

## СЕКЦІЯ 1 МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ

### ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ОХОРОНИ ЗДОРОВ'Я ТА ВИКЛИКИ ЦИФРОВОЇ МЕДИЦИНИ: АСПЕКТИ ПУБЛІЧНОГО УПРАВЛІННЯ

### STATE POLICY IN HEALTHCARE AND THE CHALLENGES OF DIGITAL MEDICINE: ASPECTS OF PUBLIC GOVERNANCE

У статті здійснено комплексне дослідження державної політики у сфері охорони здоров'я в умовах цифрової трансформації суспільства та визначено ключові виклики, зумовлені розвитком цифрової медицини. Наголошено, що сучасний етап розвитку системи охорони здоров'я характеризується активним впровадженням інноваційних цифрових технологій, зокрема телемедицини, електронних медичних карток, мобільних додатків для моніторингу стану здоров'я та функціонування електронної системи eHealth. Поряд із цим, виявлено низку проблем, які ускладнюють ефективну реалізацію державної політики в цій сфері, фрагментарність нормативно-правового регулювання, відсутність комплексної стратегії цифрової медицини, нерівномірність розвитку цифрової інфраструктури, загрози кібербезпеці та недостатній рівень цифрової компетентності населення й медичних кадрів.

Здійснено аналіз сучасних наукових підходів до дослідження цифровізації охорони здоров'я, а також практик публічного управління у цій сфері. Особливу увагу приділено європейському досвіду, що ґрунтується на принципах захисту персональних даних GDPR, стандартизації медичних інформаційних систем та інтегрованості цифрових сервісів. Визначено, що для України пріоритетним завданням є формування цілісної державної політики, спрямованої на створення стійкої системи охорони здоров'я, здатної поєднувати інноваційність технологій із гарантіями доступності, безпеки та якості медичних послуг.

На основі проведеного дослідження обґрунтовано пропозиції щодо вдосконалення механізмів публічного управління цифровою медициною, зокрема: посилення міжвідомчої координації органів державної влади, удосконалення правового регулювання телемедицини, підвищення цифрової грамотності медичних кадрів і громадян, створення партнерських платформ співпраці держави, бізнесу та громадянського суспільства.

Результати дослідження мають теоретичне та практичне значення, оскільки сприяють виробленню науково обґрунтованих підходів до модернізації державної політики у сфері охорони здоров'я та забезпечують основу для впровадження цифрових технологій у практику публічного управління.

**Ключові слова:** державна політика, публічне управління, охорона здоров'я, цифрова медицина, телемедицина, eHealth, цифрова

трансформація, кібербезпека, захист персональних даних, європейський досвід.

The article provides a comprehensive study of state policy in the field of healthcare under the conditions of digital transformation and outlines the key challenges caused by the development of digital medicine. It is emphasized that the current stage of healthcare system development is characterized by the active implementation of innovative digital technologies, including telemedicine, electronic health records, mobile applications for health monitoring, and the functioning of the national eHealth system. At the same time, a number of systemic problems that hinder the effective implementation of state policy in this domain have been identified: the fragmentation of legal regulation, the absence of a comprehensive digital medicine strategy, uneven development of digital infrastructure, cybersecurity threats, and the insufficient level of digital literacy among both the population and healthcare professionals.

The study analyzes contemporary scientific approaches to the digitalization of healthcare and examines relevant practices of public governance in this area. Special attention is given to the European experience, which is based on principles of personal data protection GDPR, standardization of medical information systems, and the integration of digital health services. It is determined that for Ukraine, a priority task is the formation of a holistic state policy aimed at building a resilient healthcare system capable of combining technological innovation with guarantees of accessibility, safety, and quality of medical services.

Based on the conducted analysis, proposals are substantiated to improve the mechanisms of public governance in the field of digital medicine. These include strengthening interagency coordination of public authorities, enhancing the legal regulation of telemedicine, improving the digital literacy of medical personnel and citizens, and establishing partnership platforms for cooperation between the state, business, and civil society.

The results of the research have both theoretical and practical significance, as they contribute to the development of scientifically grounded approaches to the modernization of state healthcare policy and provide a foundation for the integration of digital technologies into the practice of public governance.

**Key words:** state policy, public governance, healthcare, digital medicine, telemedicine, eHealth, digital transformation, cybersecurity, personal data protection, European experience.

