

Філатов В.В.

Національний технічний університет «Дніпровська політехніка»

ORCID ID: 0009-0009-3339-6623

Кравцов О.В.

Національний технічний університет «Дніпровська політехніка»

ORCID ID: 0000-0002-8027-1796

ПУБЛІЧНА ДІДЖИТАЛІЗАЦІЯ ТА Е-ДЕМОКРАТІЯ: СУЧАСНІ ІНСТРУМЕНТИ, ПРОБЛЕМИ І МОДЕЛІ РЕГУЛЮВАННЯ

У статті представлено комплексний аналіз діджиталізації як ключового інструменту удосконалення взаємодії публічної влади та громадянського суспільства в сучасних умовах глобальних трансформацій. Автор акцентує увагу на перетвореннях державного управління, становленні електронної демократії та впливі цифрових технологій на ефективність, прозорість і підзвітність владних інституцій. Досліджено теоретичні основи та моделі електронного врядування, розкрито сутність поняття «публічна діджиталізація» як багатовимірного процесу, що охоплює цифровізацію адміністративних послуг, розвиток інструментів громадської участі, прозорість державних даних і трансформацію культури взаємодії. Значна увага приділена сучасним цифровим сервісам, розвитку відкритих реєстрів, електронних закупівель, інструментам електронної демократії (петиції, консультації), а також мобільним технологіям і онлайн-платформам для залучення громадян до прийняття рішень.

Виявлені ключові виклики: цифровий розрив (нерівність доступу), низька цифрова грамотність, прогалини у нормативно-правовому регулюванні, недостатня інтеграція електронних систем, загрози кібербезпеці, недосконалість механізмів захисту персональних даних, проблеми моніторингу контенту й відповідальності за дезінформацію. Особливий акцент зроблено на синергії публічної діджиталізації та «зеленої» трансформації відповідно до стратегії «подвійного переходу», що передбачає взаємне підсилення цифрових інструментів і екологічних політик у європейських країнах. Окреслено перспективи для України: необхідність гармонізації нормативної бази з міжнародними стандартами, формування стійкої цифрової екосистеми, розвитку державно-приватного партнерства та удосконалення цифрової грамотності населення й держслужбовців.

Запропоновано рекомендації щодо формування інтегрованої цифрової політики, яка забезпечуватиме національну безпеку, захист прав громадян, відкритість даних та інноваційний розвиток, а також механізми партнерства в сфері кіберзахисту. Робиться висновок про центральну роль діджиталізації у побудові відкритої, демократичної та конкурентоспроможної держави майбутнього.

Ключові слова: діджиталізація, електронне врядування, публічне управління, цифрові сервіси, кібербезпека, нормативно-правове регулювання, електронна демократія.

Постановка проблеми. Цифровізація суспільства стала одним із ключових викликів глобального розвитку, що впливає на економічні, соціальні та політичні процеси. Однак широке впровадження цифрових технологій супроводжується викликами у сфері правового регулювання, зокрема в забезпеченні інформаційної безпеки, захисту даних та управлінні цифровими потоками. Відсутність єдиних міжнародних і національних стандартів цифрової політики створює

умови для правових колізій, нерівного доступу до технологічних ресурсів та посилює ризики кіберзагроз і впливу приватних корпорацій на критичні інфраструктури.

Необхідність розроблення нормативної бази, що відповідає б сучасним міжнародним вимогам і національним пріоритетам, зумовлює актуальність дослідження. Відсутність правових механізмів ефективного використання цифрових технологій у сфері державного управління

та міждержавних відносин ускладнює контроль над цифровими потоками та посилює глобальні виклики у сфері кібербезпеки. Створення інтегрованої правової політики сприятиме ефективному захисту прав людини та інформаційної безпеки, забезпечуючи правову визначеність і стабільність у цифровому середовищі.

