

МЕХАНІЗМИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ЦИФРОВОЇ БЕЗБАР'ЄРНОСТІ В ПУБЛІЧНИХ ЗАКУПІВЛЯХ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

© 2026 НЕЧЕПОРЧУК А. А.

УДК 351.712:004.4:004.5
JEL: H57; H83; L86

Нечепорчук А. А. Механізми державного регулювання цифрової безбар'єрності в публічних закупівлях програмного забезпечення

Перенесення адміністративних, соціальних, медичних, освітніх і фінансових послуг у цифрове середовище робить доступність програмного забезпечення передумовою фактичної рівності. В Україні вже діють ДСТУ EN 301 549:2022 та нормативні приписи щодо врахування потреб осіб з інвалідністю у технічних специфікаціях публічних закупівель. Проте посилання на стандарт не гарантує доступності релізу: бракує єдиної методики доказування відповідності, ризик-орієнтованого аудиту, правил незалежності оцінювача, вимог до компетентності команди та моніторингу після оновлень. Метою статті є обґрунтування інституційної моделі державного регулювання цифрової безбар'єрності, яка перетворює стандарти доступності на перевірявані вимоги публічної закупівлі, доказовий приймальний аудит, пропорційні кваліфікаційні критерії та безперервне забезпечення доступності протягом життєвого циклу програмного продукту. Під час дослідження використано системний, інституційний, структурно-функціональний, порівняльно-правовий та ризик-орієнтований підходи. Проаналізовано законодавство України про безбар'єрність, доступність інформаційно-комунікаційних систем, публічні закупівлі, захист інформації та персональних даних; ДСТУ EN 301 549:2022, WCAG 2.2, WAI-ARIA і WCAG-EM; акти ЄС щодо вебдоступності, моніторингу, закупівель та Європейський акт про доступність; наукові праці 2022–2025 років. Запропоновано регуляторний контур «стандарт – профіль застосування – технічна специфікація – компетентність виконавця – розроблення – комбіноване тестування – незалежне підтвердження за ризиком – приймальне рішення – заява про доступність – моніторинг змін – усунення бар'єрів». Розмежовано автоматизоване тестування, експертний аудит, перевірку з використанням допоміжних технологій та користувацьке випробування. Сформовано три рівні регуляторної інтенсивності залежно від наслідків недоступності. Доведено, що сторонній «віджет доступності» не може визнаватися доказом відповідності, а кожен сторонній сценарій має проходити оцінку доступності, кібербезпеки та приватності. Запропоновано склад доказового пакета для приймання та показники результативності державної політики. Першочерговими заходами визначено затвердження національного профілю застосування ДСТУ EN 301 549:2022 із дорожньою картою переходу до WCAG 2.2; типової бібліотеки закупівельних вимог і критеріїв приймання; методики спрощеного та поглибленого моніторингу; доступного механізму зворотного зв'язку; реєстру типових дефектів і знеособлених результатів. Пілотування доцільно розпочати з високоризикових публічних сервісів, не створюючи необґрунтованих бар'єрів для конкуренції.

Ключові слова: державне регулювання; цифрова безбар'єрність; програмне забезпечення; ДСТУ EN 301 549; WCAG 2.2; аудит доступності; публічні закупівлі; кваліфікаційні вимоги.

Табл.: 1. Бібл.: 30.

Нечепорчук Антон Анатолійович – аспірант кафедри публічного управління, адміністрування та соціальної роботи, Національний університет охорони здоров'я України імені П. Л. Шупика (вул. Дорогожицька, 9, Київ, 04112, Україна)

E-mail: necheporchukaa@gmail.com

ORCID: <https://orcid.org/0009-0003-5416-5396>

UDC 351.712:004.4:004.5
JEL: H57; H83; L86

Necheporchuk A. A. The Mechanisms of Government Regulation of Digital Accessibility in Public Procurement of Software

As administrative, social, healthcare, education and financial services move online, software accessibility becomes a precondition for substantive equality. Ukraine already applies DSTU EN 301 549:2022 and requires public procurement specifications to consider the needs of persons with disabilities. A reference to a standard, however, does not guarantee that a released product is accessible: a common evidence methodology, risk-based audit, evaluator-independence rules, competence requirements and post-release monitoring are still needed. The article aims to substantiate an institutional model for State regulation of digital accessibility that converts accessibility standards into verifiable procurement requirements, evidence-based acceptance audits, proportionate qualification criteria and continuous accessibility assurance throughout the software life cycle. The study applies systemic, institutional, structural-functional, comparative legal and risk-based approaches. The study examines Ukrainian legislation on barrier-free policy, accessibility of ICT systems, public procurement, information security and personal data; DSTU EN 301 549:2022, WCAG 2.2, WAI-ARIA and WCAG-EM; EU instruments on web accessibility, monitoring, procurement and the European Accessibility Act; and research published in 2022–2025. A regulatory chain is proposed: «standard – application profile – technical specification – supplier competence – development – combined testing – risk-based independent assurance – acceptance decision – accessibility statement – change monitoring – barrier remediation». Automated checks, expert audits, assistive-technology testing and user testing are distinguished. Three levels of regulatory intensity are linked to the consequences of inaccessibility. A third-party accessibility widget cannot constitute proof of conformance; every external script requires accessibility, cybersecurity and privacy assessment. The study defines an acceptance evidence package and policy-performance indicators. Immediate priorities are a national application profile for DSTU EN 301 549:2022 with a roadmap towards WCAG 2.2; a model library of procurement clauses and acceptance criteria; simplified and in-depth monitoring methods; an accessible feedback mechanism; and a repository of recurring defects and anonymized results. Piloting should begin with high-risk public services without creating disproportionate barriers to competition.

Keywords: State regulation; digital accessibility; software; EN 301 549; WCAG 2.2; accessibility audit; public procurement; qualification requirements.

Tabl.: 1. Bibl.: 30.

Necheporchuk Anton A. – Postgraduate Student of the Department of Public Management, Administration, and Social Work, Shupyk National Healthcare University of Ukraine (9 Dorohozhytska Str., Kyiv, 04112, Ukraine)

E-mail: necheporchukaa@gmail.com

ORCID: <https://orcid.org/0009-0003-5416-5396>

ВСТУП

Цифровізація публічних послуг змінила зміст безбар'єрності. Якщо запис до лікаря, подання заяви на соціальну допомогу, підтвердження статусу, сплата адміністративного збору або отримання повідомлення про небезпеку здійснюються через вебсайт чи мобільний застосунок, недоступний інтерфейс створює не просто технічну незручність. Він може унеможливити реалізацію права, примусити людину розкривати персональні дані сторонньому помічникові, витратити додатковий час або звертатися до фізичного офісу, який також може бути недоступним. Тому цифрова безбар'єрність має розглядатися як характеристика спроможності держави надавати рівну за результатом послугу, а не як факультативна властивість дизайну [1; 2; 5; 29; 30].

В Україні сформовано істотну нормативну основу. Постанова Кабінету Міністрів України № 757 зобов'язує визначене коло органів виконавчої влади та підпорядкованих їм установ забезпечувати дотримання ДСТУ EN 301 549:2022 під час створення, модернізації, розвитку, адміністрування і функціонування власних інформаційно-комунікаційних систем, а також під час розміщення електронних документів [3]. Закон України «Про публічні закупівлі» встановлює, що коли предмет закупівлі використовуватиметься фізичними особами, технічні специфікації мають складатися з урахуванням потреб осіб з інвалідністю або вимог проектування для всіх категорій користувачів [4]. Отже, ключовою проблемою є не відсутність будь-якого обов'язку, а недостатня операціоналізація: хто, коли, яким методом і на підставі яких доказів підтверджує його виконання.

