МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ДМИТРЕНКО ІГОР АНАТОЛІЙОВИЧ

УДК: 351.88; 343.35

ДЕРЖАВНЕ УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

Спеціальність 25.00.02 – механізми державного управління

(25 – державне управління)

РЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора наук з державного управління

Житомир – 2026

Робота виконана в Державному університеті «Житомирська політехніка» Міністерства освіти і науки України

Науковий консультант доктор наук з державного управління,
доктор економічних наук, професор,
Заслужений економіст України
ГРИЦИШЕН Димитрій Олександрович,
Державний університет «Житомирська політехніка»,
перший проректор

Офіційні опоненти: доктор наук з державного управління, доцент,
ВАКУН Оксана Володимирівна,
Івано-Франківський навчально-науковий інститут менеджменту Західноукраїнського національного університету,
доцент кафедри управління та адміністрування

доктор наук з державного управління, професор,
АНТОНОВА Людмила Володимирівна,
Чорноморський національний університет імені Петра Могили,
професор кафедри обліку і аудиту

доктор наук з державного управління, старший науковий співробітник,
ДРАГАН Ірина Василівна,
ЗВО «Університет трансформації майбутнього»,
професор кафедри бізнесу, адміністрування та права

Захист відбудеться «29» серпня 2026 року об «11-00» годині на засіданні Спеціалізованої вченої ради Д 14.052.03 в Державному університеті «Житомирська політехніка» за адресою: 10005, м. Житомир, вул. Чуднівська, 103, конференц-зала.

З дисертацією можна ознайомитись у бібліотеці Державного університету «Житомирська політехніка» за адресою: 10005, м. Житомир, вул. Чуднівська, 103

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Цифрова трансформація системи охорони здоров'я є пріоритетною сферою державної політики з декількох причин: по-перше, більшість суспільних процесів відбуваються в цифровому середовищі; по-друге, без цифрової трансформації неможливо в повному обсязі виконати євроінтеграційні вимоги; по-третє, цифрова трансформація дозволить підвищити якість медичних послуг та зменшити вплив територіальної віддаленості та охопити більшу частину населення; по-четверте, впровадження цифрових технологій підвищує ефективність управління системою охорони здоров'я. До цифрової трансформації системи охорони здоров'я у світі прикута увага політиків, вчених, бізнесу, користувачів, що зумовлено сукупністю причин:

- *динамічне зростання ринку цифрової охорони здоров'я*[1]. Цифрова охорона здоров'я сьогодні стала повноцінним міжнародним ринком послуг, вартість якого оцінюється в 347,4 млрд доларів США, в той же час за прогнозами він зросте з 420,2 млрд доларів США у 2026 році до 1830,4 млрд доларів США до 2033 року, зі середньорічним темпом зростання 23,4% з 2026 по 2033 рік.

- *збільшення інвестицій та диверсифікація фінансових інструментів щодо фінансування цифрової трансформації системи охорони здоров'я*[2]. Венчурне фінансування цифрової охорони здоров'я, що складається як з корпоративного венчурного капіталу, так і з приватного капіталу, вже досягло 14,8 мільярда доларів у 2020 році порівняно з 8,9 мільярда доларів у 2019 році, що показує загальне зростання на 66%.

- *активізація використання технологій штучного інтелекту в медицині*[3]. Ринок штучного інтелекту в системі охорони здоров'я оцінюється у 37-56 млрд. доларів, з рекордним середньорічним темпом зростання близько 35-49 % та прогнозом 740–1000 млрд. доларів до середини 2030-х років.

- *залученість населення світу до цифрової системи охорони здоров'я*[4]. У світових магазинах додатків (App Store та Google Play) доступно понад 350 000 додатків категорії Health & Fitness, а сукупна аудиторія регулярних користувачів мобільного здоров'я перевищує 1,8 млрд осіб по всьому світу.

На сьогодні Україна зробила значні кроки в цифровізації системи охорони здоров'я, особливо в техніко-технологічному забезпеченні (понад 35 млн українців внесено до електронної системи охорони здоров'я (ЕСОЗ) та мають

---

[1] Digital Health Market Size, Share & Trends Analysis Report By Technology (Tele-healthcare, mHealth, Healthcare Analytics, Digital Health Systems), By Component, By Application, By End-use, By Region, And Segment Forecasts 2026–2033. Grand View Research. URL: https://www.grandviewresearch.com/industry-analysis/digital-health-market (date of access: 27.04.2026).

[2] Digital Health Market Size, Share and Trends Analysis Report By Technology (Telehealthcare, mHealth, Healthcare Analytics, Digital Health Systems), By Component, By Application, By End-use, By Region, And Segment Forecasts 2026–2035. Precedence Research. URL: https://www.precedenceresearch.com/digital-health-market (date of access: 27.04.2026).

[3] Artificial Intelligence in Healthcare Market Size, Share & COVID-19 Impact Analysis, By Component, By Application, By End-user, and Regional Forecast 2026–2034. Fortune Business Insights. Report ID: 100534. URL: https://www.fortunebusinessinsights.com/industry-reports/artificial-intelligence-in-healthcare-market-100534 (date of access: 27.04.2026).

[4] Global Observatory for eHealth. World Health Organization. URL: https://www.who.int/observatories/global-observatory-for-ehealth (date of access: 27.04.2026).

підписані декларації з сімейними лікарями[5]). Проте залишається невирішеною сукупність проблем, що пов'язанні із правовим регулювання, забезпечення безпеки, впровадженням технологій штучного інтелекту, кадровим потенціалом, євроінтеграційними процесами.

Питання цифрової трансформації системи охорони здоров'я розглядалися багатьма вітчизняними вченими, серед яких: Александренко Г.Д., Антонова Л.В., Андрєєв Є.В., Баштанник О.В., Білинська М.М., Бачук О.Р., Вакун О.В., Грицишен Д.О., Гуща Т.К., Драган І.В., Драган І.О., Запорожець Т.В., Карамишев Д.В., Криничко Л.Р., Костров В.О., Ксендзук В.В., Криничко Ф.Р., Крикун О.Д., Курбанов А.К., Малігон Ю.В., Мотайло О.В., Миронов А.Г., Музика-Стефанчук О.А., Миргород-Карпова В.В., Опанасюк М.О., Олійник М.О., Орлова Н.С., Петрик С.М., Радиш Я.Ф., Руденко Р.І., Сергієнко Л.В., Свірко С.В., Старинський М.В., Стефанчук М.О., Тишко Д.Ф., Шпак Ю.В., Шлапко Т.В., Юнгер В.І., Якимчук Н.Я. та інші.

Значні досягнення щодо наукового обґрунтування розвитку процесів цифрової трансформації системи охорони здоров'я містяться в працях зарубіжних вчених: Федеріко Фонда (Federico Fonda), Алессандро Галацці (Alessandro Galazzi), Стефанія К'яппінотто (Stefania Chiappinotto), Лінда Юсті (Linda Justi), Мортен Сьондерсков Фрюденсберг (Morten Sønderskov Frydensberg), Ранді Леманн Боесен (Randi Lehmann Boesen), Мірна Мацур (Mirna Macur), Ерік Андрес Рейг (Erik Andrés Reig), Елісенда Рейшак Еспаульєлья (Elisenda Reixach Espaulella), Альвіза Палезе (Alvisa Palese), Давід Майхерек (Dawid Majcherek), Скотт Вільям Гегерті (Scott William Hegerty), Аркадіуш Міхал Ковальський (Arkadiusz Michał Kowalski), Малгожата Стефанія Левандовська (Małgorzata Stefania Lewandowska), Десіслава Дікова (Desislava Dikova), Ерік Балтаксе (Erik Baltaxe), Томас Ципіонка (Thomas Czypionka), Маркус Краус (Markus Kraus), Міріам Райс (Miriam Reiss), Ян Ерік Аскільдсен (Jan Erik Askildsen), Рената Гренкович (Renata Grenkovic), Торд Скогедаль Лінден (Tord Skogedal Lindén), Янош Дьордь Піттер (János György Pitter), Морін Руттен-ван Молкен (Maureen Rutten-van Molken), Оскар Соланс (Oscar Solans), Верена Штрукманн (Verena Struckmann), Жузеп Рока (Josep Roca), Ісаак Кано (Isaac Cano), Марія Габріелла Мелькіорре (Maria Gabriella Melchiorre), Роберта Папа (Roberta Papa), Міке Райкенс (Mieke Rijken), Евaут ван Гіннекен (Ewout van Ginneken), Аннелі Хуяла (Anneli Hujala), Франческо Барбабелла (Francesco Barbabella), Ганс Генрі П. Клуге (Hans Henri P. Kluge), Наташа Аццопарді-Мускат (Natasha Azzopardi-Muscat), Давід Новільйо-Ортіс (David Novillo-Ortiz), Алессандро Вінчі (Alessandro Vinci), Андреа Ванделлі (Andrea Vandelli), Алессія Капуто (Alessia Caputo), Мілена Вайньєрі (Milena Vainieri), Розанна Тарріконе (Rosanna Tarricone), Франческо Петракка (Francesco Petracca), Ганна-Марія Веллер (Hannah-Marie Weller), Стефано Дженовезе (Stefano Genovese), Рафаель Бенгоа (Rafael Bengoa), Джон Бовіс (John Bowis), Мері Гарні (Mary Harney),

[5] Electronic Health Records Market Size, Share and Trends Analysis Report By Technology, By Component, By Application, By End-use, By Region, And Segment Forecasts 2026–2033. Persistence Market Research. URL: https://www.persistencemarketresearch.com/market-research/electronic-health-records-market.asp (date of access: 27.04.2026).

