

Калюжна Юлія Іванівна

Цифрова трансформація держави та цифрове громадянство: виклики та стратегії національної безпеки

УДК 323.25:004:355.01

DOI <https://doi.org/10.24195/2414-9616.2025-2.9>

Калюжна Юлія Іванівна
кандидат політичних наук, доцент,
доцент кафедри політології, соціології
і культурології
Харківського національного
педагогічного університету
імені Г. С. Сковороди
вул. Алчевських, 29, Харків, Україна
ORCID: 0000-0002-7344-410X

В умовах інтенсивної цифрової трансформації та зростання кіберзагроз, дослідження взаємозв'язку між розвитком цифрового громадянства та національною безпекою держави набуває особливої актуальності. Світовий досвід, зокрема практики ЄС у сфері е-демократії, демонструє потенціал цифрових інструментів, але водночас актуалізує питання кіберстійкості суспільства. Цифрове громадянство, як комплексна екосистема атрибутів, є ключовим фактором ефективної взаємодії з цифровою державою та протидії деструктивним впливам у кіберпросторі. З огляду на геополітичну нестабільність та активне використання кібернетичних і інформаційних інструментів агресії, зокрема проти України, розуміння цієї взаємозалежності є критично важливим. Метою статті є комплексний огляд та систематизація наукової літератури, аналітичних матеріалів і стратегічних документів для виявлення ключових аспектів взаємозв'язку між розвитком цифрового громадянства та забезпеченням національної безпеки держави в умовах активної цифрової трансформації та зростаючих зовнішніх кіберзагроз і дезінформаційних кампаній. Завдання дослідження включають визначення сутності цифрового громадянства, обґрунтування його ролі у стійкості суспільства, аналіз актуальних цифрових загроз, та розроблення рекомендацій щодо стратегії розвитку цифрового громадянства для зміцнення національної безпеки України. Методологія базується на системному аналізі та інтеграції наукової літератури з ключових наукометричних баз даних, профільних аналітичних матеріалів та стратегічних документів міжнародних організацій і аналітичних центрів. Застосовувалися порівняльний та критичний аналіз домінуючих парадигм, систематизація та інтеграція інформації для авторського визначення цифрового громадянства та розробки рекомендацій щодо його розвитку в контексті національної безпеки цифрової епохи. Дослідження виявило тісний взаємозв'язок між розвитком цифрового громадянства та забезпеченням національної безпеки. Цифрове громадянство, що включає кіберкомпетентність, цифрову відповідальність, цифрову партисипацію та критичне цифрове мислення, є ключовим фактором зміцнення цифрової стійкості держави. Обґрунтовано стратегічну важливість формування державної політики розвитку цифрового громадянства в Україні як невід'ємної складової ефективної стратегії національної безпеки в цифрову епоху, що сприяє успішній імплементації е-демократії та загальній національній стійкості.

Ключові слова: цифрова трансформація держави, цифрова держава, цифрове громадянство, е-демократія, виклики цифрової епохи, інформаційна безпека, кіберзагрози та дезінформація, стратегія національної безпеки.

Вступ. У безпрецедентну епоху технологічної конвергенції, коли інформаційно-комунікаційні технології (ІКТ) трансформувалися з інструментів комунікації в основоположну силу сучасної цивілізації, феномен цифрової трансформації держави постає як ключовий вектор розвитку національних держав у XXI столітті. Світовий досвід демонструє різноманітні траєкторії розвитку цифрової демократії [9; 24; 40]. Флагманами в сфері цифровізації виступають країни Європейського Союзу [13], які започаткували передові цифрові практики та успішно інтегрували цифрові інструменти в політичний дизайн європейських е-демократій (ID (електронна ідентифікація), цифровий гаманець, інтерактивні державні сервіси, е-кабінет громадянина, портали відкритих даних, платформи для онлайн-петицій, віртуальні ратуші, системи е-голосування, е-декларування тощо), відкриваючи нові можливості для е-урядування та сприяючи цифровій інклюзії між громадянами та державою. Естонія є показовим прикладом, створивши інте-