УДК 35.07:614:004

DOI <https://doi.org/10.32782/rma2663-5240-2025.48.1>

рma2663-5240-2025.48.1

Стаття поширюється на умовах ліцензії CC BY 4.0

#### Лахижа М. І.

д. наук з держ. упр., професор, професор кафедри публічного управління, адміністрування та права Національний університет «Полтавська політехніка імені Юрія Кондратюка»

#### Качан Я. В.

к. наук з держ. упр., доцент, завідувач кафедри публічного управління та публічної служби Академія праці, соціальних відносин і туризму

#### Собченко А. О.

начальник відділення заготівлі донорської крові в умовах виїзду Центр крові Збройних Сил України, студент II курсу магістратури юридичного факультету Академія праці, соціальних відносин і туризму

**Постановка проблеми** у загальному вигляді. Сучасний розвиток системи охорони здоров'я відбувається в умовах глобальних трансформацій, зумовлених переходом до цифрової економіки та суспільства знань. В умовах XXI століття цифровізація стала визначальним чинником модернізації ключових сфер публічного управління, і саме медична галузь виявилася однією з найбільш чутливих та водночас перспективних для впровадження інноваційних інформаційно-комунікаційних технологій. Впровадження електронних медичних систем, телемедицини, цифрових платформ моніторингу стану здоров'я, а також національної системи eHealth розглядається як один із пріоритетних напрямів державної політики у сфері охорони здоров'я.

Разом з тим, цифрова трансформація медицини не лише відкриває нові можливості для підвищення ефективності та доступності медичних послуг, але й породжує низку складних проблем, що потребують належного врегулювання на рівні державної політики. Насамперед, постає проблема нормативно-правового забезпечення. Чинна законодавча база України характеризується фрагментарністю та несистемністю: окремі нормативні акти регулюють питання електронного документообігу чи захисту персональних даних, але відсутня єдина узгоджена стратегія цифрової медицини, що призводить до виникнення правових колізій, ускладнює міжвідомчу взаємодію та знижує рівень правової визначеності для учасників процесу.

Не менш значущим є організаційний аспект проблеми. Реалізація цифрової трансформації медицини потребує координації зусиль низки органів державної влади – Міністерства охорони здоров'я, Міністерства цифрової трансформації, Національної служби здоров'я України, органів місцевого самоврядування. Водночас на практиці спостерігається дублювання функцій, недостатня узгодженість управлінських рішень і слабка координація між центральним та регіональним рівнями управління, що призводить до нерівномірності розвитку цифрової інфраструктури в регіонах, створюючи ризик посилення територіальних диспропорцій у доступі до медичних послуг.

Окремої уваги заслуговує соціальний вимір проблеми. Розвиток цифрової медицини загострює питання соціальної нерівності, частина населення, особливо у сільських та віддалених районах, не має достатнього доступу до інтернет-інфраструктури чи цифрових пристроїв, а отже – не може скористатися можливостями телемедицини або електронних медичних сервісів. Водночас цифрова грамотність пацієнтів

і значної частини медичних працівників залишається низькою, що обмежує можливості ефективного використання нових технологій.

Надзвичайно важливою є й проблема кібербезпеки та захисту персональних даних. Масове використання електронних медичних карток і цифрових платформ для обміну медичною інформацією створює серйозні ризики витоку конфіденційних даних, що може призвести до втрати довіри громадян до системи цифрової медицини. Захист персональних даних у цій сфері має стратегічне значення, адже стосується фундаментального права людини на приватність.

Таким чином, актуальність проблеми полягає в необхідності формування сучасної, комплексної та системно орієнтованої державної політики у сфері охорони здоров'я, яка б адекватно відповідала на виклики цифрової трансформації. Йдеться не лише про технічне чи інфраструктурне забезпечення процесів, але й про створення ефективних механізмів публічного управління, які поєднуюватимуть інноваційність технологій із принципами доступності, прозорості, безпеки та інклюзивності.

Саме тому дослідження державної політики у сфері охорони здоров'я в контексті викликів цифрової медицини є надзвичайно актуальним і має вагоме як теоретичне, так і практичне значення. З одного боку, воно дозволяє сформулювати науково обґрунтовану концепцію модернізації публічного управління у медичній сфері, а з іншого сприяє розробці дієвих механізмів забезпечення сталого розвитку системи охорони здоров'я в Україні відповідно до європейських стандартів та міжнародних зобов'язань.

**Аналіз останніх досліджень і публікацій.** У сучасній науковій літературі проблема цифровізації сфери охорони здоров'я розглядається з кількох ключових аспектів: управлінського, економічного, правового та соціально-етичного. Значна увага приділяється дослідженню інституційних змін у публічному управлінні, що відбуваються під впливом цифрових технологій. Зокрема, Д. Кеттл у своїх працях акцентує на необхідності міжвідомчої координації та формуванні цілісної політики, заснованої на даних, що є критично важливим у сфері цифрової медицини. Аналогічно, К. Поллітт та К. Худ підкреслюють, що цифрові інструменти змінюють механізми прийняття рішень у публічному секторі та формують нові підходи до підзвітності та прозорості державних інституцій.

