DOI: https://doi.org/10.32782/2524-0072/2026-92-16

УДК 351:004.7

ДЕРЖАВНЕ РЕГУЛЮВАННЯ РОЗРОБКИ ТА ІНТЕГРАЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ IOT ДЛЯ БЕЗБАР'ЄРНОГО ЖИТТЄВОГО СЕРЕДОВИЩА

STATE REGULATION OF IOT SYSTEM SOFTWARE DEVELOPMENT AND INTEGRATION FOR A BARRIER-FREE LIVING ENVIRONMENT

Нечепорчук Антон Анатолійович
здобувач ступеня доктора філософії
за спеціальністю 281 «Публічне управління та адміністрування»,
Національний університет охорони здоров'я України імені П. Л. Шупика
ORCID: https://orcid.org/0009-0003-5416-5396

Necheporchuk Anton
Shupyk National Healthcare University of Ukraine

У статті обґрунтовано ризик-орієнтовану модель державного регулювання розробки та інтеграції програмного забезпечення IoT-систем у безбар'єрному життєвому середовищі. На основі системного, інституційного, структурно-функціонального та порівняльно-правового аналізу поєднано вимоги фізичної і цифрової доступності, кібербезпеки, сумісності, захисту даних та відмовостійкості. Доступність запропоновано оцінювати для наскрізного ланцюга «користувач – інтерфейс – платформа – мережа – пристрій – фізична дія». Визначено сім механізмів регулювання і три рівні вимог за наслідками відмови. Практична цінність моделі полягає в можливості її застосування під час підготовки технічних вимог, публічних закупівель, приймальних випробувань і моніторингу IoT-рішень у житлових та громадських будівлях.

Ключові слова: державне регулювання, Інтернет речей, безбар'єрне життєве середовище, цифрова доступність, кібербезпека, інтероперабельність, публічні закупівлі, універсальний дизайн.

The spread of Internet of Things systems in residential and public buildings changes the substance of accessibility policy. A person's ability to enter a building, receive an emergency warning, control lighting, or call for assistance may depend on a mobile interface, a cloud platform, network connectivity, and the software embedded in a physical device. If one element is inaccessible, incompatible, unsupported, or vulnerable, a solution intended to remove a barrier can create a new one. The purpose of the article is to substantiate a risk-based model of state regulation for the development and integration of IoT system software in a barrier-free living environment. The study uses systemic, institutional, structural-functional, and comparative legal approaches. It analyses Ukrainian strategic and regulatory documents, international and European standards on accessibility and consumer IoT security, European Union rules on digital products and connected-product data, and recent peer-reviewed research on smart-home technologies for persons with disabilities and older adults. The article proposes assessing accessibility across the end-to-end chain 'user – interface – platform – network – device – physical action' instead of limiting assessment to a mobile application or an individual device. Seven interconnected regulatory mechanisms are identified: regulatory and standardisation; procurement and contracting; conformity assessment and market oversight; cybersecurity and lifecycle governance; data protection and user autonomy; institutional coordination; and participatory monitoring. The model differentiates regulatory requirements according to the consequences of software failure. Basic contractual guarantees may be sufficient for comfort services, while functions that control access, evacuation, emergency warnings, or calls for assistance require independent testing, resilient local modes, documented updates, and continuous oversight. The practical value of the model lies in its use for national functional requirements, public procurement specifications, acceptance testing, municipal pilot projects, and post-deployment monitoring. This approach links digital accessibility with physical safety, privacy, interoperability, and the user's ability to act independently.

Keywords: state regulation, Internet of Things, barrier-free living environment, digital accessibility, cybersecurity, interoperability, public procurement, universal design.

© Нечепорчук А. А., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Постановка проблеми. Безбар'єрність життєвого середовища традиційно пов'язували з архітектурними рішеннями: доступним входом, маршрутом руху, ліфтом, санітарним приміщенням, візуальною і тактильною навігацією. Ці елементи залишаються базовими, але цифровізація будівель додає новий рівень. Автоматичні двері, домофони, освітлення, клімат-контроль, системи оповіщення, тривожні кнопки й датчики дедалі частіше працюють як єдина IoT-система, доступність якої визначається не лише фізичними характеристиками, а й програмним забезпеченням.