Посилання у договорі на WCAG або EN 301 549 часто сприймається як самодостатня гарантія. Проте стандарт описує вимоги до результату, а не автоматично створює процес управління ним. Без визначення меж продукту, критичних процесів, підтримуваних браузерів, операційних систем і допоміжних технологій, релізної версії, вибірки, критеріїв критичності дефектів і порядку повторного тестування два аудитори можуть перевіряти різні об'єкти й формально не суперечити одному

стандарту. Ще більший ризик виникає, коли автоматизований сканер або сторонній віджет подається як «сертифікат» усього продукту. У такому разі закупівельна процедура фіксує декларацію, але не створює відтворюваного доказу, що людина може завершити життєво важливу дію.

Державне регулювання має охоплювати весь життєвий цикл публічного програмного забезпечення. Результат залежить від того, чи були потреби користувачів описані до оголошення закупівлі; чи містить технічна специфікація вимірювані критерії; чи має команда необхідні компетентності; чи вбудовано доступність у дизайн-систему та архітектуру; чи перевіряється кожен критичний процес; чи пов'язаний акт приймання з релізною збіркою; чи зберігається доступність після оновлень; чи може користувач повідомити про бар'єр доступним способом. Таким чином, інституційним об'єктом регулювання є не окремий сайт і не окремий аудитор, а система розподіленої відповідальності та доказів.

ОГЛЯД ЛІТЕРАТУРИ

Наукові дослідження безбар'єрності в українському публічному управлінні обґрунтовують її як наскрізний вектор державної політики та механізм забезпечення рівних прав [29]. Новіша правова доктрина пов'язує цифрову безбар'єрність із протидією цифровій дискримінації та наголошує, що формальна наявність цифрового права без умов фактичного доступу не забезпечує його реалізації [30]. Ці положення важливі для зміни управлінської логіки: недоступність державного сервісу має оцінюватися не лише як дефект ІТ-проекту, а як ризик нерівного доступу до публічної функції.

Міжнародна технічна основа має багаторівневу структуру. EN 301 549 V3.2.1 встановлює вимоги доступності до широкого кола продуктів і послуг ІКТ, включаючи вебконтент, мобільні застосунки, документи, програмне та апаратне забезпечення [11]. WCAG 2.2 деталізує тестовані критерії для вебконтенту та розширює попередні версії вимогами, важливими для людей із когнітивними порушеннями, людей із слабким зором і користувачів мобільних пристроїв [12]. Водночас WCAG не охоплює всіх аспектів кожного програмного продукту,

а відповідність окремих вебсторінки не є тотожною успішності всього адміністративного процесу. Тому закупівельна вимога «WCAG 2.2 AA» повинна доповнюватися функціональними положеннями EN 301 549, сценаріями використання, доступністю документів, каналів підтримки та автентифікації.

WAI-ARIA дозволяє передавати допоміжним технологіям ролі, стани та властивості складних інтерфейсних компонентів. Проте W3C прямо застерігає, що неправильне ARIA-представлення може руйнівню спотворити невізуальний досвід [13]. Звідси випливає важлива регуляторна позиція: замовник не повинен вимагати певної кількості ARIA-атрибутів або наявності спеціального «режиму для незрячих». Предметом приймання має бути функціональна поведінка: логічна структура заголовків, доступне ім'я елемента, керування з клавіатури, передбачуваний фокус, коректні повідомлення про стани й помилки. Перевага надається нативній семантиці HTML, а ARIA застосовується там, де вона справді потрібна і протестована з допоміжними технологіями.

Методологія WCAG-EM показує, що оцінювання потребує визначення меж, цільового рівня відповідності, базової підтримки доступності, дослідження структури сервісу, виділення суттєвої функціональності, репрезентативної вибірки, перевірки повних процесів і документування результатів [14]. Вона також відокремлює вибіркового аудиту від безумовної заяви про відповідність усього вебсайту. Формат правил АСТ спрямований на узгодження та відтворюваність окремих тестів, але не усуває потреби в людському судженні [15]. Отже, автоматизація повинна стандартизувати повторювану частину контролю, а не приховувати межі того, що машина не здатна встановити.

Європейська модель поєднує стандарт, організаційні обов'язки та зовнішній моніторинг. Директива (ЄС) 2016/2102 вимагає доступності вебсайтів і мобільних застосунків органів публічного сектора, заяви про доступність, механізму зворотного зв'язку, моніторингу й звітування [16]. Імплементційне рішення 2018/1524 розрізняє спрощений і поглиблений моніторинг, визначає вибірку та перевірку повних процесів [17], а рішення 2018/1523 встановлює модель заяви про доступність [18]. Для України цінність цих актів полягає не в механічному копіюванні, а в інституційному балансі між масштабним автоматизованим спостереженням і глибокою перевіркою ризикових сервісів.

Європейський акт про доступність, закріплений Директивою (ЄС) 2019/882, із 28 червня 2025 року застосовується в ЄС до визначених про-

дуктів і послуг, серед яких електронна комерція, а також окремі банківські, транспортні, комунікаційні та інші сервіси [19]. Він не є автоматично прямим обов'язком для всіх українських суб'єктів, але формує орієнтир для наближення законодавства й експорту цифрових продуктів. Директива 2014/24/ЄС про публічні закупівлі розглядає доступність і дизайн для всіх у технічних специфікаціях як складову стратегічної закупівлі [20]. Це узгоджується з чинною статтею 23 Закону України «Про публічні закупівлі» [4].

Дослідження автоматизованих інструментів виявляють проблеми з прозорістю правил, пояснюваністю результатів і відмінностями між засобами оцінювання [26]. Великомасштабні метрики корисні для порівняння ресурсів і версій, але залежать від набору тестів, щільності потенційних бар'єрів та обраної агрегації [27]. Дослідники моніторингу вебдоступності пропонують централізовані заяви, шаблони зворотного зв'язку, спрощене самооцінювання і поглиблену перевірку за участю експертів і людей з інвалідністю [28]. Ці результати підтверджують, що єдиний інтегральний бал не повинен бути основою для прийняття без аналізу критичних сценаріїв і тяжкості бар'єрів.

Порівняння автоматизованої, ручної та користувачької оцінки мобільних застосунків показує, що ці методи виявляють різні класи проблем і не є взаємозамінними [25]. Емпіричне дослідження вебоверлеїв для незрячих і слабозорих користувачів зафіксувало як обмежений потенціал, так і суттєві ризики погіршення користувачького досвіду [24]. Додатковий сигнал для державної політики створює рішення Федеральної торгової комісії США 2025 року щодо оманливих тверджень про здатність автоматизованого продукту зробити будь-який вебсайт сумісним із WCAG [23]. Хоча це рішення належить до іншої юрисдикції, воно демонструє небезпеку закупівельної довіри до універсальної маркетингової обіцянки.

НАУКОВА ПРОГАЛИНА

Першим невирішеним питанням є нормативна фрагментація сфери охоплення. Постанова № 757 встановлює обов'язки для центральних органів виконавчої влади та визначеного кола підпорядкованих суб'єктів, а органам місцевого самоврядування рекомендовано дотримуватися тих самих вимог [3]. Водночас значна кількість адміністративних і соціальних сервісів створюється на місцевому рівні або надається через спільні платформи. Відмінний юридичний статус вимог може призводити до нерівного рівня захисту залежно від власника системи, хоча для користувача функція залишається публічною.

