МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ЦИФРОВА ТРАНСФОРМАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО СТАНУ

Виконав студент 2 курсу,
групи ППГЗ-2-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Дмитро БОРОДІЙ

Науковий керівник роботи:
кандидат наук з державного управління
_____ Борис ДЗЮНДЗЮК

Харків – 2025

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ВПО	внутрішньо переміщені особи
ГО	громадська організація
ЕЦП	електронний цифровий підпис
ЄС	Європейський Союз
ЗМІ	засоби масової інформації
ІКТ	інформаційно-комунікаційні технології
КМУ	Кабінет Міністрів України
НАТО	Організація Північноатлантичного договору
РНБО	Рада національної безпеки і оборони
ЦНАП	центр надання адміністративних послуг

ВСТУП

Актуальність теми. Цифрова трансформація публічного управління визначається як один із ключових напрямів модернізації державного сектору в умовах четвертої промислової революції та становлення інформаційного суспільства. Стрімкий розвиток інформаційно-комунікаційних технологій фундаментально трансформує принципи організації та функціонування органів публічної влади, механізми формування та реалізації державної політики, моделі взаємодії держави з громадянами та бізнесом. У контексті повномасштабного вторгнення Російської Федерації в Україну, розпочатого 24 лютого 2022 року, проблематика цифровізації набуває особливого, екзистенційного виміру, перетворюючись із засобу підвищення ефективності адміністрування на критично важливий інструмент забезпечення виживання державних інституцій, підтримання життєздатності економіки та суспільства в умовах безпрецедентних викликів та загроз.

Воєнний стан створює унікальний та суперечливий контекст для процесів цифрової трансформації публічного управління. З одного боку, екстремальні умови війни виступають потужним каталізатором прискорення цифровізації, стимулюючи впровадження інноваційних рішень, які в мирний час могли б зустріти інституційний опір або впроваджуватися роками. Необхідність забезпечення оперативності прийняття управлінських рішень, координації дій численних суб’єктів в умовах динамічної безпекової ситуації, підтримання комунікації з громадянами в умовах руйнування традиційних каналів зв’язку роблять цифрові технології незамінними. З іншого боку, війна породжує безпрецедентні ризики та обмеження для цифровізації: масовані кібератаки на критичну інформаційну інфраструктуру, фізичне знищення дата-центрів та телекомунікаційних мереж, дефіцит фінансових та кадрових ресурсів, необхідність балансування між відкритістю цифрових сервісів та вимогами інформаційної безпеки.

Український досвід цифрової трансформації в умовах широкомасштабної війни не має аналогів у світовій практиці за масштабом, інтенсивністю та комплексністю викликів. Попри руйнівні наслідки російської агресії, Україна не лише зберегла функціональність базових цифрових сервісів, але й продовжує активно розвивати електронне урядування, розширювати функціонал мобільного застосунку та веб-порталу «Дія», впроваджувати інноваційні цифрові рішення для підтримки оборонного сектору, допомоги внутрішньо переміщеним особам, відновлення зруйнованої інфраструктури. Цей феномен «цифрової стійкості» України привертає увагу міжнародної спільноти та потребує глибокого наукового осмислення.

Водночас, масштаб та складність завдань, що постають перед системою публічного управління в умовах війни, вимагають переходу від фрагментарних цифрових ініціатив до системної, науково обґрунтованої стратегії цифрової трансформації. Така стратегія повинна враховувати як нагальні потреби воєнного часу – забезпечення кіберстійкості, оперативності управління, доступності критичних послуг, так і довгострокові завдання повоєнного відновлення, європейської інтеграції, побудови сучасної цифрової держави. Критично важливим є також врахування соціального виміру цифровізації – забезпечення інклюзивності цифрових сервісів, подолання цифрової нерівності, збереження балансу між технологічною ефективністю та людиноцентричністю публічного управління.

Дослідження процесів цифрової трансформації публічного управління в умовах воєнного стану має важливе теоретичне та прикладне значення. З теоретичної точки зору, воно дозволяє розширити наукове розуміння закономірностей функціонування державних інституцій в екстремальних умовах, механізмів адаптації систем публічного управління до кризових ситуацій, ролі цифрових технологій у забезпеченні національної стійкості. З практичної перспективи, результати дослідження можуть слугувати основою для вироблення науково обґрунтованих рекомендацій щодо оптимізації процесів цифровізації, підвищення ефективності електронного урядування, забезпечення

кіберстійкості державних інформаційних систем в умовах триваючої війни та на етапі повоєнного відновлення.

Мета і завдання дослідження. Метою магістерської роботи є комплексний аналіз процесів цифрової трансформації публічного управління в умовах воєнного стану та обґрунтування стратегічних напрямів підвищення ефективності цифровізації для забезпечення стійкості державних інституцій та якості публічних послуг в Україні.

Для досягнення поставленої мети визначено наступні завдання дослідження:

– розкрити теоретико-методологічні засади та концептуальні основи цифрової трансформації публічного управління в контексті сучасних викликів;

– проаналізувати та систематизувати передовий міжнародний досвід цифровізації державного сектору в умовах криз та безпекових загроз;

– здійснити комплексну діагностику сучасного стану цифрової трансформації публічного управління в Україні під час воєнного стану;

– ідентифікувати та класифікувати основні виклики, ризики та бар'єри цифровізації в умовах війни;

– обґрунтувати пріоритетні механізми та інструменти поглиблення цифрової трансформації з урахуванням потреб воєнного часу та завдань повоєнного відновлення;

– розробити науково-практичні рекомендації щодо підвищення ефективності процесів цифровізації публічного управління в Україні.

Об'єкт дослідження – система публічного управління України.

Предмет дослідження – теоретичні засади, практичні механізми та інструменти цифрової трансформації публічного управління в контексті забезпечення ефективності державних інституцій та національної стійкості в умовах війни.

Методи дослідження. Методологічну основу дослідження становить комплекс загальнонаукових та спеціальних методів пізнання. Діалектичний метод використано для розкриття суперечливої природи цифровізації в умовах

війни. Системний підхід застосовано для аналізу цифрової трансформації як цілісного процесу перетворення системи публічного управління. Структурно-функціональний метод дозволив дослідити компоненти системи електронного урядування та їх взаємозв'язки. Порівняльний аналіз використано для зіставлення вітчизняного та зарубіжного досвіду цифровізації. Інституційний підхід застосовано для вивчення формальних та неформальних правил, що регулюють процеси цифрової трансформації. Метод експертних оцінок використано для визначення пріоритетів цифровізації. Статистичний аналіз застосовано для оцінки динаміки розвитку цифрових сервісів. Методи моделювання та прогнозування використано для розробки сценаріїв розвитку цифрової трансформації на повоєнний період. Соціологічні методи (аналіз документів, контент-аналіз) застосовано для вивчення громадської думки щодо цифрових послуг.

Практичне значення отриманих результатів полягає в можливості їх використання органами державної влади та місцевого самоврядування при розробці та реалізації політики цифрової трансформації, оптимізації процесів надання електронних послуг, забезпеченні кіберстійкості державних інформаційних систем. Результати дослідження можуть бути використані Міністерством цифрової трансформації України при актуалізації стратегічних документів у сфері цифровізації, іншими центральними органами виконавчої влади при впровадженні цифрових рішень, військово-цивільними адміністраціями при організації надання послуг на деокупованих територіях. Теоретичні положення та висновки роботи можуть застосовуватися в навчальному процесі при викладанні дисциплін «Електронне урядування», «Публічне управління та адміністрування», «Інформаційна безпека держави» у закладах вищої освіти.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО СТАНУ

1.1 Концептуальні основи цифрової трансформації публічного управління

Цифрова трансформація публічного управління представляє собою комплексний, багатовимірний процес фундаментального переосмислення та перебудови принципів, механізмів, процедур та інструментів діяльності органів державної влади та місцевого самоврядування на основі системного впровадження сучасних інформаційно-комунікаційних технологій [7]. На відміну від простої автоматизації існуючих бюрократичних процедур або механічного перенесення паперового документообігу в електронну форму, справжня цифрова трансформація передбачає глибинну реінженерію управлінських процесів, зміну організаційної культури державних інституцій, трансформацію моделей взаємодії між державою, громадянським суспільством та бізнесом.

У сучасній науковій літературі існують різноманітні підходи до концептуалізації феномену цифрової трансформації публічного сектору. Дослідники О.В. Карпенко та Ж.З. Денисюк визначають цифрову трансформацію як «процес інтеграції цифрових технологій у всі аспекти діяльності органів публічної влади, що призводить до кардинальних змін у способах надання публічних послуг, взаємодії з громадянами та вирішенні суспільних проблем» [10]. В.С. Куйбіда, О.В. Карпенко та В.В. Наместнік розглядають цифрову трансформацію в контексті становлення цифрового врядування як якісно нової моделі публічного управління, заснованої на

принципах відкритості, партисипативності, мережевої взаємодії та орієнтації на потреби користувачів [14].

Концептуальне розуміння цифрової трансформації спирається на кілька взаємопов'язаних теоретичних підходів та парадигм. Теорія нового публічного менеджменту акцентує увагу на підвищенні ефективності державного управління через запозичення управлінських практик приватного сектору, включаючи широке використання ІКТ [44]. Концепція належного врядування підкреслює важливість прозорості, підзвітності, участі громадян у прийнятті рішень – принципів, реалізація яких значно полегшується завдяки цифровим технологіям [18]. Парадигма мережевого врядування розглядає публічне управління як систему горизонтальних зв'язків між різноманітними акторами, координація між якими здійснюється через цифрові платформи та мережі [35].

Теоретичні засади цифрової трансформації також включають концепцію електронного урядування, яка еволюціонувала від вузького розуміння як надання послуг онлайн до комплексного бачення трансформації всієї системи публічного управління [21]. Н.В. Грицяк виділяє чотири етапи розвитку електронного урядування: інформаційна присутність (створення веб-сайтів органів влади), взаємодія (двостороння комунікація з громадянами), транзакція (повний цикл надання послуг онлайн), трансформація (інтеграція та реінженерія процесів) [5]. Сучасний етап характеризується переходом від електронного до цифрового врядування, що передбачає не просто оцифровування існуючих процесів, а їх фундаментальне переосмислення на основі можливостей цифрових технологій [30].

Принципи цифрової трансформації публічного управління формують нормативно-ціннісну основу для здійснення перетворень та визначають їх спрямованість. Принцип людиноцентричності означає, що в центрі цифрової трансформації має бути людина з її потребами, очікуваннями та правами, а не технології самі по собі [16]. Це передбачає проєктування цифрових сервісів на основі глибокого розуміння «подорожі користувача», застосування методів дизайн-мислення, постійне отримання та врахування зворотного зв'язку від

громадян.

Принцип «цифровий за замовчуванням», закріплений у Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки, передбачає пріоритетність електронної форми надання публічних послуг при обов'язковому збереженні альтернативних каналів для громадян, які не мають доступу до цифрових технологій або навичок їх використання [25]. Реалізація цього принципу вимагає не лише технологічної модернізації, але й подолання цифрової нерівності, розвитку цифрової грамотності населення, забезпечення доступності цифрової інфраструктури.

Принцип інтероперабельності забезпечує здатність різних інформаційних систем та баз даних обмінюватися інформацією та використовувати її без додаткових перетворень [9]. В українському контексті цей принцип реалізується через систему електронної взаємодії державних електронних інформаційних ресурсів «Трембіта», яка забезпечує автоматизований обмін даними між різними відомствами та рівнями влади [31]. Технічна інтероперабельність доповнюється семантичною (єдине розуміння значення даних), організаційною (узгодженість бізнес-процесів) та правовою (гармонізація нормативної бази).

Принцип однократності введення даних означає, що громадяни та бізнес повинні надавати інформацію органам влади лише один раз, після чого вона має бути доступна для повторного використання всіма уповноваженими суб'єктами [4]. Реалізація цього принципу в Україні здійснюється через створення базових державних реєстрів (Державний реєстр актів цивільного стану громадян, Єдиний державний демографічний реєстр, Державний земельний кадастр та інші) та забезпечення їх взаємодії через систему «Трембіта» [29].

Принцип відкритості та прозорості передбачає максимальне розкриття інформації про діяльність органів влади, забезпечення доступу до публічної інформації, залучення громадян до процесів прийняття рішень [2]. Цифрові технології створюють безпрецедентні можливості для реалізації цього принципу через портали відкритих даних, системи електронних петицій, платформи

громадських бюджетів, онлайн-трансляції засідань органів влади. Єдиний державний веб-портал відкритих даних data.gov.ua містить понад 40 тисяч наборів даних від різних розпорядників інформації [26].

Принцип безпечності та захищеності вимагає забезпечення конфіденційності, цілісності та доступності інформації в державних інформаційних системах, захисту персональних даних громадян, стійкості до кіберзагроз [20]. В умовах воєнного стану цей принцип набуває особливої ваги, оскільки державні інформаційні системи стають об'єктами масованих кібератак з боку агресора. Реалізація принципу безпечності передбачає впровадження комплексних систем захисту інформації, використання криптографічних засобів, резервування критично важливих даних, підвищення кіберграмотності державних службовців.

