальні стандарти, методики, аналітичні рамки, але дозволяє автономію регіональним, муніципальним чи галузевим ініціативам, які можуть адаптувати загальну рамку до специфіки конкретного контексту. Фінляндія - яскравий приклад. Тут існує національна цифрова стратегія, що задає логіку розвитку інфраструктури, але реалізація відбувається через локальні інноваційні екосистеми. Наприклад, у місті Еспоо діє модель Data as a Service (DaaS), у якій муніципалітет надає відкриті дані через API для розробників, дослідників, підприємців. У рамках ініціативи AuroraAI розроблено фреймворк, що здатен до самонавчання - система аналізує дані про життєві події, поведінкові патерни, інформацію з відкритих джерел і формує автоматизовані рекомендації для громадян. Фреймворк побудовано на концепції «сервісних шляхів» (service paths), які формуються динамічно, у відповідь на події в житті людини. Наприклад, якщо студент отримує диплом, система пропонує варіанти працевлаштування, програми кредитування, варіанти курсів підвищення кваліфікації, автоматично запускає процедури, пов'язані зі страхуванням або податковим статусом. Алгоритми тут не лише реагують, а й пропонують, навчаються з кожного кейсу, адаптуються до соціокультурного середовища, будують прогностичні моделі, що підсилюють резонанс між державою й громадянином [18, с. 85].

Південна Корея втілює подібну адаптивну гібридність, але в більш централізованій версії. Проєкт Digital New Deal, ініційований у 2020 році, передбачає інтенсивне впровадження інтелектуальних платформ у різні сектори публічного управління: освіту, охорону здоров'я, урбаністику, екологію. Зокрема, у рамках платформи AI-based Civil Service System здійснюється повна автоматизація типових адміністративних процесів - від обробки заяв до ухвалення рішення. Системи побудовані на базі фреймворків машинного навчання, які використовують методи natural language processing, sentiment analysis, image recognition. Але що важливо - в рамках цієї стратегії держава створила інституційні механізми адаптації: громадські ради цифрової етики, незалежні аудитори алгоритмів, центри цифрової інклюзії, аналітичні хаби на

місцевому рівні, що можуть змінювати налаштування фреймворків відповідно до культурних норм і поведінкових особливостей населення. Таким чином, держава зберігає стратегічний контроль, але дає можливість точкової адаптації, емпіричного тестування та соціального моделювання.

Отже, громадоцентричні й гібридні адаптивні моделі - це не просто ще один тип цифрової трансформації, а прояв нової філософії державності, що базується на довірі, взаємодії, персоналізації й когнітивній гнучкості. Вони демонструють, що цифрове врядування - це не технічна оптимізація, а складний соціотехнічний конструкт, в якому рівень сервісу визначається не лише швидкістю і зручністю, а й ступенем включеності людини, повагою до її контексту, здатністю держави бачити в громадянинові не номер, а складну, живу, динамічну істоту.

РОЗДІЛ 2. ОСОБЛИВОСТІ ТА ПЕРЕДУМОВИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ В США

2.1. Еволюція цифрових ініціатив у державному секторі США

Трансформація цифрових ініціатив у державному секторі США демонструє складну взаємодію між техноекономічними умовами, політичною волею, зміною управлінських парадигм і розвитком інформаційно-комунікаційних технологій. Починаючи з кінця 1990-х, коли були закладені основи концепції «електронного уряду» (e-Government), акценти робилися передусім на автоматизації внутрішніх процесів державного апарату. Основними цілями було підвищення прозорості адміністративних процедур, зменшення навантаження на фізичну бюрократію та впровадження цифрових засобів зв'язку між органами влади. Такі ініціативи були переважно у формі публічних порталів для отримання довідкових послуг, сплати податків чи подання форм онлайн. Однак цей етап залишався переважно лінійним - із традиційною ієрархічною логікою побудови сервісів, де користувач сприймався як споживач послуг, а не як суб'єкт управління. Паралельно розгорталася структурна реорганізація ІТ-інфраструктури в державному апараті: запроваджувалися центри обробки даних, уніфікувалися протоколи передачі інформації, консолідувалися технічні стандарти для обміну між відомствами. Але централізоване адміністрування не дозволяло гнучко реагувати на локальні запити, що зумовило поступовий перехід до наступного рівня технополітик [30, с. 17].

Упродовж 2000-х років спостерігався перехід від класичного e-government до ширшої концепції open government, яка стала відповіддю на зростання запитів суспільства до підзвітності, відкритості даних і демократизації управлінських процесів. Імпульсом до цього стали ініціативи адміністрації Барака Обами, зокрема меморандум «Transparency and Open Government» (2009), який закріпив принципи прозорості, участі та співпраці. Саме на цій основі був створений Data.gov - платформа, що надала відкритий доступ до мільйонів масивів даних федерального рівня. Цей підхід спричинив зрушення у структурі державної ІТ-

екосистеми: акцент був перенесений на API-архітектури, сумісність інтерфейсів, модульність систем. Інженерна логіка почала будуватися на cloud-first політиці - із пріоритетом хмарних сервісів і розподіленої обробки даних. Нова стратегія цифрової відкритості вимагала змін не лише в технологічному вимірі, а й у юридичному регулюванні: посилилися норми щодо конфіденційності, ідентифікації користувачів, аудиту доступу. Водночас у структурі державного управління почали з'являтися нові актори - data officer'и, chief digital officer'и, спеціалізовані аналітичні підрозділи, які забезпечували управління цифровими потоками інформації [42, с. 11].

Зі зміною адміністрацій зберігалася тенденція до нарощування цифрової складності державного сектору. В епоху Дональда Трампа у фокусі опинилася оптимізація цифрових витрат через дерегуляцію, але водночас зросла потреба в безпечному зберіганні інформації та інтеграції систем штучного інтелекту для розпізнавання шаблонів у масивних наборах адміністративних даних. Протягом 2016–2020 років активно впроваджувалися елементи когнітивної аналітики у службах охорони здоров'я (наприклад, аналітика Medicare), соціального захисту та прикордонного контролю. Поряд із цим розгортались інвестиції в створення інтероперабельних цифрових платформ - зокрема, інфраструктури для дистанційної медичної допомоги, цифрової ідентичності, автоматизованого адміністрування пільг. На рівні федеральної архітектури ІТ-систем почала застосовуватися Zero Trust Model - модель нульової довіри, що передбачає багаторівневу верифікацію користувачів, мінімізацію доступу та постійний моніторинг активності в системах, що дозволило створити більш стійке середовище для захисту конфіденційних державних даних. Водночас почалася інституціоналізація agile-методологій у державному управлінні: було створено спеціальні цифрові лабораторії (наприклад, US Digital Service), які розробляли MVP-рішення в кооперації з приватним сектором за принципами швидкого ітеративного тестування [64, с. 12].

Таблиця 2.1

Цифрова трансформація державного сектору США (2016–2020)

Сфера впровадження	Опис ініціатив / технологій	Ключові інституції / приклади	Очікувані ефекти / цілі	Взаємодія з приватним сектором
ІТ-безпека	Модель Zero Trust - мінімізація доступів, постійна верифікація та моніторинг	Федеральна архітектура, NIST	Захист конфіденційних даних, стабільність цифрових систем	Розробка політик з кібербезпеки спільно з корпораціями
Когнітивна аналітика	ШІ-алгоритми для аналізу даних Medicare, прикордонного контролю, соцзахисту	Medicare, CBP, SSA	Виявлення шаблонів, прогнозування ризиків	Залучення приватних вендорів даних і алгоритмів
Платформи цифрової ідентичності	Розробка єдиних міжвідомчих платформ для верифікації особи	Login.gov, GSA	Спростити доступ до послуг, підвищити точність аутентифікації	Спільна розробка з ІТ-компаніями
Телемедицина та пільги	Інфраструктура для дистанційної допомоги, автоматизоване адміністрування виплат	NHS, CMS	Доступність медпослуг, швидка обробка заявок	Постачальники телемедичних рішень
Agile-держуправління	Створення MVP у державі, ітеративні цикли розробки, тестування у партнерстві	US Digital Service, 18F	Гнучкість розробки, скорочення часу на впровадження	Пряме залучення ІТ-стартапів
Оптимізація цифрових витрат	Скорочення дублювання функцій, дерегуляція, прозорість фінансування	OMB, GSA	Зниження витрат, контроль над цифровими потоками	Аутсорсинг ІТ-процесів

Сучасний етап цифрових ініціатив у США зосереджується на побудові так званого сервісного державного середовища - government-as-a-platform. Це означає, що держава більше не функціонує як сукупність відомств, які реалізують свої індивідуальні цифрові стратегії, а як уніфікована технічна платформа, де всі сервіси підпорядковані логіці життєвих ситуацій користувача.

Тобто логіка цифрових рішень будується не за ознакою інституції, а за сценаріями поведінки громадянина - народження дитини, відкриття бізнесу, втрати роботи, переїзду тощо. Це вимагає зміни структури метаданих, побудови єдиного сховища ідентифікацій, централізації податкових, медичних, освітніх реєстрів у рамках Data Fabric - моделі інтегрованих даних, що дозволяє оркеструвати інформаційні потоки між сервісами в реальному часі. На технологічному рівні зростає значення платформ low-code/no-code, які дозволяють оперативно розробляти внутрішні рішення без необхідності глибокого програмування, що суттєво прискорює темпи адаптації до нових адміністративних запитів [31, с. 5].

Суттєве місце в сучасному циклі цифровізації посідає питання інклюзії - не лише в сенсі доступності, а й у площині когнітивного і лінгвістичного бар'єру. У рамках ініціативи «Digital Equity Act», яка отримала фінансування згідно з Bipartisan Infrastructure Law, розгортаються локальні програми із створення цифрової інфраструктури у віддалених регіонах, надання субсидованого інтернет-доступу, забезпечення цифрової грамотності через партнерства з освітніми установами. Особливу увагу приділяють розробці адаптивних інтерфейсів для людей з інвалідністю - зокрема, систем, що інтегрують мовленнєве керування, екранні читалки, сенсорну адаптацію. Також активно формуються міжвідомчі digital inclusion councils, які оцінюють ступінь проникнення цифрових рішень у різні соціально-економічні прошарки, впроваджуючи KPI-набір для вимірювання цифрового доступу на рівні громад.

У сфері сервісної орієнтації цифрові ініціативи США демонструють поступову відмову від суто транзакційних моделей у бік емоційного дизайну та персоналізованого UX. В основі такого підходу - використання поведінкової аналітики, емпатичного моделювання сценаріїв і застосування моделей типу Customer Journey Mapping для виявлення точок фрустрації користувача. Це породжує зміну парадигми: сервіси проектуються не лише як інструмент отримання результату, а як послідовність взаємодій, яка повинна забезпечити психологічну зручність, передбачуваність і мінімізацію когнітивного

навантаження. На практиці це виливається в оновлення архітектури державних сайтів, інтеграцію омніканальних рішень (чат-боти, голосові асистенти, мобільні застосунки), використання адаптивного інтерфейсу, що динамічно змінюється залежно від профілю користувача. Інтеграція DataOps-підходів у щоденну діяльність адміністративних структур дозволяє швидко реагувати на фідбек користувача й автоматично оновлювати сервіси через CI/CD-пайплайни [29, с. 8].