Національна стратегія із створення безбар'єрного простору в Україні до 2030 року поєднує фізичну, інформаційну та цифрову інфраструктуру і визначає безбар'єрність наскрізним принципом державної політики [1]. Проте загальний принцип ще не перетворено на узгоджені вимоги до програмного забезпечення, яке безпосередньо керує елементами житлових і громадських будівель.

Особливість IoT полягає в можливому фізичному наслідку цифрової помилки. Недоступне або скомпрометоване програмне забезпечення замка може заблокувати вхід чи вихід; відмова системи оповіщення – позбавити людину доступного сигналу; збій хмарної платформи – вимкнути дистанційне керування для користувача з порушенням моторики. Тому державні вимоги мають охоплювати інтерфейс, сумісність, кібербезпеку, оновлення, резервні режими, захист даних і відповідальність протягом життєвого циклу.

Публічно-управлінська проблема полягає у фрагментарності регулювання. Будівельні норми визначають фізичну доступність; стандарти ІКТ – доступність цифрових продуктів; законодавство про кібербезпеку і персональні дані – відповідні режими захисту; правила технічного регулювання – процедури встановлення обов'язкових вимог та оцінки відповідності [2–4; 8; 9; 11]. Користувач натомість взаємодіє з єдиним середовищем, тому ці сфери потрібно узгодити від формування технічного завдання до завершення підтримки системи.

Аналіз останніх досліджень і публікацій. У дослідженні Periša M., Teskera P., Cvitić I. та Grgurević I. [12] розкрито можливості адаптації розумного будинку до функціональних потреб людей з інвалідністю за допомогою сенсорів, застосунків і персоналізованих профілів. Автори показують, що результативність такої адаптації залежить не лише від обладнання, а й від узгодженої роботи програмних компонентів.

Vrančić A., Zadravec H. та Orehovački T. [13], а також Tian Y. J. A., Felber N. A., Pageau F., Roulet Schwab D. і Wangmo T. [14] систематизують можливості smart-home технологій для безпеки, моніторингу стану здоров'я та самостійного проживання. Водночас дослідники виокремлюють складність інтерфейсів, вартість, ризики приватності та проблеми соціального прийняття таких рішень.

Ding D., Morris L., Messina K. і Fairman A. [18], а також Ding D. та співавтори [19] досліджують використання масових smart-home рішень як асистивної технології та звертають увагу на налаштування, навчання, технічну підтримку й відповідність індивідуальним потребам. Mun K. і Kim J. [21; 22] конкретизують користувацький попит та експертні вимоги до модифікації розумного житла, а Ghorayeb A., Comber R. і Gooberman-Hill R. [17] наголошують на значенні співпроєктування з майбутніми користувачами.

Безпековий аспект опрацьовано Vardakis G., Hatzivasilis G., Koutsaki E. та Papadakis N. [15], які акцентують на гетерогенності пристроїв і протоколів, ризиках віддаленого доступу та потребі в автентифікації, шифруванні й виявленні атак. Для безбар'єрного середовища ці ризики мають не лише інформаційні, а й фізичні наслідки, оскільки користувач може залежати від безперервної роботи системи.

Percy Campbell J. та співавтори [16], Felber N.A. та співавтори [20], а також Tian Y. J. A. та співавтори [23] аналізують сприйняття домашнього моніторингу, умови прийнятності технологій і загрози приватності та автономії. Сукупність цих праць дає ґрунтовне уявлення про окремі технічні й користувацькі аспекти IoT, однак не формує цілісної моделі державного регулювання програмного забезпечення для безбар'єрного життєвого середовища.

Виділення невирішених раніше частин загальної проблеми. Наявні правила застосовуються до окремих компонентів або секторів і не утворюють цілісної моделі регулювання IoT-систем життєвого середовища. Через це фізично доступна будівля може отримати цифрову систему, яка не підтримує асистивні технології, залежить від одного хмарного постачальника або втрачає критичні функції без зовнішнього зв'язку.