Особливості публічного управління в умовах воєнного стану створюють специфічний контекст для цифрової трансформації, який характеризується поєднанням можливостей та обмежень, стимулів та ризиків. Закон України «Про правовий режим воєнного стану» визначає особливий правовий режим, що вводиться в разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності [27]. В умовах воєнного стану відбувається концентрація владних повноважень, розширення функцій військового командування, можливість обмеження конституційних прав і свобод громадян, запровадження особливих режимів роботи підприємств, установ та організацій.

Цифрова трансформація в умовах воєнного стану набуває специфічних характеристик. По-перше, прискорення темпів впровадження цифрових рішень під тиском обставин – те, що в мирний час потребувало б років узгоджень та пілотних проєктів, реалізується за лічені тижні чи місяці. Яскравим прикладом є запуск програми єПідтримка для виплат допомоги громадянам у районах бойових дій, яка була розроблена та впроваджена протягом кількох тижнів після початку повномасштабного вторгнення [32]. По-друге, пріоритизація цифрових проєктів відповідно до потреб оборони та безпеки – фокус зміщується на

системи, критично важливі для функціонування держави в умовах війни.

По-третє, посилення вимог до кібербезпеки та стійкості інформаційних систем. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кібератак на державні інформаційні ресурси зросла в рази після початку повномасштабного вторгнення [6]. Це вимагає впровадження додаткових рівнів захисту, резервування критичних систем, використання хмарних технологій для забезпечення безперервності функціонування. По-четверте, необхідність забезпечення функціонування цифрових сервісів в умовах руйнування фізичної інфраструктури – енергетичних мереж, телекомунікаційних систем, дата-центрів.

Правові засади функціонування державної влади під час війни визначаються комплексом нормативно-правових актів. Конституція України встановлює основи правового режиму воєнного стану, повноваження органів державної влади щодо його введення та забезпечення [12]. Закон України «Про національну безпеку України» визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики у цих сферах [28]. Закон України «Про оборону України» регламентує основи оборони України, повноваження органів державної влади у сфері оборони [24].

В контексті цифрової трансформації важливе значення мають спеціальні нормативно-правові акти, що регулюють функціонування електронного урядування та кібербезпеки. Закон України «Про електронні довірчі послуги» створює правову основу для використання електронного підпису та печатки, електронної позначки часу, електронної доставки [19]. Закон України «Про електронні комунікації» встановлює правові засади діяльності у сфері електронних комунікацій [17]. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» визначає правові основи захисту інформації в системах [15].

Теоретичне осмислення цифрової трансформації в умовах воєнного стану вимагає інтеграції концепцій електронного урядування з теоріями кризового управління та національної стійкості. Концепція адаптивного врядування

підкреслює важливість здатності системи публічного управління швидко реагувати на зміни середовища, навчатися на досвіді, експериментувати з новими підходами [46]. В умовах війни ця здатність стає критично важливою для виживання державних інституцій. Цифрові технології забезпечують необхідну гнучкість та швидкість реакції через автоматизацію процесів, аналітику даних в реальному часі, можливість віддаленої роботи.

Теорія національної стійкості розглядає здатність держави та суспільства протистояти, адаптуватися та відновлюватися після криз та шоків [1]. Цифрові технології виступають важливим компонентом національної стійкості, забезпечуючи безперервність критичних функцій, координацію дій різних акторів, комунікацію з населенням в кризових ситуаціях. Український досвід демонструє, як розвинена цифрова інфраструктура може стати фактором виживання держави в умовах широкомасштабної агресії.

Концепція антикрихкості, розроблена Н. Талебом, пропонує розглядати системи, які не просто витримують шоки та стреси, але стають сильнішими в результаті їх подолання [48]. В контексті цифрової трансформації це означає створення таких систем публічного управління, які використовують кризи як каталізатор для інновацій та вдосконалення. Війна, попри всі її трагічні наслідки, створює унікальне «вікно можливостей» для впровадження радикальних змін, подолання інституційної інерції, прискорення цифровізації.

Важливим аспектом концептуалізації цифрової трансформації в умовах війни є розуміння її подвійної природи як інструменту та об’єкта. З одного боку, цифрові технології є потужним інструментом забезпечення ефективності публічного управління, надання послуг громадянам, координації оборонних зусиль, протидії дезінформації. З іншого боку, цифрова інфраструктура сама стає об’єктом захисту та потенційною вразливістю, яку намагається експлуатувати противник через кібератаки, інформаційні операції, фізичне знищення критичної інфраструктури. Ця дуальність вимагає збалансованого підходу, який поєднує максимальне використання можливостей цифровізації з забезпеченням належного рівня безпеки та стійкості.

Модель цифрової зрілості публічного управління, адаптована до умов воєнного стану, включає кілька вимірів. Технологічний вимір охоплює рівень розвитку ІКТ-інфраструктури, доступність та функціональність цифрових сервісів, використання передових технологій (штучний інтелект, блокчейн, Інтернет речей). Організаційний вимір стосується готовності державних інституцій до цифрової трансформації, наявності цифрових компетенцій у державних службовців, організаційної культури, орієнтованої на інновації. Процесний вимір включає рівень автоматизації та оптимізації управлінських процесів, інтеграцію між різними системами та відомствами, використання даних для прийняття рішень.

Соціальний вимір цифрової трансформації в умовах війни набуває особливого значення. Він включає рівень цифрової грамотності населення, доступність цифрової інфраструктури для різних соціальних груп, довіру громадян до цифрових сервісів держави. Війна загострює проблему цифрової нерівності: евакуйовані особи можуть втратити доступ до цифрових пристроїв та Інтернету, літні люди стикаються з труднощами в освоєнні цифрових сервісів, мешканці прифронтових територій страждають від руйнування телекомунікаційної інфраструктури [3]. Водночас, для багатьох громадян цифрові канали стають єдиним способом отримання державних послуг, соціальної допомоги, важливої інформації.

Інституційний вимір цифрової трансформації охоплює формальні та неформальні правила, які регулюють процеси цифровізації. Формальні правила включають законодавство про електронне урядування, стандарти інтероперабельності, регламенти надання електронних послуг. Неформальні правила стосуються організаційної культури, ставлення до інновацій, готовності до змін. В умовах війни спостерігається послаблення інституційного опору змінам, прискорення прийняття рішень, готовність до експериментування з новими підходами. Водночас, зростає роль неформальних мереж та особистих зв’язків у забезпеченні функціонування державних інституцій.

Економічний вимір цифрової трансформації в умовах воєнного стану

характеризується суперечливими тенденціями. З одного боку, війна призводить до скорочення бюджетних надходжень, переорієнтації видатків на оборонні потреби, дефіциту ресурсів для цифрових проєктів. З іншого боку, цифровізація розглядається як інвестиція в підвищення ефективності державного управління, скорочення корупції, покращення бізнес-клімату. Міжнародна технічна допомога стає важливим джерелом фінансування цифрових проєктів: партнери України надають гранти, обладнання, експертну підтримку для розвитку електронного урядування [33].

Комунікаційний вимір цифрової трансформації набуває критичного значення в умовах інформаційної війни. Цифрові канали стають основним засобом комунікації держави з громадянами, протидії дезінформації, формування національного наративу. Офіційні канали в соціальних мережах, месенджери, мобільні додатки використовуються для оперативного інформування про повітряні тривоги, евакуацію, гуманітарну допомогу. Водночас, противник активно використовує цифрові канали для поширення фейків, деморалізації населення, дискредитації влади. Це вимагає розвитку стратегічних комунікацій, медіаграмотності, систем верифікації інформації.

Темпоральний вимір цифрової трансформації відображає необхідність балансування між короткостроковими та довгостроковими пріоритетами. Нагальні потреби воєнного часу вимагають швидких рішень, які не завжди є оптимальними з точки зору довгострокової перспективи. Водночас, важливо закладати фундамент для повоєнного відновлення та розвитку, створювати масштабовані та адаптивні системи, які зможуть еволюціонувати відповідно до зміни контексту. Цифрові рішення, впроваджені під час війни, повинні бути сумісними з європейськими стандартами та практиками, оскільки європейська інтеграція залишається стратегічним пріоритетом України.

Концептуальні основи цифрової трансформації публічного управління в умовах воєнного стану повинні також враховувати етичний вимір. Використання цифрових технологій для збору та обробки персональних даних, моніторингу переміщень громадян, автоматизованого прийняття рішень породжує етичні

дилеми щодо балансу між безпекою та приватністю, ефективністю та справедливістю, технологічними можливостями та людськими правами. Важливо забезпечити, щоб надзвичайні заходи воєнного часу не призвели до непропорційного обмеження прав і свобод, а тимчасові рішення не перетворилися на постійні практики після завершення війни.

1.2 Міжнародний досвід цифрової трансформації публічного управління в кризових умовах

Аналіз міжнародного досвіду цифрової трансформації публічного управління в умовах криз, конфліктів та надзвичайних ситуацій надає цінні уроки для України, дозволяючи ідентифікувати кращі практики, типові помилки, ефективні моделі та інструменти цифрової трансформації. Особливо релевантним є досвід країн, які стикалися з подібними викликами – зовнішньою агресією, гібридними загрозами, необхідністю забезпечення функціонування державних інституцій в екстремальних умовах.

Естонія по праву вважається світовим лідером у сфері електронного урядування та цифрової держави, а її досвід набуває особливої актуальності в контексті російської загрози. Естонська модель цифровізації, яка почала формуватися ще в 1990-х роках, базується на кількох фундаментальних принципах та рішеннях [41]. Універсальна система цифрової ідентифікації через ID-карти, впроваджена з 2002 року, охоплює 98% населення країни та забезпечує безпечний доступ до понад 600 електронних послуг. Mobile-ID та Smart-ID надають альтернативні канали ідентифікації через мобільні пристрої, що особливо важливо в умовах мобільності населення під час криз.

Платформа обміну даними X-Road, яка з’єднує понад 900 організацій та обробляє більше 500 мільйонів транзакцій щорічно, забезпечує безпечну та ефективну взаємодію між різними державними базами даних та системами [47].

Кожна транзакція в X-Road підписується цифровим підписом та логується, що забезпечує юридичну силу електронних документів та можливість аудиту. Принцип «лише один раз» означає, що громадяни надають інформацію державі лише одного разу, після чого вона автоматично доступна всім уповноваженим органам. Це значно скорочує адміністративне навантаження та підвищує ефективність публічного управління.

Кібератака 2007 року, яка паралізувала банківську систему, державні сайти та критичну інфраструктуру Естонії, стала поворотним моментом у розвитку національної кібербезпеки [40]. У відповідь на цю атаку Естонія розробила комплексну стратегію кіберстійкості, яка включає технічні, організаційні та правові заходи. Було створено Департамент державної інформаційної системи, який відповідає за розвиток та безпеку державної IT-інфраструктури. Таллінн став місцем розташування Центру передового досвіду НАТО з кібероборони, який розробляє доктрини, проводить навчання та дослідження у сфері кібербезпеки.

Концепція «цифрової безперервності» передбачає забезпечення функціонування державних інституцій навіть у разі окупації території або масштабних кібератак. Проєкт Data Embassy – створення «посольств даних» у дружніх країнах – забезпечує резервне копіювання критично важливих державних даних та систем за межами Естонії. У 2017 році Естонія відкрила перше таке «посольство» в Люксембурзі, де на серверах, що мають дипломатичний імунітет, зберігаються резервні копії ключових реєстрів та баз даних. Це гарантує, що навіть у разі повної втрати контролю над територією естонський уряд зможе продовжувати функціонувати та надавати послуги громадянам.

Використання технології блокчейн для забезпечення цілісності даних стало інноваційним рішенням Естонії. З 2012 року технологія блокчейн KSI використовується для захисту державних реєстрів, медичних записів, судових рішень від несанкціонованих змін. Кожна зміна в системі автоматично фіксується в блокчейні, що робить неможливим приховане маніпулювання

даними. Це особливо важливо в умовах гібридних загроз, коли противник може намагатися підірвати довіру до державних інституцій через компрометацію даних.

Латвія та Литва, які також перебувають під постійною загрозою з боку Росії, розвивають власні моделі цифровізації з акцентом на безпековому вимірі. Латвія створила централізовану платформу Latvija.lv, яка об'єднує понад 100 електронних послуг від різних державних установ та забезпечує єдину точку доступу для громадян [43]. Система eParaksts надає можливість створення юридично значущого електронного підпису, що дозволяє повністю перевести документообіг в електронну форму. Під час пандемії COVID-19 Латвія за лічені тижні запустила систему covidpass.lv для видачі цифрових сертифікатів вакцинації, продемонструвавши здатність швидко адаптувати цифрову інфраструктуру до нових викликів.