Аналіз нормативно-правової бази України показує, що попри значні досягнення у цифровізації, існують системні правові прогалини, які загострюють ризики. Серед ключових проблем – недостатня інтеграція електронних систем між відомствами, відсутність ефективних механізмів правозастосування у сфері захисту персональних даних, застарілі стандарти кібербезпеки, недостатнє регулювання криптовалютних транзакцій та нечіткі норми щодо відповідальності за поширення дезінформації. Особливо критичною є проблема взаємодії між державними та приватними структурами у сфері забезпечення безпеки критичної інформаційної інфраструктури. Як зазначено у дослідженнях, "більшість критичних об'єктів, зокрема у сферах енергетики, фінансів і телекомунікацій, перебуває в приватній власності", а відсутність уніфікованих стандартів взаємодії та централізованих каналів обміну інформацією про кіберінциденти суттєво знижує ефективність колективного захисту від кіберзагроз.

Міжнародний досвід демонструє різні моделі публічної діджиталізації з потужними інструментами регулювання. Особливу увагу привертає європейська концепція «подвійного переходу» (twin transition), яка синергетично поєднує публічну діджиталізацію та «зелену трансформацію», створюючи нову парадигму державного управління, де цифрові технології стають ключовим інструментом для досягнення цілей сталого розвитку. У цьому контексті дослідження сучасних інструментів публічної діджиталізації та е-демократії, моделей їх регулювання має не лише теоретичне значення, але й практичну цінність для формування ефективної державної політики України, особливо в умовах європейської інтеграції та післявоєнної відбудови за принципом "краще, ніж було". Подолання виявлених правових прогалин та розробка інтегрованого підходу до цифрової трансформації публічного управління є ключовим викликом для побудови сучасної, конкурентоспроможної та кіберстійкої держави.

Аналіз останніх досліджень і публікацій. Варто погодитись із підходами: 1) М. Кириченка і А. Галюка, щодо ролі державних цифрових

платформ у процесі мінімізації адміністративних бар'єрів; 2) Н. Петренко та Л. Машковської у контексті наявності правових прогалин та відсутності єдиних стандартів цифрових сервісів [2]; 3) С. Пирога щодо необхідності нормативної підтримки цифрового підприємництва для стимулювання економічного розвитку та конкурентоспроможності, що є актуальним в умовах глобальних викликів [3]; 4) І. Крикавської, щодо уніфікованих стандартів регулювання електронних послуг [4]. Також досить важливим є сучасні методологічні розробки щодо балансу між прозорістю та безпекою даних [5-6].

Загальний аналіз сучасних наукових публікацій [7-17] з питань цифровізації публічного управління та розвитку е-демократії демонструє значний поступ у нормативному, технологічному й організаційному вимірах. Проте систематизація змісту існуючих досліджень виявляє низку проблемних полів, які досі залишаються недостатньо розробленими й потребують глибшого міждисциплінарного вивчення. Зокрема, майже не розкритою в науковому дискурсі є синергія цифрових та «зелених» трансформацій у публічному управлінні (так званих twin transition), яка дозволяє об'єднувати інструменти діджиталізації з екологічними політиками для досягнення цілей сталого розвитку.

Важливою нерозв'язаною проблемою залишається інтеграція приватного сектора у національну систему кібербезпеки, що актуально в умовах підвищених ризиків для критичних інформаційних інфраструктур. Недостатньо дослідженими лишаються й інноваційні механізми протидії дезінформації в цифровому середовищі, а також правове забезпечення використання криптовалютних і blockchain-технологій у публічному секторі.

Особливої уваги потребують адаптивні підходи до захисту персональних даних в умовах воєнного стану чи надзвичайних ситуацій, оскільки традиційні моделі захисту не завжди відповідають викликам кризового періоду. Водночас бракує наукової уваги до розробки ефективних механізмів залучення малих громад до процесів е-демократії, що суттєво впливає на інклюзивність цифрових трансформацій на місцевому рівні. Окремим науковим завданням залишається комплексна оцінка ефективності електронних сервісів з урахуванням досвіду та потреб користувачів, адже саме такий підхід дозволяє забезпечити їхню реальну доступність, зручність та результативність.