Недостатньо визначено також пропорційність вимог і контроль після введення системи в експлуатацію. Однакові процедури для розумної лампи та модуля розблокування евакуаційного виходу були б необґрунтова-

ними, проте суто добровільний режим не враховує тяжких наслідків відмови. Доступність може погіршитися після оновлення, зміни API, припинення підтримки або заміни хмарного сервісу, тому регулювання має охоплювати весь життєвий цикл.

Формулювання цілей статті (постановка завдання). Мета статті – обґрунтувати ризик-орієнтовану модель державного регулювання розробки та інтеграції програмного забезпечення IoT-систем для безбар'єрного життєвого середовища. Для її досягнення потрібно визначити IoT-систему як комплексний об'єкт регулювання, поєднати будівельні, цифрові та кібербезпекові вимоги, сформувати функціональні механізми політики й запропонувати пропорційні інструменти оцінки, закупівель та моніторингу.

Матеріали та методи дослідження. Застосовано системний, інституційний, структурно-функціональний і порівняльно-правовий підходи. Джерельну базу становлять стратегічні й нормативні документи України, міжнародні та європейські стандарти, акти ЄС і рецензовані дослідження 2023–2025 років [1–23]. Дослідження має теоретико-концептуальний характер; модель сформовано шляхом синтезу вимог та управлінських інструментів, виявлених у джерелах.

Виклад основного матеріалу дослідження. Програмне забезпечення IoT-системи є об'єктом державного регулювання, якщо воно впливає на можливість людини користуватися житловим або громадським середовищем, отримувати інформацію, діяти самостійно та безпечно реагувати на небезпеку. Предмет регулювання охоплює не лише код, а й інтерфейси, автоматизовані сценарії, протоколи обміну, доступ до даних, оновлення, строк підтримки, резервні режими та відповідальність учасників ланцюга постачання.

Центральним поняттям моделі є наскрізна доступність – властивість ланцюга «користувач – інтерфейс – платформа – мережа – пристрій – фізична дія». Відмова будь-якої ланки перешкоджає досягненню результату. Відповідність застосунку критеріям вебдоступності не гарантує виконання команди без інтернету, а доступна фізична панель не компенсує відсутність альтернативи звуковому сигналу. Тому державні вимоги мають описувати кінцевий сценарій, а не ізольований компонент.

IoT не скасовує будівельних вимог і не може замінювати доступне локальне або механічне рішення [2]. Його цінність полягає в розширенні способів взаємодії. Функціональні вимоги мають передбачати сумісність з асистивними технологіями, мультимодальний зворотний зв'язок, керування без точних жестів, просту послідовність дій, запобігання помилкам і можливість скасування. Голосовий канал може доповнювати інтерфейс, але не бути єдиним; публічні та соціально значущі системи повинні мати українськомовні команди, повідомлення й доступний альтернативний спосіб виконання тієї самої дії [3; 12; 17–22].

Відмовостійкість є складовою доступності. Критичні дії не повинні безумовно залежати від зовнішньої хмари, стабільного інтернету або одного телефона. Для функцій доступу, оповіщення та виклику допомоги потрібні локальне виконання основних сценаріїв, безпечний стан у разі втрати зв'язку, резервне живлення в межах профільних вимог, ручний спосіб керування й зрозуміла індикація несправності. Під час аварії система має узгоджувати звукові, візуальні та вібраційні сигнали з проєктом протипожежного захисту.

Кібербезпеку також слід оцінювати через наслідок для людини. Компрометація замка, системи оповіщення або клімат-контролю може створити фізичну загрозу. Базові вимоги охоплюють унікальні облікові дані, безпечну автентифікацію, мінімальні привілеї, захищений обмін, перевірені оновлення, журналювання, канал повідомлення про вразливості та визначений строк підтримки [4; 5; 8; 15]. Механізми безпеки водночас мають залишатися доступними для користувача.

Регуляторний ризик закритого рішення виникає не через саму модель ліцензії, а коли замовник не може перевірити вимоги, перенести конфігурацію і дані, змінити постачальника або підтримувати критичну функцію після припинення сервісу. Тому потрібні документовані інтерфейси, експорт даних і налаштувань, опис залежностей, процедура переходу, а для високоризикових систем – матеріали для незалежного аудиту. Інтероперабельність у проєктах відновлення та публічних закупівлях особливо важлива, оскільки строк експлуатації будівлі значно перевищує життєвий цикл окремого застосунку [6; 18; 19; 21; 22].