Литва реалізує амбітну програму «держава в смартфоні», спрямовану на забезпечення доступу до всіх державних послуг через мобільні пристрої [39]. Платформа VIISP (державний портал електронної ідентифікації) забезпечує єдиний вхід до всіх електронних сервісів через різні засоби ідентифікації – ID-картки, мобільний підпис, інтернет-банкінг. Особливу увагу Литва приділяє протидії російській дезінформації: створено підрозділ стратегічних комунікацій, який моніторить інформаційний простір, виявляє фейки, координує урядові комунікації. Досвід Литви показує важливість поєднання технологічних рішень з організаційними заходами та розвитком медіаграмотності населення.

Ізраїль, який десятиліттями функціонує в умовах перманентної безпекової напруги, розробив унікальні підходи до поєднання цифровізації з вимогами національної безпеки [42]. Програма Digital Israel, запущена в 2013 році, спрямована на перетворення країни на провідну цифрову державу через розвиток цифрової інфраструктури, підвищення цифрових навичок населення, стимулювання інновацій. Особливістю ізраїльської моделі є тісна співпраця між державним сектором, армією, академічними установами та високотехнологічними компаніями.

Система Home Front Command забезпечує оперативне оповіщення населення про ракетні атаки, надає інструкції щодо дій в надзвичайних ситуаціях, координує евакуацію та надання допомоги. Мобільний додаток надсилає геолокалізовані попередження, враховуючи час підльоту ракет до конкретного району. Ця система демонструє, як цифрові технології можуть рятувати життя в умовах безпосередньої військової загрози. Водночас, ізраїльський досвід показує важливість балансування між безпековими потребами та громадянськими свободами, оскільки широке використання технологій стеження викликає дискусії про приватність та права людини.

Південна Корея, яка перебуває в стані технічної війни з КНДР з 1953 року, розвинула одну з найбільш передових систем електронного урядування у світі [45]. Концепція «Уряд 3.0» передбачає перехід від надання послуг за запитом до проактивного та персоналізованого обслуговування громадян. Система Government24 (gov.kr) надає понад 1200 адміністративних послуг онлайн, використовуючи штучний інтелект для персоналізації взаємодії та прогнозування потреб користувачів. Під час пандемії COVID-19 Південна Корея продемонструвала ефективність цифрових технологій у боротьбі з кризою: система відстеження контактів, мобільні додатки для самомоніторингу, аналітика великих даних для прогнозування спалахів дозволили стримати поширення вірусу без жорстких локдаунів.

Пандемія COVID-19 стала глобальним стрес-тестом для систем публічного управління та каталізатором цифрової трансформації. Країни з розвиненою цифровою інфраструктурою змогли швидше адаптуватися до нових умов та забезпечити безперервність надання публічних послуг [38]. Сінгапур використав комплексний підхід до цифровізації кризового управління: додаток TraceTogether для відстеження контактів, система SafeEntry для реєстрації відвідувачів публічних місць, платформа HealthHub для телемедицини. При цьому уряд приділив значну увагу захисту приватності: дані зберігалися локально на пристроях, використовувалися лише за згодою користувачів, видалялися після закінчення епідеміологічної потреби.

Данія продемонструвала важливість попередніх інвестицій у цифрову інфраструктуру: завдяки системі NemID для цифрової ідентифікації, яка охоплює 90% населення, країна змогла швидко перевести більшість державних послуг в онлайн-режим [37]. Платформа borger.dk стала єдиним вікном доступу до всіх сервісів, включаючи подачу заявок на допомогу, реєстрацію на вакцинацію, отримання результатів тестів. Фінляндія використала платформу Suomi.fi для координації надання допомоги громадянам та бізнесу, автоматизації виплат, обміну інформацією між різними відомствами.

Досвід пандемії виявив кілька універсальних уроків для цифрової трансформації в кризових умовах. По-перше, критична важливість базової цифрової інфраструктури – надійного інтернет-з'єднання, систем ідентифікації, платформ обміну даними. Країни, які інвестували в цю інфраструктуру до кризи, змогли швидко масштабувати цифрові сервіси. По-друге, необхідність інтероперабельності систем для забезпечення координації між різними відомствами та рівнями влади. По-третє, важливість цифрової інклюзії – забезпечення доступності сервісів для всіх груп населення, включаючи літніх людей, осіб з інвалідністю, мешканців віддалених районів.

Стандарти та рекомендації міжнародних організацій формують нормативну рамку для цифрової трансформації. Рамкова програма ЄС з кібербезпеки (EU Cybersecurity Act) встановлює єдині стандарти сертифікації продуктів та послуг ІКТ, що особливо важливо для забезпечення безпеки критичної інфраструктури [36]. Директива NIS2, яка набула чинності в 2023 році, посилює вимоги до кібербезпеки для широкого кола організацій, включаючи державні установи, постачальників критичних послуг, цифрові платформи. Вона вимагає впровадження систем управління ризиками, реагування на інциденти, забезпечення безперервності бізнесу.

Стратегія «Цифрове десятиліття Європи» визначає амбітні цілі цифрової трансформації до 2030 року: 100% ключових публічних послуг онлайн, 100% громадян з доступом до медичних записів, 80% населення з базовими цифровими навичками [34]. Програма Digital Europe передбачає інвестиції в розмірі 7,5 млрд

євро в розвиток цифрових технологій, включаючи суперкомп'ютери, штучний інтелект, кібербезпеку, цифрові навички. Для України, яка має статус кандидата на членство в ЄС, ці стандарти та програми визначають орієнтири для національної політики цифровізації.

НАТО розробило концепцію стійкості, яка включає сім базових вимог: забезпечення безперервності урядування, енергетичних поставок, продовольства та води, роботи систем зв'язку, транспортних систем, медичного обслуговування, управління масовими переміщеннями населення [49]. Цифрові технології відіграють ключову роль у забезпеченні кожної з цих вимог. Центр передового досвіду НАТО з стратегічних комунікацій у Ризі розробляє методології протидії дезінформації, аналізу інформаційного середовища, проведення інформаційних кампаній. Ці напрацювання особливо актуальні для України в умовах гібридної війни з Росією.

Організація економічного співробітництва та розвитку розробила Рекомендації щодо цифрового уряду, які визначають 12 принципів ефективної цифровізації публічного сектору. Серед них – відкритість за замовчуванням, орієнтація на користувача, проактивність уряду, цифровий за дизайном підхід. ОЕСР також розробила методологію оцінки цифрової зрілості урядів (Digital Government Index), яка дозволяє порівнювати прогрес різних країн та ідентифікувати кращі практики.

Адаптація міжнародного досвіду до українських реалій вимагає врахування специфічного контексту – масштабу та інтенсивності військових дій, руйнування інфраструктури, масових переміщень населення, обмеженості ресурсів. Водночас, певні універсальні принципи та підходи можуть бути успішно імплементовані. Естонський досвід показує важливість інвестицій у базову цифрову інфраструктуру та системи ідентифікації як фундаменту для всіх інших сервісів. Концепція «цифрової безперервності» через резервування критичних систем за межами країни може бути адаптована Україною через розміщення резервних копій у країнах-партнерах.

Ізраїльська модель тісної співпраці між державою, армією та

технологічним сектором резонує з українським досвідом, де ІТ-спільнота активно долучається до кіберзахисту та розробки рішень для потреб оборони. Південнокорейський підхід до використання штучного інтелекту та великих даних для персоналізації послуг може бути поступово впроваджений в Україні в міру розвитку технологічних можливостей. Досвід балтійських країн у протидії російській дезінформації безпосередньо релевантний для України.

Ключовим висновком з аналізу міжнародного досвіду є те, що успішна цифрова трансформація в кризових умовах вимагає не лише технологічних рішень, але й комплексного підходу, який включає правове регулювання, організаційні зміни, розвиток людського капіталу, забезпечення кібербезпеки, міжнародну співпрацю. Країни, які досягли найбільших успіхів у цифровізації, почали цей процес задовго до кризи, що дозволило їм мати необхідну інфраструктуру та компетенції для швидкої адаптації. Для України це означає необхідність балансування між вирішенням нагальних проблем воєнного часу та закладенням фундаменту для довгострокового цифрового розвитку.

РОЗДІЛ 2
АНАЛІЗ СТАНУ ТА ПРОБЛЕМ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

2.1 Стан цифровізації державного сектору України під час війни

Цифрова трансформація публічного управління в Україні, яка активно продовжилась з 2019 року із створенням Міністерства цифрової трансформації, зазнала фундаментальної перевірки на міцність та ефективність в умовах повномасштабної війни. Аналіз поточного стану цифровізації державного сектору під час воєнного стану дозволяє оцінити досягнення, виявити проблемні зони та визначити напрями подальшого розвитку електронного урядування в екстремальних умовах.

Нормативно-правова база цифрової трансформації в Україні формувалася поступово протягом останніх років і включає комплекс законодавчих та підзаконних актів, які регулюють різні аспекти електронного урядування. Базовим документом стратегічного характеру є Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки, яка визначила основні цілі, принципи та напрями цифровізації [25]. Хоча термін дії цієї Концепції формально завершився, її положення продовжують визначати вектор цифрового розвитку держави. У 2021 році було схвалено Концепцію розвитку електронного урядування в Україні до 2025 року, яка передбачає комплексну трансформацію системи публічного управління на основі цифрових технологій.

Законодавче забезпечення цифрової трансформації включає низку ключових законів. Закон України «Про електронні довірчі послуги» створив правову основу для використання електронного підпису та печатки, що є критично важливим для переведення документообігу в електронну форму [19]. За даними Міністерства цифрової трансформації, станом на початок 2024 року в

Україні діє понад 20 кваліфікованих надавачів електронних довірчих послуг, які видали більше 7 мільйонів активних сертифікатів електронного підпису. Закон України «Про електронні комунікації» модернізував правове регулювання телекомунікаційної сфери відповідно до європейських стандартів [17].

У 2022 році, вже в умовах воєнного стану, було прийнято Закон України «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в Україні», який спростив процедури резервування даних, забезпечення безперервності функціонування критичних систем, створення резервних копій за межами України. Постанова Кабінету Міністрів України № 749 від 2022 року затвердила перелік критично важливих державних електронних інформаційних ресурсів, які підлягають особливому захисту в умовах воєнного стану.

Інфраструктурне та технологічне забезпечення органів влади зазнало суттєвої трансформації під впливом війни. До початку повномасштабного вторгнення Україна мала відносно розвинену ІТ-інфраструктуру державного сектору: функціонувало понад 350 державних реєстрів та інформаційних систем, працювали 3 державні дата-центри, діяла система електронної взаємодії «Трембіта», яка забезпечувала понад 2 мільйони транзакцій щомісяця [31]. Водночас, фізичні атаки на критичну інфраструктуру, масові відключення електроенергії, руйнування телекомунікаційних мереж створили безпрецедентні виклики для функціонування цифрових систем.

За даними Державної служби спеціального зв’язку та захисту інформації України, з початку повномасштабного вторгнення було зафіксовано понад 2200 кібератак на об’єкти критичної інфраструктури, з яких близько 40% були спрямовані на державні інформаційні системи [6]. У відповідь на ці виклики було вжито екстрені заходи з міграції критичних систем у хмарні сервіси за межами України. Зокрема, ключові компоненти порталу «Дія», системи «Трембіта», важливі державні реєстри були перенесені на сервери Amazon Web Services, Microsoft Azure, Google Cloud Platform. Це забезпечило їх функціонування навіть

під час масованих ракетних ударів по енергетичній інфраструктурі.

Рівень цифрової зрілості державних інституцій демонструє значну диференціацію. Лідерами цифровізації є Міністерство цифрової трансформації, Міністерство юстиції (яке управляє системою державних реєстрів), Державна податкова служба (електронний кабінет платника податків обслуговує понад 2 мільйони користувачів), Пенсійний фонд України (автоматизовані процеси призначення пенсій та соціальних виплат) [8]. Водночас, багато центральних та особливо місцевих органів влади досі мають обмежені цифрові спроможності, використовують застарілі системи, не мають кваліфікованого ІТ-персоналу.

Функціонування порталу та мобільного застосунку «Дія» стало символом цифрової стійкості України під час війни. Запущена у 2020 році як «держава в смартфоні», «Дія» на початок 2024 року налічує понад 19 мільйонів користувачів та надає доступ до більш ніж 130 послуг [32]. Під час війни функціонал «Дії» був швидко адаптований до потреб воєнного часу. У березні 2022 року було запущено програму єПідтримка для виплати одноразової допомоги громадянам, які втратили роботу через війну – за перші кілька днів заявки подали понад 6 мільйонів українців. Сервіс єВідновлення дозволяє фіксувати пошкоджене війною майно для отримання компенсації – зафіксовано понад 500 тисяч об’єктів.

У «Дії» з’явилися специфічні воєнні сервіси: єВорог для повідомлення про переміщення російських військ (надійшло понад 260 тисяч повідомлень), цифрові документи для внутрішньо переміщених осіб, сервіс пошуку зниклих безвісти. Важливим досягненням стало міжнародне визнання українських цифрових документів – понад 70 країн визнають цифрові паспорти з «Дії» для ідентифікації українських біженців. Польща першою у світі на законодавчому рівні прирівняла цифрові документи з «Дії» до паперових для отримання номера PESEL та доступу до соціальних послуг.