Іншим питанням є часовий розрив між стандартами. ДСТУ EN 301 549:2022 ідентичний EN 301 549 V3.2.1 (2021-03), тоді як W3C рекомендує застосовувати WCAG 2.2 для максимальної актуальності політик [3; 11; 12]. Механічне оголошення WCAG 2.2 обов'язковим без аналізу сумісності з національним стандартом створило б правову й закупівельну невизначеність. Потрібен офіційний профіль застосування, який зіставитиме вимоги, визначить додаткові критерії, перехідний період, винятки та порядок оновлення. Версія стандарту в технічному завданні має бути зафіксована, а нові релізи – оцінюватися за правилами, погодженими до приймання.

Третім питанням є відсутність уніфікованого доказового пакета. Звіт одного аудитора може містити перелік URL і знімки екрана, іншого – лише відсоток успішності сканера. Часто не зазначаються версія застосунку, автентифікований стан, тестові облікові записи, допоміжні технології, браузер, повні користувацькі процеси, невиконані тести, межі вибірки та повторне тестування. Без цих реквізитів замовник не може відтворити висновки, а постачальник – однозначно виправити дефект. Національна методика повинна визначати мінімальний склад звіту, не нав'язуючи конкретно-го комерційного інструмента.

Четвертим питанням є інституційна незалежність. Якщо аудит виконує та сама команда, яка розробляла продукт, вона має кращий доступ до коду й середовища, але перебуває у конфлікті ролей. Повна зовнішня перевірка кожного інформаційного сайту, навпаки, може бути непропорційною і дорогою. Тому незалежність має масштабуватися за рівнем ризику: для низькоризикового ресурсу достатньо документованого самоконтролю з вибірковою наглядом; для транзакційного сервісу потрібен окремий від розробника приймальний контроль; для високоризикового сервісу – зовнішнє підтвердження, користувацькі випробування і регресійний моніторинг.

П'ятим питанням є межа кваліфікаційних вимог. Стаття 16 Закону дозволяє замовникові вимагати від працівників наявність необхідних знань та досвіду, а також документально підтвердженого досвіду укладення аналогічних договорів [4]. Проте вимога одного конкретного сертифіката, стажу виключно в державному секторі або надмірної кількості аналогічних договорів може необґрунтовано обмежити конкуренцію. Компетентність доцільно підтверджувати сукупністю еквівалентних доказів: ролями у команді, портфоліо доступних продуктів, прикладом анонімізованого звіту, виконанням тестового завдання, навчанням, досвідом роботи з до-

поміжними технологіями та процедурою внутрішнього контролю якості.

Шостим питанням є поєднання доступності, приватності та кібербезпеки. Сторонній JavaScript може змінювати клієнтський інтерфейс без контролю власника, виконувати код із широкими привілеями та створювати потоки даних до третіх сторін [22]. Для людей з інвалідністю ризик має додатковий вимір: використання спеціального віджета або профілю може опосередковано розкривати особливості взаємодії. Тому кожний оверлей, аналітичний модуль, чат, платіжний компонент або сервіс автентифікації має входити до меж аудиту, оцінки впливу на приватність і контролю за ланцюгом постачання [6–8; 22].

МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Метою дослідження є обґрунтування інституційної моделі державного регулювання цифрової безбар'єрності, яка забезпечує перехід від загального нормативного посилання до відтворюваних закупівельних вимог, пропорційного підтвердження компетентності, ризик-орієнтованого аудиту, приймального рішення та постійного моніторингу доступності програмного забезпечення.

Для досягнення мети поставлено такі завдання: уточнити співвідношення цифрової безбар'єрності й технічної доступності; проаналізувати чинні українські та європейські регуляторні передумови; визначити прогалини стандартного посилання без процедури доказування; запропонувати життєвий цикл забезпечення доступності; сформувати рівні регуляторної інтенсивності; визначити склад технічної специфікації, кваліфікаційних доказів, аудиторського звіту й приймального пакета; окреслити правила використання сторонніх компонентів; запропонувати розподіл інституційних ролей, етапи впровадження та показники результативності.

МЕТОДИ ДОСЛІДЖЕННЯ

Джерельну базу становлять нормативно-правові акти України, міжнародні й європейські стандарти, акти ЄС, методичні документи W3C та OWASP, правозастосовний матеріал і рецензовані дослідження [1–30]. Системний підхід використано для представлення доступності як безперервного процесу; інституційний – для розподілу повноважень і відповідальності; структурно-функціональний – для конструювання механізмів стандартизації, закупівлі, аудиту, моніторингу та відновлення; порівняльно-правовий – для зіставлення українського регулювання з моделлю ЄС;

ризик-орієнтований – для визначення інтенсивності контролю; моделювальний – для побудови доказового ланцюга і матриці життєвого циклу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Насамперед необхідно розмежувати цифрову безбар'єрність і цифрову доступність. Цифрова доступність є перевірюваною властивістю продукту, контенту або процесу, яка дає змогу людям із різними функціональними можливостями сприймати інформацію, керувати інтерфейсом, розуміти його та надійно з ним взаємодіяти. Цифрова безбар'єрність є ширшою управлінською категорією: вона охоплює доступ до пристроїв і зв'язку, цифрові навички, альтернативні канали, недискримінаційну ідентифікацію, доступність підтримки, документів і платежів, а також спроможність держави усунути виявлений бар'єр. Стандарт відповідності є необхідним, але лише одним елементом цієї системи.

Запропонований автором регуляторний контур має одинадцять послідовних ланок: «стандарт – національний профіль застосування – паспорт цифрової послуги – технічна специфікація – кваліфікація команди – розроблення з вбудованою доступністю – комбіноване тестування – незалежне підтвердження за ризиком – приймальне рішення – заява про доступність – моніторинг, скарга й усунення». Розрив будь-якої ланки знижує цінність наступних. Найкращий аудит не компенсує відсутності часу на виправлення; кваліфікована команда не доведе результат без тестів; доступний реліз втратить властивості після неконтрольованого оновлення; заява про доступність не допоможе, якщо повідомлення користувача не отримує відповідального виконавця.

Національний профіль застосування має виконувати роль регуляторного мосту. Він повинен визначати сферу суб'єктів і продуктів, співвідношення ДСТУ EN 301 549:2022 і WCAG 2.2, критерії для вебсайтів, мобільних і настільних застосунків, електронних документів, терміналів, комунікацій та підтримки; мінімальний набір допоміжних технологій і платформ; допустимі винятки; формат доказу; періодичність перегляду. Профіль не повинен перетворюватися на закриту інструкцію для одного сканера. Його вимоги мають бути функціональними, технологічно нейтральними, версійованими та придатними для посилання у договорах із формулюванням «або еквівалент», коли цього вимагає закупівельне законодавство [4; 11; 12].

Перед закупівлею замовник формує паспорт цифрової послуги. У ньому доцільно зазначити нормативну підставу, власника процесу, цільові

групи, критичні завдання, канали доступу, види контенту, механізми автентифікації, сторонні компоненти, категорії персональних даних, наслідки відмови, альтернативний канал і категорію ризику. Такий документ запобігає типовій помилці, коли вимоги доступності додаються наприкінці готового технічного завдання окремим абзацом. Якщо критичний процес визначено заздалегідь, бюджет і строки включають дизайн, тестування з допоміжними технологіями, виправлення та повторну перевірку.