Бастіан Гаук (Bastian Hauck), Мішель Пенже (Michel Pinget), Майк Лірс (Mike Leers), Тар'я Стенвалл (Tarja Stenvall), Нік Гюлдемонд (Nick Guldemond), Луція Мокра (Lucia Mokrá) та інші.

Попри наявність значної кількості наукових досліджень, присвячених вирішенню проблем державного управління цифровою трансформацією системи охорони здоров'я, на сьогодні невирішеною залишається сукупність проблем теоретичного та методологічного характеру: 1) питання структури та змістовного наповнення передумов і факторів розвитку цифрової трансформації системи охорони здоров'я як об'єкта державного управління; 2) методологічні положення державного управління цифровою трансформацією системи охорони здоров'я в контексті зміни її властивостей; 3) вплив євроінтеграційних процесів та визначення євроінтеграційних імперативів державного управління цифровою трансформацією системи охорони здоров'я; 4) впровадження механізмів державного регулювання використання технологій штучного інтелекту в Україні; 5) забезпечення безпеки процесів цифрової трансформації системи охорони здоров'я.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана відповідно до плану науково-дослідних робіт Державного університету «Житомирська політехніка» за темою: «Інноваційні механізми публічного управління та адміністрування» (державна реєстрація № 0121U111051). У межах тем автором проведені дослідження, пов'язані з розробкою методологічних та організаційних положень державного управління цифровою трансформацією системи охорони здоров'я.

Мета і завдання дослідження. Мета дисертації полягає в обґрунтуванні теоретичних, методологічних та організаційних положень, а також розробці практичних рекомендацій щодо розвитку механізмів державного управління цифровою трансформацією системи охорони здоров'я.

Завдання наукового дослідження:

- ідентифікувати передумови та фактори розвитку цифрової трансформації системи охорони здоров'я як об'єкту державного управління;

– здійснити оцінку публікаційної активності вітчизняних та зарубіжних вчених з проблем цифрової трансформації системи охорони здоров'я як об'єкту державного управління;

– обґрунтувати склад та змістовні властивості понятійно-категоріального апарату державного управління цифровою трансформацією системи охорони здоров'я;

– визначити вплив цифрової трансформації на властивості системи охорони здоров'я та процес прийняття державно-управлінських рішень;

- розробити систему принципів державного управління цифровою трансформацією системи охорони здоров'я;

- розвинути методологічні положення державного управління цифровою трансформацією системи охорони здоров'я;

- ідентифікувати та визначити вплив на національну правову систему вимог Європейського Союзу (ЄС) до цифрової трансформації системи охорони здоров'я;

- оцінити вимоги ЄС до безпеки процесів цифрової трансформації системи охорони здоров'я;

- вивчити особливості державного управління цифровою трансформацією в країнах-членах Європейського Союзу;

- розробити механізми адаптації державного управління цифровою трансформацією системи охорони здоров'я до вимог Європейського Союзу;

- розробити положення державного регулювання використання технологій штучного інтелекту в процесі надання медичної допомоги та реалізації медичних послуг;

- розробити механізм розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров'я.

Об'єкт дослідження – процеси цифрової трансформації системи охорони здоров'я в умовах євроінтеграції.

Предмет дослідження – теоретичні, методологічні та організаційні положення державного управління процесами цифрової трансформації системи охорони здоров'я в умовах євроінтеграції.

Методи дослідження. Методологічну основу дослідження становлять загальнонаукові та спеціальні методи аналізу суспільних явищ і процесів. З огляду на міждисциплінарний характер об'єкта дослідження застосовано комплекс методів, які дозволили повною мірою обґрунтувати теоретичні, методологічні, організаційні положення, а також надати практичні рекомендації щодо розвитку механізмів державного управління цифровою трансформацією системи охорони здоров'я. Методи бібліометричного та бібліографічного аналізу застосовано для дослідження й оцінки становлення наукового знання про цифрову трансформацію системи охорони здоров'я (п. 1.2). Обґрунтування передумов та факторів цифрової трансформації системи охорони здоров'я (п. 1.1) та обґрунтування розвитку понятійно-категоріального апарату за об'єктом дослідження (п. 1.3) здійснено шляхом застосування методів теоретичного узагальнення, систематизації, групування, абстрагування та аналогії. Для структуризації властивостей системи охорони здоров'я в умовах цифрової трансформації (п. 2.1) та розробки системи принципів державного управління цифровою трансформацією системи охорони здоров'я (2.2) використано методи моделювання, аналогії, систематизації та узагальнення, структуризації, аналізу та синтезу. Розроблено методологічні положення державного управління цифровою трансформацією системи охорони здоров'я (п. 2.3), що ґрунтуються на використанні методів моделювання, порівняння, індукції та дедукції, правового аналізу, аналогії, аналізу та синтезу. Методи статистичного спостереження та економічного аналізу були використані для оцінки сучасного стану процесів цифрової трансформації у світі, Європейському Союзі та Україні (п. 3.1, 3.2, 3.3). Методи правового аналізу, систематизації, аналогії, структуризації, аналізу та синтезу використано для оцінки вимог ЄС до цифрової трансформації системи охорони здоров'я та розробки комплексного механізму адаптації (п. 5.1), розробки системи правового регулювання використання технологій штучного інтелекту (п. 5.2) та обґрунтування напрямів розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров'я.

Інформаційною базою дослідження стали наукові джерела (монографічні праці, наукові статті вітчизняних і зарубіжних вчених із проблем охорони здоров'я; матеріали науково-практичних конференцій та семінарів); офіційні документи (нормативні документи України, країн ЄС та Парламенту ЄС, що регулюють питання цифрової трансформації охорони здоров'я); матеріали міжнародних наукометричних баз даних Scopus і WoS; статистичні матеріали міжнародної бази даних STATISTA; довідкові та інформаційні видання міжнародних організацій тощо.

Використання технологій штучного інтелекту. Технології штучного інтелекту (ChatGPT, Gemini, Claude) використовувалися для: 1) пошукових цілей при вивченні системи правового регулювання цифрової трансформації системи охорони здоров'я ЄС; 2) перекладу нормативно-правових актів ЄС та країн-членів; 3) оцінки структури, логіки тексту та пошуку граматичних і орфографічних помилок. Технології штучного інтелекту не використовувалися для генерування тексту.

Наукова новизна одержаних результатів полягає в обґрунтуванні теоретичних, методологічних та організаційних положень державного управління цифровою трансформацією системи охорони здоров'я в умовах євроінтеграційних процесів.

Основні положення наукової новизни.

вперше одержано:

- механізм адаптації державного управління цифровою трансформацією системи охорони здоров'я до положень регламентів та директив ЄС, що спрямований на подолання суттєвого розриву між наявною інфраструктурою цифрової системи охорони здоров'я і європейськими нормами та передбачає: 1) впровадження нових нормативно-правових актів (Закону України «Про захист персональних даних»; Закон України «Про обіг медичних даних», Рамковий Закон України «Про штучний інтелект»; Закон України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації»; Закон України «Про управління даними»; Закон України «Про цифрові послуги»); 2) зміни до законодавчих актів (Закон України «Основи законодавства України про охорону здоров'я»; Закон України «Про захист інформації в інформаційно-комунікаційних системах»; Закон України «Про захист економічної конкуренції»); 3) оновлення підзаконних нормативно-правових актів (Технічних регламентів щодо медичних виробів; Порядків класифікації ШІ-систем і проведення DPIA); 4) вектори трансформації інституційної структури державного управління;

- структуру державно-регуляторної діяльності щодо використання технологій штучного інтелекту в медицині, що полягає в сукупності змін до нормативно-правових актів, адаптованих до Регламентів ЄС, та передбачає: правове забезпечення (класифікацію ризиків, сертифікацію, безпеку та якість даних, етичні положення, порядок забезпечення прозорості, постійного моніторингу та людського контролю; встановлення відповідальності користувачів) та інституційне забезпечення (утворення спеціалізованого суб'єкта виконавчої влади, що реалізує державну політику в сфері технологій штучного інтелекту);

- комплексний механізм розширення інституційної спроможності державного управління забезпечення безпеки процесів цифрової трансформації, що полягає в утворенні спеціалізованих суб'єктів виконавчої влади, що реалізують державну політику в сфері інформаційної безпеки (Національного агентства з доступу до медичних даних (HDAB Ukraine), Національного регулятора у сфері штучного інтелекту, Національного центру кібербезпеки цифрової системи охорони здоров'я), також відповідних спеціалізованих структурних підрозділів у системі органів державного управління та розширення повноважень існуючих суб'єктів у сферах захисту персональних даних, ринкового нагляду за ШІ-медичними виробами та регулювання цифрових ринків;