Домашня IoT-система може формувати профіль поведінки, пересування, стану здоров'я та побутових сценаріїв. Для користувача, який залежить від допоміжної технології, згода не є вільною, якщо відмова від надмірного збору даних позбавляє базової функції. Вимоги мають конкретизувати мінімі-

зацію даних, розмежування доступу, локальну обробку, зрозуміле пояснення цілей, видалення і перенесення інформації та контроль доступу з боку доглядальників і сервісних працівників [9; 16; 20; 23].

Автоматизація не повинна позбавляти людину контролю над середовищем. Користувач має розуміти стан системи, змінювати налаштування, зупиняти некритичні сценарії й оскаржувати рішення, яке обмежує доступ до послуги. Співпроєктування з людьми, які мають різні функціональні обмеження, дає змогу виявляти бар'єри, непомітні під час суто технічної перевірки [17; 20; 21].

Для подолання фрагментарності запропоновано сім взаємопов'язаних механізмів. Модель не передбачає створення єдиного органу для будівництва, цифрових технологій, кібербезпеки й соціальних послуг. Її завдання – встановити спільний об'єкт політики, мінімум функціональних вимог і розподіл функцій між наявними інституціями (табл. 1).

Нормативно-стандартизаційний механізм доцільно реалізувати через національний профіль функціональних вимог. Він не повинен дублювати стандарти, а має визначати їх застосування до компонентів і сценаріїв, спосіб перевірки наскрізної доступності, склад документації та допустимі еквівалентні рішення [2–4; 8; 11].

Пропонується три функціональні рівні ризику. Перший охоплює сервіси комфорту, відмова яких не блокує доступ і не створює істотної небезпеки; для них достатні базові вимоги, декларація постачальника й договірні гарантії. Другий стосується функцій, що істотно впливають на повсякденну самостійність; тут потрібні документовані сценарії, тестування доступності, сумісності та резервного режиму. Третій охоплює вхід і вихід, аварійне оповіщення, евакуацію та виклик допомоги; для нього доцільні незалежна оцінка, посилена документація, аудит оновлень і постійний нагляд. Класифікація є автор-

Таблиця 1

Механізми державного регулювання програмного забезпечення IoT-систем безбар'єрного життєвого середовища

Механізм	Основні інструменти	Очікувана публічна цінність
Нормативно-стандартизаційний	Національний профіль вимог; узгодження ДБН, стандартів доступності й кібербезпеки; сценарне тестування наскрізної доступності.	Єдина мінімальна рамка якості для фізичних і цифрових компонентів.
Закупівельно-контрактний	Функціональні вимоги, приймальні випробування, строки підтримки й оновлень, резервний режим, перенесення даних та вихід від постачальника.	Формування попиту держави на доступні, сумісні та підтримувані рішення.
Оцінка відповідності та нагляд	Рівні перевірки за наслідками відмови; незалежне тестування критичних функцій; документування конфігурації та постмаркетинговий нагляд.	Пропорційний контроль без однакового навантаження на всі IoT-продукти.
Кібербезпековий і життєвого циклу	Security-by-Design, безпечні оновлення, розкриття вразливостей, журналювання, локальний і ручний резервні режими, план завершення підтримки.	Недопущення перетворення збою або кібератаки на фізичний бар'єр.
Захист даних і автономії	Мінімізація даних, розмежування доступу, локальна обробка, зрозуміла згода, видалення та перенесення даних, контроль автоматизації.	Збереження приватності, гідності та контролю людини над середовищем.
Інституційно-координаційний	Міжвідомча методика, пілоти в громадах, визначення повноважень щодо стандартів, оцінки відповідності, інцидентів і моніторингу.	Узгодження будівельної, цифрової, соціальної та безпекової політики.
Партисипативний і моніторинговий	Співпроєктування, тестування користувацьких сценаріїв, доступний зворотний зв'язок, облік відмов, бар'єрів та строків їх усунення.	Перехід від формальної відповідності до фактичної самостійності користувача.

Джерело: сформовано автором на основі [1–11; 16–23]

ською і потребує подальшої нормативної деталізації.