Технічна специфікація має описувати не лише нормативний орієнтир, а й об'єкт перевірки та способи приймання. Мінімальний склад включає: перелік платформ і версій; критичні користувацькі сценарії; цільові критерії; доступність компонентів дизайн-системи, контенту й документів; клавіатурну та голосову взаємодію; сумісність із читачами екрана; масштабування, контраст, субтитри й аудіоопис; доступні повідомлення про помилки; правила САРТСНА та багатофакторної автентифікації; формат журналу дефектів; тестові облікові записи; строки усунення; вимоги до вихідного коду, документації й передачі знань. Критерій «наявний режим для людей з інвалідністю» не є належною заміною функціональних вимог.

Критерії приймання доцільно будувати навколо завершення завдань. Для сервісу соціальної допомоги перевіряється не лише головна сторінка, а шлях від входу й автентифікації до заповнення форми, завантаження документа, підписання, виправлення, отримання підтвердження та виправлення помилки. Для мобільного застосунку окремо тестуються системні дозволи, біометрія, жести, орієнтація, екранна клавіатура, масштабування тексту та повідомлення операційної системи. Усі сторінки й стани повного процесу мають відповідати цільовому рівню; недоступність одного кроку робить послугу фактично незавершеною [12; 14].

Кваліфікаційна модель повинна бути рольовою. У складному проєкті потрібні принаймні компетентності в доступному UX, семантичній фронтенд-розробці, тестуванні, контенті та документації, мобільній доступності, інформаційній безпеці та взаємодії з користувачами. Це не означає, що кожну роль виконує окрема особа. Замовник може вимагати матрицю ролей і відповідальності, резюме ключових фахівців, підтвердження навчання або сертифікації чи еквівалентного досвіду, приклади артефактів, опис процесу якості та виконання невеликого практичного завдання. Оцінювати слід здатність команди створити доказовий результат, а не формальну належність до одного професійного реєстру.

Пропорційність кваліфікаційних критеріїв захищає конкуренцію. Для невеликого інформаційного сайту вимога кількох міжнародних сертифікатів і десятків аналогічних контрактів буде надмірною. Для національного сервісу виплат із мільйонами користувачів поверхневої декларації про досвід недостатньо.

Тому замовник має пов'язати кожен доказ із ризиком і предметом закупівлі, допускати еквівалентні способи підтвердження, не обмежувати досвід лише державними замовниками, дозволяти залучення спроможностей співвиконавців відповідно до закону та розкривати метод оцінювання. Оскаржуваність вимог є не перешкодою доступності, а запобіжником використання цієї теми для звуження ринку [4].

Доступність має бути вбудована у процес розроблення. На рівні дизайну це бібліотека перевірених компонентів, станів фокусу, масштабування, контрасту, зрозумілих повідомлень, відсутності залежності лише від кольору чи складного жесту. На рівні коду – нативні елементи, коректне дерево доступності, керування фокусом, доступні назви, стани й повідомлення, передбачувана клавіатурна модель.

На рівні контенту – структуровані заголовки, зрозуміла мова, альтернативи зображенням, субтитри, транскрипти, доступні PDF та офісні документи. На рівні DevOps – автоматичні тести критичних компонентів і регресійні сценарії. Автоматизація знижує кількість повторюваних помилок, але не приймає рішення про зрозумілість альтернативного тексту або логіку діалогу [13–15; 26].

Комбінований аудит складається щонайменше з чотирьох шарів. Перший – автоматизоване сканування, корисне для великої кількості сторінок, повторюваних помилок і регресії. Другий – ручне експертне тестування семантики, клавіатурної взаємодії, фокусу, повідомлень, збільшення, адаптивності й документів. Третій – перевірка з визначеними допоміжними технологіями та платформами. Четвертий – виконання реальних завдань людьми з різними видами інвалідності. Користувачке тестування не замінює систематичної перевірки стандарту: невелика група не представляє всіх користувачів. Так само відповідність стандарту не гарантує зручності. Поєднання методів дає різні, взаємодоповнювальні докази [14; 25–28].

Аудиторський звіт повинен бути відтворюваним. Обов'язковими реквізитами пропонується визначити: замовника й виконавця; предмет, dome-ни та межі; ідентифікатор релізу; дату й середовище; цільові стандарти; перелік технологій; метод формування вибірки; критичні процеси; браузері, операційні системи та допоміжні технології; ви-

користані інструменти і версії; результати кожного тесту; невиконані або непридатні перевірки; опис дефекту з кроками відтворення; нормативну прив'язку; групи користувачів; критичність; рекомендацію; статус виправлення; результат повторного тестування; обмеження й конфлікт інтересів. Публікувати можна зведення, а технічні деталі безпеки й персональні дані мають залишатися у захищеному контурі.

Для класифікації дефектів недостатньо лише рівня критерію WCAG. Порушення критерію рівня А на рідко відвідуваній довідковій сторінці та те саме порушення в кнопці подання заяви мають різні операційні наслідки. Критичність доцільно визначати за поєднанням п'яти факторів: вплив на завершення процесу; кількість і вразливість користувачів; наявність доступного обходу; частота прояву; суспільна значущість послуги. Критичний дефект блокує завершення або створює ризик втрати права без реальної альтернативи; високий – істотно ускладнює; середній – має обхід; низький – не блокує, але порушує якість. Така модель пов'язує аудит із рішенням про приймання.

Ризик-орієнтована модель передбачає три рівні. Рівень I охоплює переважно інформаційні ресурси з доступною альтернативою та низькими наслідками тимчасової помилки: документований самоконтроль, автоматизована регресія, ручна вибірка і вибіркового державний моніторинг. Рівень II стосується транзакційних адміністративних сервісів: окремий приймальний аудит, перевірка наскрізних процесів і допоміжних технологій, заява про доступність, строки усунення та повторне тестування. Рівень III охоплює високовпливові послуги у сфері здоров'я, соціального захисту, фінансів, безпеки й кризового інформування: незалежне підтвердження, користувацькі випробування, безперервна регресія, посилений контроль сторонніх компонентів, доступний резервний канал і скорочені строки реагування.

Приймальний пакет повинен містити не «сертифікат доступності» без визначеної сфери, а сукупність пов'язаних доказів: матрицю вимог; карту критичних процесів; ідентифікатор релізу; протоколи автоматизованих, ручних і допоміжно-технологічних тестів; звіт користувацького випробування, якщо він потрібен за ризиком; реєстр дефектів; докази виправлення; перелік залишкових відхилень із мотивованим рішенням; план моніторингу; заяву про доступність; доступний канал повідомлення; договірні строки усунення. Акт приймання має прямо посилатися на цей пакет. Після зміни релізу доказ не переноситься автоматично на нову версію.