Система надання адміністративних послуг зазнала значної трансформації в умовах війни. До початку повномасштабного вторгнення в Україні функціонувало понад 800 центрів надання адміністративних послуг (ЦНАП), які

надавали близько 2500 різних послуг [16]. Війна призвела до руйнування або тимчасової втрати понад 150 ЦНАПів на окупованих територіях та в зоні активних бойових дій. Водночас, відбулося прискорення переведення послуг в онлайн-формат: якщо до війни онлайн можна було отримати близько 120 послуг, то на початок 2024 року – понад 200.

Особливого значення набули мобільні ЦНАПи – спеціально обладнані автомобілі, які надають послуги в прифронтових районах та місцях компактного проживання переселенців. За підтримки міжнародних партнерів було розгорнуто понад 50 мобільних ЦНАПів, які обслужили більше 200 тисяч громадян. Впроваджено механізм екстериторіальності надання послуг – громадяни можуть звертатися за послугами до будь-якого ЦНАПу незалежно від місця реєстрації, що критично важливо для мільйонів внутрішньо переміщених осіб.

Цифрові рішення для підтримки громадян, бізнесу та армії стали пріоритетом державної політики. Для підтримки бізнесу запущено програму єРобота – державні гранти на відкриття або розвиток власної справи. Через портал «Дія.Бізнес» подано понад 50 тисяч заявок, видано грантів на суму понад 5 мільярдів гривень. Програма релокації бізнесу з небезпечних регіонів допомогла перемістити понад 750 підприємств, зберігши десятки тисяч робочих місць.

Для підтримки Збройних Сил України створено платформу UNITED24 – офіційну фандрейзингову платформу України, через яку зібрано понад 10 мільярдів гривень від донорів з усього світу. Армія отримала доступ до системи Delta – ситуаційної обізнаності на полі бою, яка інтегрує дані з різних джерел (супутники, дрони, розвідка) та надає командирам оперативну картину бойових дій. Система «Резерв+» дозволяє військовозобов’язаним оновлювати дані онлайн, що спрощує процедури мобілізації та військового обліку.

Електронна система охорони здоров’я продемонструвала стійкість в умовах війни. Центральна база даних eHealth, яка містить медичні записи понад 35 мільйонів українців, продовжує функціонувати навіть під час масованих атак на інфраструктуру [21]. Система дозволяє пацієнтам отримувати рецепти,

направлення, доступ до медичної історії незалежно від місця перебування. Під час війни через систему було виписано понад 100 мільйонів електронних рецептів за програмою «Доступні ліки», що забезпечило безперервність лікування для мільйонів пацієнтів з хронічними захворюваннями.

Освітня сфера також зазнала цифрової трансформації під тиском обставин. Всеукраїнська школа онлайн, запущена під час пандемії, стала критично важливою для продовження навчання в умовах війни. Платформа надає доступ до відеоуроків з усіх предметів шкільної програми, якими скористалися понад 2 мільйони учнів. Більше 4000 шкіл перейшли на повністю дистанційне навчання через руйнування або небезпеку. Університети використовують платформи Moodle, Microsoft Teams, Google Classroom для забезпечення безперервності освітнього процесу.

Система електронних закупівель ProZorro продовжує функціонувати, забезпечуючи прозорість державних закупівель навіть в умовах воєнного стану. З початку повномасштабного вторгнення через систему проведено закупівель на суму понад 800 мільярдів гривень, з яких значна частина – закупівлі для потреб оборони та відновлення інфраструктури [9]. Водночас, в умовах воєнного стану частина оборонних закупівель здійснюється в закритому режимі з міркувань безпеки, що створює виклики для забезпечення прозорості та підзвітності.

Система соціального захисту населення демонструє прогрес у цифровізації. Єдина інформаційна система соціальної сфери інтегрує дані про отримувачів соціальних послуг, автоматизує призначення допомоги, забезпечує адресність соціальної підтримки. Під час війни через систему було призначено допомогу для понад 2 мільйонів внутрішньо переміщених осіб, виплачено компенсації за зруйноване житло, організовано виплати для евакуйованих. Запровадження принципу «соціальна послуга слідує за людиною» дозволило ВПО отримувати соціальну підтримку незалежно від місця фактичного перебування.

Важливим елементом цифрової інфраструктури стала Єдина державна електронна система у сфері будівництва, яка забезпечує повний цикл

адміністрування будівельної діяльності в електронному вигляді. Система набула особливого значення в контексті відновлення зруйнованої інфраструктури: через неї оформлюються дозволи на відбудову, ведеться облік пошкоджених об’єктів, координується розподіл будівельних матеріалів та ресурсів для відновлення.

2.2 Виклики та ризики цифровізації в умовах воєнного стану

Цифрова трансформація публічного управління в умовах воєнного стану стикається з безпрецедентними викликами та ризиками, які суттєво відрізняються від типових проблем мирного часу. Комплексний аналіз цих викликів є критично важливим для розробки ефективних стратегій подолання бар’єрів та забезпечення стійкості цифрових систем в екстремальних умовах.

Кібербезпека стала найгострішим викликом для цифрової трансформації України в умовах війни. За даними Державної служби спеціального зв’язку та захисту інформації, інтенсивність кібератак на українські державні ресурси зросла в 3-4 рази порівняно з довоєнним періодом, а їх складність та координованість досягли безпрецедентного рівня [6]. Російські хакерські угруповання, які діють за підтримки спецслужб РФ, використовують весь спектр кіберзброї: від DDoS-атак та фішингу до складних APT-атак (Advanced Persistent Threat) з використанням вразливостей нульового дня.

Особливо небезпечними стали атаки на критичну інформаційну інфраструктуру. У січні 2024 року масована кібератака на телекомунікаційного оператора Київстар призвела до тимчасового порушення зв’язку для мільйонів абонентів та збоїв у роботі банківських систем, які використовували мережу оператора. Атаки на енергетичну інфраструктуру поєднують кіберкомпонент з фізичними ударами: після ракетних атак на енергооб’єкти часто слідують спроби зламати системи управління для ускладнення відновлювальних робіт.

Державні інформаційні системи стали пріоритетними цілями для

кібератак. Зафіксовано спроби злому системи «Трембіта» для порушення міжвідомчого обміну даними, атаки на портал «Дія» з метою крадіжки персональних даних громадян, спроби компрометації державних реєстрів для підриву довіри до державних інституцій. У відповідь на ці загрози Україна посилила співпрацю з міжнародними партнерами: експерти Microsoft, Amazon, Google надають технічну підтримку в захисті критичних систем, НАТО надає обладнання та експертизу для кіберзахисту.

Забезпечення кіберстійкості критичної інфраструктури вимагає комплексного підходу. Впроваджено системудля цілодобового моніторингу та реагування на інциденти. Національний координаційний центр кібербезпеки при РНБО координує зусилля різних відомств та приватного сектору. Команда CERT-UA (Computer Emergency Response Team of Ukraine) оперативно реагує на інциденти, розробляє рекомендації щодо захисту, координує дії з міжнародними CERT.

Проблеми доступності цифрових послуг загострилися через руйнування інфраструктури та масові переміщення населення. За оцінками Міністерства цифрової трансформації, близько 30% населення відчуває труднощі з доступом до цифрових сервісів через відсутність стабільного інтернет-з’єднання, особливо в прифронтових районах та на деокупованих територіях [13]. Масові відключення електроенергії, спричинені ракетними ударами по енергосистемі, призводять до періодичної недоступності цифрових сервісів навіть у великих містах.

Цифрова нерівність проявляється в кількох вимірах. Географічний вимір: жителі сільських районів, прифронтових територій мають обмежений доступ до високошвидкісного інтернету. Соціально-економічний вимір: малозабезпечені громадяни не можуть дозволити собі сучасні цифрові пристрої та оплату інтернет-послуг. Віковий вимір: літні люди часто не мають навичок користування цифровими сервісами. За даними соціологічних досліджень, близько 25% громадян старше 60 років ніколи не користувалися інтернетом, що виключає їх з цифрових процесів [2].

Для подолання цифрової нерівності запроваджено програми цифрової освіти. Проєкт «Цифрова освіта» на платформі «Дія.Цифрова освіта» пропонує безкоштовні курси з цифрової грамотності, якими скористалися понад 6 мільйонів українців. Мережа з понад 4000 хабів цифрової освіти надає безкоштовний доступ до комп'ютерів та інтернету, проводить навчання для літніх людей та інших вразливих груп.

Організаційно-управлінські бар'єри залишаються суттєвою перешкодою для цифрової трансформації. Опір змінам з боку частини державних службовців, які звикли до традиційних паперових процедур, ускладнює впровадження цифрових рішень. За результатами опитування, проведеного Національним агентством з питань державної служби, близько 40% державних службовців вважають, що їм бракує навичок для ефективної роботи з цифровими інструментами [18]. Середній вік державного службовця в Україні становить 45 років, що ускладнює адаптацію до цифрових технологій.

Дефіцит кваліфікованих ІТ-кадрів у державному секторі є системною проблемою. Низький рівень оплати праці порівняно з приватним сектором (середня зарплата ІТ-спеціаліста в державному секторі в 3-4 рази нижча, ніж у приватному) призводить до відтоку талантів. Бюрократичні процедури найму, відсутність гнучких форм зайнятості, обмежені можливості кар'єрного росту роблять державну службу непривабливою для молодих ІТ-спеціалістів. Мобілізація до лав Збройних Сил додатково скоротила кадровий потенціал.

Недостатня міжвідомча координація створює ізольовані системи різних відомств, які не можуть ефективно обмінюватися даними. Попри функціонування системи «Трембіта», багато відомств продовжують вимагати паперові довідки, які можна отримати електронно. Відсутність єдиних стандартів даних, різні технологічні платформи, відомчі інтереси ускладнюють інтеграцію систем. Це призводить до дублювання функцій, неефективного використання ресурсів, незручностей для громадян.

Фінансові обмеження стали критичним викликом для цифровізації в умовах війни. Державний бюджет України на 2024 рік передбачає дефіцит у

розмірі понад 40% ВВП, при цьому понад 50% видатків спрямовано на оборону та безпеку [22]. Фінансування цифрових проєктів здійснюється за залишковим принципом, багато ініціатив заморожено або скорочено. Водночас, підтримка міжнародних партнерів частково компенсує брак внутрішніх ресурсів: ЄС, США, Світовий банк надають гранти та технічну допомогу на цифровізацію.

Правові та регуляторні виклики ускладнюють впровадження інноваційних цифрових рішень. Застаріле законодавство не встигає за технологічним розвитком: відсутнє належне регулювання використання штучного інтелекту, блокчейну, біометричної ідентифікації в державному секторі. Надмірна зарегульованість процедур державних закупівель ІТ-послуг призводить до затягування проєктів. Невизначеність правового статусу даних, які зберігаються в хмарних сервісах за межами України, створює ризики для суверенітету даних.

Інформаційна безпека в умовах гібридної війни стала окремим викликом. Російська пропаганда активно використовує дезінформацію про цифрові сервіси для підриву довіри громадян: поширюються фейки про «злив» персональних даних з «Дії», «тотальний контроль» через цифрові документи, «продаж» державних реєстрів. Соціальна інженерія використовується для крадіжки облікових даних: громадяни отримують фішингові листи нібито від державних органів з проханням оновити дані або отримати виплати.

Технологічні виклики включають залежність від іноземних технологічних платформ та рішень. Більшість державних систем працюють на програмному забезпеченні Microsoft, Oracle, SAP, що створює ризики технологічної залежності. Санкції проти Росії призвели до припинення підтримки деяких систем, які використовувалися в державному секторі. Водночас, перехід на вітчизняні або відкриті рішення вимагає значних ресурсів та часу, яких бракує в умовах війни.

Проблема забезпечення безперервності функціонування стала критичною в умовах постійних атак на інфраструктуру. Багато державних установ не мали планів безперервності діяльності, резервних каналів зв’язку, альтернативних джерел живлення. Руйнування дата-центрів, відключення електроенергії,

пошкодження каналів зв’язку призводили до тривалих перерв у наданні послуг. Досвід війни показав необхідність створення розподілених, резервованих систем з можливістю швидкого відновлення після збоїв.

Соціально-психологічні виклики також впливають на процеси цифровізації. Стрес, травми, невизначеність майбутнього знижують готовність громадян та державних службовців освоювати нові технології. Інформаційна перевантаженість, постійний потік тривожних новин призводять до цифрової втоми. Недовіра до державних інституцій, посилена корупційними скандалами та неефективністю окремих рішень, переноситься на цифрові сервіси.