З іншого боку, у працях М. Портера та Е. Тісберг обґрунтовується концепція *value-based healthcare*, де цифрові технології відіграють центральну роль у вимірюванні

результатів лікування та оптимізації витрат. Ця парадигма отримала розвиток у роботах Т. Лі та Р. Каплана, які пропонують конкретні інструменти обліку витрат і результатів у медичній практиці, що може слугувати підґрунтям для оцінки ефективності державних інвестицій у цифрову медицину.

У сфері медичної інформатики ключовим є внесок Г. Айзенбаха, який одним із перших запропонував системне визначення поняття *eHealth* та окреслив його міждисциплінарний характер. Е. Коєра та Д. Бейтс розробляють питання безпеки пацієнта й архітектури інформаційних систем, тоді як Е. Топол акцентує увагу на потенціалі штучного інтелекту та персоналізованої медицини. У цьому контексті Т. Грінгалх та С. Шоу пропонують концепцію «соціотехнічних ансамблів», яка дозволяє пояснити, чому ефективність впровадження телемедицини залежить не лише від технічних характеристик, але й від організаційної культури та рівня підготовки кадрів.

Важливий пласт досліджень присвячено етичним та правовим аспектам цифрової медицини. Л. Флоріді аналізує ризики «датафікації» людини, Х. Ніссенбаум вводить концепт «контекстуальної цілісності приватності», а Б. Міттельштадт досліджує загрози, пов'язані з упередженістю та непрозорістю алгоритмів у сфері охорони здоров'я. Ці роботи підкреслюють необхідність розробки таких правових механізмів, які б забезпечували баланс між інноваціями та захистом фундаментальних прав людини.

Емпіричні дослідження телемедицини (зокрема роботи А. Мехротри, А. Джа, Е. Нурі) свідчать, що хоча цифрові сервіси розширюють доступ до медичної допомоги, вони водночас можуть поглиблювати соціальну нерівність. Дослідники фіксують, що найбільш уразливі категорії населення - люди похилого віку, мешканці сільських регіонів, малозабезпечені верстви частіше стикаються з бар'єрами використання цифрових медичних послуг через недостатню інфраструктуру та цифрову грамотність.

В українському науковому дискурсі цифровізація системи охорони здоров'я досліджується у працях Т. Семигіної, яка акцентує на соціальній політиці та інклюзивності послуг; В. Лехана, котрий аналізує інституційні реформи системи охорони здоров'я; С. Слабкого, який розглядає управлінські та кадрові аспекти організації медичної допомоги; О. Гладуна, що розробляє правові основи цифрової медицини; а також Н. Кризини та І. Розвадовського, які вивчають регіональні аспекти розвитку *eHealth* та проблеми нерівного доступу до цифрових послуг.

**Виділення невирішених раніше частин загальної проблеми.** Попри значну кількість наукових досліджень, низка питань залишається недостатньо розробленою. Зокрема, бракує комплексних оцінок ефективності цифрової медицини з позицій *value-based healthcare*; слабо досліджені механізми кіберстійкості медичних закладів та моделі міжвідомчої координації у сфері охорони здоров'я. Таким чином, сучасний стан наукових розробок підтверджує потребу у подальшому комплексному аналізі державної політики цифрової медицини, орієнтованій на інклюзію, безпеку та результативність.

**Метою статті** є обґрунтування організаційно-правових та управлінських основ формування і впровадження державної політики в галузі охорони здоров'я в контексті цифрової трансформації, з урахуванням викликів і можливостей, що виникають у сфері цифрової медицини.

**Виклад основного матеріалу.** Розвиток цифрової медицини в Україні відбувається на тлі постійних викликів, які ставлять під сумнів ефективність існуючої правової системи. Нині правова база є фрагментарною та переважно реактивною, що зумовлює низку проблем у процесі реалізації державної політики охорони здоров'я.

Базові положення закріплені в Конституції України стаття 49 гарантує право кожного громадянина на охорону здоров'я, медичну допомогу та медичне страхування, тоді як стаття 32 передбачає право на невтручання в особисте і сімейне життя та захист персональних даних [1]. Однак у Конституції відсутні положення, що безпосередньо стосуються цифровізації охорони здоров'я, електронних медичних записів чи телемедицини. Що свідчить про загальний характер правових гарантій, які потребують уточнення на рівні спеціального законодавства.

Важливим актом є Закон України «Основи законодавства України про охорону здоров'я» № 2801-XII від 19.11.1992 р., що визначає принципи функціонування системи охорони здоров'я [2]. Проте, попри численні зміни, цей закон лише фрагментарно торкається цифрових технологій, який не містить чітких положень про використання електронних медичних записів, цифрових платформ, *big data* чи штучного інтелекту в медицині. Таким чином, законодавча база не відповідає сучасним технологічним викликам.

Не менш важливим є Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 р., який встановлює загальні принципи обробки інформації [3].