Матриця регуляторного забезпечення цифрової доступності у життєвому циклі публічного програмного забезпечення

Етап життєвого циклу	Регуляторна або договірна вимога	Мінімальний доказ	Відповідальність і наслідок
Визначення потреби та ризику	Опис критичних користувацьких процесів, груп користувачів, каналів доступу, чутливості даних і наслідків недоступності	Паспорт цифрової послуги; карта процесів; категорія ризику; протокол консультацій із користувачами	Замовник обґрунтовує обсяг перевірки та бюджет; невідзначеність не переноситься на етап приймання
Технічна специфікація та закупівля	Функціональні вимоги ДСТУ EN 301 549:2022, цільовий профіль WCAG, підтримувані платформи, методи перевірки, еквівалентність доказів	Матриця вимог і критерії приймання; тестові сценарії; вимоги до звіту, вихідного коду та журналу дефектів	Замовник формує недискримінаційні, пропорційні умови; невиконувана або нечітка специфікація підлягає коригуванню
Проектування і розроблення	Нативна семантика, доступні компоненти, керування фокусом, клавіатурна взаємодія, альтернативи контенту, доступні документи	Дизайн-система; рішення про архітектуру; перевірки коду; автоматизовані регресійні тести; протоколи ручного тестування	Постачальник усуває дефекти у вихідному продукті; сторонній віджет не замінює виконання вимог
Передрелізний аудит	Комбіноване тестування: автоматичне, ручне експертне, з допоміжними технологіями та за наскрізними користувацькими сценаріями	Версійований звіт; вибірка; середовище тестування; докази відтворення; класифікація критичності; план усунення	Незалежність аудитора масштабується за ризиком; критичні бар'єри блокують приймання або потребують мотивованого винятку
Приймання і введення в експлуатацію	Перевірка саме релізної збірки, повторне тестування виправлень, публічна заява про доступність і канал зворотного зв'язку	Хеш або ідентифікатор версії; акт приймання; реєстр залишкових дефектів; строки їх усунення; заява про доступність	Замовник не приймає декларацію постачальника як єдиний доказ; контрактні санкції пов'язуються з підтвердженням результатом
Експлуатація та зміни	Моніторинг критичних процесів, регресійна перевірка після змін, контроль сторонніх компонентів, доступність нового контенту	Панель показників; журнал релізів і скарг; повторні аудити; SLA усунення; результати вибіркового державного моніторингу	Власник сервісу відповідає за доступність після завершення договору; повторювані дефекти впливають на оцінку постачальника
Оскарження та відновлення доступу	Доступний механізм повідомлення про бар'єр, альтернативний канал отримання послуги, пріоритетне усунення критичних порушень	Номер звернення; час реакції; рішення і доказ виправлення; статистика повторюваності; захищений журнал інцидентів	Орган-власник забезпечує негайну альтернативу й мотивовану відповідь; системні порушення стають предметом нагляду

Джерело: розроблено автором з урахуванням [3; 4; 11–18; 26–30].

Договірні механізми повинні підтримувати виправлення, а не лише покарання. Доцільно передбачити проміжні контрольні точки, резерв часу на ремедіацію, гарантійний період, SLA за рівнем критичності, повторне тестування коштом відповідальної сторони, передачу доступної дизайн-системи й документації, навчання контент-менеджерів, вимоги до субпідрядників, порядок погодження сторонніх компонентів і право замовника на незалежну перевірку. Частина оплати можна пов'язувати з підтвердженням критичних сценаріїв, але критерії мають бути відомі до подання пропозиції. Штраф без ресурсів і часу на ви-

правлення стимулює приховування дефектів, тоді як поетапне приймання робить доступність керованою властивістю.

Електронна система Prozorro є інфраструктурою прозорості й конкуренції, але не виконує автоматично технічний аудит програмного забезпечення. Її регуляторний потенціал полягає в оприлюдненні технічних специфікацій, кваліфікаційних доказів, критеріїв оцінки, договору, змін і звіту про виконання в обсязі, дозволеному законом. Для системного ефекту Уповноважений орган може розробити примірні доступні умови за-

купівель ПЗ, рекомендовані форми матриці вимог і приймального пакета, а також навчальні матеріали для уповноважених осіб. Автоматичний індикатор може виявляти відсутність розділу про доступність у ризиковій закупівлі, але не визначати фактичну відповідність продукту.

Сторонні оверлеї слід регулювати за принципом «доповнення, а не доказ». Візуальна панель зміни шрифту або контрасту може бути корисною окремим користувачам, але не виправляє недоступну клавіатурну взаємодію, некоректний порядок фокусу, відсутні назви полів, помилки в мобільному застосунку, САРТСНА, документи чи серверну логіку. Закупівельна документація має забороняти подавати сам факт встановлення віджета як підтвердження відповідності. Якщо використовується сторонній сценарій, він входить до аудиту, реєстру активів і договору з постачальником; перевіряються зміни коду, джерела даних, приватність, цілісність, політика оновлень, відмова компонента та вплив на допоміжні технології [22–24].

Заява про доступність має бути не рекламним повідомленням, а інструментом підзвітності. Вона повинна бути доступною, легко знаходитися і містити: точне найменування продукту та версії; застосований стандарт; дату й метод оцінювання; статус повної, часткової або невідповідності; відомі недоступні елементи і причини; строки виправлення; доступну альтернативу; контактний канал; порядок ескалації; дату наступного перегляду. Самооцінка допускається для певних рівнів ризику, але джерело оцінки має бути зазначене. Централізований реєстр заяв полегшить контроль актуальності й порівняння, однак не повинен перетворювати часткову відповідність на публічний рейтинг без контексту [16–18; 28].

Механізм зворотного зв'язку має бути доступним у тому самому значенні, що й сервіс. Якщо скаргу можна подати лише через недоступну форму або телефон без альтернативи для нечуючих людей, інститут не працює. Доцільно забезпечити кілька каналів, мінімізацію персональних даних, можливість описати кроки й допоміжну технологію, автоматичний номер звернення, строки реакції залежно від критичності, альтернативний спосіб отримання послуги та повідомлення про результат. Звернення про бар'єр не слід змішувати із загальною службою технічної підтримки: вони мають окрему категорію, відповідального власника, аналітику повторюваності та можливість ескалації.

Державний моніторинг доцільно організувати у двох контурах. Спрощений контур охоплює широку вибірку й автоматизовані або напівавтома-

тизовані перевірки доступності заяв, контактів, базової навігації та документів. Поглиблений контур досліджує менш ризик-орієнтовану вибірку, повні процеси, мобільні застосунки, допоміжні технології, документи, безпеку сторонніх компонентів і досвід користувачів. Вибірка має враховувати рівні влади, типи послуг, популярність, скарги, попередні порушення, нові релізи й високу суспільну значущість. Результатом є не лише звіт про порушення, а й план усунення, повторна перевірка і поширення типових рішень [16–18; 28].

Інституційний розподіл ролей пропонується будувати без створення надмірної кількості нових органів. Кабінет Міністрів формує політику та сферу обов'язків; центральний орган у сфері цифровізації координує профіль застосування, методіку, типові вимоги, навчання і реєстр заяв; національний орган стандартизації забезпечує актуалізацію стандартів; Уповноважений орган у сфері закупівель інтегрує типові положення; замовник і власник сервісу несуть відповідальність за життєвий цикл; постачальник – за договірний результат; незалежні оцінювачі – за відтворюваність висновку; органи кібербезпеки й захисту даних діють у межах компетенції; організації людей з інвалідністю беруть участь у розробленні політики та тестуванні, не підміняючи професійний аудит.

Компетентність аудиторів може підтверджуватися не обов'язковим ліцензуванням усієї професії, а рамкою знань і прозорим забезпеченням якості. Така рамка включає знання EN 301 549 і WCAG, веб- і мобільних технологій, доступних документів, допоміжних технологій, методів вибірки, користувацьких досліджень, класифікації дефектів, приватності, безпеки та підготовки звітів, що піддаються відтворенню. Для високоризикових перевірок може застосовуватися акредитація органу або інший визначений законом спосіб підтвердження компетентності, якщо створено відповідну правову і методичну основу. До її появи замовник не повинен називати будь-який приватний сертифікат державним підтвердженням.