Виклад основного матеріалу. Для системного розуміння прогалин і ризиків цифровізації сучас-

ного публічного управління доцільно здійснити системний аналіз головних напрямів нормативного регулювання та ключових викликів, актуалізованих сучасними трансформаціями. Огляд основних проблемних зон дозволяє окреслити сфери, у яких нормативно-правова база залишається недостатньо опрацьованою, а існуючі ризики поглиблюють вразливість цифрового середовища. Зокрема, у сфері електронного врядування відчутним є дефіцит інтеграції між інформаційними системами різних відомств. Це зумовлює затримки в обміні даними, виникнення дублюючих функцій та суттєво знижує ефективність роботи адмінпослуг. У сфері захисту персональних даних критичною проблемою є відсутність дієвих механізмів правозастосування, що створює ризики незаконного доступу до персональної інформації й призводить до зниження довіри громадян до цифрових сервісів.

У напрямі кібербезпеки встановлено відсутність сучасних стандартів захисту, внаслідок чого державна IT-інфраструктура стає особливо чутливою до нових типів кібератак. Що стосується цифрових фінансових операцій, неповне нормативне врегулювання криптовалютних транзакцій сприяє зростанню фінансових шахрайств і підвищує непрозорість таких операцій. Актуальною залишається й проблема чіткого правового регулювання цифрового контенту. Недостатнє визначення норм щодо відповідальності за поширення дезінформації створює сприятливі умови для маніпуляцій громадською думкою через цифрові платформи та загрожує інформаційній безпеці суспільства. Адже у сфері цифрового контенту не завжди чітко визначено, хто несе відповідальність за поширення недостовірної інформації, що дозволяє маніпулювати суспільною думкою через соціальні мережі та інші платформи [7, с. 149]. Відсутність ефективних механізмів моніторингу та контролю лише посилює ці ризики.

Отже, виявлені правові прогалини та ризики цифровізації вимагають не просто оновлення чинного законодавства, а впровадження цілісної, інтегрованої стратегії нормативного регулювання. Ключовим завданням є гармонізація національної правової бази з міжнародними стандартами та адаптація її до динамічних змін цифрового середовища. Особливої важливості набуває створення ефективних механізмів моніторингу та правозастосування, здатних оперативно реагувати на сучасні кіберзагрози, забезпечувати високий рівень інформаційної безпеки та зміцнювати довіру суспільства до цифрових процесів.

У контексті глобальної цифровізації міжнародний досвід нормативного регулювання набуває особливої цінності для формування національних підходів. Провідні держави світу активно впроваджують багаторівневі моделі регулювання, поєднуючи захист персональних даних, контроль електронних транзакцій, розвиток комплексної системи кібербезпеки та впровадження механізмів запобігання дезінформації. Зокрема, Європейський Союз є прикладом системного нормативного підходу, впроваджуючи загальнообов'язкові регламенти і директиви для всіх держав-членів, що формує єдиний простір цифрової безпеки.

Водночас США, Велика Британія та інші країни надають перевагу секторальному та гнучкому законодавчому регулюванню, оперативно вдосконалюючи нормативно-правове поле відповідно до специфіки окремих сфер цифрової діяльності. Аналіз міжнародних практик дозволяє ідентифікувати перевірені моделі та інструменти регулювання, а також сформувати стратегічні орієнтири для удосконалення національної правової системи у сфері цифрових трансформацій [18–26]

Попри запровадження уніфікованих підходів до захисту персональних даних у ЄС, зокрема через прийняття Загального регламенту про захист даних (GDPR), у сфері публічної діджиталізації зберігається низка викликів і невирішених питань. Хоча GDPR визначає загальні принципи збору, обробки та зберігання особистої інформації, практична реалізація цих норм у державному секторі часто ускладнюється фрагментарністю інформаційних систем, відсутністю єдиних стандартів сумісності й недостатньою прозорістю доступу громадян до власних даних. Це, у свою чергу, створює ризики витоків, несанкціонованої обробки й зниження довіри громадськості до цифрових сервісів держави.