Хоча регламентує питання приватності, він не враховує специфіку медичних даних, які у світовій практиці належать до «особливо чутливих» категорій. Наприклад, залишається відкритим питання вторинного використання даних у наукових і статистичних цілях, а також застосування алгоритмів штучного інтелекту до масивів медичної інформації.

На рівні підзаконних актів простежується прагнення держави врегулювати цифрові практики. Так, Постанова КМУ № 411 від 25.04.2018 р. «Деякі питання електронної системи охорони здоров'я» [4] визначила дворівневу архітектуру ЕСОЗ (центральна база даних і медичні інформаційні системи), який заклав основу функціонування електронних декларацій, рецептів, направлень. Проте питання інтероперабельності даних та стандартизації залишилися недостатньо врегульованими.

Наказ МОЗ № 681 від 19.10.2015 р. уперше унормував телемедицину [5]. У подальшому, у відповідь на кризові умови, було ухвалено накази МОЗ № 1062 від 20.06.2022 р. та № 1695 від 17.09.2022 р., що розширили застосування телемедицини у воєнний період [6; 7]. Однак вони мають тимчасовий характер і не формують сталих правил.

У 2023 р. Верховна Рада ухвалила Закон № 3301-ІХ «Про внесення змін до деяких законодавчих актів України щодо функціонування телемедицини», який унормував термінологію та визначив порядок дистанційної допомоги [8]. Хоча закон став важливим кроком уперед, він залишив поза увагою питання штучного інтелекту, вторинного використання даних та євроінтеграційної гармонізації стандартів.

Крім того, урядом затверджено Стратегію розвитку телемедицини до 2025 року Розпорядження КМУ № 625-р від 14.07.2023 р. [9], яка визначає середньострокові пріоритети, проте не формує довгострокової концепції цифрової медицини.

Як підкреслюють Malakhov зі співавт., «правове забезпечення цифрової медицини в Україні є несистемним і фрагментарним, що не дозволяє ефективно інтегрувати сучасні технології у медичну сферу» [10].

У ЄС, навпаки, діє комплексна модель Регламент ЄС 2016/679 GDPR визначає медичні дані як чутливу категорію, вводючи суворі вимоги до їх обробки та захисту [11]. Новий Регламент ЄС про Європейський простір даних про здоров'я (EHDS, 2025 р.) створює рамку для їх первинного (лікування) та вторинного (наука, статистика, інновації) використання [12], що дозволяє забезпечити баланс

між захистом прав пацієнтів і розвитком цифрових інновацій.

Тому, нинішня ситуація в Україні засвідчує невідповідність правової бази технологічним викликам та потребу в ухваленні єдиного рамкового Закону «Про цифрову медицину», що унормує ключові напрями цифровізації охорони здоров'я.

Інституційне забезпечення цифрової трансформації охорони здоров'я в Україні є багаторівневим і характеризується значним ступенем розпорошеності управлінських функцій. Сьогодні основними суб'єктами, відповідальними за реалізацію політики у цій сфері, є:

- Міністерство охорони здоров'я України – формує державну політику, затверджує нормативно-правові акти та визначає стратегічні пріоритети.

- Національна служба здоров'я України – адмініструє електронну систему охорони здоров'я (ЕСОЗ), виконує функції замовника медичних послуг, укладає договори з надавачами медичної допомоги.

- Міністерство цифрової трансформації України – відповідає за інфраструктурні рішення, інтеграцію з державними цифровими платформами, розвиток електронних довірчих послуг та захист даних.

- Органи місцевого самоврядування – впроваджують цифрові медичні сервіси на територіях, забезпечують доступ громадян до телемедичних послуг і цифрових реєстрів.

Попри чітко розмежовані компетенції, система має низку системних проблем. По-перше, відсутній єдиний координаційний центр цифрової медицини, який би інтегрував діяльність різних інституцій. По-друге, відсутні узгоджені стандарти інтероперабельності між відомствами, що ускладнює обмін даними.

Як наголошують Jayathissa R., Hewapathirana R саме інституційна асиметрія породжує «цифрову асиметрію», тобто нерівність між містом і селом у доступі до цифрових послуг [14].

Для порівняння, у країнах ЄС створені спеціалізовані органи, що відповідають за інтеграцію політики цифрової медицини:

- у Німеччині діє Federal Agency for Digital Health, яка встановлює стандарти, проводить сертифікацію постачальників і контролює розвиток електронних медичних карток [16];

- у Великій Британії функціонує NHS Digital, яке координує цифрову трансформацію системи охорони здоров'я та впроваджує єдині вимоги до обміну даними;

- в Естонії – e-Health Authority, що забезпечує роботу національної платформи eHealth та контролює дотримання стандартів інтероперабельності.