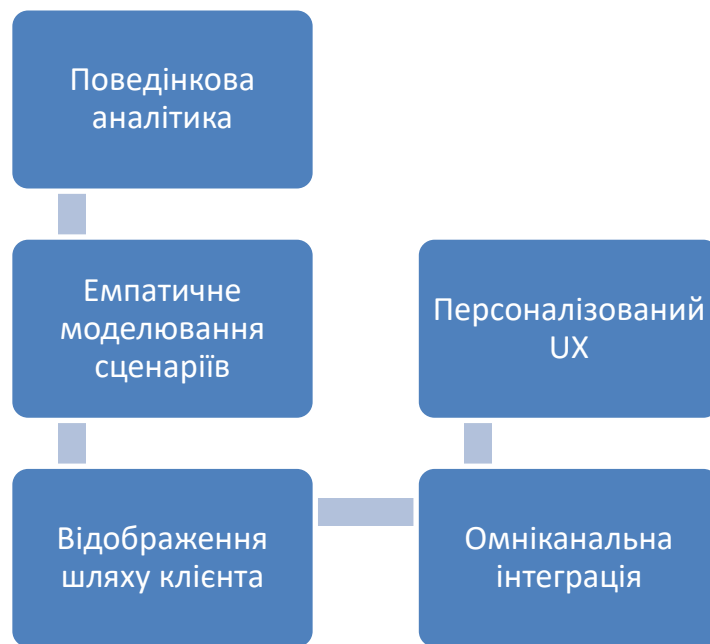


Рис. 2.1 Трансформація сервісної орієнтації

Особливе місце в еволюції цифрової моделі публічного управління посідає платформа Federal Risk and Authorization Management Program (FedRAMP), що не лише унормувала безпекову політику, а й створила стандартизовану систему оцінки відповідності хмарних рішень для органів влади. Це стало основою масштабного переходу на cloud-first policy, яка у технічному сенсі уможливила розміщення транзакційних, аналітичних і процесингових систем у хмарних середовищах з одночасним контролем доступу через ідентифікаційні системи типу FICAM (Federal Identity, Credential, and Access Management). Реалізація такої моделі змінила логіку цифрового державного адміністрування: замість сегментованих інформаційних систем кожне відомство стало елементом консолідованої екосистеми, де системи взаємодіють через сервісні шини обміну

(ESB) та API gateway'ї, а внутрішні процеси підпорядковуються архітектурі Enterprise Architecture Framework. Це дозволило здійснювати наскрізну аналітику адміністративних дій, відслідковувати повний ланцюг дій користувача, ідентифікувати збої у реальному часі та інтегрувати елементи AIOps для предиктивного управління навантаженням. Стратегічні документи типу «Cloud Smart» (2019) змістили фокус у напрямі оптимізації витрат, впровадження мультимарних стратегій, застосування edge computing для обробки даних на місці їх виникнення - зокрема в прикордонних та оборонних агенціях, де швидкість реакції є критичною для прийняття рішень [37, с. 49].

У практичному втіленні цифрова модель публічного управління, закладена стратегічними документами, реалізується через створення міжвідомчих платформ, що виконують функції інтеграційних центрів - таких як MAX.gov, яка дозволяє обмін фінансово-управлінською інформацією між агентствами; Login.gov - єдиний шлюз ідентифікації, що уніфікує доступ до послуг; або SAM.gov - платформа взаємодії з підрядниками, яка включає автоматизовані модулі оцінки відповідності та фінансового скринінгу. Ці платформи побудовані за принципами shared services, що дозволяє не лише зменшити навантаження на окремі агентства, а й забезпечити стандартизацію бекенд-логіки, єдину модель валідації даних, уніфіковані API-ендпоінти, синхронізацію метаданих через централізовані каталогізатори. Технічно це реалізується через middleware-рішення, що оркеструють виклики до баз даних, забезпечують кешування запитів, контролюють рівень доступу й здійснюють балансування навантаження між дата-центрами. Архітектура таких платформ підтримує DevSecOps-підхід, що інтегрує безпеку на кожному етапі життєвого циклу розробки - через автоматизоване сканування коду, впровадження SAST/DAST-модулів, моделювання загроз, багаторівневий аудит подій. Усе це створює передумови для динамічного масштабування систем - зокрема, під час кризових ситуацій, коли потрібне оперативне реагування на сплеск звернень або транзакцій.

Стратегії цифрового управління, підтримувані White House Office of the Federal CIO, передбачають розвиток архітектур даних на базі Data Governance

Framework, що встановлює чіткі вимоги до якості, формату, походження, умов доступу до наборів державних даних. Це не декларативна модель, а набір технічних інструкцій щодо профілювання, валідації, нормалізації й каталогізації даних, що забезпечує їх повторне використання у рамках різних сервісів і сценаріїв. На цьому підґрунті формується технічна інфраструктура для Open Data - з урахуванням структури метаданих (JSON-LD, DCAT), доступу через RESTful API, можливостей підключення зовнішніх аналітичних інструментів через стандартні шини типу GraphQL або OData. До прикладу, платформи типу HealthData.gov або DataUSA дозволяють не лише завантажувати дані, а й здійснювати інтерактивну агрегацію, візуалізацію, застосовувати попередньо налаштовані моделі прогнозування в динаміці - усе через клієнтські API, що викликаються безпосередньо з зовнішніх застосунків або систем штучного інтелекту. Це підсилює концепцію data democratization - коли кожен користувач (від аналітика в університеті до адміністратора місцевої громади) може побудувати власну модель інтерпретації даних і прийняття рішень на їхній основі [48, с. 21].

Системна інтеграція платформ у публічне адміністрування Сполучених Штатів розгортається через поступове впровадження комплексних підходів до кіберзахисту, які не просто оновлюють політику безпеки, а кардинально змінюють її засадничу логіку. Указ Президента США Executive Order 14028 «Improving the Nation's Cybersecurity» став каталізатором такого перетворення, задаючи нову архітектуру взаємодії між державними цифровими сервісами й інфраструктурою захисту. Відмова від класичної perimeter-based моделі означає перехід до архітектури Zero Trust - системи, що не довіряє жодному запиту за замовчуванням і вимагає ретельної перевірки кожної операції незалежно від місця її ініціювання. У центрі цієї концепції - принцип найменших привілеїв, що передбачає мінімізацію доступів до строго необхідного функціоналу, персоналізовану автентифікацію на всіх рівнях взаємодії з інфраструктурою, постійний моніторинг поведінкових аномалій користувачів з використанням алгоритмів User and Entity Behavior Analytics, а також обмеження

адміністративного втручання шляхом застосування технологій контролю привілейованих сесій. До цього додається інтеграція систем Security Information and Event Management та Security Orchestration, Automation and Response, що забезпечують обробку й автоматичну реакцію на події безпеки в реальному часі, з мінімальним втручанням людини у процеси.

З технічної точки зору таке переосмислення інфраструктурного захисту трансформується у побудову динамічних, гнучких архітектур, здатних до самоадаптації та ізоляції потенційно небезпечного трафіку. У цьому контексті ключовим технічним напрямом стає розгортання безпечних SD-WAN-рішень - розподілених програмно-керованих мереж, які дозволяють з'єднувати територіально віддалені підрозділи та хмарні сервіси, підтримуючи при цьому наскрізне шифрування каналів з використанням протоколу TLS 1.3. Додатково впроваджується мікросегментація трафіку, що розбиває внутрішню мережу на ізольовані логічні зони, між якими рух інформації регулюється правилами фільтрації та автентифікації. Такий підхід мінімізує площу ураження при потенційному компрометаційному сценарії, забезпечуючи ізоляцію ризиків та локалізацію загроз. Ідентифікація користувачів у подібній системі відбувається з використанням багатофакторної автентифікації, що включає біометричні шлюзи доступу - розпізнавання відбитків пальців, сканування сітківки або геометрії обличчя, а також апаратні криптографічні токени, які забезпечують стійке до атак підтвердження особи в режимі реального часу. Це гарантує, що навіть при викраденні облікових даних злоумисник не отримає змоги пройти перевірку [33, с. 10].

Формування такого рівня цифрової стійкості дозволяє державним структурам функціонувати в умовах постійного навантаження, масштабуючи свої сервіси відповідно до потреб населення й водночас зберігаючи контроль над безпекою транзакцій, конфіденційністю персональних даних і надійністю функціонування навіть у випадках аварій чи зовнішніх впливів. У разі атак або збоїв механізми автоматичного виявлення інцидентів активують заздалегідь прописані сценарії реагування, що включають ізоляцію сегментів, зупинку сесій,

зміну токенів доступу й переконфігурацію маршрутизації. Це створює передумови для відновлення роботи без значних втрат, утримуючи цифрову стійкість навіть за умов розподілених атак на кілька векторів одночасно. Особливу увагу приділено прозорості процедур аудиту - усі дії користувачів, системних адміністраторів і автоматизованих агентів фіксуються, логуються й корелюються між собою для подальшого аналізу та виявлення відхилень. Таким чином, загальна архітектура побудована не лише як бар'єр проти вторгнення, а як гнучка система саморегуляції, що здатна до адаптації, реконфігурації й підтримки цілісності сервісів у динамічному середовищі.

Результатом такої трансформації стало створення цифрового середовища, яке не лише обмежує доступ до системи для неавторизованих користувачів, а й передбачає аналітичне прогнозування загроз до того, як вони реалізуються. Поведінкові алгоритми, які аналізують контекст доступу, історію дій, час і географію підключень, дозволяють формувати профілі користувачів і блокувати нетипові сценарії. Це не ізолює систему від користувачів, а навпаки - дозволяє гнучко реагувати на зміни в поведінці без зупинки сервісів. Поєднання мікросегментації, Zero Trust та автоматизованих рішень реагування забезпечує не лише збереження даних, а й високу доступність сервісів у режимі 24/7. Такі цифрові рішення, інтегровані у модель публічного адміністрування, роблять можливим безпечно надання адміністративних, фінансових і правових послуг у розподіленому форматі - від локальних структур до федерального рівня, зі збереженням структурної цілісності, надійності і контрольованості в умовах загроз гібридного характеру, що змінюються з великою швидкістю [26, с. 11].

Окремим вектором розвитку цифрових ініціатив є використання інтелектуальних агентів і машинного навчання. У рамках ініціативи AI in Government розгорнуто систему інтеграції predictive analytics у процеси оцінювання ризиків, моделювання бюджетних сценаріїв, визначення пріоритетності соціальних програм. Розробляються системи semantic search, які дають змогу користувачеві звертатися до адміністративних даних природною мовою, отримуючи релевантні відповіді у реальному часі. Також поширюється

використання NLP-модулів для автоматизованої класифікації скарг, звернень, запитів - із подальшою маршрутизацією до відповідальних органів. Застосування reinforcement learning у сфері адміністративного планування дозволяє виявляти аномальні патерни, формувати попереджувальні моделі для недопущення неефективних витрат або соціальних збоїв [36, с. 9].

Таким чином, стратегічні документи та цифрові платформи США не є лише формальними вказівками - це повноцінна операційна інфраструктура, яка забезпечує масштабованість, взаємодію, кіберзахист і функціональну адаптивність цифрового управління. Вони задають алгоритмічну і технологічну рамку для держави як платформи, в якій ключовими є не департаменти, а сервіси, не інструкції, а події, не структура, а взаємодія. Це глибокий інженерний зсув, у якому функції уряду реалізуються як код - Government as Code - із усіма атрибутами сучасної DevOps-культури, CI/CD, автоматизованого тестування, розгортання через контейнеризовані середовища типу Kubernetes і інфраструктурою, яку можна відновити з Terraform-маніфестів за кілька хвилин.

2.2. Інституційні, нормативні та технологічні чинники цифровізації публічного управління в США

Цифровізація публічного управління у США є результатом багаторівневої взаємодії між інституційними структурами, нормативно-правовими механізмами й технологічними архітектурами, що формуються в режимі постійної адаптації до змін у соціальній, економічній та інформаційній системах. Центральним координатором цифрових реформ виступає Office of Management and Budget (OMB), а саме його підрозділ - Office of the Federal Chief Information Officer (OFCIO), який виконує функцію архітектора стратегічних напрямів цифрової трансформації, формує міжвідомчі стандарти, затверджує обов'язкові до виконання технічні директиви (Circular A-130), а також адмініструє процеси валідації IT-бюджетів, що дозволяє впливати на практичне впровадження цифрових рішень у кожному федеральному агентстві. Крім цього, структура OMB інтегрує функцію Federal Enterprise Architecture (FEA), що описує

міжагентну інтеграцію цифрових процесів, класифікує сервіси, визначає стандарти обміну даними, підтримує створення єдиної словникової бази для метаданих, а також координує інтеграцію аналітичних інструментів у публічне адміністрування. Через ці механізми вибудовується єдина цифрова топологія, у якій кожна агенція виступає елементом вищого рівня цифрової екосистеми [41, с. 6].

Впливовим актором у реалізації цифрових інновацій є General Services Administration (GSA), зокрема її спеціалізований підрозділ - Technology Transformation Services (TTS), що акумулює технічну експертизу, керує розробкою цифрових сервісів, адмініструє урядові платформи (Login.gov, Cloud.gov, FedRamp) і забезпечує підтримку впровадження новітніх архітектур - від Serverless до Event-Driven Frameworks. Під егідою GSA функціонує також 18F - організація, яка надає консалтингові послуги для державних установ у сфері UX-дизайну, API-інженерії, розгортання CI/CD-процесів, а також реалізації гнучких підходів до закупівель програмного забезпечення, що ґрунтується на підходах Agile Acquisition. За своєю природою 18F діє як внутрішній цифровий акселератор, що залучає мультидисциплінарні команди для швидкого створення прототипів, проведення user research, визначення pain-points у громадянських сценаріях та реалізації сервісів відповідно до принципів human-centered design. Завдяки гнучкій структурі цей підрозділ має можливість масштабувати MVP-рішення у продакшн без втрати якості завдяки застосуванню інфраструктур типу Kubernetes, Helm Charts, Terraform-скриптів, які дозволяють відтворювати середовища за короткий час і забезпечувати гнучке адміністрування.