удосконалено:

- структуру системи принципів державного управління цифровою трансформацією системи охорони здоров'я, що передбачає: 1) їх поділ на стратегічні принципи, принципи організації, принципи цифрового функціонування та принципи забезпечення; 2) визначення змісту кожного принципу та особливості їх дотримання при цифровій трансформації системи охорони здоров'я, що дало можливість розширити теоретико-методологічні положення та визначити вектори розвитку державної політики;

- понятійний апарат державного управління цифровою трансформацією системи охорони здоров'я через уточнення змісту: система охорони здоров'я (багаторівнева соціально-економічної система, що об'єднує взаємопов'язані суб'єкти (суб'єкти державного регіонального, місцевого управління, заклади охорони здоров'я, виробників та постачальників ліків, наукові установи, заклади вищої освіти, інститути громадського суспільства та інші), ресурси, інфраструктуру та процеси (управлінські, медичні (профілактики, діагностування, лікування, реабілітація), організаційні, інформаційні, регламентаційні), функціонування якої регулюється державою та спрямоване на формування, збереження, зміцнення та відновлення здоров'я населення та забезпечення високого рівня громадського здоров'я як складової соціальної функції), цифрова трансформація (цілеспрямований, керований і комплексний процес якісної зміни властивостей, структури, функцій, процесів, моделей взаємодії та способів функціонування певного об'єкта шляхом системного впровадження й використання цифрових технологій, даних та цифрових рішень, що приводить до формування його нового стану і потребує відповідних організаційних, інституційних, правових, кадрових та ресурсних змін) та цифрова трансформація системи охорони здоров'я (цілеспрямований, комплексний і керований процес якісної зміни структури, властивостей, функцій, процесів, механізмів державного управління, моделей взаємодії суб'єктів та способів реалізації медичних послуг шляхом системного впровадження цифрових технологій, цифрових даних і цифрових сервісів, результатом якого є формування цифрової системи охорони здоров'я, здатної забезпечити більш ефективне, доступне, безпечне, інтегроване та людиноцентричне функціонування сфери охорони здоров'я);

- методологічні положення державного управління цифровою трансформацією системи охорони здоров'я, що сформовані з урахуванням техніко-технологічні особливості цифровізації, євроінтеграційні процеси, національні

політико-правові традиції та включають змістовне наповнення об'єктно-предметного поля, визначення функціональних складових через мету і завдання, змістовне наповнення, порядок формування та реалізації правового, інформаційного, організаційного, фінансового та кадрового механізмів;

набуло подальшого розвитку:

- обґрунтування сукупності факторів впливу на формування та реалізацію державно-управлінських рішень в сфері цифрової трансформації системи охорони здоров'я, що включають: 1) політико-правові (правові, політичні, євроінтеграційні) - визначають особливості легітимізації цифрових практик та гармонізації їх із європейськими стандартами; 2) ресурсні (фінансові, кадрові, інфраструктурні, техніко-технологічні) - створюють матеріальний і технологічний фундамент реформи та забезпечують комплексність досягнення цілей цифрової трансформації; 3) державно-управлінські (інституційні, організаційні, інформаційні) - визначають керованість, узгодженість дій суб'єктів державного управління та якість прийняття рішень на основі даних; безпекові (інформаційно-безпекові, кібербезпекові, медико-безпекові) – забезпечення життєздатності, захищеності та безперервності функціонування медичної системи в умовах криз та загроз;

- обґрунтування властивостей системи охорони здоров'я, яка об'єднує її базові соціально-економічні характеристики та параметри розвитку, зокрема встановлено, що цифрова трансформація якісно змінює ці властивості, наділяючи систему новими перевагами (інтероперабельність, прогностичність, масштабованість) та викликами (кібер-, технологічна та інфраструктурна залежності) та доведено, що цифровізація вимагає від держави не лише технічних рішень, а й комплексної трансформації управління (фінансового, правового та організаційного забезпечення);

- обґрунтування стратегічних імперативів державного управління цифровою трансформацією системи охорони здоров'я на основі систематизації глобальних тенденцій цифровізації (аналіз міжнародних індексів (EGDI, Digital Health Index, GDHM)) та визначення переходу від технологічно орієнтованої до людиноцентричної моделі управління через забезпечення стійкості, ефективності, інтероперабельності, безпеки функціонування цифрових систем охорони здоров'я;

- періодизація та обґрунтування еволюції нормативно-правового регулювання цифрової трансформації охорони здоров'я в ЄС , що, на відміну від наявних підходів, систематизує цей процес за чотирма етапами (від фрагментарних експериментальних проєктів 1990-х років до сучасної повномасштабної цифрової інтеграції на базі Регламенту про Європейський простір даних охорони здоров'я, AI Act та GDPR) та виявлення системних ризиків регуляторного перевантаження й фрагментації правозастосування, що має бути враховано при розробці державної політики.

- обґрунтування напрямів адаптації державного управління безпекою процесів цифрової трансформації системи охорони здоров'я до норм ЄС (MDR, IVDR, NIS2, Cybersecurity Act, CRA) через гармонізацію нормативно-правових актів, розширення мережі органів оцінки відповідності, підготовки кваліфікованих кадрів та централізованого захисту медичних реєстрів і цифрових сервісів;

- порівняльно-правове дослідження зарубіжних моделей публічного управління та нормативно-інституційного забезпечення цифрової трансформації охорони здоров'я (на прикладі Бельгії, Данії та Естонії), яке, на відміну від існуючих підходів, систематизує інституційно-інфраструктурні особливості кожного підходу (децентралізовано-мережевого бельгійського, централізовано-координаційного данського та системно-інтегрованого естонського) й обґрунтовує адаптаційні орієнтири для України, що передбачають розмежування повноважень між регуляторними органами, розбудову сумісної цифрової інфраструктури медичних даних, посилення секторної кібербезпеки та впровадження правових механізмів безпечного застосування штучного інтелекту.

Практичне значення одержаних результатів. Результати, що полягають в удосконаленні механізмів державного управління цифровою трансформацією системи охорони здоров'я використані в практичній діяльності органів державної влади та місцевого самоврядування в межах їхніх повноважень, визначених законодавством. Окремі положення також були застосовані в процесі підготовки фахівців із публічного управління та адміністрування.

Особистий внесок здобувача. Дисертація є самостійно виконаним науковим дослідженням. Розробки, висновки та пропозиції, що містяться в роботі, належать особисто автору. З наукових праць, опублікованих у співавторстві, у дисертації використано лише ті положення, які є результатом особистої роботи здобувача, що полягає у вивченні комплексу питань, пов'язаних із державним управлінням цифровою трансформацією системи охорони здоров'я.

Апробація результатів дисертації. Основні положення дослідження, які викладені в дисертації, доповідалися, обговорювалися та отримали позитивну оцінку на 10 міжнародних та всеукраїнських наукових і науково-практичних конференціях, що відображено в публікаціях [25–33].

Публікації. Основні положення дисертаційної роботи опубліковано в 33 наукових працях, із них: дві монографії (одна одноосібна), 7 статей у зарубіжних виданнях, що включенні до міжнародних наукометричних баз даних Scopus та WoS, 15 статей у наукових фахових виданнях України, 9 тез доповідей на міжнародних та всеукраїнських конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, п'яти розділів, висновків, списку використаних джерел та додатків. Основний зміст викладено на 369 сторінках друкованого тексту. Робота містить 15 таблиць та 43 рисунків. Список використаних джерел нараховує 282 найменувань, розміщених на 36 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дослідження, визначено стан її наукової розробки, розкрито зв'язок з науковими програмами, планами, темами, визначено мету, завдання, об'єкт, предмет і методи дослідження, наукову новизну та практичне значення отриманих результатів, наведено відомості про їх апробацію.

У першому розділі **«Теоретичні положення державного управління цифровою трансформацією системи охорони здоров'я»** обґрунтовано передумови, факторну базу, джерельний фундамент та понятійно-категоріальний апарат дослідження.

Систематизація факторів впливу засвідчує, що цифрова трансформація системи охорони здоров’я детермінується сукупністю зовнішніх суспільних викликів та внутрішніх інституційно-ресурсних спроможностей держави (табл. 1). Зовнішнє середовище - зокрема соціальні, демографічні, медичні та економічні чинники (старіння нації, депопуляція, зростання рівня хронічних захворювань та зниження доходів населення) виступає первинним каталізатором змін. Ці чинники формують підвищений попит на дистанційний догляд, оптимізацію мережі закладів і моніторинг здоров'я, змушуючи державні органи прискорювати цифровізацію для збереження доступності та якості медичної допомоги.

Успішність реалізації відповідних державно-управлінських рішень безпосередньо залежить від внутрішнього середовища, де політико-правові та ресурсні фактори створюють нормативно-процесуальне підґрунтя й практичну базу реформ. Гармонізація законодавства з вимогами ЄС та стратегічна наступність державної політики задають вектор розвитку, тоді як фінансове забезпечення, розбудова інфраструктури, техніко-технологічний інструментарій і цифрові компетентності кадрів є матеріальним двигуном змін. Водночас державно-управлінські чинники (інституційні, організаційні та інформаційні) визначають спроможність суб’єктів владних повноважень ефективно координувати процеси, адаптувати процедури та забезпечувати аналітичний супровід прийняття рішень.