Дані приклади свідчать про те, що централізовані моделі управління дозволяють уникати дублювання завдань, встановлювати єдині вимоги для всіх учасників та забезпечувати контроль за якістю цифрових сервісів.

В Україні ж відсутність єдиного координаційного органу призводить до фрагментарності та неузгодженості дій. Тому доцільним виглядає створення Координаційної ради з цифрової медицини при Кабінеті Міністрів України, до складу якої входили б представники МОЗ, НСЗУ, Мінцифри, органів місцевого самоврядування та професійних асоціацій. Така інституція могла б забезпечити:

1. Єдину політику у сфері цифрової медицини.
2. Стандартизацію вимог до інформаційних систем.
3. Координацію ресурсів та фінансування.
4. Розробку механізмів контролю та аудиту якості послуг.

Таким чином, інституційний аспект є критичним для переходу від декларативних намірів до системної реалізації цифрової трансформації охорони здоров'я в Україні

Одним із найбільш критичних соціально-економічних викликів цифрової медицини в Україні є цифрова нерівність, яка проявляється як у доступі до інтернет-інфраструктури, так і у здатності населення користуватися цифровими сервісами.

За даними Національної служби здоров'я України, у 2022–2023 рр. кількість телемедичних консультацій у сільських громадах була майже удвічі нижчою, ніж у міських [13]. Це пояснюється як слабким розвитком інтернет-мереж у віддалених регіонах, так і обмеженою забезпеченістю комп'ютерною технікою та смартфонами серед населення.

Подібні тенденції простежуються і в міжнародній практиці. Дослідження Baker R довели, що навіть у США телемедицина не усуває соціальну нерівність, а навпаки відтворює її мешканці сільських територій та малозабезпечені верстви населення користуються такими послугами значно рідше [15].

Показовим є приклад Естонії, де ще у 2010-х роках держава інвестувала у розвиток широкопasmового інтернету навіть у найменших населених пунктах, а для літніх людей запровадила пільгові програми придбання планшетів. Польща реалізувала загальнонаціональний проєкт «eRecepta», який забезпечує єдиний доступ до електронних рецептів незалежно від місця проживання. Такі програми дали змогу мінімізувати розрив між містом і селом у сфері цифрової медицини.

Для України цифрова нерівність є не лише технічною, а й соціальною проблемою, вона

позбавляє значну частину громадян можливості отримати сучасні медичні послуги, поглиблює соціальну маргіналізацію й створює ризик виникнення «цифрового поділу» у системі охорони здоров'я.

Другим суттєвим викликом є кадровий дефіцит у сфері цифрової медицини. Більшість українських медичних працівників не володіють достатніми цифровими навичками для повноцінного використання електронних систем охорони здоров'я.

Як зазначають Dickey C., Wasko M низький рівень цифрової грамотності лікарів і пацієнтів є одним із ключових бар'єрів цифровізації охорони здоров'я [16]. А дослідження Ladin K., Portz J., Miake-Lye I. підкреслюють, що старші люди частіше скептично ставляться до дистанційних консультацій через труднощі з цифровими навичками [17].

Міжнародний досвід підтверджує цю тезу. У Великій Британії функціонує NHS Digital Academy, що готує управлінців цифрової медицини та формує компетентності у сфері big data, штучного інтелекту та кібербезпеки. В Естонії курси з цифрової медицини інтегровані у навчальні програми університетів, а післядипломна освіта лікарів включає тренінги з роботи з електронними медичними картками.

Для України проблема кадрового забезпечення має комплексний характер:

1. Системна відсутність цифрових компетентностей у медичних вишах.
2. Нерівномірна підготовка кадрів у міських і сільських громадах.
3. Брак кваліфікованих ІТ-спеціалістів у медичній сфері, здатних підтримувати та розвивати цифрові платформи.

Ці фактори формують ризик того, що цифрова медицина залишатиметься інструментом «для обраних», а не загальнодоступною послугою.

Поєднання цифрової нерівності та кадрового дефіциту створює подвійну пастку для державної політики:

- з одного боку, громадяни в сільських та віддалених регіонах позбавлені доступу до телемедичних сервісів;
- з іншого навіть у містах, де є технічні можливості, лікарі часто не володіють необхідними навичками для роботи з ЕСОЗ.

Це знижує ефективність реалізації державної політики цифровізації медицини й загрожує розривом між нормативно-правовими новаціями та їх практичним втіленням.

У сучасних умовах цифрова медицина ґрунтується на обробці великих масивів даних, що включають не лише результати медичних оглядів і лабораторних аналізів, але й дані з мобільних додатків, носимих пристроїв,

систем віддаленого моніторингу пацієнтів. Це створює нову етичну дилему з одного боку, доступ до такої інформації відкриває можливості для більш точної діагностики й прогнозування, а з іншого формує загрозу порушення приватності та автономії людини.