РОЗДІЛ 3
СТРАТЕГІЧНІ НАПРЯМИ ВДОСКОНАЛЕННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ

3.1 Пріоритетні механізми поглиблення цифровізації в умовах війни та повоєнного відновлення

Стратегічне планування цифрової трансформації публічного управління в Україні вимагає комплексного підходу, який враховує як нагальні потреби воєнного часу, так і довгострокові завдання повоєнного відновлення та європейської інтеграції. Визначення пріоритетних механізмів поглиблення цифровізації базується на аналізі поточного стану, виявлених викликів та кращих міжнародних практик, адаптованих до українського контексту. Унікальність української ситуації полягає в необхідності одночасного вирішення завдань екстреної цифровізації для забезпечення безпеки та життєдіяльності держави в умовах війни, а також закладення фундаменту для майбутнього цифрового суспільства європейського зразка.

Цифровізація критично важливих державних функцій в умовах війни стає першочерговим пріоритетом, що визначає виживання та ефективність держави. Сфера оборони потребує подальшого розвитку цифрових систем управління військами, ситуаційної обізнаності, логістичного забезпечення. Система Delta, яка вже довела свою ефективність у координації дій підрозділів, має бути розширена для охоплення всіх рівнів військового управління від тактичного до стратегічного та інтеграції з системами союзників по НАТО. Це включає створення єдиного цифрового простору бойових дій з можливістю обміну даними в режимі реального часу, інтеграцію розвідувальної інформації з різних джерел, автоматизоване планування операцій з використанням алгоритмів штучного інтелекту.

Створення єдиної цифрової платформи оборонних закупівель забезпечить прозорість та ефективність використання оборонного бюджету при збереженні необхідного рівня секретності. Платформа має інтегрувати функції планування потреб, проведення тендерів, моніторингу виконання контрактів, контролю якості продукції. Використання технології блокчейн для критичних операцій забезпечить незмінність записів та можливість повного аудиту всього ланцюга постачань. Впровадження системи електронних сертифікатів якості продукції та цифрових паспортів озброєння підвищить прозорість та відповідальність у сфері оборонних закупівель.

Цифрова логістика оборонного сектору потребує створення інтегрованої системи управління матеріальними потоками від складів до передової. Використання технологій IoT для відстеження переміщення вантажів, предиктивної аналітики для прогнозування потреб, автоматизованих систем управління складами дозволить оптимізувати витрати та забезпечити своєчасне постачання необхідних ресурсів. Інтеграція з цивільними логістичними системами у випадку необхідності забезпечить гнучкість та масштабованість під час критичних ситуацій.

Система соціального захисту населення вимагає створення єдиного цифрового профілю громадянина, який інтегруватиме всю інформацію про соціальний статус, потреби, отримані послуги, історію звернень. Це дозволить автоматизувати призначення допомоги на основі життєвих обставин без необхідності збирання довідок та багаторазового подання одних і тих же документів. Алгоритми штучного інтелекту можуть аналізувати дані для виявлення найбільш вразливих категорій населення та проактивного надання підтримки ще до того, як люди самі звернуться за допомогою. Особливої уваги потребує цифровізація послуг для ветеранів війни: електронний облік з автоматичним визначенням статусу та пільг, автоматичне призначення виплат та компенсацій, психологічна підтримка онлайн через відеоконсультації та чат-боти, програми реабілітації з можливістю віддаленого моніторингу прогресу, платформи працевлаштування з урахуванням набутих навичок та обмежень

здоров’я.

Створення цифрової екосистеми підтримки ветеранів має включати інтеграцію з медичними, освітніми, працевлаштувальними та соціальними сервісами. Єдина платформа надасть комплексну підтримку на всіх етапах повернення до цивільного життя: від демобілізації та отримання статусу до професійної перепідготовки та інтеграції у громаду. Персоналізовані програми підтримки, сформовані на основі аналізу індивідуальних потреб, підвищать ефективність реабілітаційних заходів.

Цифровізація системи допомоги внутрішньо переміщеним особам потребує створення динамічної бази даних з можливістю відстеження переміщень, потреб, отриманої допомоги. Автоматизоване співставлення потреб ВПО з наявними ресурсами дозволить оптимізувати розподіл допомоги та уникнути дублювання. Геоінформаційні системи допоможуть планувати розміщення пунктів надання допомоги, прогнозувати міграційні потоки, оцінювати навантаження на місцеву інфраструктуру.

Управління критичними ресурсами в умовах війни вимагає створення цифрових систем моніторингу та розподілу, здатних працювати в умовах часткової втрати інфраструктури та постійних загроз. Цифрова платформа управління енергетичними ресурсами має інтегрувати дані про виробництво на різних типах електростанцій, поточне та прогнозне споживання, стан передавальних мереж, пошкодження інфраструктури внаслідок атак для оптимізації розподілу електроенергії в умовах дефіциту. Система має використовувати алгоритми машинного навчання для прогнозування попиту, оптимізації навантаження на мережу, мінімізації втрат при передачі. Інтеграція з системами розумних лічильників дозволить впроваджувати динамічне ціноутворення для стимулювання споживання у години низького навантаження.

Система управління гуманітарною допомогою повинна забезпечити прозорий облік та розподіл допомоги від міжнародних партнерів, виключити дублювання та корупцію. Цифровий реєстр вантажів гуманітарної допомоги має відстежувати кожну партію від точки входу в країну до кінцевого отримувача з

використанням QR-кодів та RFID-міток. Інтеграція з базами даних потребуючих допомоги дозволить автоматизувати розподіл відповідно до пріоритетів та реальних потреб. Мобільні додатки для бенефіціарів забезпечать можливість відстеження статусу доставки та підтвердження отримання допомоги.

Цифровізація системи цивільного захисту включає створення єдиної платформи оповіщення про загрози з інтеграцією всіх наявних каналів комунікації: мобільні додатки, SMS, сирени, месенджери, соціальні мережі. Система має автоматично визначати зону загрози та надсилати персоналізовані попередження громадянам у цій зоні з рекомендаціями щодо дій. Координація евакуації через цифрову платформу дозволить оптимізувати маршрути, розподілити потоки людей, організувати транспорт та тимчасове розміщення.

Цифровий реєстр укриттів має містити актуальну інформацію про місцезнаходження, місткість, технічний стан, оснащення кожного укриття з можливістю прокладання маршруту від поточного місцезнаходження користувача. Система моніторингу заповненості укриттів в режимі реального часу допоможе перенаправляти людей до найближчих вільних місць. Інтеграція з медичними сервісами забезпечить наявність необхідної допомоги в укриттях для людей з особливими потребами.

Концептуальна модель стійкої цифрової екосистеми для України має базуватися на принципах розподіленості, резервування, адаптивності, що набувають критичного значення в умовах постійних кіберзагроз та фізичних атак на інфраструктуру. Архітектура систем повинна передбачати відсутність єдиної точки відмови: критичні компоненти мають бути продубльовані в різних фізичних локаціях, дані розподілені між кількома дата-центрами всередині країни та хмарними сервісами за межами України, мережева інфраструктура побудована з можливістю автоматичного перемаршрутизування трафіку при пошкодженні окремих вузлів.

Розвиток національної системи кіберстійкості вимагає створення багаторівневої системи захисту, що поєднує технологічні, організаційні та людські компоненти. На технічному рівні це включає впровадження Zero Trust

Architecture – моделі безпеки, яка не довіряє жодному користувачу чи пристрою за замовчуванням, навіть всередині периметру мережі. Кожен запит на доступ до ресурсів має бути автентифікований, авторизований та зашифрований незалежно від того, звідки він надходить. Мікросегментація мережі обмежує поширення атак, навіть якщо зловмисник отримав доступ до окремого сегмента.

Використання технологій штучного інтелекту для виявлення аномалій та прогнозування кібератак дозволить переходити від реактивного до проактивного захисту. Системи машинного навчання, навчені на історичних даних про атаки, можуть виявляти підозрілу активність на ранніх стадіях, ще до завдання шкоди. Автоматизоване реагування на інциденти скорочує час від виявлення до нейтралізації загрози з годин до хвилин.

Створення національного резерву кіберфахівців – підготовлених спеціалістів з приватного сектору, академічної спільноти, волонтерських організацій, які можуть бути швидко мобілізовані для реагування на масштабні інциденти – забезпечить масштабованість системи кіберзахисту. Регулярні навчання та тренування, у тому числі з міжнародною участю, підтримуватимуть готовність резерву та актуалізуватимуть навички.

Розробка національної стратегії кіберстійкості має виходити за межі технічного захисту та включати економічні стимули для бізнесу впроваджувати кібербезпеку, освітні програми для підвищення обізнаності громадян, міжнародну співпрацю для спільної протидії загрозам, нормативно-правову базу для кримінального переслідування кіберзлочинців.

Інституційні реформи є необхідною передумовою успішної цифрової трансформації, оскільки технологічні зміни без організаційних перетворень не дають очікуваного ефекту. Створення посади Government Chief Digital Officer на рівні віце-прем’єра забезпечить політичну підтримку цифровізації на найвищому рівні, координацію між різними відомствами, контроль за реалізацією національної стратегії цифрової трансформації. GCDO має мати повноваження щодо затвердження великих IT-проєктів, розподілу бюджетних коштів на цифровізацію, встановлення стандартів та вимог.

Реформа державної служби повинна включати обов'язкову цифрову сертифікацію для всіх категорій посад з диференційованими вимогами залежно від функцій. Створення окремої кар'єрної траєкторії для ІТ-фахівців у державному секторі з привабливими умовами оплати праці (на рівні ринкових), гнучким графіком роботи, можливостями професійного розвитку дозволить залучати та утримувати таланти. Програми обміну кадрами між державним та приватним сектором збагатять обидві сторони новим досвідом.

Розвиток цифрових компетенцій державних службовців та громадян є критичним фактором успіху, оскільки найдосконаліші технології безкорисні, якщо люди не вміють ними користуватися. Національна програма цифрової освіти має охопити всі категорії населення з диференційованими програмами для різних груп та врахуванням їх специфічних потреб. Для державних службовців – обов'язкові курси з кібербезпеки (розпізнавання фішингу, безпечна робота з даними, реагування на інциденти), роботи з даними (основи аналітики, візуалізація, інтерпретація результатів), використання цифрових інструментів (електронний документообіг, системи управління проєктами, засоби комунікації). Для громадян – програми базової цифрової грамотності (користування комп'ютером та смартфоном, безпечна робота в інтернеті, захист персональних даних), безпечної поведінки онлайн (розпізнавання шахрайства, керування приватністю в соціальних мережах, цифрова гігієна), використання державних цифрових сервісів (отримання послуг через «Дію», електронні петиції, онлайн-звернення). Особлива увага має приділятися цифровій освіті дітей як інвестиції в майбутнє цифрове суспільство – від базових навичок програмування до критичного мислення та медіаграмотності.

Створення національної мережі центрів цифрової освіти у всіх регіонах забезпечить доступність навчання для всіх категорій населення. Ці центри мають бути обладнані сучасною технікою, підключені до швидкого інтернету, укомплектовані кваліфікованими тренерами. Мобільні навчальні центри можуть охопити віддалені населені пункти та тимчасові поселення ВПО. Онлайн-платформи з курсами різного рівня складності забезпечать можливість

самостійного навчання у зручний час.

Спеціальні програми для вразливих груп – літніх людей, осіб з інвалідністю, мешканців сільської місцевості – мають враховувати їхні специфічні потреби. Для літніх людей – повільніше темп навчання, більше практичних вправ, фокус на найбільш необхідних навичках. Для осіб з інвалідністю – адаптовані інтерфейси, асистивні технології, індивідуальний підхід. Для сільських мешканців – акцент на практичному застосуванні цифрових інструментів у сільському господарстві, малому бізнесі, отриманні державних послуг.

Сертифікація цифрових навичок за міжнародними стандартами (наприклад, European Digital Competence Framework) дозволить об'єктивно оцінювати рівень компетенцій та визнавати їх на ринку праці. Цифрові значки за проходження курсів можуть мотивувати до постійного навчання та відображатися в електронних резюме.

Створення національної системи управління даними забезпечить ефективне використання даних як стратегічного ресурсу для прийняття управлінських рішень та створення цінності для суспільства. Це включає розробку національної стратегії даних, яка визначить пріоритети, принципи, механізми роботи з державними даними. Створення єдиного каталогу державних даних з метаданими, описом якості, умовами доступу дозволить користувачам легко знаходити потрібну інформацію. Впровадження принципів FAIR (Findable, Accessible, Interoperable, Reusable) для державних даних забезпечить їх максимальну корисність для різних користувачів – від дослідників до підприємців.

Центри компетенцій з аналітики даних у ключових міністерствах (економіки, охорони здоров'я, освіти, соціальної політики) забезпечать evidence-based прийняття рішень на основі аналізу великих масивів даних. Ці центри мають включати аналітиків даних, статистиків, галузевих експертів, що працюють спільно над складними питаннями політики. Використання передових методів аналітики – машинного навчання, предиктивного моделювання,

симуляцій – дозволить прогнозувати наслідки різних політичних рішень до їх впровадження.