У нормативному вимірі цифровізація державного управління в США функціонує в межах кількох паралельних правових режимів, які утворюють адаптивну систему контролю, відповідальності та технічної реалізованості цифрових ініціатив. Одним із базових документів є Federal Information Security Modernization Act (FISMA), який встановлює принципи управління інформаційною безпекою в державних структурах, вимагає регулярного аудиту

кіберзахисту, впровадження політик моніторингу інцидентів, а також інтеграцію систем виявлення вторгнень на основі машинного навчання.

Таблиця 2.2

Нормативні основи цифровізації державного управління США

Нормативний акт / документ	Функціональний фокус	Інституційна підтримка	Цифрові інструменти / технології
Federal Information Security Modernization Act (FISMA)	Інформаційна безпека, аудит, моніторинг	Office of Management and Budget (OMB), DHS	Інтеграція SIEM-систем, ML-алгоритми виявлення вторгнень
E-Government Act	Цифрова доступність, відкритість, міжвідомча інтеграція	General Services Administration (GSA), OMB	Електронний документообіг, відкриті дані, доступ до реєстрів
Framework for Improving Critical Infrastructure Cybersecurity (NIST)	Захист критичної цифрової інфраструктури	National Institute of Standards and Technology (NIST)	Модель: ідентифікація – захист – виявлення – реагування – відновлення
NIST Special Publications Series	Стандарти управління ризиками, технічні протоколи	NIST Cybersecurity Framework Program	Політики авторизації, стандарти шифрування, безпечне зберігання даних
Continuous Diagnostics and Mitigation Program (CDM)	Безперервне оцінювання безпеки цифрових ресурсів	Department of Homeland Security (DHS), CISA	Агентно-орієнтовані сканери, автоматичне оновлення політик доступу
Trusted Internet Connections (TIC) initiative	Захист міжмережних з'єднань, централізація контролю доступу	Federal CIO Council	VPN-інфраструктура, сегментовані шлюзи, централізовані політики контролю

Іншим структуроутворювальним елементом є E-Government Act, який задає рамкові орієнтири щодо цифрової доступності, відкритості даних, формування міжвідомчих платформ, впровадження електронного документообігу та інтеграції з публічними реєстрами. На рівні стандартів особливо значущою є серія документів, що видаються Національним інститутом

стандартів і технологій (NIST), зокрема Framework for Improving Critical Infrastructure Cybersecurity, яка встановлює модель ідентифікації, захисту, виявлення, реагування та відновлення цифрових активів. Ця модель реалізується через системи типу SIEM (Security Information and Event Management), які автоматично індексують, аналізують, класифікують інциденти, виявляють закономірності в потоках даних, і через алгоритми поведінкової аналітики визначають потенційні вектори атак або несанкціонованого доступу [56, с. 75].

Інституційно уряд США використовує горизонтально-мережеву модель координації цифрових реформ. Federal CIO Council - міжвідомча платформа, що об'єднує керівників цифрових трансформацій усіх федеральних агентств, створює архітектурні шаблони, публікує інструкції з впровадження micro frontends, API-first policy, керує реєстрами відкритих даних, а також координує використання комерційних рішень у межах blanket purchase agreements. На додачу функціонує U.S. Digital Service (USDS), яка є аналогом технологічного стартапу в межах уряду, що працює за принципами інтенсивної ітерації, стрімкої прототипізації та користувацького тестування. USDS концентрує увагу на проєктах із високою соціальною значущістю - від цифрових послуг для ветеранів до оптимізації податкових сервісів, діючи через впровадження компонентної архітектури, моноліт-декомпозиції, спліт-тестування функціоналу та машинної обробки звернень. Технічно USDS активно застосовує механізми контейнеризації, оркестрації через Docker Swarm або Kubernetes, використовуючи Helm для управління складними середовищами, що дозволяє масштабування без втрати стабільності [27, с. 10].

На рівні технологічних детермінантів цифровізація публічного управління США базується на архітектурі децентралізованих даних, в якій ключову роль відіграють технології blockchain для аудиту ланцюжків транзакцій, homomorphic encryption для обчислень над зашифрованими даними, edge analytics для передобробки інформації безпосередньо в точках збору. Для забезпечення доступності платформи впроваджуються serverless-рішення - AWS Lambda, Azure Functions - що дозволяють динамічно масштабувати сервіси залежно від

навантаження, мінімізуючи витрати на інфраструктуру. Водночас моделі digital twin використовуються в урядовому прогнозуванні інфраструктурних змін - зокрема, для імітації міграційних процесів, аналізу трафіку, симуляції зміни демографічного профілю у визначених районах. Використання таких моделей вимагає тісної інтеграції з системами геоінформаційного аналізу (GIS), багатоварштовної агрегації з open-source репозиторіїв (OpenStreetMap, Census APIs) і поєднання з модулями агентного моделювання для вивчення поведінкових реакцій у кризових сценаріях.

Системна підтримка інновацій на федеральному рівні здійснюється через структури типу Office of Science and Technology Policy (OSTP), яка координує розробку довгострокових стратегій у сфері штучного інтелекту, квантових обчислень, біометрії, біоінформатики, аналізу великих даних. OSTP адмініструє White House National AI Initiative, що передбачає розгортання нейронних систем у судових реєстрах, податковій аналітиці, передбаченні соціальних ризиків. На технічному рівні це підтримується через національні лабораторії DOE (Department of Energy), які виступають тестовими майданчиками для моделювання великих обчислювальних навантажень, калібрування систем НРС (High Performance Computing), тренування моделей трансформерів на масивах даних, зібраних із різних реєстрів. Це дозволяє державі виступати не лише користувачем технологій, а й їхнім розробником, забезпечуючи суверенність алгоритмів і контроль над критичною обчислювальною інфраструктурою [24, с. 12].

У контексті соціотехнологічної взаємодії в межах цифрової трансформації важливо враховувати вплив civic tech-екосистем - децентралізованих спільнот розробників, дизайнерів, аналітиків, які у партнерстві з державними агентствами створюють сервісні продукти, адаптовані до локальних контекстів. Такі ініціативи, як Code for America, реалізують пілотні проєкти із залученням відкритого коду, хакатонів, civic design sessions, де рішення тестуються з реальними користувачами до виходу у публічне середовище. У технічному плані вони базуються на відкритих фреймворках - React, Vue, Node.js, що дозволяє

гнучко масштабувати рішення, з урахуванням вимог ADA (Americans with Disabilities Act), WCAG і рекомендацій щодо mobile-first design. Через такі платформи відбувається включення громадян у процес формування цифрових сервісів, що змінює баланс сил у цифровій демократії - з одностороннього інформування до ко-дизайну публічних сервісів.

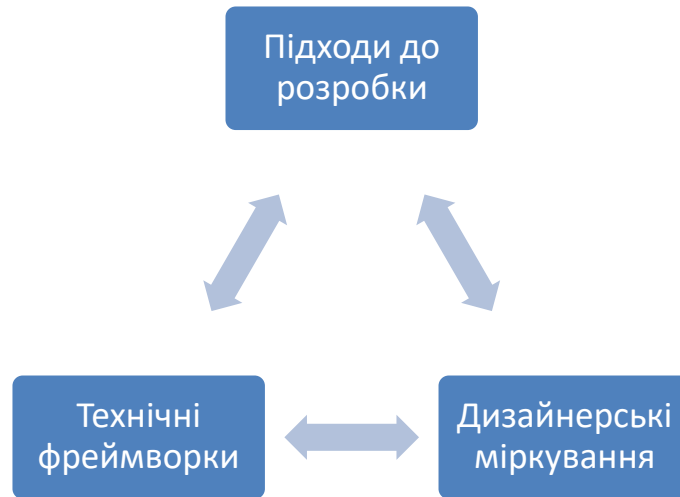


Рис. 2.2 Компоненти екосистеми civic tech

Формування законодавчого фундаменту для цифровізації публічного управління у США відбувається через багаторівневу систему актів, регламентів, технічних директив і міжагентних угод, які створюють нормативну архітектуру для впровадження, оцінювання та стандартизації цифрових рішень у межах державного сектору. Одним із ключових документів, що визначає стратегічні рамки цифрової трансформації, є E-Government Act of 2002, який формалізує обов'язок федеральних установ застосовувати електронні засоби взаємодії, впроваджувати веб-сервіси для публічного доступу, забезпечувати інтеоперабельність внутрішніх систем та створювати інклюзивні інтерфейси. Цей нормативний акт закладає концепцію «performance-based and citizen-centric government», у межах якої електронні послуги мають не лише підвищувати ефективність внутрішніх процедур, а й бути інтегрованими в життєві сценарії громадян. Реалізація такого підходу передбачає перехід від моделі «static content delivery» до «dynamic service orchestration», де всі транзакції, запити, інформаційні обміни базуються на стандартизованих API, з чітким маршрутом

обробки, контрольованими точками входу та виходу й повною фіксацією логів взаємодії. Цей підхід знаходить реалізацію в обов'язковій вимозі до відомств публікувати документи в електронному форматі, підтримувати цифрові канали комунікації й дотримуватися принципів доступності відповідно до вимог Section 508, що регламентує цифрову інклюзію для осіб з інвалідністю [22, с. 6].

Наступним етапом у нормативному забезпеченні стала поява Federal Information Security Modernization Act (FISMA), який установив обов'язкові практики з управління ризиками, захисту даних, моніторингу інцидентів і реагування на загрози в інформаційних системах федеральних установ. У рамках цього закону була впроваджена модель циклічного оцінювання безпеки на основі Risk Management Framework (RMF), розробленої NIST, яка вимагає від агентств ідентифікації цифрових активів, класифікації рівня ризику, формування control baseline на основі NIST SP 800-53 та регулярного проведення Penetration Testing і Security Assessment Reports. Згідно з цим підходом, кожна система має документально зафіксований АТО (Authorization to Operate), який підтверджує її відповідність стандартам безпеки й дозволяє інтеграцію з іншими елементами цифрової екосистеми. Застосування цього інструментарію має пряме технологічне відображення у побудові SIEM/SOAR-середовищ, що автоматично виявляють аномальні активності, проводять кореляцію подій, верифікують ідентичність через багатфакторні шлюзи й активують протоколи реагування у випадку порушення політик безпеки.

Законодавча парадигма цифрової трансформації також ґрунтується на принципах відкритості даних, закріплених у Freedom of Information Act (FOIA), а також у більш сучасному Foundations for Evidence-Based Policymaking Act (2018), що зобов'язує органи влади створювати політики керування даними, призначати CDO (Chief Data Officers) і забезпечувати публічний доступ до структурованих масивів інформації у форматах, сумісних з машинною обробкою. У рамках цього правового підходу створюються механізми для реалізації Open Data Policy - зокрема, Data.gov як агрегатор публічних ресурсів, що підтримує каталогізацію за DCAT-стандартами, забезпечує RESTful-доступ

до масивів, фіксацію версій, контроль консистентності й валідацію метаданих за допомогою JSON Schema. Такі платформи дозволяють аналітичним агентствам, дослідницьким інституціям і приватному сектору взаємодіяти з адміністративними даними в режимі near real time, створюючи вторинні сервіси, прогностичні моделі, інтегровані в життєві системи охорони здоров'я, мобільності, інфраструктурного управління чи екологічного моніторингу [52, с. 61].

Крім загальнонаціональних нормативів, функціонує низка регламентів і директив, що деталізують вимоги до цифрової інфраструктури. Federal Identity, Credential, and Access Management (FICAM) Framework унормовує систему електронної ідентифікації, використання цифрових сертифікатів, Single Sign-On, автентифікаційних механізмів на основі PKI (Public Key Infrastructure), FIDO2-протоколів і біометрії. У межах цієї структури реалізовано платформу Login.gov, що забезпечує централізовану автентифікацію в державних сервісах, інтегруючи SAML і OpenID Connect, дозволяючи користувачам мати єдиний профіль доступу до десятків агентств. Така архітектура потребує чітких технічних регламентів доступу, контрольних точок перевірки, визначення ролей і прав доступу, що реалізується через RBAC (Role-Based Access Control) і ABAC (Attribute-Based Access Control), моделі, в яких права користувача залежні не лише від ролі, а й від динамічних умов середовища - місцезнаходження, типу пристрою, характеру запиту.