Філософ інформаційного суспільства Floridi L вказує, що процес «дата фікації» людини може призвести до втрати автономності пацієнта та підвищення ризиків дискримінації [18].

Водночас виникають питання щодо алгоритмічної справедливості. Mittelstadt B наголошує, що алгоритмічна упередженість у штучному інтелекті може закріпити нерівність і відтворити дискримінаційні практики в системі охорони здоров'я [19].

Американська дослідниця Nissenbaum H пропонує концепцію «контекстуальної цілісності приватності», яка вимагає, щоб використання даних завжди було прив'язане до конкретного соціального та медичного контексту [20]. Це означає, що згода має бути не лише формальною, але й змістовною, з чітким розумінням пацієнта, у яких саме цілях і яким чином його дані будуть застосовані.

Другим ключовим блоком є кібербезпека, яка стає критично важливою умовою довіри до цифрової медицини. Медичні дані – це одна з найбільш цінних категорій інформації на «чорному ринку» кіберзлочинності, оскільки вони містять не лише ідентифікаційні дані, а й деталі про стан здоров'я, які можуть бути використані для шантажу, дискримінації або фінансового шахрайства.

В Україні кіберризик у сфері цифрової медицини посилюється після початку повномасштабної війни. Медичні реєстри, що містять дані мільйонів громадян, стали потенційними цілями кібератак. Втрата або викрадення такої інформації може мати не лише індивідуальні наслідки для пацієнтів, а й стратегічні наслідки для національної безпеки.

На відміну від України, у країнах ЄС функціонують комплексні механізми кіберзахисту. Зокрема, Директива NIS2 передбачає обов'язкові заходи для секторів критичної інфраструктури, включаючи охорону здоров'я, а GDPR вимагає обов'язкового повідомлення про витік даних упродовж 72 годин. В Естонії діє національна служба CERT, яка спеціалізується на кіберзахисті державних інформаційних систем, включно з медичними реєстрами.

В Україні ж досі немає системної політики кіберстійкості закладів охорони здоров'я. Більшість лікарень не мають спеціалізованих підрозділів IT-безпеки, а протоколи реагування на кіберінциденти залишаються недостатньо розробленими.

Особливістю сучасної цифрової медицини є те, що етичні та безпекові виклики взаємопов'язані. Недостатній рівень кіберзахисту автоматично означає ризик порушення етичних стандартів, оскільки витік даних ставить під загрозу приватність пацієнтів. І навпаки, відсутність чітких етичних норм призводить до безконтрольного збирання та використання даних, що ускладнює формування системи кіберзахисту.

Тому стратегічно важливим для України є формування єдиної політики етико-безпекового регулювання цифрової медицини, яка передбачала б:

- стандарти інформованої згоди;
- аудит алгоритмів штучного інтелекту;
- обов'язкові протоколи кіберзахисту;
- систему моніторингу та реагування на інциденти.

Дослідження міжнародного досвіду підтверджує, що цифрова медицина може стати дієвим інструментом підвищення якості охорони здоров'я, якщо її розвиток базується на трьох складових: системному законодавчому регулюванні, інституційній координації та цифровій інклюзії населення.

Естонія є одним із найуспішніших прикладів цифровізації медицини. Уже у 2008 р. було запроваджено єдину електронну медичну картку для кожного громадянина, яка інтегрована з іншими державними реєстрами через систему X-Road, що забезпечує безпечний обмін даними між установами. Доступ пацієнтів до власної інформації забезпечується через електронний ID, а будь-який вхід до медичної картки фіксується в журналі, що підвищує довіру громадян до системи та знижує ризики корупції.

У Польщі цифрова медицина почала активно розвиватися з впровадженням національної системи eRecepta, яка охопила всі медичні заклади, дане рішення забезпечило уніфікований доступ до ліків і спростило облік фармако-терапії. Подальший розвиток відбувся завдяки системі eSkierowanie (електронні направлення), що забезпечила інтеграцію лікарів первинної та спеціалізованої ланки. Польський досвід доводить, що поетапне впровадження цифрових рішень із чітким фокусом на практичні послуги дає швидкий ефект.