Окремим критичним виміром у структурі факторів є безпековий блок, що поєднує інформаційну, кібернетичну та медичну безпеку. Зростаюча цифровізація медичних даних та інфраструктури генерує нові ризики для конфіденційності, цілісності інформації та безперервності надання допомоги, що перетворює кіберзахист і медико-безпекові гарантії на складник національної безпеки. Відтак, ефективне державне управління цифровою трансформацією медицини вимагає застосування цілісного, ризик-орієнтованого підходу, який балансує між прискореним впровадженням інновацій і жорсткими вимогами до безпеки даних, інфраструктури та пацієнтів.

Бібліометричний аналіз публікацій у Scopus за запитом «digital healthcare systems» засвідчив стрімке зростання наукового інтересу до цієї тематики після 2020 року (рис. 1). Ключові дослідження зосереджені на застосуванні штучного інтелекту, машинному навчанні, розвитку телемедицини, електронних медичних записів та кібербезпеці. Міждисциплінарний характер проблеми підтверджується переважанням публікацій у галузях комп’ютерних наук, інженерії та медицини. Лідерами за кількістю праць, цитувань і міжнародною співпрацею є Індія, США, Південна Корея, Велика Британія, Австралія та Китай, де активну підтримку надають державні фонди. Подальші вишукування доцільно спрямувати на безпеку штучного інтелекту, сумісність цифрових платформ, захист даних та оцінку ефективності впроваджених рішень.

Встановлено відсутність єдиного підходу до розуміння понять, які характеризують державне управління цифровою трансформацією системи охорони здоров’я. Більшість наукових підходів та нормативне визначення трактують охорону здоров’я переважно як систему заходів, спрямованих на збереження, зміцнення та відновлення здоров’я населення.

Таблиця 1. Характеристика факторів впливу на формування та реалізацію державно-управлінських рішень в сфері цифрової трансформації системи охорони здоров'я

<table>
<tr><th colspan="3">ФАКТОРИ, ЩО ОБУМОВЛЕННІ ЗОВНІШНІМ СЕРЕДОВИЩЕМ</th></tr>
<tr><td colspan="3">СУСПІЛЬНІ ФАКТОРИ</td></tr>
<tr><td>Соціальні</td><td colspan="2">Демографічні</td></tr>
<tr><td>- сукупність умов соціокультурного середовища та поведінкових патернів населення (рівень стресогенності суспільства, шкідливі звички, малорухливий спосіб життя, цифрова залежність, соціальна ізоляція), які безпосередньо детермінують погіршення стану громадського здоров'я (спричиняючи розлади ментальної сфери, ожиріння, гіподинамію) та змушують державні органи прискорювати цифровізацію системи охорони здоров'я</td><td colspan="2">- кількісні та структурні зміни в складі населення (старіння нації, депопуляція, внутрішня та зовнішня міграція), які докорінно змінюють віковий і територіальний профіль громадського здоров'я, створюють географічні дисбаланси в доступі до медицини та змушують державу прискорено впроваджувати цифрові рішення для дистанційного догляду та оптимізації медичної інфраструктури</td></tr>
<tr><td>Медичні</td><td colspan="2">Економічні</td></tr>
<tr><td>- зміна показників здоров'я нації (зростання хронічних хвороб, тривалість та складність перебігу захворювань), що створює надмірне фізичне навантаження на мережу лікарень і змушує державу впроваджувати цифрові системи для безперервного дистанційного моніторингу пацієнтів та профілактики хвороби</td><td colspan="2">- фінансово-макроекономічні умови життєдіяльності суспільства (рівень доходів, інфляція, безробіття), погіршення яких обмежує доступ громадян до якісного харчування, ліків та здорового способу життя, що призводить до стрімкого зниження громадського здоров'я та змушує прискорювати цифровізацію системи охорони здоров'я</td></tr>
<tr><th colspan="3">ФАКТОРИ, ЩО ОБУМОВЛЕННІ ВНУТРІШНІМ СЕРЕДОВИЩЕМ</th></tr>
<tr><td colspan="3">ПОЛІТИКО-ПРАВОВІ ФАКТОРИ</td></tr>
<tr><td>Правові</td><td>Міжнародні (євроінтеграційні)</td><td>Політичні</td></tr>
<tr><td>- пов'язані із формуванням нормативно-правового середовища цифрової трансформації, забезпеченням прав людини, захистом персональних даних, медичної таємниці, етичним використанням цифрових технологій і систем штучного інтелекту</td><td>- визначають необхідність гармонізації цифрової трансформації системи охорони здоров'я з політикою Європейського Союзу, інтеграції до європейського цифрового медичного простору та впровадження європейських стандартів</td><td>- характеризують рівень політичної підтримки цифрової трансформації, стратегічну наступність державної політики, стабільність реалізації реформ та політичну готовність до довгострокового розвитку цифрової системи охорони здоров'я</td></tr>
<tr><td colspan="3">РЕСУРСНІ ФАКТОРИ</td></tr>
<tr><td colspan="2">Фінансові</td><td>Кадрові</td></tr>
<tr><td colspan="2">- сукупність фінансових ресурсів, механізмів фінансування та інвестиційних можливостей держави, органів місцевого самоврядування і закладів охорони здоров'я, які визначають спроможність впроваджувати, підтримувати та масштабувати цифрові технології, інформаційні системи й цифрову інфраструктуру системи охорони здоров'я</td><td>- сукупність кількісних і якісних характеристик кадрового потенціалу СОЗ (рівень професійної підготовки, цифрових компетентностей, готовності до цифрових змін та безперервного професійного розвитку), які визначають спроможність ефективно впроваджувати, використовувати та розвивати цифрові технології у сфері охорони здоров'я</td></tr>
</table>

Продовження табл. 1

Інфраструктурні	*Техніко-технологічні*
- стан розвитку цифрової, телекомунікаційної, енергетичної та інженерної інфраструктури, що забезпечує функціонування інформаційних систем, цифрових платформ, центрів обробки даних і каналів передачі інформації, визначаючи можливість безперервної реалізації процесів цифрової трансформації системи охорони здоров'я	- рівень розвитку цифрових технологій, програмного забезпечення, медичного обладнання, систем штучного інтелекту, телемедицини, Інтернету медичних речей та інших інноваційних технологічних рішень, що визначають функціональні можливості цифрової трансформації системи охорони здоров'я

ДЕРЖАВНО-УПРАВЛІНСЬКІ ФАКТОРИ		
Інституційні	*Організаційні*	*Інформаційні*
- сукупність суб'єктів, їх повноважень, механізмів взаємодії та інституційної спроможності забезпечувати формування, реалізацію і координацію державної політики цифрової трансформації системи охорони здоров'я, що визначає результативність впровадження цифрових змін	- сукупність організаційних механізмів, управлінських процесів, моделей взаємодії та внутрішніх процедур функціонування системи охорони здоров'я, які визначають здатність суб'єктів державного управління та закладів охорони здоров'я адаптуватися до цифрових змін та ефективно інтегрувати цифрові технології у професійну діяльність	- сукупність факторів, що визначають ефективність інформаційної взаємодії між суб'єктами державного управління, інформаційного супроводу управлінських процесів, інформаційно-аналітичного забезпечення та обміну інформацією, необхідних для реалізації цифрової трансформації системи охорони здоров'я
БЕЗПЕКОВІ ФАКТОРИ		
Інформаційно-безпекові	*Кібербезпекові*	*Медико-безпекові*
- сукупність загроз, пов'язаних із порушенням конфіденційності, цілісності та доступності медичної інформації, які можуть негативно впливати на функціонування цифрової системи охорони здоров'я та потребують впровадження ефективних механізмів інформаційного захисту	- сукупність кіберзагроз і кіберризиків, що виникають у процесі функціонування цифрової інфраструктури системи охорони здоров'я та можуть порушувати безперервність надання медичної допомоги, функціонування інформаційних систем і безпеку медичних даних, обумовлюючи необхідність розвитку системи кіберзахисту	- сукупність загроз, що виникають під час надання медичної допомоги та можуть негативно впливати на життя і здоров'я пацієнтів і медичних працівників, обумовлюючи необхідність використання цифрових технологій для підвищення безпечності медичних процесів, мінімізації медичних помилок та забезпечення безперервного моніторингу стану здоров'я