З погляду стандартизації, критичним елементом є серія документів NIST, серед яких SP 800-63 (Digital Identity Guidelines), SP 800-171 (Protecting Controlled Unclassified Information), SP 800-207 (Zero Trust Architecture), які мають статус обов'язкових до імплементації у державних системах. Вони регламентують мінімальні вимоги до автентифікації, протоколи обміну, політики конфіденційності, архітектуру мереж, шифрування даних у транзиті та у спокої, а також поведінкову аналітику. У результаті кожна агенція повинна інтегрувати Zero Trust-принципи - тобто відмову від довіри до будь-якого пристрою чи користувача без перевірки, реалізацію постійного моніторингу доступу, micro-segmentation інфраструктури, контроль lateral movement через

системи IDS/IPS. У поєднанні з SOC (Security Operations Center) це створює замкнуту систему кібернагляду, у якій будь-яка аномалія ініціює автоматизовану перевірку, блокує доступ і формує розгорнутий інцидент-репорт [59, с. 9].

Законодавчо унормоване також використання хмарних технологій: Cloud Smart Strategy, затверджена OMB, передбачає імператив до використання cloud-native сервісів, а FedRAMP (Federal Risk and Authorization Management Program) виконує функцію авторизаційного фреймворку, що визначає процедуру безпекової оцінки, тестування, валідації та моніторингу хмарних сервісів для федеральних агенцій. FedRAMP передбачає поділ провайдерів за Impact Levels, що відповідають категоріям конфіденційності, цілісності та доступності. Процедура авторизації включає SSP (System Security Plan), тестування згідно з Penetration Testing Framework, контроль вразливостей через CVSS, постійний моніторинг з генерацією щоквартальних ConMon Reports. Усе це дозволяє агентствам обирати провайдерів, які довели відповідність архітектур, протоколів шифрування, процедур disaster recovery і обробки інцидентів вимогам нормативної системи.

У площині прозорості законодавство США передбачає низку механізмів, спрямованих на контроль за використанням даних, прозорість адміністративних рішень і доступ громадян до механізмів зворотного зв'язку. Paperwork Reduction Act зобов'язує агентства зменшувати адміністративне навантаження, автоматизувати процеси збору інформації, забезпечити можливість користувачам відстежувати статус звернень через цифрові кабінети. Data Transparency Act (DATA Act) зобов'язує оприлюднювати дані про витрати, фінансування, закупівлі у відкритому форматі, інтегрувати фінансові дані з системами аналітики, публікувати їх на платформах типу USASpending.gov. Законодавчо передбачено функціонування систем FOIA Online, що дозволяють громадянам запитувати й отримувати документи, відстежувати статус запитів, подавати скарги - усе через інтегровану цифрову інфраструктуру з єдиною точкою входу. У поєднанні з аналітичними платформами на базі Power BI або

Tableau це дає змогу користувачам самостійно формувати візуалізації, проводити аналіз і поширювати результати серед спільнот [17, с. 9].

Загалом законодавче забезпечення цифрової трансформації в США є технічно орієнтованим, функціонально деталізованим і побудованим за принципом гнучкої стандартизації - коли імперативи відповідності доповнюються можливостями адаптації під конкретні технологічні сценарії. Це дозволяє створювати регламентовані, прозорі й безпечні цифрові середовища, у яких кожен компонент - від хмарного сервісу до механізму подачі FOIA-запиту - функціонує в рамках чітко визначеної нормативної матриці. У цій системі немає місця спонтанності чи інтуїтивному рішення: кожна зміна, кожен новий модуль, кожне підключення нового компонента має пройти валідацію, оцінювання ризиків, технічне тестування, опис у відповідних policy documents і бути зафіксованим у відповідних каталогах. Це й забезпечує сталість цифрових реформ - не через централізований контроль, а через нормативно формалізовану логіку розгортання змін.

Технологічна інфраструктура, що формує основу цифрових перетворень у публічному управлінні США, є багаторівневою, гетерогенною та динамічною архітектурою, яка постійно адаптується до зростаючих вимог до масштабованості, безпеки, інтероперабельності та аналітичної спроможності державних систем. У фундаменті цієї інфраструктури лежить концепція government-as-a-platform, що передбачає створення уніфікованого цифрового середовища, побудованого на принципах сервісної орієнтації, розподіленої обробки даних, логіки подій і стандартів відкритої взаємодії. Центральним компонентом такої архітектури виступають хмарні сервіси, які забезпечують не лише зберігання, а й обробку, маршрутизацію, агрегацію та аналіз даних у реальному часі. Урядові органи використовують гібридні хмарні моделі - зокрема AWS GovCloud, Azure Government, Google Cloud for Government - які мають сертифікацію FedRAMP, підтримують високий рівень ізоляції, відповідають вимогам до обробки даних з обмеженим доступом (CUI) та забезпечують політику zero trust за замовчуванням. Такі середовища дозволяють

реалізовувати кластеризовані архітектури за допомогою Kubernetes, підтримувати багаторівневу розгортку через Helm Charts, автоматизувати інфраструктуру за допомогою Terraform і контролювати доступ через IAM-політики, інтегровані з FICAM-рішеннями [25, с. 7].

В основі більшості цифрових платформ, які функціонують у межах публічного адміністрування США, знаходяться мікросервісні архітектури з подієво-орієнтованою логікою. Системи побудовані на основі RESTful API з можливістю масштабування через API gateway (зокрема Amazon API Gateway або Apigee), де кожен функціональний модуль - це автономний сервіс із власною схемою даних, протоколом виклику, лімітом запитів і логікою моніторингу. Усі транзакції логуються через distributed tracing системи, такі як OpenTelemetry або Zipkin, які дозволяють відслідковувати маршрут запиту від користувача до базового обчислювального вузла, включаючи всі рівні обробки. Для обробки подій застосовуються брокери повідомлень типу Apache Kafka, RabbitMQ, Amazon EventBridge - вони дозволяють реалізувати асинхронну обробку, оркеструвати мільйони подій на секунду й забезпечити масштабованість критичних компонентів без деградації системи. Інфраструктура подібного рівня вимагає функціонального поділу компонентів за принципом bounded context, що дозволяє уникати надмірної залежності між модулями та знижує ризики каскадних збоїв. Застосування такої архітектури є особливо ефективним для побудови сервісів соціального захисту, охорони здоров'я та податкового адміністрування, де кожна підсистема має власну логіку, але повинна інтегруватися з єдиним інформаційним середовищем.

Ключовим елементом цифрової інфраструктури є аналітичні системи, які виконують функцію не лише ретроспективного аналізу, а й предиктивного моделювання, симуляції варіантів дій та оптимізації ресурсів у реальному часі. Для цього використовуються сховища типу data lake - наприклад Amazon S3 або Azure Data Lake - які інтегруються з ETL-пайплайнами на базі Apache NiFi, AWS Glue, Airflow. Дані зчитуються, трансформуються, очищаються та уніфікуються відповідно до схем Avro, Parquet або ORC, після чого зберігаються у вигляді

структурованих масивів, готових до аналізу. Для реалізації моделей прогнозування застосовуються інструменти машинного навчання - Scikit-learn, TensorFlow, Amazon SageMaker, Azure ML - які тренуються на великих масивах історичних даних, включаючи фінансові транзакції, звернення громадян, індикатори соціального ризику, геопросторові патерни. Аналітична інфраструктура підтримує концепцію Feature Store - централізованого репозиторію попередньо оброблених ознак (features), які використовуються в різних моделях без необхідності дублювання процесу підготовки. Це дозволяє зменшити час тренування моделей, підвищити узгодженість прогнозів і забезпечити explainability через інтеграцію з SHAP, LIME, ELI5 [38, с. 46].

Безпекова складова цифрової інфраструктури США побудована за принципами багаторівневої ізоляції, логічного поділу трафіку та поведінкової аналітики. Реалізація Zero Trust Architecture здійснюється через мікросегментацію мережевого доступу, де кожен сегмент ізолюваний у межах віртуальних приватних мереж (VPC), контролюється через мережеві ACL і Cloud Firewall з DPI-модулями. Ідентифікація користувачів здійснюється через MFA з біометричними компонентами (Face ID, Touch ID, FIDO2 tokens), а контроль доступу до ресурсів реалізується через dynamic attribute-based policies, де права залежать від реального контексту сесії - локації, часу, типу пристрою. Системи захисту включають NGFW, IDS/IPS, EDR-рішення, централізовані SIEM-платформи - зокрема Splunk, ELK Stack, QRadar - які виконують кореляцію подій, виявляють аномалії та активують playbooks через SOAR-системи типу Palo Alto Cortex XSOAR. Поведінковий аналіз (UEBA) виконується на основі патернів доступу, швидкості навігації, типових маршрутів запитів, що дозволяє виявляти навіть низькоінтенсивні атаки з lateral movement. Після виявлення аномалії система може ініціювати блокування, активувати sandbox-оточення або ізолювати інцидент у віртуальному середовищі для детального аналізу без ризику для основної системи [55, с. 6].

Підтримка стабільної роботи інфраструктури реалізується через автоматизовані інструменти управління конфігурацією (Ansible, Puppet, Chef),

CI/CD-середовища (Jenkins, GitHub Actions, GitLab Runners) та системи спостереження (Prometheus, Grafana, Datadog). Усі цифрові сервіси функціонують відповідно до принципів site reliability engineering (SRE), що передбачає встановлення SLO (Service Level Objectives), визначення бюджетів помилок (error budgets) і постійне тестування навантаження за допомогою chaos engineering. Це дозволяє імітувати збої, змінювати умови середовища, порушувати залежності - з метою виявлення вузьких місць і підвищення стійкості до аварій. Такі практики особливо важливі в умовах роботи критично важливих сервісів, де навіть декілька хвилин простою можуть призвести до порушення життєво значущих адміністративних процесів.

РОЗДІЛ 3. МОЖЛИВОСТІ, РИЗИКИ ТА НАПРЯМИ РОЗВИТКУ ЦИФРОВОГО УПРАВЛІННЯ В КОНТЕКСТІ ГЛОБАЛЬНИХ ТЕНДЕНЦІЙ

3.1. Переваги та ризики цифрової трансформації державного управління США

Цифрова трансформація державного управління у США становить системну реконфігурацію адміністративної діяльності на основі алгоритмізації процесів, автоматизації транзакцій, уніфікації інформаційних потоків і впровадження машинної логіки прийняття рішень. Одним із ключових позитивних ефектів є радикальне підвищення ефективності операційного адміністрування, що досягається через застосування DevOps-підходів у розробці державних сервісів, реалізацію інфраструктур як коду (IaC), впровадження CI/CD-конвеєрів для автоматичного розгортання змін і безперервного оновлення. У практичному сенсі це дозволяє скоротити час реалізації нових політик із місяців до тижнів, як це сталося у випадку екстреного запуску програм підтримки малого бізнесу під час пандемії COVID-19 через платформи Small Business Administration, що базувались на modular cloud architecture. Автоматизоване верифікування даних, використання workflow-рушіїв типу Camunda або Apache Airflow для маршрутизації заявок, застосування SSO-систем для уніфікації доступу призвели до ліквідації ручної обробки великої частини адміністративного навантаження, особливо в сферах обслуговування населення - медичних, соціальних, фінансових. У підсистемах внутрішньої координації між агентствами було реалізовано інтеграційні шини обміну (ESB) і API-шлюзи, що дозволили автоматично агрегувати, маршрутизувати і реплікувати дані без необхідності дублювання структур або звернень між відомствами. Це забезпечило одномоментний доступ до актуальних наборів даних із різних систем, зменшивши затримки в ухваленні рішень і кількість транзакцій, необхідних для виконання однієї управлінської дії [44, с. 14].