Додатково, вимоги щодо кібербезпеки, визначені Директивою NIS, охоплюють ключові сфери – енергетику, транспорт, цифрові послуги – однак їх адаптація до особливостей публічного адміністрування відбувається нерівномірно. Національні адміністрації часто стикаються з труднощами інтеграції безпекових стандартів у розгалужені цифрові структури, що посилює вразливість державних інституцій до кібератак та ускладнює ефективний контроль за інформаційними потоками.

У США прийняття CLOUD Act дало можливість правоохоронним органам отримати доступ до даних, які зберігаються на серверах за кордоном, що є важливим для розслідування кіберзло-

чинів. Водночас закон ССРА захищає права споживачів, дозволяючи їм контролювати оброблення своїх даних та вимагати видалення персональної інформації [20-22].

У Великій Британії Закон «Про захист даних» адаптований до вимог GDPR і передбачає додаткові заходи щодо контролю державних та комерційних структур у сфері оброблення даних. Національна стратегія кібербезпеки акцентує увагу на впровадженні стандартів інформаційної безпеки для забезпечення стійкості критичних систем до кібератак [23].

Закон NetzDG у Німеччині спрямований на боротьбу з поширенням незаконного контенту, особливо в соціальних мережах, шляхом установлення обов'язку видаляти небезпечний контент у визначені строки. У випадку порушення цих вимог накладаються значні штрафи, що стимулює компанії дотримуватись стандартів безпеки контенту [24].

Естонія демонструє одну з найуспішніших моделей цифрового врядування завдяки системі електронного резидентства, яка функціонує відповідно до закону «Про документи, що посвідчують особу». Водночас офіційний сайт програми електронного резидентства забезпечує доступ до інформації про процедури, реєстрацію та можливості, що надаються е-резидентам. Захищені електронні системи голосування забезпечують прозорість виборчого процесу та високий рівень довіри громадян [25-26].

Таким чином, міжнародні практики показують, що ефективне регулювання цифрових технологій потребує комплексного підходу з урахуванням особливостей конкретних держав, що дозволяє досягти балансу між безпекою, конфіденційністю та прозорістю цифрових процесів.

Стан взаємодії між державним і приватним секторами у сфері цифрової безпеки в Україні характеризується відсутністю належної координації та значними системними недоопрацюваннями. Наразі існує дефіцит єдиної платформи для обміну оперативною інформацією щодо кіберінцидентів, а розрізненість моніторингових систем нерідко призводить до затримки виявлення та реагування на кіберзагрози. Основною проблемою лишається низький рівень горизонтальної інтеграції між залученими інституціями та недостатня чіткість розподілу відповідальності між державними органами й приватними власниками критичної інфраструктури.

Це ускладнює формування довгострокової стратегії кіберстійкості та створює передумови

для зловживань чи неузгоджених дій у кризових ситуаціях. Брак довіри та обмежена прозорість у взаємодії додатково посилюють ризики для захисту персональних даних, функціонування ключових IT-ресурсів і підтримання цифрової інфраструктури в належному стані.

У контексті зростання зовнішніх і внутрішніх кіберзагроз виникає нагальна потреба в розробці та реалізації інтегрованої цифрової політики на основі багаторівневого партнерства. Йдеться не лише про впровадження сучасних технічних стандартів, але й про створення чітких регламентів публічно-приватної взаємодії, формалізацію обміну даними між учасниками, а також підвищення відповідальності за колективну кібербезпеку. Необхідними кроками на цьому шляху виступають: 1) створення Національної стратегії цифрової безпеки, інтегрованої з міжнародно визнаними протоколами й стандартами; 2) інституціоналізація державно-приватного партнерства, що дозволить координувати спільні дії з попередження і подолання кіберінцидентів та розвивати інновації у сфері кібербезпеки; 3) розгортання мережі центрів реагування на кіберінциденти (CERT), які здійснювали б оперативний обмін інформацією, надавали підтримку учасникам цифрової інфраструктури та шукали системні рішення для убезпечення держави і бізнесу; 4) регулярний аудит і стрес-тестування цифрових систем для своєчасного виявлення вразливостей і постійного підвищення кіберстійкості на критичних ділянках.