Оцінювати потрібно не лише код або окремий пристрій, а встановлену конфігурацію. Для високоризикових функцій приймальні випробування мають включати втрату інтернету й хмарного сервісу, розрядження основного пристрою, помилкову команду, зміну ролі користувача, відновлення після оновлення та аварійний сценарій. Критерієм є можливість людини зрозуміти стан, завершити дію або перейти до безпечної альтернативи.

Публічні закупівлі можуть стати першим каналом практичного впровадження моделі. Технічна специфікація повинна описувати користувацькі сценарії, застосовні стандарти, строк безпекових оновлень, документований API, експорт конфігурації, резервний режим, навчання персоналу та доступну підтримку. Договір має визначати приймальні випробування, строки усунення дефектів, повідомлення про вразливості й міграцію після завершення контракту [10].

Регулювання не потребує адміністративного дозволу для кожного рішення. Пропорційна модель поєднує обов'язкові кінцеві вимоги для високоризикових функцій, стандарти як спосіб доведення відповідності, відповідальність виробника й інтегратора, незалежну оцінку за істотних наслідків та ринковий нагляд. Закон України «Про технічні регламенти та оцінку відповідності» надає загальну правову конструкцію для такого підходу [11].

Інституційна координація має охоплювати органи, відповідальні за розвиток громад і будівництво, цифрову трансформацію, кібербезпеку, соціальний захист та стандартизацію. На першому етапі доцільно створити міжвідомчий механізм підготовки методики й визначити прогалини компетенції, а потім закріпити відповідальність за стандарт, оцінку відповідності, ринковий нагляд, інциденти та моніторинг. Організації осіб з інвалідністю мають брати формалізовану участь у підготовці вимог і оцінюванні пілотів.

Пілотування доцільно проводити в громадах для типових сценаріїв: доступу до будівлі, мультимодального оповіщення, керування освітленням і кліматом, виклику допомоги та підтримки самостійного проживання. Моніторинг повинен оцінювати не кількість датчиків, а частку сценаріїв, які користувачі виконують самостійно, доступність критичних функцій без зовнішнього зв'язку, своєчасність оновлень, строки усунення вразливостей, можливість перенесення даних і доступність підтримки. Цільові значення слід визначати після пілотування.

Фінансова доступність також має бути предметом політики. У публічних проєктах потрібно оцінювати повну вартість життєвого циклу: придбання, інтеграцію, зв'язок, оновлення, аудит, підтримку, навчання, резервні компоненти та міграцію [13; 14; 19; 22]. Відкриті протоколи й переносимість можуть зменшити залежність від постачальника, але їхню економічну перевагу слід перевіряти для конкретного проєкту.

У соціальному житлі, підтриманому проживанні та догляді вдома IoT може посилювати автономність, але також створювати ризик прихованого спостереження і заміни людської підтримки алгоритмом. Правила встановлення датчиків та доступу до інформації мають формуватися за участю користувача, а відмова від надмірного моніторингу не повинна позбавляти соціальної послуги.

В умовах війни та відновлення стійкість цифрового середовища є складовою безбар'єрності. Відключення електроенергії, пошкодження мережі, евакуація, тимчасове житло й зміна постачальника є реальними сценаріями [1]. Проєкти відбудови мають закладати доступність, локальне керування та резервування на етапі проєктування, а не додавати окремі пристрої після введення об'єкта в експлуатацію.

Отже, питання полягає не в тому, чи потрібен державний контроль IoT, а в його формі та межах. Найсуворіші процедури мають стосуватися функцій, від яких залежать життя, фізична безпека і базова автономність. Для сервісів низького ризику достатні стандарти, контрактні механізми та контроль після введення продукту в експлуатацію.

Висновки. Проведене дослідження дає підстави розглядати програмне забезпечення IoT-систем як самостійний об'єкт державного регулювання у політиці безбар'єрності, оскільки саме через нього цифрова команда перетворюється на фізичну дію. Оцінювання доступності не може обмежуватися інтерфейсом або окремим пристроєм: воно має охоплювати повний ланцюг «користувач – інтерфейс – платформа – мережа – пристрій – фізична дія» та враховувати можливість безпечного завершення дії за відмови однієї з ланок.