Впровадження моделі пропонується здійснювати у чотири етапи. На підготовчому етапі проводяться інвентаризація публічних цифрових сервісів, визначення ризику, аналіз прогаин ДСТУ EN 301 549:2022 і WCAG 2.2, розроблення типових документів. На пілотному етапі обираються сервіси рівнів II–III, проводяться незалежні аудити, тестуються строки й вартість. На етапі масштабування запроваджуються навчання замовників, централізовані заяви, спрощений і поглиблений моніторинг, а також бібліотека компонентів. На етапі правового закріплення уточнюються

сфера обов'язків, порядок нагляду, еквівалентність доказів, пропорційні наслідки та періодичність перегляду стандартів.

Пілот має перевірити не лише відсоток відповідності, а й адміністративну здійсненість. Необхідно вимірювати час на формування специфікації, кількість запитань учасників, вплив вимог на конкуренцію, вартість різних рівнів аудиту, частку дефектів, виявлених до релізу, розбіжності між автоматичним і ручним тестуванням, час усунення, повторюваність після оновлень, успішність виконання критичних завдань для людей з різними інвалідностями, кількість скарг і доступність альтернативи. Якщо вимога не має зрозумілого доказу або створює витрати без зниження ризику, її слід переглянути.

Показники державної політики мають унікати стимулу до формального звітування. Кількість сайтів із віджетом або кількість автоматично просканованих сторінок не свідчить про доступність. Доцільнішими є: частка високоризикових сервісів із паспортом і актуальною заявою; частка закупівель із вимірюваними критеріями; охоплення критичних процесів; частота критичних дефектів на реліз; медіанний строк усунення; частка повторних дефектів; успішність користувацьких сценаріїв; доступність електронних документів; частка звернень, за якими надано альтернативу; результати повторного моніторингу; відмінності між центральним і місцевим рівнями. Дані публікуються агреговано з поясненням методики.

ОБГОВОРЕННЯ

Запропонована модель узгоджується з результатами досліджень прозорості автоматизованих інструментів [26], комплементарності автоматизованої, експертної та користувацької оцінки [25] і обмежень сторонніх оверлеїв [24]. Відмінність авторського підходу полягає в тому, що ці технічні висновки включено до регуляторного циклу публічної закупівлі: від формування технічної специфікації та кваліфікаційних критеріїв до приймання релізу й моніторингу після оновлень. Масштабні метрики та вибіркового моніторинг [27; 28] у такій моделі виконують функцію раннього виявлення ризиків, але не замінюють перевірки критичних користувацьких сценаріїв.

Економічний ефект моделі полягає у перенесенні витрат на ранні стадії. Виправлення семантики компонента в дизайн-системі поширюється на багато екранів; виправлення після запуску потребує зміни коду, контенту, навчання підтримки, повторного аудиту та комунікації з користувачами. Публічна закупівля може враховувати вартість

життєвого циклу: розроблення, тестування, оновлення, доступність документів, ліцензії сторонніх компонентів, підтримку та повторні перевірки [4]. Найнижча початкова ціна без цих витрат створює прихований борг доступності, який сплачують і держава, і користувач.

Водночас регулювання не повинно блокувати інновації. Функціональні вимоги й відкриті докази дають постачальникові свободу обирати фреймворк, інструмент автоматизації або архітектуру. Держава визначає результат, критичні процеси, мінімальну доказовість і правила відповідальності. Експериментальний компонент може бути використаний у контрольованому середовищі, якщо відомі його межі, передбачено людський контроль, альтернативу і можливість відкликання. Оверлей, генеративний інтерфейс або автоматичне виправлення не відхиляються через назву технології, але не отримують презумпції відповідності без перевірки фактичної поведінки.

Особливої уваги потребує воєнний і кризовий контекст. Повідомлення про тривогу, евакуацію, гуманітарну допомогу, відновлення документів, реабілітацію та виплати мають високу ціну недоступності. Тут виправдані найкоротші строки усунення, офлайн- або телефонні альтернативи з доступними каналами для різних користувачів, перевірка за слабого зв'язку, старих пристроїв, збільшеного тексту, читачів екрана, простої мови й кількох форматів інформації. Водночас публікація детальних технічних звітів про критичні системи може створити безпековий ризик; тому прозорість результату поєднується з обмеженим доступом до вразливостей [2; 7; 8].

Обмеження методології полягає в концептуальному характері дослідження. Стаття не містить репрезентативного вимірювання доступності всіх державних ресурсів і не оцінює конкретної системи закупівель. Запропоновані пороги ризику, строки усунення та вибірка мають бути перевірені пілотами. Окремі тексти стандартів захищені авторським правом, тому національна бібліотека закупівельних вимог повинна відтворювати дозволений обсяг і посилалися на офіційні джерела. Висновки щодо сторонніх сценаріїв не означають презумпції їхньої небезпечності, а вимагають документованої оцінки конкретної інтеграції.

ВИСНОВКИ

Чинна українська нормативна база вже містить опорні елементи державного регулювання цифрової доступності: політичну рамку безбар'єрності, застосування ДСТУ EN 301

549:2022 для визначеного кола публічних суб'єктів і обов'язок урахувати потреби осіб з інвалідністю у технічних специфікаціях закупівель. Проблема полягає в інституційному розриві між нормою і доказом: немає єдиного профілю застосування, ризик-орієнтованої методики аудиту, мінімального складу звіту, узгодженої заяви про доступність, правил моніторингу оновлень і доступного механізму відновлення порушеного доступу.

Наукова новизна полягає у запропонованій моделі безперервного регуляторного забезпечення, де стандарт не є кінцевим сертифікатом, а початковою ланкою доказового циклу. Контур «стандарт – профіль – паспорт послуги – специфікація – компетентність – вбудована доступність – комбінований аудит – незалежне підтвердження за ризиком – приймання – заява – моніторинг і усунення» поєднує технічні, закупівельні, організаційні, безпекові та правозахисні механізми. Автоматизований тест, експертний аудит, допоміжно-технологічна перевірка і користувацьке випробування мають різний доказовий статус і повинні застосовуватися разом відповідно до ризику.

Практичними заходами першої черги визначено: розроблення національного профілю ДСТУ EN 301 549:2022 із картою переходу до WCAG 2.2; типові закупівельні вимоги та критерії приймання; рольову рамку компетентності з визнанням еквівалентних доказів; методики спрощеного й поглибленого моніторингу; мінімальний формат аудиторського звіту і приймального пакета; централізовану доступну заяву та механізм зворотного зв'язку; правила оцінки сторонніх сценаріїв; пілотування на високоризикових сервісах. Установлення конкретних санкцій має відбуватися після оцінки витрат, ринкової спроможності та результатів пілоту.

Перспективи подальших досліджень охоплюють емпіричний аудит репрезентативної вибірки українських публічних сервісів; зіставлення вимог ДСТУ EN 301 549:2022 із WCAG 2.2; визначення національної базової матриці допоміжних технологій; експериментальну оцінку трьох рівнів ризику; аналіз закупівельної документації й рішень органу оскарження щодо пропорційності кваліфікаційних критеріїв; вимірювання вартості життєвого циклу доступності; розроблення захищеного машинозчитуваного формату звітів; дослідження впливу оверлеїв, генеративних інтерфейсів і автоматичних виправлень на різні групи користувачів. ■