Реалізація таких підходів дозволить не лише підвищити рівень захищеності цифрового середовища, а й зміцнити довіру між усіма учасниками цифрової трансформації, забезпечивши стійкий розвиток інформаційного простору України в умовах сучасних викликів.

Ефективна еволюція національного цифрового законодавства має базуватися на гармонізації з провідними міжнародними нормативами й угодами, що забезпечить узгодженість правових механізмів і мінімізує ризики виникнення міждержавних та внутрішньодержавних колізій. Поряд із цим критично важливо впроваджувати принципи кіберсуверенітету як здатності держави самостійно визначати політику в цифровій сфері, не порушуючи при цьому власні зобов'язання перед світовим співтовариством [4, с. 163].

Розвиток цифрової політики потребує не лише створення сучасних правових рамок, а й активної підтримки наукових досліджень та інноваційних проєктів. Державне стимулювання технологічних

стартапів і залучення молодих фахівців до розробки ІТ-продуктів стає потужним фактором підвищення конкурентоспроможності країни на глобальному ринку цифрових послуг.

Окремим стратегічним напрямом є підвищення рівня цифрової компетентності населення, з особливим акцентом на підготовці кадрів для державного сектора. Недостатній рівень цифрової грамотності досі залишається однією з головних причин неефективного впровадження електронних рішень і підвищеної вразливості до кіберзагроз, обмежуючи потенціал державних цифрових проєктів [10, с. 763].

Відтак формування інтегрованої цифрової політики має передбачати побудову гнучкої системи регулювання, яка забезпечує одночасний захист державних інтересів, інформаційної безпеки, прав і свобод громадян, а також активну міжнародну співпрацю. Запровадження сучасних технологічних стандартів, регулярний перегляд нормативів і постійне оновлення знань учасників цифрової екосистеми дозволять не лише знизити уразливість критичної ІТ-інфраструктури, а й посилити довіру суспільства до державних цифрових сервісів, створюючи передумови для динамічного й сталого цифрового розвитку України.

Висновки. Дослідження показало, що нормативно-правове регулювання цифрової політики є визначальним фактором для забезпечення національної безпеки та безперебійного функціонування цифрової інфраструктури в кризових ситуаціях. Аналіз правової бази України виявив істотні прогалини, які особливо загострились в умовах воєнного стану – від недосконалості механізмів електронної ідентифікації переміщених осіб до відсутності чітких протоколів функціонування критичних цифрових систем під час бойових дій.

Серед критичних проблем найгостріше постають: відсутність адаптивних правових режимів для захисту персональних даних в умовах воєнної необхідності, недостатня регламентація використання хмарних технологій для зберігання державних реєстрів за кордоном, а також правова невизначеність щодо застосування електронних доказів для фіксації воєнних злочинів. Особливо проблематичним залишається правове забезпечення кібербезпеки об'єктів критичної інфраструктури, що можуть стати мішенню під час гібридних атак, зокрема відсутні ефективні механізми координації між військовими та цивільними органами у разі кіберінцидентів.