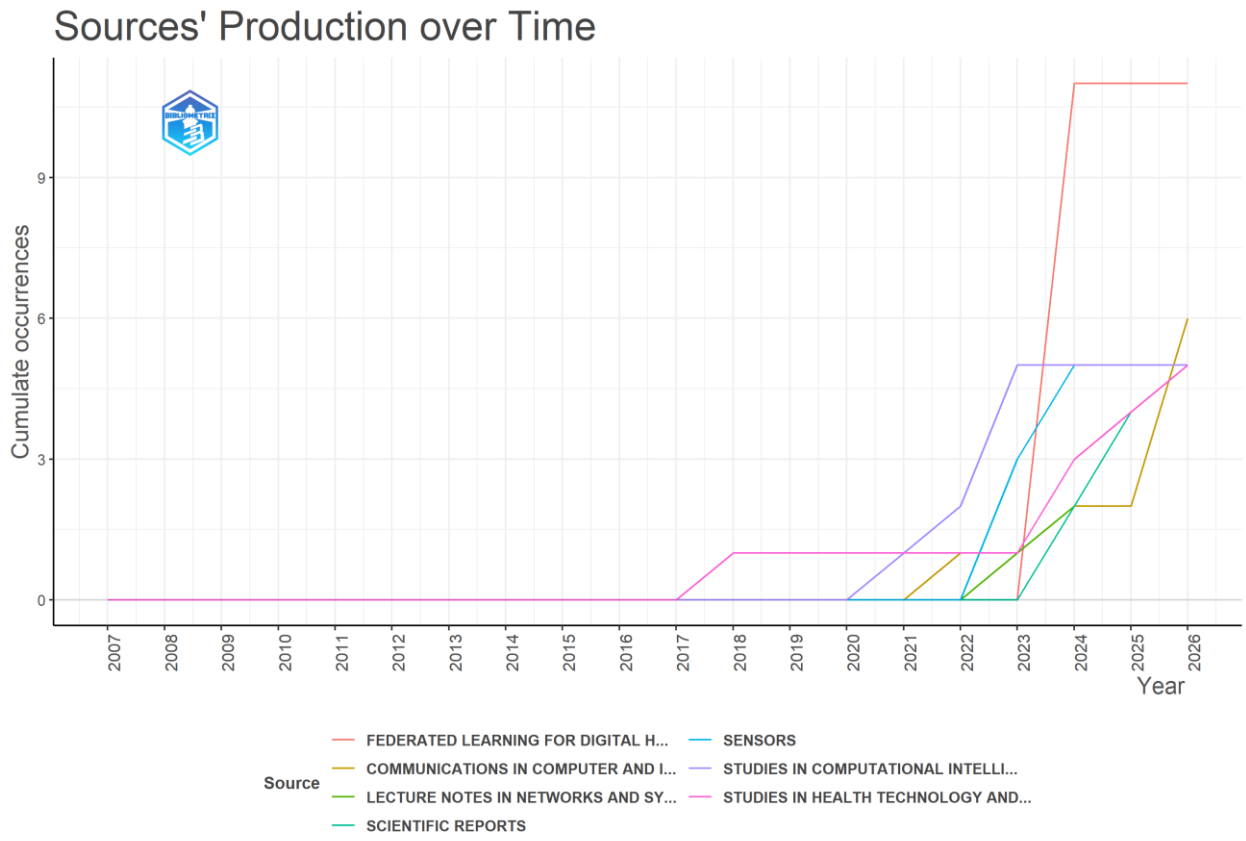


Рис. 1. Динаміка публікаційної активності провідних наукових джерел за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: сформовано автором за даними наукометричної бази Scopus із використанням програмного пакета Bibliometrix

Відмінності між підходами полягають насамперед у переліку суб'єктів, видах заходів та цілях їх реалізації, однак їх об'єднує функціональне розуміння охорони здоров'я. Зважаючи на сучасні властивості системи охорони здоров'я та вплив на неї соціально-економічних, політико-правових, культурно-ментальних та техніко-технологічних факторів вважаємо, що під системою охорони здоров'я варто розуміти: багаторівневу соціально-економічну систему, що об'єднує взаємопов'язані суб'єкти (суб'єкти державного регіонального, місцевого управління, заклади охорони здоров'я, виробників та постачальників ліків, наукові установи, заклади вищої освіти, інститути громадського суспільства та інші), ресурси, інфраструктуру та процеси (управлінські, медичні (профілактики, діагностування, лікування, реабілітація), організаційні, інформаційні, регламентаційні), функціонування якої регулюється державою та спрямована на формування, збереження, зміцнення та відновлення здоров'я населення та забезпечення високого рівня громадського здоров'я як складової соціальної функції.

Дослідження змісту понять цифрова трансформація та цифрова трансформація системи охорони здоров'я, які містяться в науковій та довідковій літературі дозволило встановити, що існуючі підходи до визначення цифрової трансформації системи охорони здоров'я переважно концентруються на впровадженні цифрових технологій, розвитку інформаційних систем, використанні електронних медичних даних, телемедицини, штучного інтелекту та інших цифрових інструментів. Значна частина авторів розглядає цифрову трансформацію як процес цифровізації окремих елементів системи або як розвиток інформаційно-комунікаційної інфраструктури

охорони здоров’я. Для розширення розуміння зазначених процесів запропоновано зміст понять: цифрова трансформація (цілеспрямований, керований і комплексний процес якісної зміни властивостей, структури, функцій, процесів, моделей взаємодії та способів функціонування певного об’єкта шляхом системного впровадження й використання цифрових технологій, даних та цифрових рішень, що приводить до формування його нового стану і потребує відповідних організаційних, інституційних, правових, кадрових та ресурсних змін) та цифрова трансформація системи охорони здоров’я (цілеспрямований, комплексний і керований процес якісної зміни структури, властивостей, функцій, процесів, механізмів державного управління, моделей взаємодії суб’єктів та способів реалізації медичних послуг шляхом системного впровадження цифрових технологій, цифрових даних і цифрових сервісів, результатом якого є формування цифрової системи охорони здоров’я, здатної забезпечити більш ефективне, доступне, безпечне, інтегроване та людиноцентричне функціонування сфери охорони здоров’я).

У другому розділі **«Методологія державного управління цифровою трансформацією системи охорони здоров’я»** розкрито вплив цифровізації на властивості системи охорони здоров’я, обґрунтовано принципи державного управління та розвинуто методологічні положення досліджуваної сфери.

В результаті вивчення властивостей системи охорони здоров’я було обґрунтовано їх зміст та визначено напрями групування. Встановлено, що системними властивостями системи охорони здоров’я, які характеризують її як соціально-економічну систему є наступні: відкритість, ієрархічність, керованість, інтегрованість, координованість, підзвітність, багатогалузевість, наукоємність, соціальність, професійність. Визначено, що рівень розвитку системи охорони здоров’я та її відповідність запитам суспільства визначається наступними властивостями: цілісність, комплексність, адаптивність, стійкість, безперервність, доступність, якість, ефективність, безпечність, прозорість. В свою чергу процеси цифрової трансформації системи охорони здоров’я видозмінюють, посилюють, розширюють та пришвидшують окремі системні властивості та посилюють, забезпечують, розвивають та підвищують рівень властивостей розвитку системи (рис. 2).

Визначено, що цифрова трансформація наділяє систему охорони здоров’я новими властивостями, які згруповано на властивості-переваги та властивості-загрози. До властивостей-переваг належать: інтероперабельність, простежуваність, автоматизованість, інтелектуальність, прогностичність, просторова незалежність, масштабованість. До властивостей-загроз належать: кіберзалежність, інформаційна залежність, технологічна залежність, інфраструктурна залежність, правова залежність. Дослідження властивостей системи охорони здоров’я в умовах цифрової трансформації визначає потребу в трансформації системи державного управління, адже цифровізація вимагає фінансового забезпечення, інформаційного супроводу, правового регулювання та організаційної трансформації. Визначенні та згруповані властивості системи охорони здоров’я розширюють теоретичне наукове знання та формують методологічне підґрунтя державного управління цифровою трансформацією системи охорони здоров’я.