гровану цифрову екосистему, де абсолютна більшість державних послуг доступні онлайн, а електронне голосування стало усталеною практикою [7; 37]. Данія вирізняється високим рівнем цифрової грамотності населення та активним впровадженням онлайн-платформ для взаємодії громадян з органами влади [10; 29]. Фінляндія та Нідерланди експериментують з інноваційними формами електронної участі, залучаючи громадян до процесу розробки політик на ранніх стадіях [6; 23]. Франція та Німеччина, усвідомлюючи складність імплементації, поступово розширюють спектр онлайн-послуг та інструментів електронної демократії [25]. Крім того, в умовах загострення глобальної геополітичної нестабільності та усвідомлюючи стратегічну вагу цифрової сфери, ЄС активно формує далекоглядну концепцію лідерства у цифровій трансформації, спрямовану на побудову стійкої екосистеми, що базується на принципах справедливості, конкуренції, прозорості, демократії та безпеки. Цей цілісний підхід, відображений у програмному доку-

менті «2030 Digital Compass: the European way for the Digital Decade» [8], передбачає спільні зусилля для забезпечення європейської стійкості через глибоку цифровізацію. Ці приклади підкреслюють, що успішна цифрова трансформація держави вимагає не лише технологічної інфраструктури, але й стратегічного бачення, політичної волі та орієнтації на новітні виклики й потреби громадян [39].

Ця нова реконфігурація парадигми державного управління, що охоплює вектори цифровізації публічних сервісів, імплементації електронного урядування та культивування цифрової залученості громадян [11; 30], є нерозривно пов'язаною з генезисом цифрового громадянства. Останнє постає як багатогранна та інтегративна концепція, що є визначальним елементом у процесі трансформації держави до цифрової ери. На відміну від обмеженого розуміння, що зводиться до фізичного доступу до цифрової інфраструктури та опанування елементарних навичок її експлуатації, цифрове громадянство являє собою складну екосистему взаємодетермінованих атрибутів, критично важливих для повноцінної та результативної участі індивіда в інформаційному суспільстві та його інтеракції з цифровою державою. Таким чином, цифрове громадянство слід розглядати не як дискретний набір технічних компетенцій, а як цілісну систему когнітивних структур, практичних умінь, етичних імперативів та моделей поведінки, що є необхідною передумовою для ефективної взаємодії громадянина з цифровою державою, його всебічної інтеграції в інформаційне суспільство та повної реалізації потенціалу цифрової трансформації державних інститутів [1; 2; 3; 4; 19; 24; 26; 27; 33; 40].

У контексті ескалації викликів цифрової епохи, зокрема експоненційного зростання кіберзагроз та інтенсифікації дезінформаційних кампаній, рівень цифрової компетентності громадян демонструє пряму кореляцію з національною безпекою. Оволодіння навичками критичного мислення, медіаграмотності та кібергігієни формує резильєнтність суспільства щодо маніпулятивних впливів та кібератак, що є фундаментальним елементом забезпечення національних інтересів у цифровому просторі. Показово, що амбітні перспективи цифрової трансформації держави та консолідації цифрового громадянства наражаються на зростаючі загрози національній безпеці, особливо в умовах складної геополітичної кон'юнктури. Російська Федерація, застосовуючи гібридні стратегії ведення війни, активно використовує кібернетичні атаки та широкомасштабні інформаційні операції з метою дестабілізації не лише України, але й держав Європейського Союзу та інших демократичних акторів. Ці ворожі дії спрямовані на підлив критичної інфраструктури, втручання в електоральні процеси, поширення дезінформації для поглиблення

суспільної поляризації та дискредитації інститутів державної влади. Кіберпростір детермінується як нова арена конфронтації, де кібератаки на державні та приватні інституції, а також цілеспрямоване маніпулювання інформаційними потоками через соціальні медіа та контрольовані медіаресурси, становлять безпосередню загрозу суверенітету та національній стійкості.