Механізми забезпечення довіри до цифрових сервісів включають технологічні, організаційні та комунікаційні компоненти, що в сукупності формують екосистему довіри. Впровадження технології блокчейн для критичних реєстрів (земельний кадастр, реєстр прав власності, корпоративний реєстр) забезпечить незмінність даних та можливість аудиту всіх операцій будь-якою зацікавленою стороною. Публічний блокчейн для хешів критичних документів дозволить будь-кому перевірити автентичність документа без доступу до його змісту. Система цифрових довірчих послуг має бути розширена для включення нових методів ідентифікації – біометрії (відбитки пальців, розпізнавання обличчя, райдужна оболонка ока), мобільної ідентифікації (на основі SIM-карти), відеоідентифікації (для віддаленого підтвердження особи).

Прозорість алгоритмів, які використовуються для автоматизованого прийняття рішень, підвищить довіру громадян до цифрових сервісів та дозволить контролювати справедливість рішень. Громадяни мають право знати, на основі яких критеріїв приймаються рішення, що впливають на їх життя – від призначення соціальної допомоги до оцінки податкових ризиків. Механізми оскарження автоматизованих рішень мають бути вбудовані в кожну систему, що використовує штучний інтелект.

Регулярні незалежні аудити безпеки та захисту персональних даних державних систем з публікацією результатів (у формі, що не розкриває вразливості) підвищать довіру громадян. Сертифікація систем на відповідність міжнародним стандартам безпеки та захисту даних підтвердить належний рівень захисту. Програми пошуку помилок, що заохочують дослідників безпеки знаходити та повідомляти про вразливості, посилять захист систем.

Комунікаційні кампанії для підвищення обізнаності громадян про їхні права щодо персональних даних, можливості цифрових сервісів, заходи безпеки сформують культуру відповідального використання цифрових технологій. Прозора комунікація про інциденти безпеки (якщо вони відбуваються) замість

замовчування підвищує довіру та показує готовність вчитися на помилках.

3.2 Оцінка ефективності та рекомендації щодо цифрової трансформації

Комплексна оцінка ефективності цифрової трансформації публічного управління вимагає розробки системи індикаторів та критеріїв, які враховують специфіку воєнного стану та завдання повоєнного відновлення. Методологія оцінювання має базуватися на міжнародних стандартах з адаптацією до українського контексту, забезпечуючи можливість порівняння з іншими країнами та відстеження прогресу в часі. Ефективна система оцінки не лише вимірює досягнуті результати, але й надає зворотний зв'язок для коригування стратегії, виявлення кращих практик для масштабування та проблемних зон, що потребують додаткової уваги.

Багаторівнева система показників має включати індикатори на різних рівнях: національному (загальні показники цифровізації країни, позиції в міжнародних рейтингах), галузевому (специфічні показники для кожної сфери – охорони здоров'я, освіти, соціального захисту), інституційному (показники окремих організацій та установ), проєктному (метрики конкретних проєктів цифровізації). Це дозволить виявляти як загальні тренди, так і специфічні проблеми окремих секторів чи організацій.

Динамічне відстеження показників у часі дозволить оцінювати швидкість трансформації та ефективність втручань. Квартальні огляди ключових індикаторів з публічним оприлюдненням результатів забезпечать прозорість та підзвітність. Порівняльний аналіз з країнами-лідерами та країнами зі схожим рівнем розвитку допоможе визначити реалістичні цілі та виявити відставання. Україна може орієнтуватися на показники Естонії як країни-лідера цифровізації та Польщі як країни зі схожою траєкторією розвитку.

Також участь у міжнародних рейтингах цифровізації надає об'єктивну оцінку прогресу України та визначає пріоритетні напрями покращення. UN E-Government Development Index (EGDI) оцінює три компоненти: онлайн-сервіси, телекомунікаційну інфраструктуру, людський капітал. Україна у 2022 році посіла 46 місце зі 193 країн з індексом 0.7944, покращивши позицію на 23 місця порівняно з 2020 роком. Цільовий показник – увійти до топ-30 до 2027 року та топ-20 до 2030 року, що вимагатиме значного прогресу в усіх трьох компонентах.

Digital Economy and Society Index (DESI), що використовується для країн ЄС, може бути адаптований для оцінки України. Індекс включає п'ять вимірів: зв'язок (покриття широкосмугового інтернету, швидкість, ціни), людський капітал (базові та продвинуті цифрові навички), використання інтернету, інтеграція цифрових технологій у бізнесі, цифрові публічні сервіси. Регулярний моніторинг за методологією DESI дозволить оцінювати прогрес на шляху до європейської інтеграції.

Network Readiness Index оцінює готовність країн використовувати цифрові технології для економічного та соціального розвитку. Індекс включає 60 показників у чотирьох категоріях: технології (доступ, зміст, майбутні технології), люди (окремі особи, бізнес, уряд), управління (довіра, регулювання, інклюзія), вплив (економіка, якість життя, внесок у SDG). Україна у 2023 році посіла 59 місце, що відображає як досягнення, так і простір для покращення.

Cyber security Index оцінює національні можливості у сфері кібербезпеки за п'ятьма напрямами: правові заходи, технічні заходи, організаційні заходи, розвиток потенціалу, співпраця. Покращення позицій у цьому індексі критично важливо в умовах війни та постійних кіберзагроз. Створення спеціальної робочої групи для систематичної роботи над покращенням показників у міжнародних рейтингах забезпечить цілеспрямовані зусилля.

Інноваційні технології відкривають нові горизонти для цифровізації та створення принципово нових типів сервісів. Блокчейн забезпечує незмінність та прозорість державних реєстрів, створюючи довіру через технологію, а не через довіру до інституцій. Земельний кадастр на блокчейні робить неможливою

маніпуляцію з записами про власність, що критично важливо для захисту прав власності. Освітні та професійні кваліфікації на блокчейні можуть легко верифікуватися роботодавцями та освітніми закладами без необхідності звернення до установи, що видала документ. Смарт-контракти автоматизують виконання угод відповідно до попередньо визначених умов, виключаючи необхідність довіряти контрагенту чи посереднику – код гарантує виконання.

На базі проведеного дослідження було сформульовано рекомендації стосовно здійснення цифрових трансформації в умовах воєнного стану для центральних органів виконавчої влади, для місцевих органів влади, щодо забезпечення кібербезпеки, щодо розвитку людського капіталу, щодо міжнародної співпраці.

Рекомендації для центральних органів виконавчої влади:

– Розробити та затвердити детальні галузеві стратегії цифрової трансформації з чіткими KPI, термінами реалізації та відповідальними виконавцями. Кожне міністерство повинно мати дорожню карту цифровізації своєї сфери відповідальності з конкретними проєктами на кожен рік, розрахованими бюджетами та джерелами фінансування, чітким розподілом відповідальності. Стратегії мають бути публічними та регулярно оновлюватися на основі прогресу та нових викликів.

– Створити позиції Chief Digital Officer (CDO) у кожному міністерстві з повноваженнями та статусом на рівні заступника міністра. CDO має очолювати цифрову трансформацію відомства, координувати всі цифрові ініціативи від різних департаментів для уникнення дублювання та забезпечення інтеграції, забезпечувати їх відповідність загальнодержавній стратегії та стандартам, контролювати ефективність використання ресурсів на IT-проєкти, представляти відомство в міжвідомчих робочих групах з питань цифровізації. CDO має мати прямий доступ до міністра та право вето на IT-рішення, що суперечать стратегії.

– Впровадити обов’язкову цифрову експертизу всіх проєктів нормативно-правових актів на предмет їх впливу на цифровізацію. Жоден закон чи постанова не повинні створювати бар’єри для цифрової трансформації,

вимагати паперового документообігу там, де можливий електронний, встановлювати необґрунтовані вимоги до фізичної присутності для отримання послуг, перешкоджати використанню електронних підписів та ідентифікації, обмежувати відкритість даних без обґрунтованих причин безпеки чи конфіденційності. Цифрова експертиза має бути обов'язковою стадією законодавчого процесу.

– Запустити програми глибокої внутрішньої цифрової трансформації міністерств і відомств: повний перехід на електронний документообіг без паперових дублікатів, впровадження сучасних систем управління проєктами та завданнями для прозорості та підзвітності, автоматизація рутинних процесів (узгодження документів, формування звітності, планування зустрічей), використання аналітики даних для внутрішнього менеджменту, створення внутрішніх баз знань та процедур для онбордингу нових співробітників. Це дозволить вивільнити до 30% робочого часу службовців для виконання більш складних аналітичних завдань, що вимагають людського судження.

– Розробити та впровадити системи показників ефективності (KPI) для оцінки прогресу цифровізації на рівні міністерств та окремих проєктів: відсоток процесів, що повністю оцифровані, середній час обробки звернень громадян, рівень задоволеності користувачів послугами, обсяг заощаджених коштів та часу, кількість транзакцій через цифрові канали, показники безпеки та доступності систем. Регулярний моніторинг (щоквартально) та публічне оприлюднення результатів у доступних візуалізаціях забезпечать підзвітність та прозорість, стимулюватимуть відстаючих до покращення.

– Створити механізми швидкого масштабування успішних пілотних проєктів на національний рівень. Часто хороші ініціативи застрягають на стадії пілоту через бюрократичні перешкоди чи брак фінансування. Спеціальний фонд швидкого масштабування та спрощені процедури для проєктів, що довели ефективність, прискорять поширення інновацій.

Рекомендації для місцевих органів влади:

– Створити цифрові офіси в кожній обласній та районній адміністрації,

великій територіальній громаді з мандатом на координацію всіх цифрових ініціатив на території. Ці структури мають координувати цифровізацію на місцевому рівні відповідно до національної стратегії, надавати методичну підтримку установам та організаціям на території, забезпечувати навчання державних службовців та громадян цифровим компетенціям, сприяти впровадженню кращих практик з інших регіонів, представляти інтереси регіону в національних цифрових ініціативах.

– Розвивати мережу ЦНАПів як центрів цифрової трансформації на місцях з розширеними функціями. Крім традиційного надання послуг, ЦНАПи мають стати хабами цифрової освіти з регулярними тренінгами та консультаціями для громадян, точками доступу до технологій для тих, хто не має власних пристроїв або інтернету, центрами технічної підтримки для користувачів цифрових сервісів, майданчиками для демонстрації нових цифрових можливостей та інновацій. Мобільні ЦНАПи можуть обслуговувати віддалені населені пункти.

– Впровадити платформи електронної демократії для підвищення залученості громадян: електронні петиції з нижчими порогами для розгляду порівняно з національним рівнем (наприклад, 100 підписів замість 25000), онлайн-голосування з важливих питань місцевого значення (не обов’язково юридично зобов’язуюче, але консультативне), громадські бюджети з можливістю подавати проєкти та голосувати за них повністю онлайн, прямі трансляції та архіви сесій місцевих рад з можливістю залишати коментарі, цифрові платформи для діалогу між владою та громадою з обов’язковими відповідями на питання. Регулярні звіти про результати електронної участі стимулюватимуть громадян до активності.

– Забезпечити спеціалізовану цифровізацію критичних послуг для ВПО на місцевому рівні: спрощену онлайн-реєстрацію за новим місцем проживання з автоматичним оформленням необхідних документів, єдине вікно для отримання всіх видів допомоги з мінімальними формальностями, цифрову платформу пошуку житла з верифікованими пропозиціями, онлайн-платформу

працевлаштування з урахуванням навичок та потреб ВПО, доступ до психологічної підтримки через телемедицину. Створити єдині бази даних ВПО на рівні області з можливістю безпечного обміну інформацією між громадами для координації допомоги.

– Розробити та регулярно оновлювати плани цифрової стійкості для забезпечення безперервності критичних сервісів: багаторівневе резервне копіювання даних з зберіганням копій у різних фізичних локаціях, альтернативні канали зв'язку (супутниковий інтернет, радіозв'язок) на випадок пошкодження основних, автономні джерела живлення для критичних систем з можливістю роботи кілька днів, чіткі протоколи дій персоналу у кризових ситуаціях з призначенням відповідальних, регулярні навчання та тренування (щоквартально) для перевірки готовності та виявлення слабких місць. Координація планів стійкості з сусідніми громадами для взаємодопомоги.

Рекомендації для забезпечення кібербезпеки:

– Впровадити обов'язкові регулярні аудити кібербезпеки для всіх державних інформаційних систем з періодичністю залежно від критичності: критичні системи – щоквартально, важливі – раз на півроку, решта – щорічно. Аудити мають проводитися як внутрішніми, так і зовнішніми експертами для об'єктивності. Виявлені вразливості мають класифікуватися за рівнем критичності та усуватися в терміновому порядку відповідно до класу (критичні – негайно, високі – протягом тижня, середні – протягом місяця). Публічна звітність про кількість знайдених та усунених вразливостей (без деталей) підвищить довіру.

– Створити галузеві центри безпеки для цілодобового моніторингу та реагування на кіберінциденти у критичних секторах: енергетика, фінанси, транспорт, охорона здоров'я, державне управління. Централізований підхід дозволить ефективніше використовувати обмежені ресурси кіберзахисту, забезпечити єдині стандарти та процедури, швидше виявляти та реагувати на складні скоординовані атаки, акумулювати експертизу та кращі практики. Інтеграція галузевих центрів з національним центром кіберзахисту забезпечить

цілісну картину кіберзагроз.