У Великій Британії цифрова медицина координується централізовано через NHS Digital, яка встановлює стандарти інтегрованості, проводить сертифікацію постачальників і впроваджує єдині інформаційні системи. Важливим елементом є NHS Digital Academy, що готує управлінців для цифрової трансформації. Особливий акцент

Таблиця 1

Порівняльна таблиця

Країна / регіон	Правова база	Інституційна модель	Ключові цифрові сервіси	Особливості інклюзії	Кіберзахист
Україна	Конституція (ст. 32, 49); Закон «Про захист персональних даних»; постанова КМУ №411; накази МОЗ; Закон №3301-IX	МОЗ, НСЗУ, Мінцифра; відсутній єдиний координаційний орган	ЕСОЗ, електронні рецепти, телемедицина (обмежено)	Відсутність масштабних програм; значна різниця між містом і селом	Політика кіберстійкості не сформована
Естонія	Закон про електронну медицину (2008)	e-Health Authority; інтеграція з X-Road	Єдина ЕМК, доступ пацієнта через eID	Державні інвестиції в інтернет; програми для літніх	Нац. CERT, суворий аудит
Польща	Законодавство про eRecepta та eSkierowanie	МОЗ Польщі + централізована платформа P1	eRecepta, eSkierowanie, інтегровані реєстри	Загальнонаціональний доступ, навіть у сільських громадах	Перехід до стандартів ЄС
Велика Британія	Законодавство NHS, стандарти DSP Toolkit	NHS Digital – єдиний координатор	NHS Spine, цифрова академія	Програми для вразливих груп (літні, інваліди)	Обов'язковий аудит DSPT
ЄС	GDPR (2016), EHDS (2025)	Health Data Access Bodies у країнах-членах	Єдиний простір даних здоров'я	Європейські програми цифрової інклюзії	NIS2, GDPR-вимоги
США	21st Century Cures Act (2016), ONC rules	ONC, приватні провайдери	Пацієнтські портали, API FHIR	Широке використання мобільних додатків	Приватно-державні стандарти безпеки

робиться на кіберзахисті, кожен медичний заклад зобов'язаний щорічно проходити аудит за стандартами Data Security and Protection Toolkit.

На рівні ЄС визначальними документами є GDPR, який закріплює принципи обробки персональних даних, та новий Європейський простір даних про здоров'я, система забезпечує єдині правила для обміну даними між країнами-членами ЄС, а також створює правові механізми для їх використання в наукових і статистичних цілях. Таким чином, ЄС переходить від національних систем до наднаціональної цифрової екосистеми.

Американська модель акцентує увагу на інтероперабельності. 21st Century Cures Act та нормативи Офісу національного координатора встановили вимоги щодо запобігання «інформаційним блокуванням» і зобов'язали постачальників забезпечити доступ пацієнтів до медичних даних через стандартизовані API. Такий підхід підкреслює принцип «пацієнт власник своїх даних», що може бути корисним і для України.

Міжнародна практика свідчить, що ключовими умовами успішної цифровізації є:

1. Наявність єдиної правової рамки (GDPR, EHDS, 21st Century Cures Act).

2. Централізована інституційна координація (NHS Digital, gematik, e-Health Authority).

3. Програми цифрової інклюзії, які ліквідують розрив між містом і селом.

4. Системна підготовка кадрів (курси з цифрових компетентностей, спеціалізовані академії).

5. Кіберстійкість та етика як базові елементи довіри до системи.

Для України це означає, що без прийняття рамкового закону «Про цифрову медицину», створення координаційного органу та запуску програм цифрової інклюзії реформу буде складно реалізувати.

**Висновки.** Проведене дослідження засвідчило, що державна політика у сфері охорони здоров'я в умовах цифрової трансформації стикається з комплексом викликів, які охоплюють правові, інституційні, соціально-економічні та етико-безпекові виміри. Аналіз показав, що:

1. Нормативно-правова база України є фрагментарною та реактивною. Попри ухвалення низки законів і підзаконних актів, зокрема Закону № 3301-IX, постанови КМУ № 411, наказів МОЗ, досі відсутній єдиний рамковий Закон «Про цифрову медицину», який би інтегрував усі аспекти розвитку галузі та забезпечив гармонізацію з європейським правом.

2. Інституційне забезпечення цифрової медицини характеризується розпорошеністю функцій між МОЗ, НСЗУ, Мінцифрою та місцевим самоврядуванням, що зумовлює дублювання повноважень та «цифрову асиметрію» між регіонами. Порівняння з досвідом Німеччини, Великої Британії та Естонії підтверджує ефективність централізованих моделей координації.

3. Соціально-економічні виклики проявляються у цифровій нерівності (місто ↔ село, молодь ↔ літні люди) та кадровому дефіциті цифрових компетентностей у медичних працівників. Відсутність системної підготовки кадрів знижує ефективність використання навіть тих цифрових інструментів, які вже впроваджені.

4. Етичні та безпекові виклики пов'язані з обробкою великих масивів медичних даних, ризиком алгоритмічної упередженості та кіберзагрозами. В умовах воєнного стану кіберстійкість медичних закладів набуває стратегічного значення як елемент національної безпеки.

5. Міжнародний досвід Естонія, Польща, Велика Британія, ЄС, США свідчить, що успішна цифровізація медицини базується на трьох ключових чинниках: системному правовому регулюванні, централізованій інституційній координації та програмах цифрової інклюзії.