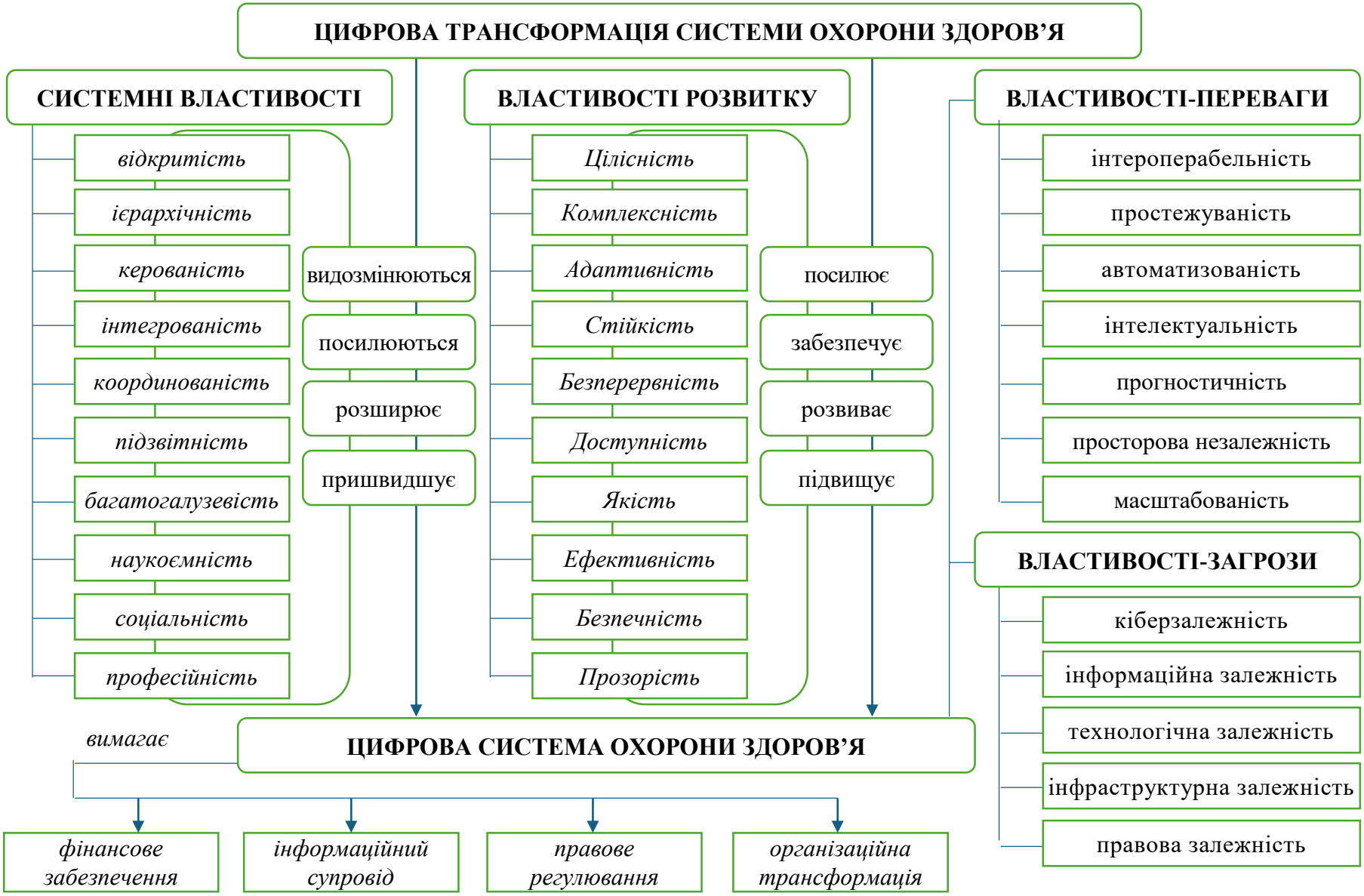


Рис. 2. Властивості системи охорони здоров'я в умовах цифрової трансформації

Зважаючи на властивості системи охорони здоров’я, процесів цифрової трансформації трансформуються теоретико-методологічні положення державного управління, зокрема структура та зміст принципів. За результатами аналізу наукової літератури щодо принципів державного управління системою охорони здоров’я встановлено відсутність єдиного підходу як до структури принципів так і їх змісту.

Для вирішення зазначеного розроблено багаторівневу структуру принципів державного управління цифровою трансформацією та цифровою системою охорони здоров’я, зокрема: стратегічні принципи (сукупність фундаментальних положень, які визначають довгострокові орієнтири, пріоритети та напрями державного управління цифровим розвитком системи охорони здоров’я, забезпечуючи узгодженість цифрової трансформації зі стратегічними цілями державної політики та суспільними потребами); принципів організації (сукупністю фундаментальних положень, які визначають інституційні особливості, розподіл повноважень, сферу відповідальності, порядок взаємодії суб’єктів державного управління та організацію процесів формування, реалізації, моніторингу й коригування державно-управлінських рішень щодо цифрової трансформації та цифрового розвитку системи охорони здоров’я); принципи цифрового функціонування (сукупність фундаментальних положень, які визначають вимоги до функціонування цифрової системи охорони здоров’я, забезпечуючи ефективне використання цифрових технологій, інформаційних ресурсів та цифрової інфраструктури для реалізації медичної допомоги й інформаційного забезпечення державного управління системою); принципи забезпечення (сукупність фундаментальних положень, які визначають правові, фінансово-економічні, кадрові, інформаційні та безпекові умови формування, функціонування і подальшого розвитку цифрової системи охорони здоров’я) (рис. 3).

Розвинено методологічні положення державного управління цифровою трансформацією системи охорони здоров’я шляхом визначення особливостей об’єктно-предметного поля, мети, завдань та механізмів державно-управлінського впливу. Обґрунтовано специфіку цифрової трансформації як об’єкта державного управління та визначено її взаємозв’язок із процесами функціонування системи охорони здоров’я і формуванням цифрової системи охорони здоров’я. Встановлено, що об’єкт державного управління є складним, полісуб’єктним і динамічним, оскільки охоплює одночасно процеси цифрової трансформації, функціонування системи в перехідний (гібридний) період та функціонування зрілої цифрової системи охорони здоров’я. Обґрунтовано комплексний підхід до його розуміння як триєдиної структури, що ґрунтується на розмежуванні процесів цифрової трансформації, функціонування системи охорони здоров’я в перехідний період та функціонування цифрової системи охорони здоров’я, та охоплює процеси трансформації, ресурси й інфраструктуру, учасників відносин, медичні та суміжні послуги й управлінські процеси.

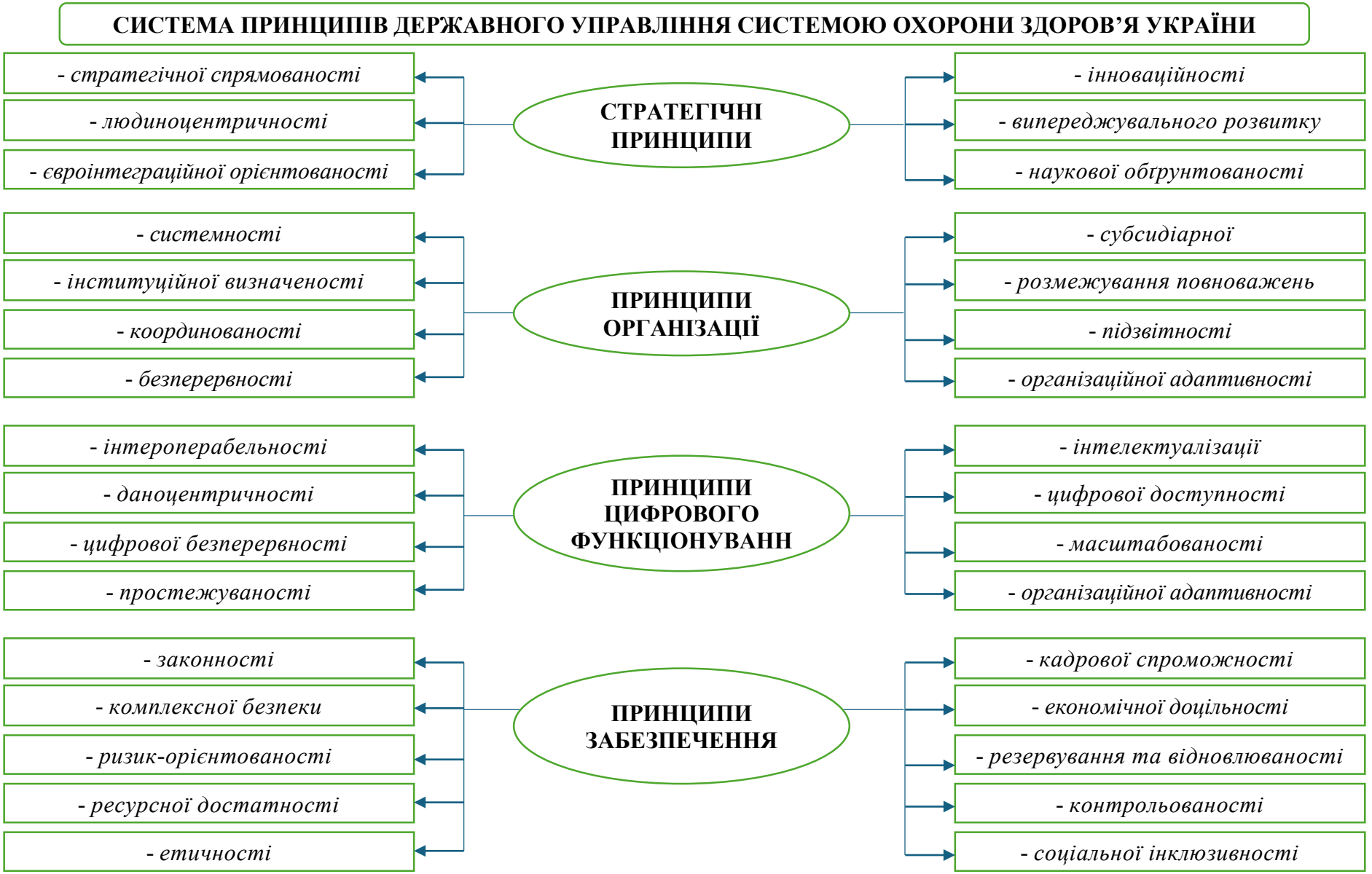


Рис. 3. Структура системи принципів державного управління цифрової трансформації системи охорони здоров'я

Уточнено зміст мети та представлено структуру та зміст завдань державного управління цифровою трансформацією системи охорони здоров'я з урахуванням багаторівневості, комплексності управлінського впливу та динамічності об'єкта. Встановлено, що державне управління в досліджуваній сфері здійснюється не статичним станом, а керованим переходом, який реалізується через синергію правового, організаційного, інформаційного, кадрового та фінансового механізмів. Обґрунтовано зміст зазначених механізмів, та визначено ключові вектори розвитку методів їх реалізації. Перевагою запропонованого підходу є його цілісність і практична спрямованість, оскільки він узгоджує теоретичні положення (об'єкт, предмет, мету) із конкретним переліком завдань та механізмів, що створює методологічне підґрунтя для формування й реалізації результативних державно-управлінських рішень в умовах цифрової трансформації та подальшого функціонування цифрової системи охорони здоров'я.