– Розробити та впровадити обов’язкові програми підвищення кіберграмотності для всіх державних службовців з диференційованим змістом: базовий рівень для всіх (розпізнавання фішингу, безпечні паролі, захист пристроїв), поглиблений для тих, хто працює з конфіденційною інформацією, спеціалізований для ІТ-персоналу. Регулярні симуляції фішингових атак для перевірки пильності та виявлення тих, хто потребує додаткового навчання. Сертифікація з кібербезпеки має бути обов’язковою для певних посад.

– Забезпечити використання вітчизняних або довірених криптографічних засобів для захисту критично важливої інформації. Технологічний суверенітет у сфері кібербезпеки є питанням національної безпеки, особливо в умовах війни. Розвиток власних або адаптація перевірених відкритих рішень для шифрування, електронного підпису, автентифікації знизить ризики закладок та вразливостей. Підтримка української криптографічної індустрії через державні замовлення стимулюватиме розвиток компетенцій.

– Налагодити систематичний оперативний обмін інформацією про кіберзагрози між державним та приватним секторами через спеціалізовані платформи. Створення довірених каналів комунікації з гарантіями конфіденційності для компаній дозволить швидше виявляти нові типи атак та методи, розробляти спільні стратегії захисту, координувати реагування на масштабні інциденти. Правовий захист для компаній, що діляться інформацією про інциденти, стимулюватиме відкритість.

Рекомендації для розвитку людського капіталу:

– Запровадити національну програму цифрових стажувань для студентів ІТ-спеціальностей у державних органах з компенсацією на конкурентному рівні. Це дозволить залучити молоді таланти, які принесуть свіжі ідеї та сучасні підходи, дасть студентам цінний досвід роботи над реальними проблемами державного масштабу, створить кадровий резерв фахівців, які розуміють специфіку держсектору, підвищить престиж роботи в державному

секторі серед ІТ-спільноти. Кращі стажери можуть отримувати пропозиції постійної роботи.

– Розробити привабливі умови для ІТ-спеціалістів у державному секторі, що дозволять конкурувати з приватним сектором: конкурентна оплата праці (не обов'язково на рівні топ-компаній, але достатня для гідного життя), гнучкий графік роботи та можливість віддаленої роботи (навіть з-за кордону у виняткових випадках), сучасне обладнання та інструменти розробки, можливості професійного розвитку (конференції, курси, сертифікації за рахунок роботодавця), значущі проєкти, що впливають на життя мільйонів людей, кар'єрне зростання з чіткими критеріями просування. Без кваліфікованих кадрів цифрова трансформація неможлива, тому інвестиції в людей критично важливі.

– Створити національну онлайн-платформу цифрової освіти для державних службовців з обов'язковою сертифікацією за різними напрямами: базові цифрові навички, робота з офісними додатками, електронний документообіг, кібербезпека, робота з даними та аналітика, проєктний менеджмент, agile-методології, специфічні системи для конкретних галузей. Кожен службовець має проходити мінімум 40 годин цифрового навчання щорічно з підтвердженням сертифікатами. Геймфікація навчання (значки, рейтинги, змагання між установами) підвищить мотивацію.

– Впровадити програми обміну досвідом з країнами-лідерами цифровізації для накопичення експертизи: довгострокові стажування українських держслужбовців у цифрових агенціях Естонії, Данії, Сінгапуру (від 3 до 6 місяців), навчальні візити команд для вивчення конкретних рішень (е-резиденство, цифрова ідентифікація, смарт-сіті), спільні проєкти з обміном експертами для взаємного навчання, запрошення міжнародних консультантів для менторства українських команд, участь у міжнародних конференціях та воркшопах за рахунок держави. Систематичне документування та поширення вивченого досвіду через внутрішні бази знань забезпечить його використання.

– Розвивати мережу амбасадорів цифровізації – ентузіастів з числа державних службовців, які просувають цифрові зміни у своїх організаціях на

волонтерських засадах. Ці люди мають отримувати спеціальне навчання, підтримку з боку центральних органів, визнання через нагороди та публічність, можливості нетворкінгу з амбасадорами з інших установ для обміну досвідом. Зміни знизу, підтримані неформальними лідерами, часто ефективніші за формальні директиви згори, оскільки долають культурний опір.

– Створити програму залучення української ІТ-діаспори до державних проєктів цифровізації. Десятки тисяч українських ІТ-фахівців працюють у провідних компаніях світу та можуть віддалено консультувати, менторити команди, брати участь у проєктуванні архітектури складних систем. Патріотична мотивація та гнучкі форми співпраці (кілька годин на тиждень, конкретні консультації, рев'ю коду) дозволять залучити цей ресурс без великих витрат.

Рекомендації для міжнародної співпраці:

– Активізувати участь у європейських програмах цифровізації та максимізувати залучення фінансування, подавати заявки на проєкти з штучного інтелекту, кібербезпеки, цифрових навичок, брати участь у дослідницьких проєктах з цифрових технологій, залучати фінансування для розвитку цифрової інфраструктури. Створювати спеціалізовані команди для написання грантових заявок, що підвищить їх успішність.

– Розвивати поглиблену двосторонню співпрацю з країнами-лідерами через формальні угоди про партнерство: підписання меморандумів про співпрацю у сфері цифровізації з Естонією (е-урядування), Данією (цифрові послуги), Сінгапуром (смарт-нація), Південною Кореєю (широкосмугові мережі), Ізраїлем (кібербезпека, інновації), призначення цифрових аташе в ключових країнах для систематичної роботи, створення спільних робочих груп з конкретних напрямів, організація регулярних (щоквартальних) обмінів делегаціями. Адаптація успішних рішень партнерів з урахуванням українського контексту прискорить трансформацію.

– Залучати міжнародну технічну допомогу для критичних проєктів через багатосторонні та двосторонні канали: Світовий банк, ЄБРР, British Council та інші донори часто фінансують проєкти цифровізації в країнах, що

розвиваються. Пріоритети: кібербезпека та резервування даних критичних систем за кордоном, розвиток широкосмугової інфраструктури у сільській місцевості та постраждалих регіонах, навчання державних службовців цифровим компетенціям, створення інноваційних хабів та песочниць, фінансування пілотних проєктів з впровадження передових технологій. Підтримка партнерів допоможе компенсувати брак внутрішніх ресурсів в умовах війни.

– Систематично просувати український досвід цифровізації в умовах війни на міжнародних майданчиках як унікальну експертизу: виступи на провідних міжнародних конференціях з е-урядування, цифрової трансформації, кібербезпеки, публікація кейсів у міжнародних виданнях та дослідницьких звітах, організація міжнародних конференцій в Україні для демонстрації досягнень, створення англомовного контенту про українські цифрові рішення, пропонування консультаційних послуг іншим країнам, що стикаються з кризами. Це не лише підвищить престиж України, але й може створити нові джерела доходів.

– Забезпечити повну гармонізацію національних стандартів та процедур з європейськими для технічної інтероперабельності: імплементація стандартів eIDAS для взаємного визнання електронної ідентифікації та довірчих послуг, приєднання до European Interoperability Framework для сумісності інформаційних систем, адаптація європейських стандартів відкритих даних та їх метаданих, приєднання до Single Digital Gateway для надання транскордонних послуг, гармонізація регулювання захисту даних з GDPR. Це критично важливо для майбутньої інтеграції України в єдиний цифровий ринок ЄС та економічних вигод від неї.

ВИСНОВКИ

За результатами дослідження можна зробити такі узагальнені висновки:

1. Концептуальні основи цифрової трансформації публічного управління набувають особливого значення в умовах воєнного стану, коли цифровізація перетворюється з інструменту підвищення ефективності на критично важливий чинник виживання державних інституцій. Цифрова трансформація в умовах війни характеризується подвійною природою: з одного боку, екстремальні умови виступають каталізатором прискорення впровадження інноваційних рішень та подолання інституційного опору змінам; з іншого боку, війна породжує безпрецедентні виклики у вигляді кібератак, руйнування інфраструктури, дефіциту ресурсів. Принципи цифрової трансформації – людиноцентричності, цифрового за замовчуванням, інтероперабельності, однократності введення даних, відкритості та безпечності – формують нормативно-ціннісну основу перетворень, але вимагають адаптації до специфіки воєнного стану. Особливості публічного управління в умовах війни створюють унікальний контекст, що характеризується прискореними темпами впровадження, пріоритизацією критичних функцій, посиленими вимогами до кібербезпеки, необхідністю забезпечення функціонування в умовах руйнування фізичної інфраструктури. Теоретичне осмислення цифровізації в умовах воєнного стану вимагає інтеграції концепцій електронного урядування з теоріями кризового управління, національної стійкості та антикрихкості. Розуміння цих концептуальних основ є необхідною передумовою для розробки науково обґрунтованих стратегій цифрової трансформації, здатних забезпечити як нагальні потреби воєнного часу, так і довгострокові завдання побудови сучасної цифрової держави європейського зразка.

2. Аналіз міжнародного досвіду цифрової трансформації публічного управління в кризових умовах демонструє універсальність певних принципів та підходів при необхідності їх адаптації до національного контексту. Естонська

модель цифровізації, що базується на універсальній цифровій ідентифікації, платформі обміну даними X-Road, концепції цифрової безперервності через резервування критичних систем за межами країни, використанні блокчейну для забезпечення цілісності даних, демонструє важливість системного підходу та попередніх інвестицій у цифрову інфраструктуру. Досвід балтійських країн – Латвії та Литви – показує ефективність централізованих платформ надання послуг, важливість протидії дезінформації як невід'ємної складової цифровізації в умовах гібридних загроз. Ізраїльська модель поєднання цифровізації з вимогами національної безпеки, тісної співпраці держави, армії та високотехнологічного сектору є релевантною для України. Південнокорейський досвід проактивного та персоналізованого обслуговування громадян, використання штучного інтелекту та великих даних визначає майбутні горизонти розвитку. Пандемія COVID-19 продемонструвала критичну важливість попередньо розвиненої цифрової інфраструктури, інтероперабельності систем, цифрової інклюзії для ефективного реагування на кризи. Стандарти та рекомендації міжнародних організацій – ЄС, НАТО, ОЕСР – формують нормативну рамку для цифрової трансформації України в контексті євроатлантичної інтеграції. Ключовим висновком є те, що успішна цифровізація в кризових умовах вимагає не лише технологічних рішень, але й комплексного підходу, який включає правове регулювання, організаційні зміни, розвиток людського капіталу, забезпечення кібербезпеки, міжнародну співпрацю. Критичне осмислення та творча адаптація зарубіжного досвіду з урахуванням українських реалій здатні суттєво підвищити ефективність національної моделі цифровізації.

3. Стан цифровізації державного сектору України під час війни характеризується поєднанням значних досягнень та системних викликів, що вимагають стратегічного осмислення та цілеспрямованих дій. Нормативно-правова база цифрової трансформації, сформована на основі концепцій розвитку цифрової економіки та електронного урядування, ключових законів про електронні довірчі послуги та електронні комунікації, створила правову основу

для цифровізації, хоча потребує постійної актуалізації відповідно до нових викликів. Інфраструктурне та технологічне забезпечення зазнало суттєвої трансформації: міграція критичних систем у хмарні сервіси за межами України забезпечила їх функціонування навіть під час масованих атак на інфраструктуру, що демонструє успішність стратегії розподіленості та резервування. Мобільний застосунок «Дія» став символом цифрової стійкості, швидко адаптувавши функціонал до потреб воєнного часу. Система надання адміністративних послуг продемонструвала здатність до трансформації через прискорене переведення послуг в онлайн-формат, запровадження мобільних ЦНАПів, забезпечення екстериторіальності надання послуг для внутрішньо переміщених осіб. Цифрові рішення для підтримки громадян, бізнесу та армії – від програм єРобота та релокації бізнесу до платформи UNITED24 та системи Delta – показали можливості швидкого розгортання інноваційних сервісів в екстремальних умовах. Електронна система охорони здоров'я, освітні платформи, система електронних закупівель ProZorro продовжили функціонування, забезпечуючи безперервність критичних послуг. Водночас виявлено значну диференціацію цифрової зрілості між різними відомствами та рівнями влади, що вказує на необхідність системних зусиль для вирівнювання спроможностей. Український досвід цифровізації в умовах повномасштабної війни є унікальним у світовій практиці та потребує систематичного документування та наукового осмислення як важливого внеску у глобальну теорію та практику цифрової трансформації в кризових умовах.