БІБЛІОГРАФІЯ

1. Про схвалення Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року : Розпорядження Кабінету Міністрів України від 14.04.2021 № 366-р. URL: <https://zakon.rada.gov.ua/laws/show/366-2021-%D1%80>
2. Про затвердження плану заходів на 2025–2026 роки з реалізації Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року : Розпорядження Кабінету Міністрів України від 25.03.2025 № 374-р. URL: <https://zakon.rada.gov.ua/laws/show/374-2025-%D1%80>
3. Деякі питання доступності інформаційно-комунікаційних систем та документів в електронній формі : Постанова Кабінету Міністрів України від 21.07.2023 № 757. URL: <https://zakon.rada.gov.ua/laws/show/757-2023-%D0%BF>
4. Про публічні закупівлі : Закон України від 25.12.2015 № 922-VIII. URL: <https://zakon.rada.gov.ua/laws/show/922-19>
5. Конвенція про права осіб з інвалідністю : Конвенція ООН від 13.12.2006; ратифікована Законом України від 16.12.2009 № 1767-VI. URL: https://zakon.rada.gov.ua/laws/show/995_g71
6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
8. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-BP. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
9. Про адміністративну процедуру : Закон України від 17.02.2022 № 2073-IX. URL: <https://zakon.rada.gov.ua/laws/show/2073-20>
10. Пріоритети та виклики політики безбар'єрності : аналітичні матеріали до розробки Плану заходів на 2025–2026 роки з реалізації Національної стратегії із створення безбар'єрного простору в Україні. Київ : НІСД, 2024. 136 с. URL: <https://mindev.gov.ua/storage/app/sites/1/uploaded-files/prioriteti-ta-vikliki-politiki-bezbarjernosti-200325.pdf>
11. ETSI EN 301 549 V3.2.1 (2021-03). Accessibility requirements for ICT products and services. European Telecommunications Standards Institute. URL: https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf
12. Web Content Accessibility Guidelines (WCAG) 2.2. W3C Recommendation, 12 December 2024. URL: <https://www.w3.org/TR/WCAG22/>
13. WAI-ARIA Authoring Practices Guide. Read Me First. World Wide Web Consortium. URL: <https://www.w3.org/WAI/ARIA/apg/practices/read-me-first/>

14. Website Accessibility Conformance Evaluation Methodology (WCAG-EM) 1.0. W3C Working Group Note, 10 July 2014. URL: <https://www.w3.org/TR/WCAG-EM/>
15. Accessibility Conformance Testing (ACT) Rules Format 1.1. W3C Recommendation, 12 May 2022. URL: <https://www.w3.org/TR/act-rules-format/>
16. Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L2102>
17. Commission Implementing Decision (EU) 2018/1524 of 11 October 2018 establishing a monitoring methodology and arrangements for reporting under Directive (EU) 2016/2102. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D1524>
18. Commission Implementing Decision (EU) 2018/1523 of 11 October 2018 establishing a model accessibility statement under Directive (EU) 2016/2102. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018D1523>
19. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0882>
20. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement. URL: <https://eur-lex.europa.eu/eli/dir/2014/24/oj>
21. ISO/IEC 30071-1:2019. Information technology – Development of user interface accessibility – Part 1: Code of practice for creating accessible ICT products and services. URL: <https://www.iso.org/standard/70913.html>
22. Third Party JavaScript Management Cheat Sheet. OWASP Cheat Sheet Series. URL: https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html
23. FTC Order Requires Online Marketer to Pay \$1 Million for Deceptive Claims that its AI Product Could Make Websites Compliant with Accessibility Guidelines. Federal Trade Commission. 2025. URL: <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-order-requires-online-marketer-pay-1-million-deceptive-claims-its-ai-product-could-make-websites>
24. Makati T., Tigwell G. W., Shinohara K. The Promise and Pitfalls of Web Accessibility Overlays for Blind and Low Vision Users. *Proceedings of the 26th International ACM SIGACCESS Conference on Computers and Accessibility*. 2024. P. 1–12. DOI: <https://doi.org/10.1145/3663548.3675650>
25. Mateus D. A., Souza M. R. A., Freire A. P. Accessibility of Mobile Apps for Visually Impaired Users: Problems Encountered by User Evaluation, Inspections and Automated Tools. *Proceedings of the XXII Brazilian Symposium on Human Factors in Computing Systems*. 2024. Article 32. P. 1–11. DOI: <https://doi.org/10.1145/3638067.3638101>
26. Manca M., Palumbo V., Paternò F., Santoro C. The Transparency of Automatic Web Accessibility Evaluation Tools: Design Criteria, State of the Art, and User Perception. *ACM Transactions on Accessible Computing*. 2023. Vol. 16. No. 1. Article 3. P. 1–36. DOI: <https://doi.org/10.1145/3556979>
27. Martins B., Duarte C. Large-scale study of web accessibility metrics. *Universal Access in the Information Society*. 2024. Vol. 23. P. 411–434. DOI: <https://doi.org/10.1007/s10209-022-00956-x>
28. Debevc M., Škraba T., Cerovac B., Kožuh I., Rajh N. Monitoring website accessibility: Evaluating current approaches and a proposal for improvements. *Journal of Accessibility and Design for All*. 2023. Vol. 13. No. 2. DOI: <https://doi.org/10.17411/jacces.v13i2.485>
29. Помаза-Пономаренко А. Л. Безбар'єрність як вектор розвитку системи публічного управління у сфері забезпечення рівних прав громадян. *Дніпровський науковий часопис публічного управління, психології, права*. 2023. Вип. 5. С. 42–49. DOI: <https://doi.org/10.51547/ppp.dp.ua/2023.5.7>
30. Верлос Н. В., Коломоець Т. О., Воронкова В. Г., Нікітенко В. О. Цифрова безбар'єрність як правовий інструмент реалізації конституційного принципу рівності та протидії цифровій дискримінації. *Юридичний науковий електронний журнал*. 2025. № 4. С. 601–605. DOI: <https://doi.org/10.32782/2524-0374/2025-4/145>

REFERENCES

- Debevc M., Škraba T., Cerovac B., Kožuh I. & Rajh N. (2023). Monitoring website accessibility: Evaluating current approaches and a proposal for improvements. *Journal of Accessibility and Design for All*, 2(13). <https://doi.org/10.17411/jacces.v13i2.485>
- eur-lex.europa.eu. (2014, February 26). Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement. <https://eur-lex.europa.eu/eli/dir/2014/24/oj>
- eur-lex.europa.eu. (2016, October 26). Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L2102>
- eur-lex.europa.eu. (2018, October 11). Commission Implementing Decision (EU) 2018/1523 of 11 October 2018 establishing a model accessibility statement under Directive (EU) 2016/2102. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018D1523>