Мета та завдання. Мета дослідження полягає у здійсненні комплексного огляду та систематизації наукової літератури, аналітичних матеріалів і стратегічних документів для виявлення ключових аспектів взаємозв'язку між розвитком цифрового громадянства та забезпеченням національної безпеки держави в умовах активної цифрової трансформації та зростаючих зовнішніх кіберзагроз і дезінформаційних кампаній.

Для досягнення поставленої мети передбачається виконання наступних завдань дослідження: визначення сутності та ключових характеристик цифрового громадянства як багатовимірного концепту в контексті цифрової трансформації держави на основі аналізу наукової літератури; обґрунтування ключової ролі цифрового громадянства як фактора стійкості суспільства до маніпулятивних впливів та кібератак у контексті забезпечення національної безпеки на основі синтезу наявних досліджень; аналіз актуальних загроз національній безпеці України в цифровому просторі, зокрема кібератак та дезінформаційних кампаній, з урахуванням геополітичного контексту на основі огляду аналітичних матеріалів та стратегічних документів; розроблення рекомендацій щодо формування ефективної стратегії розвитку цифрового громадянства в Україні з метою зміцнення національної безпеки та стійкості держави в цифрову епоху на основі узагальнення проведеного огляду та аналізу.

Методи дослідження. Методологія даної оглядової статті базується на системному аналізі та інтеграції наукової літератури, профільних аналітичних матеріалів і стратегічних документів, релевантних взаємозв'язку цифрового громадянства та національної безпеки в умовах цифрової трансформації. Пошук здійснювався в ключових наукометричних базах даних (Scopus, Web of Science, Google Scholar) та на офіційних ресурсах аналітичних центрів. Відбір джерел ґрунтувався на їхній академічній значущості та відповідності тематиці. Аналіз включав порівняльне та критичне дослідження домінуючих парадигм і концептуальних розбіжностей для виявлення ключових факторів впливу. Систематизація та інтеграція отриманої інформації за тематичними блоками слугувала підґрунтям для авторського визначення цифрового громадянства та розробки рекомендацій щодо стратегії його розвитку в контексті національної безпеки цифрової епохи.

Результати. Цифрова епоха ознаменувала фундаментальну трансформацію політичного ландшафту, центральним елементом якої постає е-демократія – парадигма використання цифрових технологій для якісного переосмислення політичних процесів [1; 2; 4; 6; 12; 16]. Ця революційна зміна відкриває безпрецедентні можливості для поглиблення громадянської участі, підвищення транспарентності та підзвітності урядування, а також оптимізації функціонування демократичних інститутів. Завдяки онлайн-платформам, електронному голосуванню та інструментам подання петицій [5; 31; 40], е-демократія потенційно розширює можливості громадян впливати на політичні рішення, стираючи географічні та часові бар'єри [1; 2; 15]. Цифрові кампанії та онлайн-дискусії стають потужними інструментами артикуляції громадської думки та формування політичного порядку денного.

Однак, стрімке впровадження е-демократії супроводжується низкою суттєвих викликів та ризиків [14]. Цифровий простір, будучи середовищем вільного обміну інформацією, водночас стає живильним середовищем для поширення дезінформації та мови ворожнечі, що підриває якість публічного дискурсу та може призводити до поляризації суспільства. Проблема «цифрового розриву» створює нерівні умови для участі, виключаючи значну частину населення з демократичних процесів [17; 18; 39]. Крім того, питання прозорості алгоритмів прийняття рішень, безпеки персональних даних та забезпечення довіри до цифрових політичних інститутів набувають особливої гостроти. Ідея повної автоматизації управління на основі великих даних та штучного інтелекту, хоча й обіцяє підвищення ефективності, викликає обґрунтовані сумніви щодо ролі людського чинника, етичних міркувань та здатності алгоритмів враховувати складність соціально-культурного контексту [1; 2; 26; 14; 34]. У цьому складному та динамічному середовищі, де цифрові технології радикально переформатовують політичну взаємодію, постає нагальна потреба у формуванні зрілого та відповідального цифрового громадянства.