Наукова новизна дослідження полягає у комплексному розгляді цифрової медицини як багатовимірного феномена, що поєднує правові, інституційні, соціально-економічні та етико-безпекові аспекти. Уперше в українському контексті обґрунтовано:

- необхідність ухвалення рамкового Закону «Про цифрову медицину»;
- доцільність створення єдиного координаційного органу при Кабінеті Міністрів;
- трактування цифрової інклюзії та кіберстійкості як стратегічних пріоритетів державної політики у сфері охорони здоров'я.

Практичне значення результатів дослідження полягає в тому, що вони можуть бути використані для розробки нових нормативно-правових актів, формування освітніх програм для медичних працівників, створення державних програм цифрової інклюзії та розбудови системи кіберзахисту у сфері охорони здоров'я.

Таким чином, цифрова медицина має стати не лише інструментом модернізації медичної сфери, але й потужним драйвером розвитку державної політики у сфері охорони здоров'я, що поєднує інновації з принципами доступності, безпеки та справедливості.

#### ЛІТЕРАТУРА:

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-ВР> (дата звернення: 01.10.2025).
2. Основи законодавства України про охорону здоров'я : Закон України від 19 листоп. 1992 р. URL: <https://zakon.rada.gov.ua/laws/show/2801-12> (дата звернення: 01.10.2025).
3. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 01.10.2025).
4. Деякі питання електронної системи охорони здоров'я : Постанова Кабінету Міністрів України від 25 квіт. 2018 р. № 411. URL: <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF> (дата звернення: 01.10.2025).
5. Про затвердження Порядку застосування телемедицини у закладах охорони здоров'я : Наказ МОЗ України від 19 жовт. 2015 р. № 681. URL: <https://zakon.rada.gov.ua/laws/show/z1400-15> (дата звернення: 01.10.2025).
6. Про організацію надання медичної допомоги із застосуванням телемедицини в умовах воєнного стану : Наказ МОЗ України від 20 черв. 2022 р. № 1062. URL: <https://zakon.rada.gov.ua/go/z0728-22> (дата звернення: 01.10.2025).
7. Про затвердження Порядку надання медичної та/або реабілітаційної допомоги із застосуванням телемедицини на період дії воєнного стану : Наказ МОЗ України від 17 верес. 2022 р. № 1695. URL: <https://zakon.rada.gov.ua/go/z1155-22> (дата звернення: 01.10.2025).
8. Про внесення змін до деяких законодавчих актів України щодо функціонування телемедицини : Закон України від 29 черв. 2023 р. № 3301-IX. URL: <https://zakon.rada.gov.ua/laws/show/3301-20> (дата звернення: 01.10.2025).
9. Про схвалення Стратегії розвитку телемедицини до 2025 року : Розпорядження Кабінету Міністрів України від 14 лип. 2023 р. № 625-р. URL: <https://zakon.rada.gov.ua/laws/show/625-2023-p#-Text> (дата звернення: 01.10.2025).
10. Malakhov K. S., et al. Insight into the Digital Health System of Ukraine (eHealth): Trends, Definitions, Standards, and Legislative Revisions. *Biomedicines*. 2023. Vol. 11 (12). P. 3271.
11. Kotenko S., Bohnhardt A. Digital Transformation of Healthcare in Ukraine: Challenges and Prospects. *Health Policy and Technology*. 2022. Vol. 11 (4). P. 100684.
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 01.10.2025).
13. European Commission. Proposal for a Regulation on the European Health Data Space (EHDS). 2022. URL: <https://health.ec.europa.eu/ehealth-digital->

health-and-care/european-health-data-space\_en (дата звернення: 01.10.2025).

14. Jayathissa R., Hewapathirana R. Interoperability Challenges in Health Information Systems in Low- and Middle-Income Countries. *Journal of Health Informatics in Developing Countries*. 2021. Vol. 15 (2).

15. Baker R. Telemedicine and Health Inequalities: Risks and Opportunities. *Journal of Medical Internet Research*. 2021. Vol. 23 (4). P. e27130.

16. Dickey C., Wasko M. Telemedicine Adoption and Digital Literacy: A Patient-Centered Perspective. *BMC Health Services Research*. 2023. Vol. 23. Article 450.

17. Ladin K., Portz J., Miake-Lye I., et al. Older Adults' Experiences with Telemedicine during COVID-19: Equity, Access, and Quality of Care. *JAMA Network Open*. 2021. Vol. 4 (12). P. e2137675.

18. Floridi L. The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford : Oxford University Press, 2019. 256 p.

19. Mittelstadt B. Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*. 2019. Vol. 1. P. 501–507.

20. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford : Stanford University Press, 2010. 304 p.

Дата першого надходження рукопису до видання: 26.09.2025  
 Дата прийнятого до друку рукопису після рецензування: 30.10.2025  
 Дата публікації: 25.11.2025