- eur-lex.europa.eu. (2018, October 11). Commission Implementing Decision (EU) 2018/1524 of 11 October 2018 establishing a monitoring methodology and arrangements for reporting under Directive (EU) 2016/2102. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D1524>
- eur-lex.europa.eu. (2019, April 17). Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0882>
- European Telecommunications Standards Institute (2021). *ETSI EN 301 549 V3.2.1 (2021-03). Accessibility requirements for ICT products and services*. European Telecommunications Standards Institute. https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf
- Federal Trade Commission. (2025). FTC Order Requires Online Marketer to Pay \$1 Million for Deceptive Claims that its AI Product Could Make Websites Compliant with Accessibility Guidelines. <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-order-requires-online-marketer-pay-1-million-deceptive-claims-its-ai-product-could-make-websites>
- iso.org. (2019). ISO/IEC 30071-1:2019. Information technology – Development of user interface accessibility – Part 1: Code of practice for creating accessible ICT products and services. <https://www.iso.org/standard/70913.html>
- Makati T., Tigwell G. W. & Shinohara K. (2024). The Promise and Pitfalls of Web Accessibility Overlays for Blind and Low Vision Users. *Proceedings of the 26th International ACM SIGACCESS Conference on Computers and Accessibility* (pp. 1–12). <https://doi.org/10.1145/3663548.3675650>
- Manca M., Palumbo V., Paternò F. & Santoro C. (2023). The Transparency of Automatic Web Accessibility Evaluation Tools: Design Criteria, State of the Art, and User Perception. *ACM Transactions on Accessible Computing*, 1(16), 1–36. <https://doi.org/10.1145/3556979>
- Martins B. & Duarte C. (2024). Large-scale study of web accessibility metrics. *Universal Access in the Information Society*, 23, 411–434. <https://doi.org/10.1007/s10209-022-00956-x>
- Mateus D. A., Souza M. R. A. & Freire A. P. (2024). Accessibility of Mobile Apps for Visually Impaired Users: Problems Encountered by User Evaluation, Inspections and Automated Tools. *Proceedings of the XXII Brazilian Symposium on Human Factors in Computing Systems* (pp. 321–11). <https://doi.org/10.1145/3638067.3638101>
- NISD (2024). *Priorytety ta vyklyky polityky bezbariernosti: analitychni materialy do rozrobky Planu zakhodiv na 2025–2026 roky z realizatsii Natsionalnoi stratehii iz stvorennia bezbariernoho prostoru v Ukraini* [Priorities and challenges of the barrier-free policy: analytical materials for the development of the Action Plan for 2025–2026 on the implementation of the National Strategy for creating a barrier-free space in Ukraine]. Kyiv: NISD. <https://mindev.gov.ua/storage/app/sites/1/uploaded-files/prioryteti-ta-viklyki-politiki-bezbarjernosti-200325.pdf>
- OWASP Cheat Sheet Series. Third Party JavaScript Management Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html
- Pomaza-Ponomarenko A. L. (2023). Bezbariernist yak vektor rozvytku systemy publichnoho upravlinnia u sferi zabezpechennia rivnykh prav hromadian [Barrier-friendliness as a vector of development of the public administration system in the sphere of ensuring equal rights of citizens]. *Dniprovskiyi naukovyi chasopys publichnoho upravlinnia, psykholohii, prava*, 5, 42–49. <https://doi.org/10.51547/ppp.dp.ua/2023.5.7>
- Verlos N. V., Kolomoiets T. O., Voronkova V. H. & Nikitenko V. O. (2025). Tsyfrova bezbariernist yak pravovyi instrument realizatsii konstytutsiinoho pryntsyphu rivnosti ta protyidii tsyfrovii dyskryminatsii [Digital barrier-friendliness as a legal instrument for realizing the constitutional principle of equality and countering digital discrimination]. *Yurydychnyi naukovyi elektronnyi zhurnal*, 4, 601–605. <https://doi.org/10.32782/2524-0374/2025-4/145>
- W3C Working Group Note. (2014, July 10). Website Accessibility Conformance Evaluation Methodology (WCAG-EM) 1.0. <https://www.w3.org/TR/WCAG-EM/>
- W3C Recommendation. (2022, May 12). Accessibility Conformance Testing (ACT) Rules Format 1.1. <https://www.w3.org/TR/act-rules-format/>
- W3C Recommendation. (2024, December 12). Web Content Accessibility Guidelines (WCAG) 2.2. <https://www.w3.org/TR/WCAG22/>
- World Wide Web Consortium. WAI-ARIA Authoring Practices Guide. Read Me First. <https://www.w3.org/WAI/ARIA/apg/practices/read-me-first/>
- zakon.rada.gov.ua. (1994, July 5). Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Zakon Ukrainy vid 05.07.1994 № 80/94-VR [On information protection in information and communication systems: Law of Ukraine dated July 5, 1994 No. 80/94-VR]. <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
- zakon.rada.gov.ua. (2006, December 13). Konventsiiia pro prava osib z invalidnistiu: Konventsiiia OON vid 13.12.2006; ratyfikovana Zakonom Ukrainy vid 16.12.2009 № 1767-VI [Convention on the Rights of Persons with Disabilities: UN Convention dated December 13, 2006; ratified by the Law of Ukraine dated December 16, 2009 No. 1767-VI]. https://zakon.rada.gov.ua/laws/show/995_g71
- zakon.rada.gov.ua. (2010, June 1). Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 № 2297-VI [On the protection of personal data: Law of Ukraine dated June 1, 2010 No. 2297-VI]. <https://zakon.rada.gov.ua/laws/show/2297-17>

zakon.rada.gov.ua. (2015, December 25). Pro publichni zakupivli: Zakon Ukrainy vid 25.12.2015 № 922-VIII [On public procurement: Law of Ukraine dated December 25, 2015 No. 922-VIII]. <https://zakon.rada.gov.ua/laws/show/922-19>

zakon.rada.gov.ua. (2017, October 5). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII]. <https://zakon.rada.gov.ua/laws/show/2163-19>

zakon.rada.gov.ua. (2021, April 14). Pro skhvalennia Natsionalnoi stratehii iz stvorennia bezbariernoho prostoru v Ukraini na period do 2030 roku: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 14.04.2021 № 366-r [On the approval of the National Strategy for creating a barrier-free space in Ukraine for the period up to 2030: Order of the Cabinet of Ministers of Ukraine dated April 14, 2021 No. 366-r]. <https://zakon.rada.gov.ua/laws/show/366-2021-%D1%80>

zakon.rada.gov.ua. (2022, February 17). Pro administrativnu protseduru: Zakon Ukrainy vid 17.02.2022 № 2073-IX [On administrative procedure: Law of Ukraine dated February 17, 2022 No. 2073-IX]. <https://zakon.rada.gov.ua/laws/show/2073-20>

zakon.rada.gov.ua. (2023, July 21). Deiaki pytannia dostupnosti informatsiino-komunikatsiinykh system ta dokumentiv v elektronni formi: Postanova Kabinetu Ministriv Ukrainy vid 21.07.2023 № 757 [Some issues of accessibility of information and communication systems and electronic documents: Resolution of the Cabinet of Ministers of Ukraine dated July 21, 2023 No. 757]. <https://zakon.rada.gov.ua/laws/show/757-2023-%D0%BF>

zakon.rada.gov.ua. (2025, March 25). Pro zatverdzhennia planu zakhodiv na 2025–2026 roky z realizatsii Natsionalnoi stratehii iz stvorennia bezbariernoho prostoru v Ukraini na period do 2030 roku: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 25.03.2025 № 374-r [On the approval of the action plan for 2025–2026 for the implementation of the National Strategy for creating a barrier-free space in Ukraine for the period up to 2030: Order of the Cabinet of Ministers of Ukraine dated March 25, 2025 No. 374-r]. <https://zakon.rada.gov.ua/laws/show/374-2025-%D1%80>

Дослідження не отримувало зовнішнього фінансування.

Автор заявляє про відсутність конфлікту інтересів.

Внесок автора:

Нечепорчук А. А.: розробка концепції; методологія; формальний аналіз; дослідження; візуалізація; управління проєктом; написання – оригінальний рукопис; написання – рецензування та редагування.

Дослідження має теоретико-концептуальний характер і не передбачало створення емпіричного набору даних. Нормативні акти, стандарти та відкриті наукові джерела наведено у списку використаних джерел.

Під час підготовки цієї роботи автор використав ChatGPT (OpenAI, GPT-5) з метою структурного опрацювання матеріалу, мовно-стилістичного редагування та технічного оформлення рукопису. Після застосування зазначеного інструменту автор критично перевіряв та відредагував отримані матеріали і несе повну відповідальність за зміст публікації.

Стаття надійшла до редакції / Received: 25.07.2026

Статтю прийнято до публікації / Accepted: 10.08.2026

Оприлюднено / Published: 08.10.2026