Доступність сервісів зазнала якісної трансформації внаслідок впровадження мобільно-орієнтованої логіки розробки (mobile-first), оптимізації інтерфейсів за принципами US Web Design System, а також завдяки переходу до адаптивних моделей обслуговування, що враховують поведінкові патерни користувачів. Через системи A/B-тестування, поведінкової аналітики (Google Tag Manager, Segment, Mixpanel), та синтетичного моніторингу користувацького досвіду здійснюється динамічне налаштування контенту, структури взаємодії та навігації, що підвищує індекс завершеності транзакцій (completion rate), зменшує кількість звернень до офлайн-каналів та покращує інклюзивність сервісу для маргіналізованих груп. Платформи Login.gov, USA.gov, Benefits.gov функціонують як єдині точки входу в цифрову державу, агрегуючи сотні послуг і застосовуючи модульну архітектуру, яка дозволяє підключати нові сервіси без потреби у створенні нових фронтендів. Ця централізація доступу сприяє усуненню інформаційної фрагментації, забезпечує узгодженість даних, дозволяє повторне використання верифікованої інформації через уніфіковані API, що не лише економить час користувача, а й знижує адміністративні витрати на верифікацію, дублювання й архівацію. Додатково, інтеграція голосових інтерфейсів, чат-ботів на базі GPT-моделей, адаптивних помічників з елементами машинного навчання створює новий тип сервісної взаємодії - контекстуальний, персоналізований, з прогнозуванням потреб і проактивним інформуванням громадянина [61, с. 10].

Цифрові інструменти стали основою залучення громадян до прийняття рішень і контролю за діяльністю адміністрації. Через платформи типу regulations.gov користувачі можуть подавати коментарі до проєктів нормативно-правових актів, брати участь у консультаціях, впливати на формулювання політик. Впровадження Civic Tech-ініціатив на кшталт Code for America, які співпрацюють з муніципалітетами, створюють відкриті дашборди, публічні API, інтерактивні карти інфраструктури, бюджетів, виборчих даних, дозволяє спільнотам самостійно моніторити ситуацію, будувати власні сервіси та генерувати зворотний зв'язок. Це забезпечує емерджентне середовище

інституційної взаємодії, де громадянська аналітика підсилює управлінські функції, виводячи державу з ролі виключного монополіста на знання. В умовах систем Open Data, які підтримуються національними платформами типу Data.gov, створюються цілі екосистеми аналітичного підприємництва, зокрема у сферах транспорту, енергетики, охорони здоров'я, екології - де приватні компанії та НУО розробляють сервіси на основі відкритих наборів, тим самим розширюючи функціональність державного управління без прямої участі органів влади [43, с. 12].

Таблиця 3.1

Вплив цифрових інструментів на громадянську участь та публічне управління

Категорія впливу	Цифрові рішення / інструменти	Форми участі громадян	Результати для державного управління	Сфери застосування
Онлайн-консультації	Платформи типу regulations.gov	Подання коментарів до законопроектів, участь у консультаціях	Врахування публічної думки, прозорість формування політик	Нормотворчість, регулювання
Civic Tech ініціативи	Code for America, хакатони з органами місцевої влади	Створення додатків, співпраця з муніципалітетами	Спільна розробка сервісів, зменшення навантаження на адміністративні ресурси	Урбаністика, бюджетування, транспорт
Візуалізація даних	Публічні дашборди, інтерактивні мапи, графіки в реальному часі	Самостійний моніторинг, контроль використання коштів	Підвищення підзвітності органів влади	Інфраструктура, вибори, бюджетна прозорість
Відкриті API	API-доступ до державних даних	Розробка власних інструментів громадами, аналітиками	Залучення ІТ-спільноти до вирішення соціальних задач	Енергетика, екологія, охорона здоров'я
Open Data екосистеми	Платформи типу Data.gov, національні реєстри відкритих даних	Пошук, обробка, повторне використання наборів	Поява аналітичного підприємництва, зниження монополії на знання	Бізнес-аналітика, громадські ініціативи

Громадянська аналітика	Застосування дата-наборів для локального аналізу	Побудова звітів, оцінка ефективності рішень	Виведення держави з ролі єдиного джерела аналітики	Освіта, соціальні дослідження
------------------------	--	---	--	-------------------------------

Водночас цифрова трансформація породжує низку ризиків, які мають як технічну, так і організаційно-поведінкову природу. У технічному вимірі найгострішими є проблеми кібербезпеки та стійкості до атак. Атаки типу supply chain compromise, використання zero-day у бібліотеках з відкритим кодом, експлуатація вразливостей у інтерфейсах API, впровадження зловмисного коду в CI/CD-конвеєри - усе це створює передумови для системних збоїв, витоку персональних даних або паралічу ключових адміністративних процесів. Реалізація Zero Trust Architecture, впровадження SIEM/SOAR-рішень, використання EDR, мікросегментація трафіку, криптографічне шифрування даних - це лише базовий набір відповідей, які потребують постійного оновлення, сканування, тестування та перехоплення сигнатур загроз. Не менш проблемною є ймовірність технологічного зносу - застарілі системи управління ідентифікацією, непідтримувані фреймворки, обмеження старих API - що гальмує адаптацію, ускладнює інтеграцію й збільшує вартість модернізації [46, с. 63].

З боку організаційного управління постає проблема залежності від технологічних монополістів, що постачають пропріетарні рішення з обмеженою можливістю модифікації. В умовах централізації хмарних потужностей у руках кількох постачальників існує ризик vendor lock-in - неможливості оперативної міграції між середовищами, що обмежує стратегічну гнучкість держави. Ця ситуація підсилюється відсутністю у деяких агентствах достатньої внутрішньої експертизи, яка дозволила б розгортати інфраструктури самостійно, здійснювати аудит, підтримку й оновлення без залучення зовнішніх консультантів. Ризики пов'язані також з фрагментацією цифрової компетентності серед персоналу, нерівномірністю впровадження DevOps-культури, недостатньою інтеграцією з управлінськими циклами. Це ускладнює трансформацію організаційної

культури, призводить до опору змінам, створює паралельне існування традиційних і цифрових практик, які можуть конфліктувати між собою.



Рис. 3.1 Виклики цифрової трансформації

Поведінковий ризик пов'язаний із зниженням приватності, надмірною алгоритмізацією рішень та непрозорістю логіки роботи систем. Застосування систем машинного навчання для соціального скринінгу, виявлення шахрайства, прогнозування поведінки може створювати ефект *algorithmic bias* - упередженості, що виникає внаслідок невірно підібраних навчальних вибірок, асиметричного врахування змінних або некоректної інтерпретації даних. Це може призвести до дискримінаційних практик, автоматизованих рішень, які не підлягають оскарженню, втрати довіри до держави. Відсутність *explainability* у моделях глибокого навчання обмежує можливість контролю за обґрунтованістю адміністративних дій, а недосконалість механізмів аудиту алгоритмів створює сліпі зони, в яких цифрова система діє автономно без механізмів втручання. Підсилює цю проблему й інформаційна асиметрія - користувачі не розуміють, як працює система, які дані збираються, як вони обробляються, кому доступні, яким чином формуються рекомендації чи рішення. Це веде до ефекту *algorithmic*

oracity - відчуження, зниження залученості, зростання емоційної відстані між громадянином і державою.

Ризики цифрової трансформації державного управління у США набувають дедалі більшої складності внаслідок глибокої інтеграції цифрових інфраструктур у всі рівні публічної взаємодії - від процедур ідентифікації до алгоритмізації прийняття рішень. У системі, побудованій на розподілених сервісах, віртуалізованих середовищах і взаємопов'язаних API, кожен компонент стає потенційною вразливістю, що відкриває шлях для цільових кіберзагроз. Основною проблемою є зростання складності attack surface - площини атаки - внаслідок динамічного масштабування, мультимарної архітектури, використання серверлес-фреймворків і взаємодії з third-party інтеграціями [53, с. 9].

Це створює ситуацію, в якій навіть незначна вразливість у відкритій бібліотеці, застарілий dependency або неоновлений endpoint можуть стати точкою входу для lateral movement і privilege escalation. Класичні підходи до perimeter security більше не працюють - система має працювати в моделі Zero Trust, де жоден компонент не отримує довіри без постійної перевірки. Для цього в державних платформах США застосовується комплекс із SIEM/SOAR, EDR/XDR, UEBA, NDR - зокрема Splunk, Sentinel, CrowdStrike Falcon, Darktrace, які в режимі 24/7 здійснюють telemetry capture, threat intelligence ingestion, sandbox-емуляцію і автоматичне реагування через playbook-driven orchestration. Проте попри масштабованість і технічну витонченість, жодна система не гарантує повної недоторканності. Навпаки - сам факт глибокої цифровізації означає зростання потенційного збитку у випадку компрометації. Злом єдиного компонента ідентифікації (як-от SAML-ключа в Login.gov) відкриває доступ до критичних транзакцій, до повного профілю громадянина, до процедур, які мають юридичну чинність. [45, с. 8].

Цифровий розрив (digital divide) у цьому контексті виступає не лише як проблема доступу до інтернету, а як багатовимірний бар'єр - інфраструктурний, когнітивний, соціокультурний. У США, попри наявність національних програм

на кшталт Broadband Equity, Access, and Deployment Program (BEAD), десятки мільйонів громадян залишаються поза зоною стабільного підключення або не мають доступу до пристроїв, які дозволяють повноцінно взаємодіяти з адміністративними порталами. Більше того, навіть за наявності технічного каналу, значна частина населення не має достатньої цифрової грамотності, щоб ефективно користуватись сервісами. Це спричиняє ефект соціальної стратифікації: одні отримують доступ до швидких, зручних, персоналізованих послуг, а інші змушені звертатися до перевантажених кол-центрів, фізичних офісів або взагалі залишаються поза цифровою державою. Розрив посилюється серед вразливих категорій - літніх людей, осіб з інвалідністю, мігрантів, малограмотних користувачів. Навіть інтерфейси, оптимізовані за WCAG 2.1, не завжди покривають повний спектр комунікативних моделей. Системи voice-to-text не завжди коректно розпізнають акценти, візуальні інтерфейси не адаптуються до специфіки когнітивних розладів, багатомовність у багатьох випадках реалізована через автоматичний переклад без семантичного коригування. Це не просто технічна проблема - це ризик сегментації публічного управління, коли держава починає функціонувати асиметрично щодо своїх громадян.

Окремий шар загроз породжують етичні дилеми, пов'язані з алгоритмізацією ухвалення рішень. Застосування моделей машинного навчання для скорингу, розподілу пільг, прогнозування ризиків у правосудді або соціальній політиці неминуче призводить до появи algorithmic bias - викривлення, що зумовлене нерепрезентативністю тренувальних вибірок, латентною дискримінацією або некоректною постановкою задачі. Моделі, які використовуються в Predictive Policing, можуть реплікувати расові упередження, які присутні у вхідних даних. Алгоритми, що оцінюють кредитоспроможність або ймовірність безробіття, можуть спиратись на ознаки, що корелюють із демографічними чинниками, фактично обмежуючи доступ до пільг або можливості участі в програмах. У державному секторі це означає, що формально «нейтральні» системи можуть ухвалювати рішення, які мають дискримінаційний

характер, без явного втручання людини. Відсутність explainability у глибоких моделях (особливо в LSTM, transformers, ensemble-моделях) означає, що громадянин не може зрозуміти, чому саме його заявку було відхилено, а отже - не має права на обґрунтоване оскарження. Це ставить під сумнів принцип адміністративної справедливості та знижує довіру до цифрових інститутів, які починають сприйматись як opaque systems - непрозорі, неконтрольовані й автономні [19, с. 13].

Приватність в умовах цифрової держави перетворюється на складну конструкцію, що постійно балансує між зручністю, безпекою й контролем. У системах, які використовують єдину цифрову ідентичність, відбувається концентрація величезних обсягів персональних даних - біометричних, поведінкових, транзакційних, геолокаційних. Використання технологій трекінгу в реальному часі, аналізу цифрового сліду, логування сесій через системи centralized identity management означає, що будь-який запит, будь-яке натискання клавіші або навігаційний клік залишає цифрову мітку, яка може бути агрегована, проаналізована й збережена. У багатьох випадках громадяни навіть не знають про обсяг зібраної інформації, її джерела, цілі обробки, терміни зберігання або умови передачі третім сторонам. У правовому полі США діє складна система регулювання - FISMA, Privacy Act, CCPA на рівні Каліфорнії, але відсутність єдиного федерального регламенту означає фрагментарність політик і неоднозначність тлумачень. Це створює ситуації, в яких один і той самий набір даних може оброблятися по-різному залежно від юрисдикції, що знижує прогнозованість і ускладнює правозастосування. Приватність більше не є стабільною категорією - це динамічна змінна, що залежить від архітектури платформи, протоколів аутентифікації, політик доступу та логіки обробки даних.