Концептуалізація цифрового громадянства є предметом інтенсивної наукової дискусії, що набула особливої актуальності на початку XXI століття, про що свідчить експоненційне зростання публікаційної активності у цій сфері [20]. Ця стійка тенденція відображає не лише зростаючу значущість цифрової трансформації для суспільства, але й багатогранність та складність самого феномену цифрового громадянства, що зумовлює розширення наукового інтересу до його теоретичних та практичних аспектів. Зокрема, фундамент для розуміння цифрового громадянства як ключового фактора соціальної та політичної партисипації в інформаційному суспільстві було закладено

у ранніх дослідженнях К. Моссбергер та К. Толберт (2007, 2008) [27; 28]. Водночас, подальші наукові розвідки, як-от праця В. Буенте (2015) [3], акцентували увагу на потенційних соціальних нерівностях, що можуть супроводжувати процеси цифрової інтеграції, а дослідження Я. Л. Енсена (2011) [21] зосередилося на національній специфіці прояву цифрового громадянства.

Критичне переосмислення сутності цифрового громадянства представлено у працях Е. Ф. Ісіна та Е. Рупперт (2015) [19], які розглядають його як динамічний процес конструювання політичної суб'єктності в цифровому просторі, уникаючи фіксованих категорій та наголошуючи на перформативному вимірі цифрової взаємодії. Аналогічний підхід простежується у роботах Я. Шоу (2018) [36], який підкреслює плинність та контекстуальну обумовленість розуміння громадянства в цифрову епоху, застерігаючи від його зведення до статичних вимірюваних категорій [35]. У цьому контексті, С. Вів'єнн, А. МакКоскер та А. Джонс (2016) [38] наголошують на постійній перебудові та багатовимірності цифрового громадянства, вбудованого в складну мережу влади, дискурсу та емерджентних значень, що визначає його як феномен, який важко піддається усталеному визначенню. Такий контекстуальний підхід, підтриманий Л. Йоррінг, А. Валентім та П. Портен-Шее (2019) [22], розглядає цифрове громадянство як залежне від конкретних обставин та плинне явище, що охоплює широкий спектр індивідуального досвіду громадянства в цифрову епоху, зокрема й у контексті взаємодії з політичною спільнотою та умовами політичної залученості [27].

Фундаментальне значення для розуміння цифрового громадянства має концептуальна модель М. Чой (2016) [4], яка артикулює цифрового громадянина як суб'єкта, що володіє інтегрованим комплексом когнітивних та поведінкових компетенцій, включаючи етичну свідомість, медіаграмотність, активну участь у громадському житті та критичне мислення. Запропонована парадигма підкреслює багатовимірність цифрового громадянства та його нерозривний зв'язок із традиційними формами громадянства, водночас виокремлюючи новітні виклики та можливості, детерміновані цифровою ерою. Отже, синергетичний розвиток цифрової грамотності, етичних норм поведінки в онлайн-середовищі та активної громадянської позиції є необхідною умовою для забезпечення безпечного й ефективного функціонування громадян у складному цифровому просторі сучасності. Крім того, вагомий внесок у дослідження цифрового громадянства робить структурована модель М. Ріббла (2008, 2012) [32; 33], яка артикулює дев'ять ключових елементів, що охоплюють різні рівні відповідальності в технологічному середовищі, від цифрового доступу до цифрової безпеки. Ця так-

сономія є цінним інструментом для аналізу багатогранності цифрового громадянства, підкреслюючи взаємозалежність між технологічними можливостями та відповідальною поведінкою, та формуючи цілісне розуміння цифрового громадянства як важливої складової сучасного суспільства знань.