Діджиталізація публічного управління в умовах воєнного стану виявила додаткові правові виклики: нерегламентованість процедур дистанційного прийняття управлінських рішень, недостатня цифрова інтероперабельність систем військового та цивільного призначення, а також відсутність правових механізмів для швидкої цифрової трансформації адміністративних послуг у районах, наближених до бойових дій. Для подолання виявлених проблем необхідне формування інтегрованої цифрової політики воєнного часу, що передбачає: по-перше, розробку спеціальних правових режимів функціонування цифрових систем в умовах надзвичайних ситуацій, з чіткими протоколами резервного копіювання, відновлення та забезпечення безперервності публічних сервісів; по-друге, створення єдиного центру кіберзахисту критичної цифрової інфраструктури, що координуватиме взаємодію між військовими, державними та приватними структурами під час кібератак; по-третє, впровадження гнучкої нормативної бази для прискореної діджиталізації адміністративних процесів з урахуванням безпечових ризиків воєнного часу, включно з мобільними застосунками для надання адміністративних послуг у районах з обмеженою інфраструктурою; розробку правових механізмів транскордонного обміну цифровими даними для ефективної взаємодії з міжнародними партнерами у сфері безпеки та гуманітарної допомоги; по-четверте, формування спеціалізованого правового режиму цифрової ідентифікації внутрішньо переміщених осіб та громадян на окупованих територіях.

Перспективними напрямками подальших досліджень є розробка методології оцінки ефективності цифрових інструментів в умовах воєнного стану, визначення правових механізмів забезпечення цифрового суверенітету та відновлення цифрової інфраструктури на деокупованих територіях. Особливу увагу слід приділити формуванню системи цифрової стійкості публічного управління, що поєднує технологічні, організаційні та правові аспекти функціонування державних електронних сервісів в умовах підвищеної загрози.

Список використаної літератури:

1. Кириченко М., Галюк А. Цифровізація в умовах глобальних викликів: азійський досвід та перспективи. *Економіка та суспільство*. 2024. Вип. 68. DOI: <https://doi.org/10.32782/2524-0072/2024-68-139>.
2. Петренко Н. О., Машковська Л. В. Цифровізація державних адміністративних послуг в Україні: нормативно-правові аспекти. *Право і суспільство*. 2020. № 2. С. 112–119. URL: http://pravoisuspsilstvo.org.ua/archive/2020/2_2020/part_1/20.pdf.

3. Пиріг С. О. Державна політика цифрового розвитку та е-бізнесу в Україні. *Економічні науки. Серія «Регіональна економіка»*. 2023. Вип. 20 (79). С. 178–185. DOI: [https://doi.org/10.36910/2707-6296-2023-20\(79\)-23](https://doi.org/10.36910/2707-6296-2023-20(79)-23).
4. Криківська І. Нормативно-правове регулювання впровадження та використання цифрових технологій у сфері надання адміністративних послуг. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2020. № 2. С. 162–165. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2020/sep/22149/27.pdf>.
5. Linkov I., Trump B. D., Poinsatte-Jones K., Florin M. Governance strategies for a sustainable digital world. *Sustainability*. 2018. Vol. 10 (2). Article 440. DOI: <https://doi.org/10.3390/su10020440>.
6. Schou J., Hjelholt M. *Digitalization and public sector transformations*. Springer. 2018. URL: <https://books.google.com.ua/books?hl=uk&lr=&id=tqIVDwAAQBAJ&oi=fnd&pg=PR5>.
7. Di Giulio M., Vecchi G. Implementing digitalization in the public sector: Technologies, agency, and governance. *Public Policy and Administration*. 2023. Vol. 38 (2). P. 133–158. DOI: <https://doi.org/10.1177/0952076721102328>.
8. Kianpour M., Øverby H., Kowalski S. J., Frantz C. Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. In: Moallem A. (ed.) *HCI for Cybersecurity, Privacy and Trust*. HCII 2019. Lecture Notes in Computer Science, vol 11594. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-22351-9_1.
9. Shtets T., Lupak R., Vasylytsiv T. General aspects of state policy for the digital transformation of the national economy. *International Independent Scientific Journal*. 2020. Issue 20-2. P. 14–19. URL: <https://elibrary.ru/item.asp?id=44082084> (date of access: 07.01.2025).
10. Tokar M., Shybirina S., Kolosovska I., Khmarska I. Digital Aspects of the Ukrainian Digitalization. *Economic Affairs*. 2022. Vol. 67 (04s). P. 755–764. DOI: <https://doi.org/10.46852/0424-2513.4s.2022.9>.
11. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.
12. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>.
13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
14. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.
15. Про платіжні послуги: Закон України від 30.06.2021 р. № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text>.
16. Про медіа: Закон України від 13.12.2022 р. № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>.
17. Про рекламу: Закон України від 03.07.1996 р. № 270/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/270/96-вр#Text>.
18. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
19. Directive on Security of Network and Information Systems (NIS Directive): Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016. URL: <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>.
20. Clarifying Lawful Overseas Use of Data Act (CLOUD Act): Enacted as part of the Consolidated Appropriations Act, 2018, Public Law No: 115-141 (03/23/2018). URL: <https://www.congress.gov/bill/115th-congress/house-bill/4943>.
21. California Consumer Privacy Act (CCPA): California Civil Code Title 1.81.5, added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2020. URL: https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=&chapter=&part=4.&lawCode=CIV&article=.
22. Data Protection Act 2018: An Act to make provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. URL: <https://www.legislation.gov.uk/ukpga/2018/12/enacted>.
23. National Cyber Security Strategy 2022: Policy paper by the UK Government outlining the strategic framework for cyber security. URL: <https://www.gov.uk/government/publications/national-cyber-strategy-2022>.
24. Netzwerkdurchsetzungsgesetz (NetzDG): Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken vom 1. September 2017 (BGBl. I S. 3352). URL: <https://www.gesetze-im-internet.de/netzdg/>.
25. E-residency of Estonia: Official website of the Estonian e-residency program. URL: <https://e-resident.gov.ee>.
26. Isikut tõendavate dokumentide seadus (Identity Documents Act): Passed on 15 February 2000, RT I 2000, 26, 150. URL: <https://www.riigiteataja.ee/akt/104072014003>.
27. Locked Shields – International Cyber Defence Exercise: Official website of the NATO Cooperative Cyber Defence Centre of Excellence. URL: <https://ccdc.org/exercises/locked-shields>.
28. Кібербезпека-Україна – національні навчання з кіберзахисту: офіційний вебсайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua>.