У третьому розділі **«Сучасний стан та наслідки цифрової трансформації системи охорони здоров'я як об'єкту державного управління»** досліджено світові тенденції цифровізації медичної галузі, оцінено рівень цифрової зрілості національних систем охорони здоров'я та проаналізовано сучасний стан цифрової трансформації в Україні.

Встановлено, що цифровізація системи охорони здоров'я на сучасному етапі вийшла за межі автоматизації окремих адміністративних і медичних процесів та набула характеру комплексної управлінської трансформації. Її зміст охоплює розвиток електронних медичних записів, телемедицини, цифрових платформ, систем управління медичними даними, технологій штучного інтелекту та аналітики великих даних, що змінюють не лише технологічну основу надання медичної допомоги, а й характер взаємодії між державою, закладами охорони здоров'я, медичними працівниками та пацієнтами. За результатами порівняльного аналізу встановлено, що результативність цифрової трансформації пов'язана з рівнем розвитку цифрового врядування, стратегічного планування, інституційної спроможності, нормативно-правового забезпечення, цифрової інфраструктури, інтероперабельності інформаційних систем та цифрових компетентностей. Це дає підстави розглядати цифрову трансформацію охорони здоров'я як самостійний напрям державної політики, що потребує узгодженого застосування технологічних, інституційних, правових, кадрових та організаційних механізмів.

Дослідження рівня цифрової зрілості систем охорони здоров'я засвідчило значну диференціацію між країнами навіть за умов високого загального рівня цифрового розвитку (рис. 4).

Встановлено, що найбільш розвиненими складовими цифрової трансформації є лідерство та врядування, стратегічне планування, інвестиційне забезпечення і розвиток цифрових сервісів, тоді як найбільш вразливими залишаються кадровий потенціал, інтероперабельність інформаційних систем та нормативно-правове регулювання новітніх цифрових технологій. Особливого значення набуває управління медичними даними, які в цифровій системі охорони здоров'я виконують не лише інформаційну функцію, а формують основу для моніторингу стану здоров'я населення, оцінювання якості медичної допомоги, проведення наукових досліджень, стратегічного планування та прийняття доказових управлінських рішень.

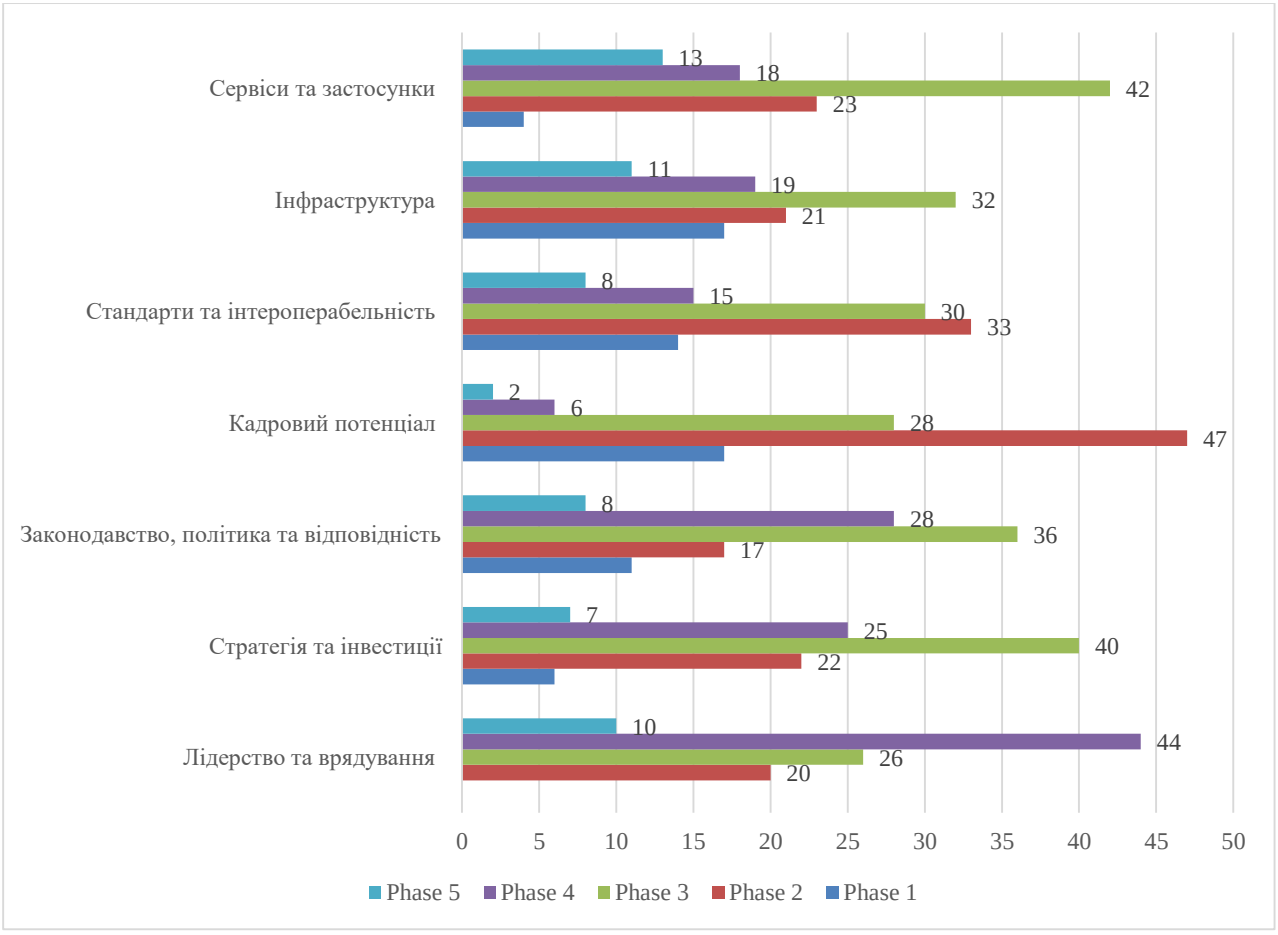


Рис. 4. Розподіл країн за фазами цифрової зрілості систем охорони здоров'я за основними доменами оцінювання у 2024 році, %

Відповідно, подальший розвиток цифрового здоров'я має передбачати забезпечення якості, достовірності, стандартизованості, захищеності та сумісності медичних даних, а також системний розвиток цифрових компетентностей медичних працівників і населення.

Виявлено посилення людиноцентричного характеру цифрової трансформації охорони здоров'я, що проявляється у поступовому переході від цифровізації внутрішніх процесів медичних установ до розвитку сервісів, орієнтованих на потреби громадян. Розширення доступу до електронних медичних записів, розвиток пацієнтських порталів і персональних цифрових сервісів посилюють можливості громадян щодо отримання та використання власної медичної інформації. Також відмінності у рівні цифрової грамотності населення підтверджують необхідність урахування доступності цифрових медичних сервісів для різних соціальних та освітніх груп. Одним із найбільш динамічних напрямів цифровізації визначено телемедицину, яка після пандемії COVID-19 трансформувалася з переважно кризового інструменту забезпечення безперервності медичного обслуговування у постійний елемент системи охорони здоров'я. Поряд із цим зростає роль штучного інтелекту та великих масивів даних у підтримці клінічних і управлінських рішень, що одночасно актуалізує питання захисту персональних даних, етичності використання алгоритмів, відповідальності за прийняті із застосуванням штучного інтелекту рішення та якості даних, на яких ґрунтується їх функціонування.

За результатами дослідження європейського досвіду встановлено, що цифрова трансформація систем охорони здоров'я країн Європи відбувається у напрямі формування інтегрованого цифрового простору, заснованого на інтероперабельності інформаційних систем, розвитку електронних медичних записів, транскордонному обміні медичною інформацією та розширенні цифрових сервісів для пацієнтів. Важливим етапом цього процесу стало формування European Health Data Space, що створює правові та організаційні передумови для безпечного обміну електронними даними про здоров'я, забезпечення доступу громадян до власної медичної інформації та використання медичних даних для наукових досліджень, інновацій і формування політики у сфері охорони здоров'я. Водночас встановлено неоднорідність цифрового розвитку європейських держав, що підтверджує відсутність єдиної швидкості цифрової трансформації та свідчить про поступове зближення національних систем через гармонізацію стандартів, правил обміну даними і принципів цифрового врядування. Для України зазначені тенденції визначають необхідність послідовного наближення національної цифрової системи охорони здоров'я до європейських вимог щодо інтероперабельності, захисту та управління медичними даними.