Різноманіття інтерпретацій цифрового громадянства відображає його полісемантичну природу в контексті динамічних викликів та можливостей цифрової ери. Діапазон його охоплення варіюється від проактивної цифрової публічності, спрямованої на консолідацію громадянської спільноти через політичну партисипацію, волонтерські ініціативи та підтримку суспільно значущих проєктів, до цифрової самосвідомості, що включає відповідальну поведінку в кіберпросторі, пильність щодо кібербезпеки, протекцію персональних даних та дезавування дезінформаційних наративів. Фундаментальна преміса концепції Digital Citizenship полягає у синергетичній інтеграції зусиль кожного суб'єкта громадянського суспільства задля конструювання безпечного та справедливого цифрового середовища, що базується на універсальних цінностях, таких як повага до приватності, толерантність та громадянська відповідальність, через культивування цифрових компетентностей, критичного мислення та здатності до колаборації [1; 2; 19; 28; 34]. Шляхом встановлення та підтримки горизонтальних і вертикальних взаємозв'язків із застосуванням онлайн-платформ для партисипативної демократії, відкритих даних та систем електронного волевиявлення, відкривається перспектива наближення до інклюзивної демократичної держави, де артикульований голос кожного громадянина має значущість, а фундаментальні права людини шануються та захищаються незалежно від модальності їхньої реалізації.

Саме концепція цифрового громадянства, що охоплює не лише навички використання цифрових інструментів, але й етичну поведінку, критичне мислення та активну участь у цифровому публічному просторі, стає ключовим елементом для нівелювання ризиків та повноцінної реалізації потенціалу е-демократії [26; 24; 39; 40]. Відтак, забезпечення інформаційної безпеки та нейтралізація кіберзагроз і дезінформації набувають критичної значущості для збереження національної державності та демократичного конституційного ладу. Формування дієвої стратегії національної безпеки в цифровій сфері імперативно потребує комплексного підходу, що включає посилення кібернетичного захисту критичної інфраструктури, розвиток національних спроможностей у галузі кібербезпеки, підвищення рівня медіаграмотності громадян як інструменту протидії маніпулятивним впливам, а також розробку законодавчих та регуляторних механізмів для протидії дезінформації та кіберзлочинності. Маючи безпосередню кореляцію

з практичною імплементацією концепції цифрового громадянства, зазначені заходи є фундаментальними для створення безпечного та верифікованого цифрового середовища, в якому громадяни можуть повноцінно реалізовувати свої цифрові права та обов'язки. Розвиток цифрової грамотності та кібергігієни серед громадян, що є ключовими складовими цифрового громадянства, зміцнює резильєнтність суспільства до інформаційних загроз та сприяє ефективній взаємодії з цифровою державою. Таким чином, забезпечення інформаційної безпеки є імперативною умовою для успішної реалізації потенціалу цифрового громадянства та розбудови стійкої, інклюзивної та демократичної цифрової держави.

Висновки. У контексті активної цифровізації усіх сфер суспільно-політичного життя та ескалації геополітичної напруженості в кіберпросторі, авторське розуміння цифрового громадянства виходить за межі традиційних інтерпретацій, набуваючи стратегічного значення для забезпечення національної безпеки держави. Цифрове громадянство розглядається як динамічна екосистема усвідомленої та відповідальної поведінки громадян у цифровому просторі, що зміцнює цифрову стійкість держави. З цієї перспективи, цифрове громадянство є багаторівневим конструктом, що включає такі ключові елементи, як цифрова компетентність як елемент національної кібергігієни, цифрова відповідальність як вираження національної свідомості, цифрова партисипація як інструмент зміцнення демократичних інститутів та національної єдності, а також критичне цифрове мислення як запорука інформаційної стійкості. Кожен з цих елементів відіграє важливу роль у забезпеченні інформаційної безпеки та стійкості суспільства до цифрових загроз.