**Filatov V.V., Kravtsov O.V. PUBLIC DIGITALIZATION AND E-DEMOCRACY:
CONTEMPORARY TOOLS, CHALLENGES, AND REGULATORY MODELS**

The article presents a comprehensive analysis of digitalization as a key instrument for improving the interaction between public authorities and civil society in the context of contemporary global transformations. The author emphasizes changes in public administration, the emergence of electronic democracy, and the impact of digital technologies on the efficiency, transparency, and accountability of government institutions. Theoretical foundations and models of e-governance are explored, alongside the concept of “public digitalization” as a multidimensional process encompassing the digitalization of administrative services, the development of civic participation tools, transparency of governmental data, and the transformation of interaction culture. Significant attention is paid to modern digital services, the development of open registries, electronic procurement, e-democracy tools (petitions, consultations), as well as to mobile technologies and online platforms for engaging citizens in decision-making.

Key challenges identified include the digital divide (unequal access), low digital literacy, gaps in legal regulation, insufficient integration of electronic systems, cybersecurity threats, deficiencies in personal data protection mechanisms, and issues of content monitoring and liability for disinformation. Special focus is placed on the synergy of public digitalization and the “green” transition in line with the dual transition strategy, which involves the mutual reinforcement of digital tools and environmental policies in European countries. Prospects for Ukraine are outlined, including the need to harmonize the regulatory framework with international standards, form a resilient digital ecosystem, develop public-private partnerships, and enhance digital literacy among citizens and civil servants.

The article offers recommendations for establishing an integrated digital policy that will ensure national security, protection of citizens’ rights, data openness, and innovative development, as well as mechanisms for partnership in the field of cybersecurity. The central conclusion highlights the crucial role of digitalization in building an open, democratic, and competitive state of the future.

Key words: digitalization, e-governance, public administration, digital services, cybersecurity, legal regulation, e-democracy.