Авторська ризик-орієнтована модель поєднує сім взаємопов'язаних механізмів і розмежовує три рівні вимог залежно від

можливих наслідків відмови. Найсуворіший контроль обґрунтований для функцій входу і виходу, аварійного оповіщення, евакуації та виклику допомоги; для сервісів комфорту достатніми можуть бути базові стандарти, договірні гарантії та нагляд після введення в експлуатацію. Такий поділ дає змогу узгодити вимоги доступності, кібербезпеки, сумісності, захисту даних і відмовостійкості без однакового адміністративного навантаження на всі IoT-рішення.

Практичне застосування моделі доцільно розпочати з підготовки міжвідомчого національного профілю функціональних вимог та його апробації у публічних закупівлях і муніципальних пілотах. Наступний етап дослідження має охопити деталізацію критеріїв ризику, розроблення методики сценарних випробувань, визначення показників фактичної доступності після введення системи в експлуатацію та оцінювання повної вартості її життєвого циклу.

Заява про використання штучного інтелекту. Під час підготовки рукопису автор використовував ChatGPT (OpenAI) для поліпшення читабельності, усунення мовних повторів і технічного оформлення. Інструмент не використовувався для створення емпіричних даних або зображень. Автор перевірив фактичні твердження, джерела та остаточний текст і несе повну відповідальність за його зміст.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

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. ДБН В.2.2-40:2018. Інклюзивність будівель і споруд. Основні положення (зі змінами). Єдина державна електронна система у сфері будівництва. URL: https://e-construction.gov.ua/laws_detail/3869316279311533309

3. Про прийняття національного стандарту : наказ ДП «УкрНДНЦ» від 05.05.2022 № 68. URL: https://zakon.rada.gov.ua/laws/show/v0068774-22

4. ETSI EN 303 645 V3.1.3 (2024-09). Cyber Security for Consumer Internet of Things: Baseline Requirements. URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

5. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

6. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data. URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

7. 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/eli/dir/2019/882/oj/eng (дата звернення: 28.07.2026).

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

9. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17

10. ETSI TR 101 551 V2.1.1 (2026-02). Guidelines for public procurement of ICT products and services in the EU; Accessibility award criteria and conformity assessment. URL: https://www.etsi.org/deliver/etsi_tr/101500_101599/101551/02.01.01_60/tr_101551v020101p.pdf

11. Про технічні регламенти та оцінку відповідності : Закон України від 15.01.2015 № 124-VIII. URL: https://zakon.rada.gov.ua/laws/show/124-19

12. Periša M., Teskera P., Cvitić I., Grgurević I. Empowering People with Disabilities in Smart Homes Using Predictive Informing. *Sensors*. 2025. Vol. 25, No. 1. Article 284. DOI: https://doi.org/10.3390/s25010284.

13. Vrančić A., Zadravec H., Orehovački T. The Role of Smart Homes in Providing Care for Older Adults: A Systematic Literature Review from 2010 to 2023. *Smart Cities*. 2024. Vol. 7, No. 4. P. 1502–1550. DOI: https://doi.org/10.3390/smartcities7040062.

14. Tian Y. J. A., Felber N. A., Pageau F., Roulet Schwab D., Wangmo T. Benefits and barriers associated with the use of smart home health technologies in the care of older persons: a systematic review. *BMC Geriatrics*. 2024. Vol. 24. Article 152. DOI: https://doi.org/10.1186/s12877-024-04702-1.

15. Vardakis G., Hatzivasilis G., Koutsaki E., Papadakis N. Review of Smart-Home Security Using the Internet of Things. *Electronics*. 2024. Vol. 13, No. 16. Article 3343. DOI: https://doi.org/10.3390/electronics13163343.

16. Percy Campbell J., Buchan J., Chu C. H., Bianchi A., Hoey J., Khan S. S. User Perception of Smart Home Surveillance Among Adults Aged 50 Years and Older: Scoping Review. *JMIR mHealth and uHealth*. 2024. Vol. 12. Article e48526. DOI: https://doi.org/10.2196/48526.

17. Ghorayeb A., Comber R., Gooberman-Hill R. Development of a Smart Home Interface With Older Adults: Multi-Method Co-Design Study. *JMIR Aging*. 2023. Vol. 6. Article e44439. DOI: https://doi.org/10.2196/44439.