Отже, цифрове громадянство в контексті національної безпеки постає не як проста сукупність індивідуальних цифрових навичок, а як синергетична колективна сила, спрямована на зміцнення цифрового суверенітету та інформаційної резильєнтності держави. Розвиток цифрового громадянства є стратегічним імперативом не лише для України, що перебуває в умовах гібридної війни, де кіберпростір є одним з ключових доменів протистояння, але й для країн Європейського Союзу та інших демократій світу, які зазнають безпрецедентного тиску з боку агресивної геополітики авторитарних режимів. В умовах зростання кіберзагроз, дезінформаційних кампаній та спроб втручання у внутрішні політичні процеси, інвестиції в цифрову освіту, підвищення рівня кіберграмотності населення та формування відповідальної цифрової культури є невід'ємними складовими ефективної стратегії національної безпеки в цифрову епоху, сприяючи як успішній імплементації інструментів е-демократії, так і загальній національній стійкості демократичних суспільств.

REFERENCES:

1. AbdulKareem, A. K., & Oladimeji, K. A. (2024). Cultivating the digital citizen: trust, digital literacy and e-government adoption. *Transforming Government: People, Process and Policy*, 18(2), 270–286. <https://doi.org/10.1108/TG-11-2023-0196>
2. Alrakhman, R., & Fauzi, A. (2025, March). Navigating the Digital Landscape: The Role of Digital Citizenship Education in Cultivating Ethical Social Media Behavior. In 5th Annual Civic Education Conference (5th ACEC 2024) (pp. 40–54). Atlantis Press. https://doi.org/10.2991/978-2-38476-372-6_5
3. Buente, W. (2015). Digital Citizenship or Inequality? Linking Internet Use and Education to Electoral Engagement in the 2008 U.S. Presidential Election Campaign. *Bulletin of Science, Technology & Society*, 35(5/6), 145–157. <https://doi.org/10.1177/0270467615624756>
4. Choi, M. (2016). A concept analysis of digital citizenship for democratic citizenship education in the internet age. *Theory & research in social education*, 44(4), 565–607. URL: <https://www.tandfonline.com/doi/abs/10.1080/00933104.2016.1210549>
5. Dahlberg, L. (2011). Re-constructing digital democracy: An outline of four 'positions'. *New media & society*, 13(6), 855–872. <http://dx.doi.org/10.1177/1461444810389569>
6. Duenas-Cid, D. (2024, June). Trust and distrust in electoral technologies: what can we learn from the failure of electronic voting in the Netherlands (2006/07). In *Proceedings of the 25th Annual International Conference on Digital Government Research* (pp. 669–677). <https://doi.org/10.1145/3657054.3657262>
7. Espinosa, V. I., & Pino, A. (2025). E-Government as a development strategy: The case of Estonia. *International Journal of Public Administration*, 48(2), 86–99. <https://doi.org/10.1080/01900692.2024.2316128>
8. European Commission. (2021). 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0118>
9. Fischli, R., & Muldoon, J. (2024). Empowering digital democracy. *Perspectives on Politics*, 22(3), 819–835. <https://doi.org/10.1017/S1537592724000409>
10. Gad, C. (2024). Trusting elections: complexities and risks of digital voting in Denmark. *Journal of Cultural Economy*, 17(6), 757–774. <https://doi.org/10.1080/17530350.2023.2246991>
11. Goldsmith, S., & Eggers, W. D. (2005). *Governing by network: The new shape of the public sector*. Rowman & Littlefield.
12. Hague, B. N., & Loader, B. D. (Eds.). (2005). *Digital democracy: Discourse and decision making in the information age*. Routledge.
13. Hallward-Driemeier, M., Nayyar, G., Fengler, W., Aridi, A., & Gill, I. (2020). Europe 4.0: Addressing the digital dilemma. <http://dx.doi.org/10.1596/34746>
14. Helbing, D. (2015). The automation of society is next: How to survive the digital revolution. Available at SSRN 2694312.
15. Helbing, D., & Klauser, S. (2018). How to make democracy work in the digital age. In *Towards digital enlightenment: Essays on the dark and light sides of the digital revolution* (pp. 157–162). Cham: Springer International Publishing. <http://dx.doi.org/10.13140/RG.2.1.4103.5761>
16. Helbing, D., Mahajan, S., Fricker, R. H., Musso, A., Hausladen, C. I., Carissimo, C., ... & Pournaras, E. (2023). Democracy by design: Perspectives for digitally assisted, participatory upgrades of society. *Journal of Computational Science*, 71, 102061. <https://doi.org/10.1016/j.jocs.2023.102061>
17. Helsper, E. (2021). The digital disconnect: The social causes and consequences of digital inequalities.
18. Imran, A. (2023). Why addressing digital inequality should be a priority. *The Electronic Journal of Information Systems in Developing Countries*, 89(3), e12255. <https://doi.org/10.1002/isd2.12255>
19. Isin, E. F. & Ruppert, E. (2015). *Being Digital Citizens*. London: Rowman and Littlefield.
20. Jæger, B. (2021). Digital Citizenship: A review of the academic literature, *Der Moderne Staat. Zeitschrift Für Public Policy, Recht Und Management*, Vol. 14, No. 1, Pp. 24–42. URL: <https://forskning.ruc.dk/da/publications/498e0a5d-87c3-4a88-b7dd-408cea7d4831>
21. Jensen, J. L. (2011). Citizenship in the Digital Age: The Case of Denmark. *Policy & Internet*, 3(3), Article 4. <https://doi.org/10.2202/1944-2866.1106>
22. Jørring, L., Valentim, A. & Porten-Cheé, P. (2019). Mapping a Changing Field. A Literature Review on Digital Citizenship. *Digital Culture and Society*, 4(2), 11–37.
23. Koivula, A., Räsänen, P., & Keipi, T. (2024, June). Digital Democracy, Digital Dangers: Tracing Cybercrime Victimization in Finnish Online Political Discourse. In *International Conference on Human-Computer Interaction* (pp. 78–86). Cham: Springer Nature Switzerland http://dx.doi.org/10.1007/978-3-031-61966-3_9
24. Landemore, H. (2021). Open democracy and digital technologies. In *Digital technology and democratic theory* (pp. 62–89). Routledge. <https://doi.org/10.7208/9780226748603-003>
25. Liu, T. C. (2022). Digital policy in European countries from the perspective of the Digital Economy and Society Index. *Policy & Internet*, 14(1), 202–218. <http://dx.doi.org/10.1002/poi3.274>
26. Mattson, K. (2024). Digital citizenship in action: empowering students to engage in online communities. *International Society for Technology in Education*.
27. Mossberger, K. (2008). Toward digital citizenship. Addressing inequality in the information age. In Chadwick, Andrew & Howard, Philip N.: *Routledge Handbook of Internet Politics* (pp. 173–185). Hoboken: Taylor and Francis
28. Mossberger, K., & Tolbert, C. (2007). *Digital Citizenship: The Internet, Society, and Participation*. MIT Press. URL: <https://doi.org/10.7551/mitpress/7428.001.0001>
29. Papazu, I., Simonsen, T., & Reime, L. (2024). The digital state overflowing its boundaries: considering the case of digital inclusion in Denmark. *Digitalization in Practice: Intersections, Implications and Interventions*. De Gruyter. A.
30. Ramiro Troitiño, D., & Mazur, V. (2024). The Strategy of the European Institutions on Digital Integra-