4. Виклики та ризики цифровізації в умовах воєнного стану мають комплексний характер та охоплюють технологічні, організаційні, фінансові, правові, соціальні виміри, вимагаючи системного підходу до їх подолання. Кібербезпека стала найгострішим викликом: інтенсивність та складність кібератак зросли в декілька разів, атаки на критичну інформаційну інфраструктуру поєднуються з фізичними ударами, створюючи синергетичний ефект руйнування. Проблеми доступності цифрових послуг загострилися через руйнування інфраструктури, масові відключення електроенергії, обмежений

доступ до високошвидкісного інтернету на прифронтових та сільських територіях. Цифрова нерівність проявляється в географічному, соціально-економічному та віковому вимірах, виключаючи значну частину населення з цифрових процесів та створюючи загрозу соціальній єдності. Організаційно-управлінські бар'єри, включаючи опір змінам з боку частини державних службовців, дефіцит кваліфікованих ІТ-кадрів через низьку оплату праці порівняно з приватним сектором, недостатню міжвідомчу координацію, продовжують гальмувати цифрову трансформацію. Фінансові обмеження в умовах війни, коли понад половина бюджету спрямовується на оборону, призводять до недофінансування цифрових проєктів, хоча міжнародна технічна допомога частково компенсує брак ресурсів. Правові та регуляторні виклики, пов'язані з відставанням законодавства від технологічного розвитку, надмірною зарегульованістю процедур державних закупівель, невизначеністю правового статусу даних у хмарних сервісах, створюють додаткові перешкоди. Інформаційна безпека в умовах гібридної війни вимагає постійної протидії дезінформації та фішингу, спрямованим на підрив довіри до цифрових сервісів. Технологічні виклики, включаючи залежність від іноземних платформ, проблеми забезпечення безперервності функціонування, соціально-психологічні фактори, формують багатовимірну картину ризиків. Ефективне подолання цих викликів вимагає не лише технічних рішень, але й стратегічного підходу, що поєднує інвестиції в інфраструктуру та людський капітал, вдосконалення правового регулювання, посилення міжнародної співпраці, розвиток культури кібербезпеки та цифрової грамотності на всіх рівнях суспільства.

5. Пріоритетні механізми поглиблення цифровізації в умовах війни та повоєнного відновлення повинні базуватися на стратегічному баченні, що поєднує нагальні потреби сьогодення з довгостроковими завданнями побудови сучасної цифрової держави. Цифровізація критично важливих державних функцій – оборони, соціального захисту, управління критичними ресурсами, цивільного захисту – має стати абсолютним пріоритетом, оскільки визначає виживання та ефективність держави в екстремальних умовах. Розвиток системи

Delta для координації військових дій, створення платформи оборонних закупівель з використанням блокчейну, впровадження цифрової логістики, формування єдиного цифрового профілю громадянина для автоматизації соціальної підтримки, створення цифрової екосистеми для ветеранів, впровадження систем управління енергетичними та гуманітарними ресурсами, модернізація системи цивільного захисту через інтеграцію всіх каналів оповіщення – ці напрями вимагають концентрації зусиль та ресурсів. Концептуальна модель стійкої цифрової екосистеми має базуватися на принципах розподіленості, резервування, адаптивності, передбачаючи відсутність єдиної точки відмови, застосування штучного інтелекту для виявлення аномалій, створення національного резерву кіберфахівців. Створення національної системи управління даними, впровадження механізмів забезпечення довіри через блокчейн, прозорість алгоритмів, регулярні незалежні аудити, комунікаційні кампанії сформують екосистему довіри, без якої неможливе широке використання цифрових сервісів. Ці механізми мають реалізовуватися комплексно та узгоджено, з чітким розподілом відповідальності, достатнім ресурсним забезпеченням, постійним моніторингом прогресу та готовністю до коригування стратегії на основі отриманого досвіду та зміни зовнішніх умов.

6. Оцінка ефективності цифрової трансформації та розроблені на її основі рекомендації формують дорожню карту подальшого розвитку цифровізації публічного управління в Україні. Багаторівнева система показників, що включає індикатори на національному, галузевому, інституційному та проєктному рівнях, динамічне відстеження в часі, участь у міжнародних рейтингах дозволяє об’єктивно оцінювати прогрес та порівнювати досягнення України з іншими країнами. Рекомендації для центральних органів виконавчої влади охоплюють розробку детальних галузевих стратегій з чіткими KPI, впровадження обов’язкової цифрової експертизи нормативно-правових актів, запуск програм глибокої внутрішньої цифрової трансформації відомств, створення механізмів швидкого масштабування успішних пілотів. Рекомендації

для місцевих органів влади включають створення цифрових офісів в адміністраціях, розвиток ЦНАПів як хабів цифрової трансформації, впровадження платформ електронної демократії, спеціалізовану цифровізацію послуг для внутрішньо переміщених осіб, розробку планів цифрової стійкості. Рекомендації щодо кібербезпеки передбачають обов'язкові регулярні аудити всіх державних систем, створення галузевих центрів безпеки, програми підвищення кіберграмотності державних службовців, систематичний обмін інформацією про загрози між державним та приватним секторами. Рекомендації з розвитку людського капіталу охоплюють національну програму цифрових стажувань, створення привабливих умов для ІТ-спеціалістів у держсекторі, національну платформу цифрової освіти для держслужбовців, програми обміну досвідом з країнами-лідерами, розвиток мережі амбасадорів цифровізації, залучення української ІТ-діаспори. Рекомендації щодо міжнародної співпраці включають активізацію участі у європейських програмах, поглиблену двосторонню співпрацю з країнами-лідерами, залучення міжнародної технічної допомоги, систематичне просування українського досвіду на міжнародних майданчиках, гармонізацію національних стандартів з європейськими. Комплексна реалізація цих рекомендацій дозволить Україні не лише подолати виклики воєнного часу, але й створити передові цифрові спроможності, що стануть конкурентною перевагою в повоєнний період та сприятимуть успішній євроатлантичній інтеграції. Цифрова трансформація публічного управління в умовах війни є не лише технологічним проєктом, але й стратегічною інвестицією в майбутнє України як сучасної, ефективної, орієнтованої на громадян європейської держави, здатної протистояти будь-яким викликам та забезпечувати високу якість життя своїх громадян.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алєксєєва Т. І. Національна стійкість в умовах гібридної війни: концептуальні засади та практичні механізми. *Стратегічні пріоритети*. 2022. № 2. С. 42-51.

2. Андрусів У. Я., Симчук О. М. Цифрова нерівність в Україні: соціологічний вимір проблеми. *Український соціум*. 2023. № 1. С. 78-92.

3. Бєлікова Н. В. Проблеми цифрової інклюзії в умовах воєнного стану. *Публічне управління та адміністрування в Україні*. 2023. № 34. С. 45-50.

4. Брайчевський С. М., Фоменко О. В. Принцип однократності в електронному урядуванні: європейський досвід та українська практика. *Аспекти публічного управління*. 2021. Том 9, № 2. С. 34-42.

5. Грицяк Н. В. Етапи розвитку електронного урядування: світовий досвід та українські реалії. *Державне управління: теорія та практика*. 2018. № 2. С. 12-23.

6. Державна служба спеціального зв'язку та захисту інформації України. Звіт про стан кібербезпеки в Україні за 2023 рік. К.: ДССЗЗІ України, 2024. 145 с.

7. Дубов Д. В. Цифрова трансформація як чинник публічного управління в умовах глобалізаційних змін. *Стратегічні пріоритети*. 2020. № 3-4. С. 95-104.

8. Єганов В. В. Цифрова зрілість органів державної влади: критерії оцінювання та шляхи підвищення. *Державне управління: удосконалення та розвиток*. 2023. № 5. URL: http://www.dy.nayka.com.ua (дата звернення: 29.10.2025).

9. Клименко І. В., Нескородєва А. О. Система ProZorro як інструмент забезпечення прозорості публічних закупівель в умовах війни. *Інвестиції: практика та досвід*. 2023. № 8. С. 71-76.

10. Карпенко О. В., Денисюк Ж. З. Цифрова трансформація публічного управління: теоретичні засади та практичні виміри. *Вісник НАДУ при Президентові України*. 2021. № 1. С. 47-55.

11. Клімушин П. С., Спасібов Д. В. Еволюція підходів до інформатизації органів публічної влади в Україні. *Теорія та практика державного управління*. 2019. № 4. С. 178-186.

12. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

13. Корнійчук О. П. Доступність цифрових послуг в умовах воєнного стану: виклики та рішення. *Економіка та держава*. 2023. № 3. С. 89-94.

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

15. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

16. Литвин Н. А. Трансформація системи надання адміністративних послуг в умовах воєнного стану. *Публічне адміністрування: теорія та практика*. 2022. Вип. 2(28). URL: http://www.dridu.dp.ua/zbirnik/2022-02(28)/8.pdf (дата звернення: 29.10.2025).

17. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. *Офіційний вісник України*. 2021. № 4. Ст. 198.

18. Національне агентство України з питань державної служби. Оцінка потреб державних службовців у розвитку цифрових компетенцій: аналітичний звіт. К.: НАДС, 2023. 67 с.

19. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 400.

20. Панченко О. А. Інформаційна безпека в умовах гібридної війни: виклики для системи публічного управління. *Ефективність державного управління*. 2022. Вип. 70. С. 13-23.

21. Парубчак І. О., Радченко А. М. Трансформація системи охорони здоров'я через цифровізацію: досвід eHealth. *Державне управління: удосконалення та розвиток*. 2023. № 2. URL: http://www.dy.nayka.com.ua (дата звернення: 29.10.2025).

22. Про Державний бюджет України на 2024 рік : Закон України від 09.11.2023 № 3460-IX. *Офіційний вісник України*. 2023. № 95. Ст. 3.

23. Почепцов Г. Г. Інформаційна політика в умовах гібридної війни / Г. Г. Почепцов. К.: Видавничий дім «Києво-Могилянська академія», 2020. 238 с.

24. Про оборону України : Закон України від 06.12.1991 № 1932-XII. *Відомості Верховної Ради України*. 1992. № 9. Ст. 106.

25. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки : Розпорядження Кабінету Міністрів України від 17.01.2018 № 67-р. *Офіційний вісник України*. 2018. № 16. Ст. 560.

26. Романенко К. М. Портал відкритих даних як інструмент забезпечення прозорості публічного управління. *Публічне управління та митне адміністрування*. 2021. № 2. С. 47-52.

27. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. *Відомості Верховної Ради України*. 2015. № 28. Ст. 250.

28. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

29. Семенченко А. І., Журавльов А. В. Базові державні реєстри як основа цифрової трансформації. *Вісник НАДУ*. 2020. № 3. С. 37-44.

30. Соловйов В. М. Від електронного до цифрового урядування: еволюція концепцій. *Актуальні проблеми державного управління*. 2021. № 1. С. 87-95.

31. Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта»: досвід впровадження та перспективи розвитку / За ред. С. К. Полумієнка. К.: НІСД, 2022. 124 с.

32. Федоренко М. В., Риженко О. В. Портал та застосунок «Дія» як флагман цифрової трансформації України. *Науковий вісник: Державне управління*. 2023. № 1. С. 234-245.

33. Український IT-сектор у 2023 році: аналітичний огляд / IT Ukraine Association. К.: IT Ukraine, 2024. 86 с.

34. European Commission. A Digital Single Market Strategy for Europe. COM(2015) 192 final. Brussels, 2015. 20 p.

35. Brown A., Fishenden J., Thompson M. Digitizing Government: Understanding and Implementing New Digital Business Models. London: Palgrave Macmillan, 2014. 292 p.

36. Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act). Official Journal of the European Union. 2019. L 151. P. 15-69.

37. Denmark's Digital Strategy 2022-2025. Copenhagen: Agency for Digital Government, 2022. 48 p.

38. Digital Government in the Decade of Action for Sustainable Development. UN E-Government Survey 2022. New York: United Nations, 2022. 323 p.

39. E-Government in Lithuania: Factsheet 2023. European Commission, 2023. 24 p.

40. Czosseck C., Ottis R., Talihärm A. Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. International Journal of Cyber Warfare and Terrorism. 2011. Vol. 1, No. 1. P. 24-34.

41. E-Estonia: The Digital Society. Tallinn: e-Estonia Briefing Centre, 2023. 36 p.

42. Israel's Digital Government Strategy 2021-2026. Jerusalem: Government ICT Authority, 2021. 54 p.

43. Latvia's Digital Transformation Guidelines 2021-2027. Riga: Ministry of Environmental Protection and Regional Development, 2021. 72 p.

44. National Risk Register 2023. London: Cabinet Office, HM Government, 2023. 142 p.

45. Moon M. J., Lee J. Critical Factors for Korean Digital Government Development. Public Performance & Management Review. 2019. Vol. 42, No. 3. P. 561-585.

46. OECD. The E-Government Imperative. Paris: OECD Publishing, 2003. 198 p.

47. Piperal V. X-Road: A Secure Data Exchange Layer for e-Government Services. Tallinn: Information System Authority, 2023. 42 p.

48. Taleb N. N. Antifragile: Things That Gain from Disorder. New York: Random House, 2012. 519 p.

49. NATO. Resilience and Article 3. Brussels: NATO Public Diplomacy Division, 2022. 8 p.

50. World Bank. GovTech Maturity Index: The State of Public Sector Digital Transformation. Washington, DC: World Bank, 2022. 168 p.