18. Ding D., Morris L., Messina K., Fairman A. Providing mainstream smart home technology as assistive technology for persons with disabilities: a qualitative study with professionals. *Disability and Rehabilitation: Assistive Technology*. 2023. Vol. 18, No. 7. P. 1192–1199. DOI: https://doi.org/10.1080/17483107.2021.1998673.

19. Ding D., Morris L., Novario G., Fairman A., Roehrich K., Foschi Walko P., Boateng J. Mainstream Smart Home Technology–Based Intervention to Enhance Functional Independence in Individuals With Complex Physical Disabilities: Single-Group Pre-Post Feasibility Study. *JMIR Rehabilitation and Assistive Technologies*. 2025. Vol. 12. Article e70855. DOI: https://doi.org/10.2196/70855.

20. Felber N. A., Lipworth W., Tian Y. J. A., Roulet Schwab D., Wangmo T. Informing existing technology acceptance models: a qualitative study with older persons and caregivers. *European Journal of Ageing*. 2024. Vol. 21. Article 12. DOI: https://doi.org/10.1007/s10433-024-00801-5.

21. Mun K., Kim J. Development of a Smart Home Modification Program: A Delphi Survey of Multidisciplinary Health Care Experts. *American Journal of Occupational Therapy*. 2024. Vol. 78, No. 5. Article 7805205130. DOI: https://doi.org/10.5014/ajot.2024.050651.

22. Mun K., Kim J. Survey on demand for smart home technology as assistive technology for people with physical disabilities in Korea. *Disability and Rehabilitation: Assistive Technology*. 2025. Vol. 20, No. 6. P. 1764–1773. DOI: https://doi.org/10.1080/17483107.2025.2475144.

23. Tian Y. J. A., Duong M. T., Buhr P., Felber N. A., Roulet Schwab D., Wangmo T. Monitored and Cared for at Home? Privacy Concerns When Using Smart Home Health Technologies to Care for Older Persons. *AJOB Empirical Bioethics*. 2025. Vol. 16, No. 2. P. 61–76. DOI: https://doi.org/10.1080/23294515.2024.2416121.

REFERENCES:

1. Cabinet of Ministers of Ukraine. (2021). Pro skhvalennia Natsionalnoi stratehii iz stvorennia bezbariernoho prostoru v Ukraini na period do 2030 roku: Rozporiadzhennia vid 14.04.2021 No. 366-r [On approval of the National Strategy for Creating a Barrier-Free Space in Ukraine until 2030]. https://zakon.rada.gov.ua/laws/show/366-2021-%D1%80 (in Ukrainian)

2. Ministry for Communities and Territories Development of Ukraine. (2018). DBN V.2.2-40:2018. Inkliuzyvnist budivel i sporud. Osnovni polozhennia (zi zminamy) [Inclusiveness of buildings and structures. Basic provisions, as amended]. https://e-construction.gov.ua/laws_detail/3869316279311533309 (in Ukrainian)

3. Ukrainian Research and Training Center for Standardization, Certification and Quality. (2022). Pro pryiniattia natsionalnoho standartu: Nakaz vid 05.05.2022 No. 68 [On adoption of the national standard]. https://zakon.rada.gov.ua/laws/show/v0068774-22 (in Ukrainian)

4. European Telecommunications Standards Institute. (2024). ETSI EN 303 645 V3.1.3 (2024-09). Cyber Security for Consumer Internet of Things: Baseline Requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

5. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

6. European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data. https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

7. European Parliament and Council of the European Union. (2019). Directive (EU) 2019/882 of 17 April 2019 on the accessibility requirements for products and services. https://eur-lex.europa.eu/eli/dir/2019/882/oj/eng

8. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 No. 2163-VIII [On the basic principles of ensuring cybersecurity of Ukraine]. https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian)

9. Verkhovna Rada of Ukraine. (2010). Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 No. 2297-VI [On personal data protection]. https://zakon.rada.gov.ua/laws/show/2297-17 (in Ukrainian)