tion. In *E-Governance in the European Union: Strategies, Tools, and Implementation* (pp. 23–38). Cham: Springer Nature Switzerland. http://dx.doi.org/10.1007/978-3-031-56045-3_3

31. Rattanasevee, P., Akarapattananukul, Y. & Chirawut, Y. (2024). Direct democracy in the digital age: opportunities, challenges, and new approaches. *Humanit Soc Sci Commun* 11, 1681 <https://doi.org/10.1057/s41599-024-04245-1>

32. Ribble, M. (2008). Passport to digital citizenship. *Learning & leading with technology*, 36(4), 14–17.

33. Ribble, M. (2012). Digital citizenship for educational change. *Kappa Delta Pi Record*, 48(4), 148–151. <https://doi.org/10.1080/00228958.2012.734015>

34. Sadiku, M. N., Tembely, M., & Musa, S. M. (2018). Digital citizenship. *International Journal of Advanced Research in Computer Science and Software Engineering*, 8(5), 18–20. URL: https://www.researchgate.net/publication/326083989_DIGITAL_CITIZENSHIP

35. Schou, J. & Pors, A. S. (2018). Digital by default? A qualitative study of exclusion in digitalised welfare. *Social Policy & Administration*, 53(3), 464–477. <https://doi.org/10.1111/spol.12470>

36. Schou, J. (2018). *Remaking Citizenship. Welfare Reform and Public Sector Digitalization*. Ph.D. dissertation, Department of Business IT. Copenhagen: IT University of Copenhagen.