Ризики посилюються в умовах взаємодії держави з приватними провайдерами технологій. Передача частини функцій (ідентифікація, хмарне зберігання, аналітика) зовнішнім компаніям означає втрату контролю над ланцюгом обробки - особливо коли йдеться про використання closed-source моделей, алгоритмів з комерційною ліцензією, обчислювальної інфраструктури,

розміщеної поза юрисдикцією США. Це породжує загрозу external inference - коли провайдер, маючи доступ до метаданих або логів, може здійснювати аналітику другого порядку, генеруючи нові знання про користувачів без прямого доступу до вмісту. Такі знання можуть бути використані для побудови профілів, поведінкових матриць, прогнозних моделей, що виходить за межі початкової мети збирання даних. В умовах відсутності абсолютної прозорості алгоритмів, навіть шифрування й токенизація не дають повного захисту - достатньо патерну запитів, таймінгів або частоти взаємодій, щоб відновити частину семантики. Це означає, що приватність - це не тільки питання захисту вмісту, а й захисту контексту, який дедалі важче контролювати [20, с. 8].

Таким чином, цифрова трансформація державного управління США формує надзвичайно складну динамічну систему, у якій кожна перевага має тіньову сторону, а кожне покращення функціональності - потенційну вразливість. Кібербезпека, етика, приватність і доступність більше не можуть розглядатися окремо - вони мають існувати в єдиному управлінському каркасі, який постійно тестується, переглядається, оновлюється. Потрібні нові моделі ризик-менеджменту - інтегративні, поведінкові, гібридні, здатні поєднувати технічний аудит, соціальну аналітику, юридичну відповідність і алгоритмічний контроль. У цьому полягає реальний виклик цифрової епохи: не в тому, щоб автоматизувати, а в тому, щоб гарантувати, що автоматизоване не стане джерелом нової несправедливості, непрозорості або відчуження. Державне управління, з одного боку, отримує безпрецедентні інструменти точності, передбачення й масштабованості, але з іншого - втрачає прямий контакт із контекстом, у якому живе громадянин. І якщо ці ризики не будуть системно вбудовані в архітектуру цифрового управління, вони трансформуються з технічних загроз у політичні кризи.

3.2. Перспективи розвитку цифрового врядування в умовах глобальної цифрової епохи

Перспективи розвитку цифрового врядування в умовах глобальної цифрової епохи визначаються сукупністю потужних технологічних зрушень, що перетворюють публічне адміністрування з реактивної бюрократичної структури на проактивну, динамічну, інтелектуалізовану систему прийняття рішень у реальному часі. Центральною технологічною вісьовою лінією цього процесу є конвергенція штучного інтелекту, аналізу великих даних та обчислень на периферії (edge computing), яка формує нову архітектуру державного управління - розподілену, контекстно-чутливу, здатну до самонавчання й автоматизованого коригування поведінки адміністративної системи залежно від змін середовища. Штучний інтелект у цій конфігурації виконує не функцію допоміжного інструменту, а виступає як когнітивне ядро державного організму - засіб для формування моделей політик, пріоритетизації бюджетних потоків, оцінювання ефективності втручань, персоналізації державних сервісів. У Сполучених Штатах уже сформовано стратегічний напрямок AI-enabled governance, який розгортається через ініціативи National AI Initiative, активну інтеграцію GPT-моделей в обробку адміністративного контенту, NLP-модулів для класифікації звернень і reinforcement learning у системах управління ризиками та прогнозування. Застосування методів нейронної інференції на кластерах GPU/TPU дозволяє здійснювати обробку тисяч запитів одночасно, виявляти закономірності у поведінкових паттернах громадян, моделювати результативність альтернативних управлінських сценаріїв, що значно перевершує можливості традиційної статистичної аналітики [40, с. 7].

Інтеграція великих даних у цифрове врядування також означає перехід від дискретного збору інформації до побудови постійно оновлюваного data fabric - багатовимірної інфраструктури, де потоки даних з різних джерел зливаються в єдиний когнітивний простір. Такі дані - це не лише адміністративна звітність, а й потоки сенсорної інформації, телеметрія інфраструктури, мобільні трекери, соціальні медіа, фінансові сигнали, публічні репозиторії, дані IoT-пристроїв. Об'єднання цих джерел вимагає застосування advanced data lakehouse архітектур (на кшталт Delta Lake, Apache Iceberg), які дозволяють одночасно підтримувати

транзакційні властивості, гнучку агрегацію, паралельну обробку за допомогою Spark, Dask або Ray. Інструменти stream analytics (Flink, Kafka Streams, AWS Kinesis) використовуються для аналізу подій у реальному часі - наприклад, для прогнозування навантаження на транспортні системи, ідентифікації соціальних збурень, оцінювання ефективності програм допомоги. На основі таких даних формуються моделі adaptive policy feedback loop, які дозволяють коригувати політики не після аудиту чи звітності, а на підставі живих сигналів, інтегрованих у state dashboard системи [16, с. 10].

Таблиця 3.2

Інтеграція Big Data в цифрове врядування

Компонент системи	Опис функціоналу	Технології / Платформи	Типи даних	Приклади застосування
Data fabric	Єдина інфраструктура для поєднання багатьох джерел у когнітивний простір	Spark, Dask, Ray, Delta Lake, Iceberg	Адміністративні реєстри, сенсори, трекери, соцмережі	Об'єднання фінансових, соціальних, геопросторових сигналів
Data lakehouse архітектура	Комбінує зберігання в стилі lake + керованість у стилі warehouse	Delta Lake, Apache Hudi, Apache Iceberg	Табличні, часові ряди, log-файли, telemetria	Централізоване збереження даних IoT і муніципальних систем
Stream analytics	Аналіз подій у реальному часі	Flink, Kafka Streams, AWS Kinesis	Потокові події, поведінкові сигнали, трафік	Виявлення транспортних аномалій, соціального тиску
Джерела даних	Багатовекторна система генерації сигналів	IoT, мобільні пристрої, фінансові API, публічні реєстри	GPS-треки, телеметрія, голосування, відкриті API	Прогнозування напруг у медичній/соціальній сферах

Edge computing, у свою чергу, відкриває нові можливості для децентралізованої обробки інформації без затримок, характерних для централізованих обчислювальних центрів. У публічному управлінні це особливо важливо для систем, що працюють з критичною інфраструктурою - енергетичні мережі, водопостачання, громадська безпека, охорона здоров'я. Edge-архітектури дозволяють розміщення обчислювальних потужностей

безпосередньо в точках збору інформації - на базових станціях, у муніципальних вузлах, на вулицях із сенсорами - і здійснювати локальну обробку подій із мінімальною затримкою. При цьому оброблені результати передаються до центральних систем лише в узагальненому вигляді, що знижує навантаження на основні канали, зменшує ризики втрати даних у випадку збоїв і дозволяє дотримуватись принципу *data minimization*. Це відкриває шлях до побудови автономних систем публічного реагування, де рішення можуть прийматись без участі центральних органів - зокрема, адаптивне управління світлофорами, моніторинг якості повітря з автоматичним запуском систем фільтрації, виявлення порушень порядку через аналіз відеопотоку на *edge*-сервері з інтеграцією у відповідні патрульні протоколи. Усе це формує передумови до *emergence-driven governance* - коли управлінські реакції виникають не в результаті планування, а як відповідь на сингулярні події, оброблені розподіленим інтелектом [49, с. 7].

У глобальному контексті формування майбутніх моделей цифрового врядування дедалі більше залежить від взаємодії між національними системами стандартів, технічних політик і регуляторних підходів. Сполучені Штати беруть активну участь у низці міжнародних платформ, що визначають напрямки цифрового розвитку - зокрема, у рамках Організації економічного співробітництва та розвитку (OECD), де США виступають співрозробником принципів відповідального використання ШІ, управління даними, цифрової інклюзії та інтероперабельності. Ці принципи - зокрема OECD AI Principles - мають імплементаційні наслідки у національних стратегіях, наприклад через створення *explainable AI*-модулів у федеральних службах або обов'язкову оцінку соціального впливу алгоритмів у системах державного скринінгу. У рамках Digital Nations - міжурядової коаліції держав, орієнтованих на інновації у публічному секторі - США беруть участь у проєктах зі спільного тестування протоколів безпечного обміну даними, побудови інтероперабельних відкритих API, стандартизації цифрової ідентичності. Це дає можливість не лише

обмінюватися досвідом, а й формувати транскордонні рішення, які можуть бути масштабовані у сфері імміграційних сервісів, торгівлі, цифрової спадщини.

Особливе значення має співпраця США з World Economic Forum (WEF), де активно обговорюється майбутнє цифрової політики, моделі data stewardship, метастандарти для децентралізованої ідентичності (DID), питання цифрової суверенності. У цьому контексті Сполучені Штати розвивають підхід federated governance - де різні органи, незалежні платформи й міжнародні партнери можуть разом адмініструвати спільні цифрові активи через розподілену відповідальність. Це актуально для ініціатив у сфері охорони здоров'я (наприклад, COVID-credentials), кібербезпеки (наприклад, обмін threat intelligence через CISA-ENISA протоколи) або стандартів етичного програмування в системах високого ризику. У результаті цифрове врядування перестає бути суто національною прерогативою - воно розгортається як глобальна мережа правил, стандартів, механізмів верифікації, де довіра забезпечується не ієрархією, а алгоритмізованим консенсусом [60, с. 12].



Рис. 3.2 Глобальна цифрова гармонія

У найближчій перспективі можна очікувати ще більшу інтенсифікацію гібридних моделей управління - коли частина рішень приймається централізовано (з огляду на регуляторні функції), але все більше операцій делегується інтелектуальним агентам, розподіленим протоколам і сервісним

платформам. Така трансформація потребуватиме нового типу інституційної грамотності - зокрема вміння оцінювати поведінку машин, перевіряти обґрунтованість рішень, здійснювати аудит не лише фінансовий, а й алгоритмічний, аналізувати вплив змін у параметрах моделі на соціальні наслідки. Це передбачає розвиток спеціалізованих органів типу Algorithmic Impact Assessment Boards, наділених повноваженнями тимчасово зупиняти алгоритми у випадку потенційних ризиків, запроваджувати мораторії на впровадження моделей без проходження обов'язкових тестів і формалізовувати етичні критерії ще до моменту розгортання коду. Поряд із цим розгортатиметься інфраструктура довіри (trust infrastructure), побудована на цифрових сертифікатах, реєстрах відповідності, механізмах цифрового підпису рішень і технічній можливості громадян здійснювати незалежну верифікацію логіки взаємодії з системою [18, с. 85].

Отож, майбутнє цифрового врядування у США - це не просто продовження лінійної автоматизації, а формування інтелектуалізованого, емерджентного, модульного середовища, у якому влада не є набором повноважень, а платформою, здатною до взаємодії, навчання, самоаналізу й реактивного оновлення. Вона функціонує на перетині національного інтересу, глобального технологічного порядку денного та локального досвіду, який постійно транслюється через інтерфейси, API, алгоритми. І саме через таку поліцентричну структуру - гнучку, але керовану - держава матиме змогу залишатися релевантною у світі, де швидкість змін вже перевищила здатність до їх бюрократичного оформлення. Це буде врядування, що не виписується в інструкції, а реалізується в протоколах, не контролюється наказами, а оцінюється за поведінкою алгоритмів, і не гарантується статусом, а підтверджується кожною транзакцією довіри.

Сценарії подальшого розвитку цифрового врядування у глобальній цифровій епосі формуються на перетині технологічного прогресу, соціодинамічних трансформацій і трансдисциплінарної рефлексії щодо природи державності як форми організації взаємодії. Умовно ці сценарії можна

розглядати в межах спектра від технократичного автоматизму до децентралізованої сервісної сингулярності. У першому випадку передбачається домінування алгоритмічного управління, тотальна автоматизація процедур, фрагментація державної функції на масиви модулів, що виконують логіку адміністративного коду - такий підхід базується на моделі *rule-as-code*, в якій нормативні приписи кодуються у вигляді алгоритмічних умов, зберігаються в логічних контейнерах, обробляються онтологічними компіляторами й інтегруються в сервіси, що взаємодіють із громадянами. Тут держава постає не як інституція, а як інтегрована інфраструктура, де «повноваження» - це API, «рішення» - це результат виконання логіки, а «контроль» - це телеметрія відповідності. У такій парадигмі відбувається зміщення управлінського суб'єкта: людина поступається місцем складній комбінації моделей штучного інтелекту, правових фреймворків і обчислювальних середовищ, що функціонують у багатоточковій, хмарній та розподіленій реальності. Це відкриває простір для моделювання автоматичних держав, де поняття вертикалі управління стає непридатним, а замість неї діє *topological state system* - складна матриця процесів, які обмінюються сигналами, приймають рішення та самооновлюються згідно із заданими метамоделями [21, с. 7].