10. European Telecommunications Standards Institute. (2026). ETSI TR 101 551 V2.1.1 (2026-02). Guidelines for public procurement of ICT products and services in the EU; Accessibility award criteria and conformity assessment. https://www.etsi.org/deliver/etsi_tr/101500_101599/101551/02.01.01_60/tr_101551v020101p.pdf

11. Verkhovna Rada of Ukraine. (2015). Pro tekhnichni rehlamenty ta otsinku vidpovidnosti: Zakon Ukrainy vid 15.01.2015 No. 124-VIII [On technical regulations and conformity assessment]. https://zakon.rada.gov.ua/laws/show/124-19 (in Ukrainian)

12. Periša, M., Teskera, P., Cvitić, I., & Grgurević, I. (2025). Empowering people with disabilities in smart homes using predictive informing. *Sensors*, 25(1), 284. DOI: https://doi.org/10.3390/s25010284

13. Vrančić, A., Zadravec, H., & Orehovački, T. (2024). The role of smart homes in providing care for older adults: A systematic literature review from 2010 to 2023. *Smart Cities*, 7(4), 1502–1550. DOI: https://doi.org/10.3390/smartcities7040062

14. Tian, Y. J. A., Felber, N. A., Pageau, F., Roulet Schwab, D., & Wangmo, T. (2024). Benefits and barriers associated with the use of smart home health technologies in the care of older persons: A systematic review. *BMC Geriatrics*, 24, 152. DOI: https://doi.org/10.1186/s12877-024-04702-1

15. Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the Internet of Things. *Electronics*, 13(16), 3343. DOI: https://doi.org/10.3390/electronics13163343

16. Percy Campbell, J., Buchan, J., Chu, C. H., Bianchi, A., Hoey, J., & Khan, S. S. (2024). User perception of smart home surveillance among adults aged 50 years and older: Scoping review. *JMIR mHealth and uHealth*, 12, e48526. DOI: https://doi.org/10.2196/48526

17. Ghorayeb, A., Comber, R., & Gooberman-Hill, R. (2023). Development of a smart home interface with older adults: Multi-method co-design study. *JMIR Aging*, 6, e44439. DOI: https://doi.org/10.2196/44439

18. Ding, D., Morris, L., Messina, K., & Fairman, A. (2023). Providing mainstream smart home technology as assistive technology for persons with disabilities: A qualitative study with professionals. *Disability and Rehabilitation: Assistive Technology*, 18(7), 1192–1199. DOI: https://doi.org/10.1080/17483107.2021.1998673

19. Ding, D., Morris, L., Novario, G., Fairman, A., Roehrich, K., Foschi Walko, P., & Boateng, J. (2025). Mainstream smart home technology–based intervention to enhance functional independence in individuals with complex physical disabilities: Single-group pre-post feasibility study. *JMIR Rehabilitation and Assistive Technologies*, 12, e70855. DOI: https://doi.org/10.2196/70855

20. Felber, N. A., Lipworth, W., Tian, Y. J. A., Roulet Schwab, D., & Wangmo, T. (2024). Informing existing technology acceptance models: A qualitative study with older persons and caregivers. *European Journal of Ageing*, 21, 12. DOI: https://doi.org/10.1007/s10433-024-00801-5

21. Mun, K., & Kim, J. (2024). Development of a smart home modification program: A Delphi survey of multidisciplinary health care experts. *American Journal of Occupational Therapy*, 78(5), 7805205130. DOI: https://doi.org/10.5014/ajot.2024.050651

22. Mun, K., & Kim, J. (2025). Survey on demand for smart home technology as assistive technology for people with physical disabilities in Korea. *Disability and Rehabilitation: Assistive Technology*, 20(6), 1764–1773. DOI: https://doi.org/10.1080/17483107.2025.2475144

23. Tian, Y. J. A., Duong, M. T., Buhr, P., Felber, N. A., Roulet Schwab, D., & Wangmo, T. (2025). Monitored and cared for at home? Privacy concerns when using smart home health technologies to care for older persons. *AJOB Empirical Bioethics*, 16(2), 61–76. DOI: https://doi.org/10.1080/23294515.2024.2416121

Дата надходження статті: 28.07.2026
Дата прийняття статті до публікації: 27.10.2026
Дата публікації статті: 06.11.2026