37. Velvet, A. (2025). Free to Choose: E-voting, Infrastructure and the Origins of Estonia's Digital Republic. *Contemporary European History*, 1–18. <https://doi.org/10.1017/S0960777324000031>

38. Vivienne, S., McCosker, A. & Johns, A. (2016). Digital Citizenship as Fluid Interface: Between Control, Contest and Culture. In Anthony McCosker, Sonja Vivienne & Amelia Johns (Eds.). *Negotiating Digital Citizenship: Control, Contest and Culture* (pp. 1–18). London: Rowman & Littlefield.

39. Vlahos, N. (2025). Digital Grassroots Organizing: How Residents Are Shaping Local Civic Participation. *Canadian Public Administration*. <http://dx.doi.org/10.1111/capa.70004>

40. Weinhardt, C., Fegert, J., Hinz, O., & van der Aalst, W. M. (2024). Digital democracy: A wake-up call: How is research can contribute to strengthening the resilience of modern democracies. *Business & Information Systems Engineering*, 66(2), 127–134. <http://dx.doi.org/10.1007/s12599-024-00862-x>

Digital transformation of the state and digital citizenship: challenges and strategies for national security

Kaliuzhna Yuliia Ivanivna

Candidate of Political Sciences,
Associate Professor,
Associate Professor at the Department
of Political Science, Sociology
and Culturology
H. S. Skovoroda Kharkiv National
Pedagogical University
Alchevskykh str., 29, Kharkiv, Ukraine
ORCID: 0000-0002-7344-410X

Amidst intensive digital transformation and the escalating threat of cyberattacks, the study of the interconnectedness between the development of digital citizenship and the national security of the state is gaining particular relevance. Global experience, notably the practices of the EU in the sphere of e-democracy, demonstrates the potential of digital tools while simultaneously highlighting the issue of societal cyber resilience. Digital citizenship, as a complex ecosystem of attributes, constitutes a key factor in effective interaction with the digital state and in countering destructive influences in cyberspace. Given geopolitical instability and the active employment of cyber and information instruments of aggression, particularly against Ukraine, understanding this interdependence is critically important. The aim of this article is a comprehensive review and systematization of scholarly literature, analytical materials, and strategic documents to identify key aspects of the relationship between the development of digital citizenship and ensuring the national security of the state within the context of active digital transformation and increasing external cyber threats and disinformation campaigns. The research objectives include defining the essence of digital citizenship, substantiating its role in societal resilience, analyzing current digital threats, and developing recommendations for a strategy for the development of digital citizenship to strengthen Ukraine's national security. The methodology is based on a systematic analysis and integration of scholarly literature from key scientometric databases, specialized analytical materials, and strategic documents of international organizations and think tanks. Comparative and critical analysis of dominant paradigms, as well as the systematization and integration of information, were employed for the author's definition of digital citizenship and the development of recommendations for its advancement in the context of the national security of the digital age. The research revealed a close relationship between the development of digital citizenship and ensuring national security. Digital citizenship, encompassing cyber competence, digital responsibility, digital participation, and critical digital thinking, is a key factor in strengthening the state's digital resilience. The strategic importance of formulating a state policy for the development of digital citizenship in Ukraine as an integral component of an effective national security strategy in the digital age, facilitating the successful implementation of e-democracy and overall national resilience, is substantiated.

Key words: digital transformation of the state, digital state, digital citizenship, e-democracy, challenges of the digital age, information security, cyber threats and disinformation, national security strategy.