Інший сценарій передбачає глибоку соціотехнічну інтеграцію, в якій цифрове врядування зберігає людський вимір, орієнтуючись на когнітивно-емпатичну взаємодію, динамічну участь громадян і інституціональне моделювання довіри як основи публічного життя. Тут цифрові системи не заміщують державу, а розширюють її здатність до адаптації, верифікації, аналітичного осмислення. Йдеться про сценарії *participatory intelligent governance*, де інструменти штучного інтелекту слугують посередниками між масивами даних і громадськими процесами, де політики кодуються як сценарії (*policy-as-simulation*), проходять краудсорсинг, симуляційне тестування та ітеративне коригування в реальному часі. Такі моделі вже частково реалізуються у пілотних проєктах США - зокрема, у використанні *civic tech*-лабораторій для моделювання реакцій на зміну транспортної логіки, розрахунку динаміки

зайнятості в певних демографічних групах, побудови систем пріоритетності програм субсидій. Це перехід від «закону як структури» до «закону як поведінки», де норми не стільки формалізовані, скільки матеріалізуються через поведінку алгоритмів, верифікуються результатами і коригуються за фідбеком користувачів [50, с. 5].

Ключовим соціотехнічним викликом для будь-якого із цих сценаріїв є проблема рівноваги між автономією машинного управління та відповідальністю людських суб'єктів. У системах, де рішення ухвалюються автоматизовано (наприклад, про нарахування допомоги, перегляд статусу, доступ до програм), виникає потреба в *auditability* - здатності відтворити логіку алгоритмічного рішення, простежити джерело даних, виявити приховані упередження. Це вимагає формування інфраструктури *algorithmic accountability*, з обов'язковою інституційною незалежною експертизою, реєстрами моделей, відкритим кодом для публічної перевірки, описом гіперпараметрів і логіки навчання. Проблема посилюється в умовах використання *reinforcement learning*, де модель змінює свою поведінку на основі нових даних - тобто, один і той самий алгоритм, використаний сьогодні і через тиждень, може ухвалити протилежні рішення на одному й тому ж кейсі. Тому потрібна версіонізація моделей, збереження «цифрових тіней» рішень, *time-based audit trail* і пояснення у зрозумілій формі для некваліфікованого користувача.

Зміна державних функцій у цьому новому ландшафті передбачає перехід від прямого адміністрування до оркестрації екосистем. Держава більше не є єдиним виробником публічних сервісів, а стає організатором взаємодії між державними, приватними, громадськими та гібридними структурами через сервіси, контракти, протоколи. Це вимагає інституалізації API-стратегій, створення публічних SDK для підключення зовнішніх розробників, нормування умов входу в державну екосистему - від модулів перевірки даних до постачальників аналітики. Визначальною тут є роль *data governance*: державні функції дедалі більше поляризуються навколо двох векторів - управління потоками даних і підтримка інфраструктури довіри. У першому випадку - це Data

Fabric, стандарти інтероперабельності, політики щодо доступу, консистентності та якості. У другому - РКІ, криптографія, протоколи верифікації, сертифікати доброчесності алгоритмів, цифрова ідентичність. Це не класична адміністративна робота - це техніко-правове адміністрування, яке реалізується через технічні модулі й підтримується нормативними інструкціями, побудованими за принципами Digital Rulemaking [58, с. 7].

На фоні цих сценаріїв ключовим питанням стає не «що» може держава, а «як» вона це реалізує - у межах яких рамок, з якими гарантіями, за яких умов. Майбутнє цифрового врядування не полягає в повній автоматизації чи повній децентралізації - воно в побудові гнучкої, реактивної, конфігурованої системи, яка здатна одночасно масштабуватись, локалізуватись і модифікувати свою логіку без втрати цілісності. Це вимагає від держави нового типу цифрової компетентності - не лише технічної, а й архітектурної, тобто вміння мислити у термінах структури систем, взаємозв'язків, обмежень і поведінки компонентів. В умовах глобальної цифрової епохи держава - це не об'єкт, не суб'єкт, а конфігурація взаємодій, у якій інституції, алгоритми, громадяни й середовище перебувають у постійній рекурсивній петлі. Тому розвиток цифрового врядування потребує не тільки нових технологій, а й нових форм управлінської рефлексії, нових структур адаптації, нових моделей легітимації рішень - таких, що можуть витримати і швидкість змін, і складність наслідків. У цьому й полягає нова політична функція цифрової держави - бути не гарантом сталості, а гарантом зворотного зв'язку, не адміністратором стабільності, а дизайнером змін.

ВИСНОВКИ

Цифрова трансформація публічного управління постає як складний процес інституційної, нормативної та інфраструктурної реконфігурації, в основі якої лежить перехід від ієрархічної бюрократії до гнучких сервісних моделей, побудованих на основі даних, алгоритмів і розподіленої обчислювальної потужності. В межах теоретико-концептуального блоку доведено, що цифровізація не є простим перенесенням адміністративних процедур у цифрову площину, а трансформує саму логіку взаємодії між державою та громадянином. Сутність цих змін полягає в заміщенні лінійних функціональних структур поліцентричними платформами, де цифрові сервіси створюються відповідно до життєвих ситуацій, а процеси формалізуються у вигляді керованих подій, сигналів і моделей. Сучасна модель цифрового управління базується на логіці оркестрації сервісів, інтеграції баз даних, міжвідомчої сумісності та використанні штучного інтелекту як когнітивного посередника між запитом і рішенням. Порівняльний аналіз міжнародних моделей цифрового врядування дав змогу виявити три основні підходи: платформно-орієнтовану модель (США, Естонія), сервісно-інклюзивну (Канада, Велика Британія) та нормативно-функціональну (Країни ЄС). Моделі відрізняються ступенем інституційної централізації, характером технічних стандартів, рівнем автономії відомств і глибиною використання даних, але всі демонструють рух до сценаріїв сервісної інтероперабельності, стандартизації API, автоматизованих систем прийняття рішень і формування цифрової ідентичності як основи управлінської взаємодії.

У структурі цифрових реформ США домінує еволюційний підхід, де державне управління поступово переходить від моделі електронного урядування до повноцінної платформи інтегрованих сервісів. Історична динаміка відображає зміну пріоритетів: початково цифрові ініціативи були зосереджені на автоматизації документообігу та онлайн-доступі до послуг, далі фокус змістився на відкриті дані, інтероперабельність і підзвітність, а на сучасному етапі - на побудову аналітичної та когнітивної інфраструктури, яка дозволяє формувати

адаптивні політики та прогнозувати вплив адміністративних рішень на різні групи населення. Розвиток стратегічних документів, таких як Digital Government Strategy, Cloud Smart і Federal Data Strategy, створив підґрунтя для уніфікації цифрової архітектури, розгортання хмарних сервісів із FedRAMP-сертифікацією, централізації систем ідентифікації (Login.gov), створення аналітичних платформ на базі Data.gov і впровадження DevOps-культури в розробку державних рішень. Роль інституційних акторів - OFCIO, TTS, USDS - полягає не лише у забезпеченні реалізації політик, а й у створенні технічних фреймворків, модульних бібліотек, API-стандартів і флагманських сервісів, які демонструють архітектурну сумісність, масштабованість і користувацьку зручність.

Цифрове врядування в США формується під впливом трьох основних детермінант - нормативних, інституційних та технологічних. Нормативний каркас базується на таких актах, як E-Government Act, FISMA, Privacy Act, які встановлюють вимоги до безпеки, прозорості, захисту персональних даних, обов'язкової аудиторії алгоритмічних систем і забезпечення цифрової інклюзії. Технологічна інфраструктура побудована на мультихмарних середовищах (AWS GovCloud, Azure Government), мікросервісній логіці з подієвою обробкою (Kafka, RabbitMQ), інструментах аналітики в реальному часі (Flink, Spark), серверлес-компонентах (Lambda, Azure Functions) та edge-модулях, які дозволяють обробку даних на периферії. Інституційна підтримка реформ забезпечується не лише через урядові агенції, а й через публічно-приватні партнерства, хакатони, civic tech-ініціативи (Code for America, Civic Hall), що розширюють базу впровадження інновацій у муніципальних сервісах.

Позитивні ефекти цифрової трансформації в державному управлінні США проявляються через підвищення адміністративної ефективності, зниження витрат на обробку звернень, персоналізацію сервісів та підвищення доступності адміністративних процедур. Платформи типу Benefits.gov, USAJobs, DisasterAssistance працюють як інтегровані шлюзи, які агрегують дані з десятків джерел, забезпечують авторизацію, персоніфікацію й автоматичну маршрутизацію на основі профілю користувача. Участь громадян у формуванні

політик підсилюється через системи регуляторних консультацій, інструменти відкритих даних і візуалізації, що дає змогу залучати спільноти до моделювання варіантів рішень. Водночас система стикається з ризиками, які мають як технічний, так і соціальний характер. Кібербезпека вимагає постійного оновлення систем SIEM/SOAR, реагування на zero-day загрози, захисту API, контролю за pipeline CI/CD. Ризики digital divide загрожують маргіналізацією частини населення - особливо в регіонах без стабільного інтернету чи серед осіб із низькою цифровою грамотністю. Проблеми algorithmic bias, непрозорості моделей, відсутності explainability у глибоких мережах створюють загрозу порушення адміністративної справедливості, втрати довіри до системи й неможливості оскарження автоматизованих рішень.

Майбутні сценарії цифрового врядування окреслюються як перехід до когнітивної держави - інституційного середовища, де рішення приймаються на основі прогнозів, адаптивного моделювання, потокової аналітики та симуляцій. Використання AI-first політик дозволяє переходити до anticipatory governance, де система самостійно ідентифікує потреби й запускає сервіси до моменту звернення. Edge computing, data fabric, federated identity, blockchain-based governance, AI observability - усе це технічні компоненти, які забезпечують динамічну масштабованість, конфігуровану модульність і гнучку інтеграцію. Водночас держава повинна переосмислити свою функцію - не лише як надавача послуг, а як архітектора довіри, модератора взаємодії, адміністратора рішень, що формуються в кооперації між громадянами, системами й інституційними платформами. І саме в такій системі цифрове врядування США виходить за межі національного досвіду, стаючи лабораторією глобальної державності нового покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Батракова Т.І. Линовецька В.Ю. *Особливості та принципи цифрової економіки в Україні*. URL: <https://journals.indexcopernicus.com/api/file/viewByFileId/623580.pdf> (дата звернення: 28.03.2025)
2. Білан М. *Як бізнес може використовувати штучний інтелект*. URL: <https://www.epravda.com.ua/columns/2023/05/8/699875> (дата звернення: 28.03.2025)
3. Величко К. Цибульська Е. Трансформація бізнесмоделей компаній. Сучасні виклики та перспективи у цифровій економіці. *Економіка та суспільство*. 2023. Вип. 52. DOI: <https://doi.org/10.32782/2524-0072/2023-52-393>
4. Гавриленко І. Здійснення м'якої сили через багатосторонню дипломатію у зовнішньополітичному дискурсі США. *Актуальні проблеми міжнародних відносин*. 2016. С. 51-54
5. Гачкевич А. Николишин М. Дипломатичний набір інструментів штучного інтелекту. *International Science Journal of Jurisprudence and Philosophy*. 2023. 2(3). С. 45-54
6. Гражевська Н.І. *Цифрова трансформація економіки в умовах посилення глобальних ризиків і загроз*. *Економіка та держава*. 2021. № 8. URL: <https://economy.in.ua> (дата звернення: 28.03.2025)
7. Гупта Суніл. *Цифрова стратегія. Посібник із переосмислення бізнесу*. Київ. КМ-БУКС. 2020. 320 с.
8. Дзямулич М.І. Шматковська Т.О. Вплив сучасних інформаційних систем і технологій на формування цифрової економіки. *Економічний форум*. 2022. Вип. 2. С. 3–8
9. Деретюк С. Пілінський В. *Визначення пріоритетних напрямків розвитку цифрової економіки в Україні*. *Фінансовий простір*. 2017. № 3(27)
10. Кай-Фу Лі. *Наддержави штучного інтелекту. Китай Кремнієва долина і новий світовий лад*. Київ. Форс Україна. 2020. 303 с.

11. Левицька Н.О. *Сучасні тенденції розвитку нормативно-правового регулювання цифрової економіки. Юридичний науковий електронний журнал.* 2019. № 5. С. 26-29. URL: <http://www.lsej.org.ua/index.php/arkhiv-nomeriv/2-uncategorised/117-5-2019-ukr> (дата звернення: 28.03.2025)
12. Олійник Д.І. *Щодо вимірювання процесів цифровізації в контексті цілей економічного відновлення.* URL: <https://niss.gov.ua/tsyfrovizatsiya1.pdf> (дата звернення: 28.03.2025)
13. Про тренди digital-маркетингу для малого бізнесу. 2017. URL: <https://psm7.com/blogs/o-trendax-digitalmarketinga-dlya-malogo-biznesa-v-2017-godu.html> (дата звернення: 28.03.2025)
14. Пустоваров А.І. *Закордонний досвід цифрової трансформації управління розвитком національної економіки.* URL: http://bses.in.ua/journals/2020/51_2020/44.pdf (дата звернення: 28.03.2025)
15. Вролова Л.В. Бойко І.М. *Трансформація підприємництва в умовах цифрової економіки.* URL: <https://economics.net.ua/47.pdf> (дата звернення: 28.03.2025)
16. Стріжкова А.В. *Віртуалізація як каталізатор суспільних трансформацій.* URL: [https://ndipzir.org.ua/wp-content/uploads/2020/02/Strizhkova19Mono/Strizhkova19Mono%20\(4\).pdf](https://ndipzir.org.ua/wp-content/uploads/2020/02/Strizhkova19Mono/Strizhkova19Mono%20(4).pdf) (дата звернення: 28.03.2025)
17. Струтинська І.В. *Дефініції поняття «цифрова трансформація».* URL: <https://bses.in.ua/19.pdf> (дата звернення: 28.03.2025)
18. Тихоненко І. *Цифрова дипломатія як інструмент зовнішньої політики США у ХХІ столітті. Політичне життя.* 2019. С. 85-90
19. Фіщук В. Матюшко В. Чернів Є. Юрчак О. Лаврик Я. Амелін А. *Україна 2030Е – країна з розвинутою цифровою економікою.* URL: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html> (дата звернення: 28.03.2025)
20. Alden C. Chan K. *Twitter and Digital Diplomacy. China and COVID-19. Strategic Update.* 2021

21. Australian Government. *Digital Sourcing Policies*. URL: <https://www.dta.gov.au/help-and-advice/ict-procurement/digital-sourcing-framework-ict-procurement/digital-sourcing-policies> (дата звернення: 28.03.2025)
22. Bartolome G. A Digital Strategy for Post Pandemic Diplomacy. *Medium*. URL: <https://medium.com/digital-diplomacy/a-digital-strategy-for-post-pandemic-diplomacy-bbc505947aaf> (дата звернення: 28.03.2025)
23. Bjola C. Cassidy J. Manor I. Public Diplomacy in the Digital Age. *Hague Journal of Diplomacy*. 2019
24. Chen K. US Diplomacy on Twitter and Why It Should Remain There. *The Diplomat*. URL: <https://thediplomat.com/2022/12/us-diplomacy-on-twitter-and-why-it-should-remain-there> (дата звернення: 28.03.2025)
25. Chhabra R. Twitter Diplomacy. A Brief Analysis. *ORF Issue Brief*. 2020. № 335
26. China Radio International. *Цифрова економіка та можливості для бізнесу*. URL: <https://ukrainian.cri.cn/2022/10/31/ARTI9NfQ0z0fCD7mKSaWXZzC221031.shtml> (дата звернення: 28.03.2025)
27. Cirera X. Comin D.A. Cruz M. Lee K.M. *Digital Progress and Trends Report* 2023. URL: https://docs.google.com/document/d/1NYkuA9vO_q6TU7TD6OUhQapjGiNH8Txl3AfOjfgKIVQ/edit (дата звернення: 28.03.2025)
28. Demirguc-Kunt A. Klapper L. Singer D. Financial inclusion and inclusive growth. A review of recent empirical evidence. *The World Bank Research Observer*. 2017. Vol. 32. № 1. С. 1–28
29. European Commission. *Markets in Crypto-Assets MiCA and pilot regime for market infrastructures based on DLT*. 2020
30. Fei W. Yao J. The Development and Game of US Digital Diplomacy Under Geopolitics. *International Relations and Diplomacy*. 2022. 10(5). С. 197-206

31. Gada K. *The Digital Economy In 5 Minutes*. URL: <https://www.forbes.com/sites/koshagada/2016/06/16/what-is-the-digitaleconomy> (дата звернення: 28.03.2025)
32. *Going Digital. Making the Transformation Work for Growth and Well-being*. URL: <http://www.oecd.org/going-digital/project> (дата звернення: 28.03.2025)
33. Goldberg M. Joseph Nye on Soft Power Competition Between China and the United States. *UN Dispatch*. URL: <https://undispatch.com/joseph-nye-on-soft-power-competition-with-china> (дата звернення: 28.03.2025)
34. Howell S.T. Niessner M. Yermack D. Initial coin offerings. Financing growth with cryptocurrency token sales. *The Review of Financial Studies*. 2018. Vol. 32. № 9. С. 1–42
35. Huang R. Wang W. Wang C. The path of blockchain adoption. Evidence from China. *Fintech Research*. 2019. Vol. 1. № 2. С. 1–24
36. It enterprise. *Industry 5.0*. URL: <https://www.it.ua/knowledge-base/technology-innovation/industry-50> (дата звернення: 28.03.2025)
- Zewdie T.G. Girma A. *IOT Security and the Role of AI/ML*. URL: <https://www.nist.gov/system/files/documents/2020/07/13/TemechuIoT%20Security%20%20Final.pdf> (дата звернення: 28.03.2025)
37. Ittefaq M. Digital Diplomacy via Social Networks. A Cross-National Analysis of Governmental Usage of Facebook and Twitter for Digital Engagement. *Journal of Contemporary Eastern Asia*. 2019. 18(1). С. 49-69
38. Ivanov I. Reshaping U.S. Smart Power. Towards a Post-Pandemic Security Architecture. *Journal of Strategic Security*. 2020. 13(3). С. 46-74
39. Ivanova A. Petrov D. Utilizing Big Data for Enhanced Decision Making in Business Management. *International Journal of Data Analytics*. 2023. Vol. 15. С. 145–162
40. Kavanagh J. The Ukraine War Shows How the Nature of Power Is Changing. *Carnegie*. URL: <https://carnegieendowment.org/2022/06/16/ukraine-war-shows-how-nature-of-power-is-changing-pub-87339> (дата звернення: 28.03.2025)

41. Krishnamoorthi R. The U.S. Cannot Afford to Lose a Soft-Power Race With China. *Foreign Policy Magazine*. URL: <https://foreignpolicy.com/2023/09/29/congress-shutdown-us-china-ccp-soft-power-competition-biden-xi-jinping-beijing> (дата звернення: 28.03.2025)
42. Kurbalija J. Digital diplomacy. *Diplo*. URL: <https://www.diplomacy.edu/topics/digital-diplomacy> (дата звернення: 28.03.2025)
43. Lips D. A New Strategy for U.S. Public Diplomacy. Using Virtual Education and Incentives to Promote Understanding of American Values. *Lincoln Policy*. 2021
44. Macchiavello E. Digital Platforms Capital Raising and EU Capital Markets Law. Different Shades of Decentralisation. *SSRN Electronic Journal*. 2022. URL: <https://doi.org/10.2139/ssrn.4157582> (дата звернення: 28.03.2025)
45. Main Areas of Digital Transformation. URL: <https://www.bdodigital.com/insights/digital-transformation/main-areas-of-digital-transformation> (дата звернення: 28.03.2025)
46. Nye J. Get Smart. Combining Hard and Soft Power. *Soft Power and Great-Power Competition. China and Globalization*. 2023. С. 63-66
47. Nye J. Soft Power After Ukraine. *Project Syndicate*. URL: <https://www.project-syndicate.org/commentary/soft-power-after-russia-war-in-ukraine-by-joseph-s-nye-2022-05> (дата звернення: 28.03.2025)
48. Nye J. State Smart Power Strategies. *Soft Power and Great-Power Competition. China and Globalization*. 2023. С. 21-28
49. Oxford University Press. *Oxford Dictionary*. URL: <https://www.oxfordreference.com/view/10.1093/acref/9780199684984.001.0001/acref-9780199684984-e-7478> (дата звернення: 28.03.2025)
- UNCTAD. *Конференція ООН по торгівлі і розвитку*. URL: <https://unctad.org/en/Pages/Home.aspx> (дата звернення: 28.03.2025)
50. British Computer Society. *The Digital Economy*. URL: https://policy.bcs.org/position_statements/digital-economy (дата звернення: 28.03.2025)

51. Samuelson P. *Intellectual Property and the Digital Economy*. URL: <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/berktech14&id=527> (дата звернення: 28.03.2025)
52. Seoane M. China's digital diplomacy on Twitter. The multiple reactions to the Belt and Road Initiative. *Global Media and Communication*. 2023. 19(2). С. 161-183
53. Shabout S. The Subtlety of Influence. America's Soft Power Strategy in the Middle East. *International Policy Digest*. URL: <https://intpolicydigest.org/the-subtlety-of-influence-america-s-soft-power-strategy-in-the-middle-east> (дата звернення: 28.03.2025)
54. Shevchenko I. *Digital transformation of the Japanese economy and prospects for the implementation of experience in the development of digital trade in Ukraine*. URL: <https://www.researchgate.net/publication/370278052> (дата звернення: 28.03.2025)
55. Sinha S. *State of IoT 2023*. URL: <https://iot-analytics.com/number-connected-iot-devices> (дата звернення: 28.03.2025)
56. Sobel M. Riffe D. Hester J. Twitter Diplomacy. A Content Analysis of Eight U.S. Embassies' Twitter Feeds. *The Journal of Social Media in Society*. 2016. 5(2). С. 75-107
57. Spitsina A. Plukar L. Maslyhan O. Moroz T. Kasmin D. Nazarenko I. *Digitalization of the economy as a factor of sustainable state development*. URL: http://repository.hneu.edu.ua/bitstream/123456789/29353/1/стаття_Касмін.pdf (дата звернення: 28.03.2025)
58. Statista. Digital Capital Raising. Market data & analysis. 2023a. URL: <https://www.statista.com/study/47352/fintech-report-alternative-financing/> (дата звернення: 28.03.2025)
59. Statista. Digital Capital Raising. Worldwide Africa Asia Americas Europe. 2023b. URL: <https://www.statista.com/outlook/dmo/fintech/digital-capital-raising/custom?currency=USD&locale=en&token=qcgajGhsKKa1l5kogjqT22DnoA>

[TUfzDBY4M4SDMzzBDFFC58mMQH1IE_HlgS76mrZDj4hikt7SfAVrofF74fyyw0Emic_H2thzmx15d28bsgoDptlRCkIHERA0P](https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US&view=chart) (дата звернення: 28.03.2025)

60. Tambe P. Hitt L. Rock D. Brynjolfsson E. *Digital Capital and Superstar Firms*. Cambridge. National Bureau of Economic Research. 2020

61. The World Bank. *World Bank Data*. URL: <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US&view=chart> (дата звернення: 28.03.2025)

62. Voronkova V. Nikitenko V. Oleksenko R. Andriukaitiene R. Kharchenko Ju. Kliuienko E. Digital technology evolution of the industrial revolution from 4G to 5G in the context of the challenges of digital globalization. *TEM Journal*. 2023. Vol. 12. Issue 2. С. 732–742. URL: https://www.temjournal.com/content/122/TEMJournalMay2023_732_742.pdf (дата звернення: 28.03.2025)

63. Wu Y. *Understanding China's Digital Economy. Policies, Opportunities, and Challenges*. URL: <https://www.china-briefing.com/news/understanding-chinas-digital-economy-policies-opportunities-and-challenges> (дата звернення: 28.03.2025)

64. Zetsche D.A. Buckley R.P. Arner D.W. Decentralized finance. *Journal of Financial Regulation*. 2020. Vol. 6. № 2. С. 172–203.