Оцінювання сучасного стану цифрової трансформації системи охорони здоров'я України засвідчило формування масштабної цифрової інфраструктури, ядром якої є електронна система охорони здоров'я. Розвиток електронних декларацій про вибір лікаря, медичних записів, рецептів, направлень та інших цифрових сервісів забезпечив перехід від цифровізації окремих процедур до системної електронної взаємодії між пацієнтами, медичними працівниками, закладами охорони здоров'я та державними органами управління. Станом на 2025 р. ЕСОЗ охоплювала понад 49 тис. медичних та аптечних закладів, близько 475 тис. медичних і фармацевтичних працівників, а кількість накопичених електронних медичних записів наблизилася до 5 млрд.

У четвертому розділі **«Євроінтеграційні імперативи державного управління процесами цифрової трансформації»** обґрунтовано вимоги ЄС до цифрової трансформації системи охорони здоров'я, розкрито регулювання безпеки цих процесів та узагальнено досвід окремих країн-членів ЄС.

Встановлено, що ЄС як унікальне наднаціональне утворення сформував обов'язкові для держав-членів вимоги до цифрової трансформації системи охорони здоров'я, які поєднують правовий, технологічний, безпековий та етичний виміри. Цифрова трансформація системи охорони здоров'я є пріоритетним і стратегічним завданням ЄС, спрямованим на підвищення ефективності державного управління, захист фундаментальних прав пацієнтів та забезпечення кібербезпеки критичної інфраструктури.

Аналіз еволюції нормативно-правового регулювання цифрової трансформації охорони здоров'я в ЄС свідчить про поступовий перехід від окремих цифрових ініціатив до комплексної багаторівневої регуляторної системи. Даний перехід відбувався в чотири періоди від фрагментарних експериментальних проєктів кінця 1990-х років через формування перших стратегій (2004–2010 рр.) і законодавчу стандартизацію та розбудову транскордонної інфраструктури (2011–2019 рр.) до повномасштабної цифрової інтеграції, каталізатором якої стала пандемія COVID-19 (рис. 5).

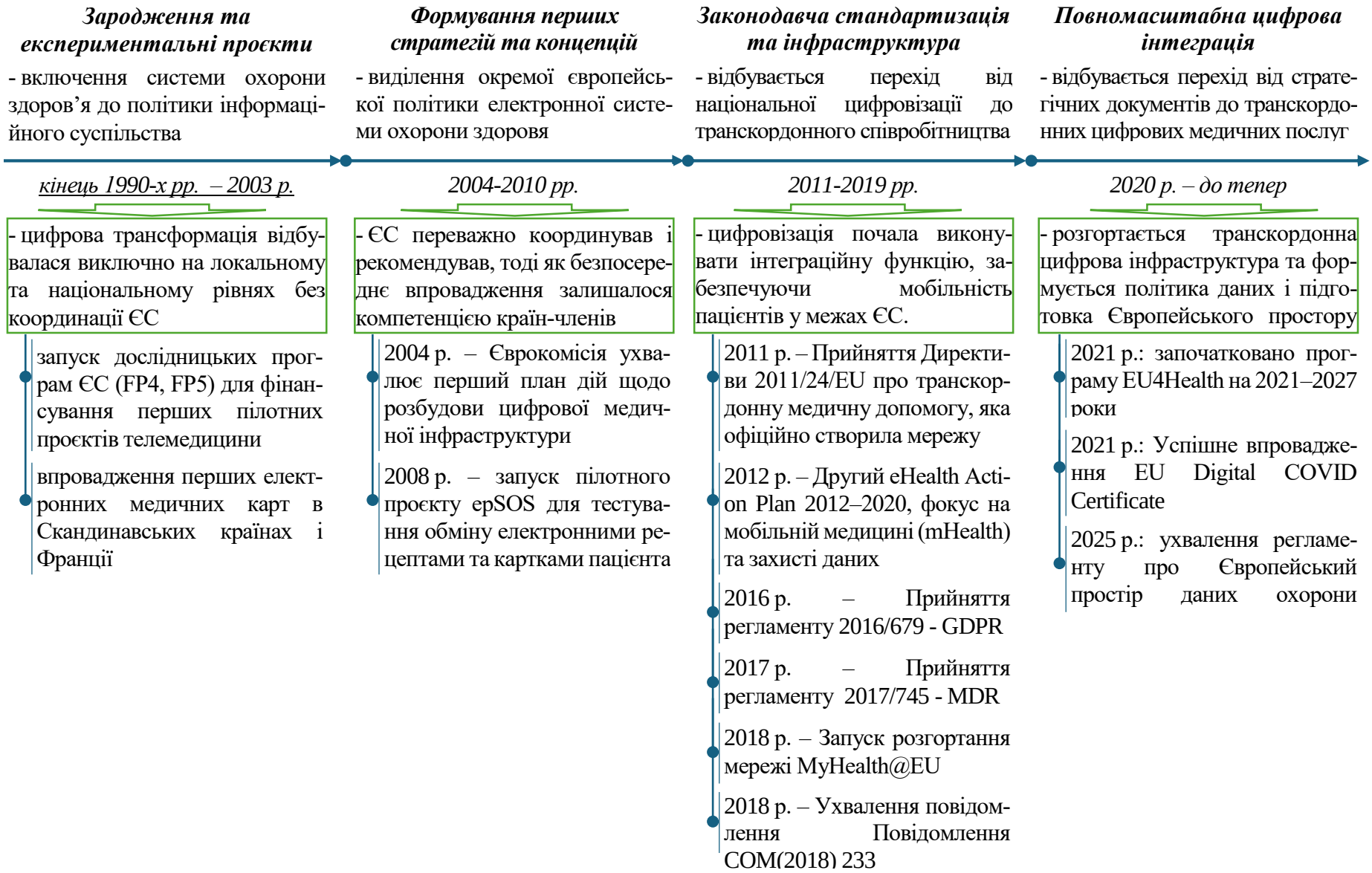


Рис. 5. Еволюція системи регулювання Європейським Союзом процесів цифрової трансформації системи охорони здоров'я

Результатом цієї еволюції є цілісна система нормативно-правових актів (рис. 6), ядро якої становлять Регламент (ЄС) 2025/327 про Європейський простір даних охорони здоров'я, AI Act, GDPR, eIDAS, Data Governance Act, Data Act, а також галузеві MDR і IVDR та акти регулювання цифрових послуг (DSA, DMA). Ця система забезпечує перехід від національної цифровізації до єдиного інформаційного й технологічного простору, заснованого на інтероперабельності, пацієнтоцентричності та можливості вторинного використання медичних даних. Водночас критичний аналіз наукових джерел засвідчує наявність системних проблем європейського регулювання: надмірної централізації та регуляторного перевантаження, правової невизначеності окремих понять, фрагментації правозастосування між державами-членами, ризиків алгоритмічної дискримінації та послаблення фактичного контролю особи над власними даними, а також обмеженої інституційної спроможності органів оцінки відповідності. Це доводить, що механічне копіювання європейських норм є неприйнятним, а гармонізація має супроводжуватися врахуванням виявлених недоліків і національного контексту.

Для України, яка вже створила базові організаційні та технологічні передумови (електронна система охорони здоров’я, електронні медичні записи, рецепти й направлення, законодавство про електронну ідентифікацію), пріоритетними завданнями залишаються гармонізація законодавства щодо прав пацієнтів на доступ до електронних даних, нормативне врегулювання вторинного використання медичних даних, досягнення повної інтероперабельності з технічними специфікаціями ЄС та визначення компетентних органів цифрової охорони здоров’я. Окремої уваги потребує кадрове, фінансове, безпекове й інфраструктурне забезпечення цих процесів, оскільки цифрова трансформація є ресурсомістким і фінансово затратним процесом.

Проведений політико-правовий аналіз Регламентів (ЄС) 2017/745 (MDR), (ЄС) 2017/746 (IVDR), Директиви (ЄС) 2022/2555 (NIS2), Регламентів (ЄС) 2019/881 (Cybersecurity Act) та (ЄС) 2024/2847 (Cyber Resilience Act) дає підстави для висновку, що безпека цифрової трансформації системи охорони здоров’я в праві ЄС забезпечується не окремими актами, а взаємопов’язаною системою регулювання, побудованою на єдиній логіці: ризик-орієнтованій класифікації об’єктів, контролі протягом усього життєвого циклу, обов’язковому залученні незалежних органів оцінки відповідності для об’єктів підвищеного ризику та інституціоналізованому постмаркетинговому нагляді з обов’язковою звітністю про інциденти. Ці акти є взаємодоповнювальними: MDR та IVDR охоплюють медичні вироби, включно з програмним забезпеченням медичного призначення; NIS2 регулює кіберстійкість самих закладів охорони здоров’я як суб’єктів критично важливого сектору; Cyber Resilience Act встановлює вимоги до цифрових продуктів, що не підпадають під спеціальне медичне регулювання; Cybersecurity Act забезпечує сертифікаційний інструментарій, до якого відсилають інші акти. Відповідно безпека цифрової охорони здоров’я є не технічною, а управлінською категорією, що охоплює вироби, дані, інфраструктуру, персонал, постачальників і процеси відновлення.

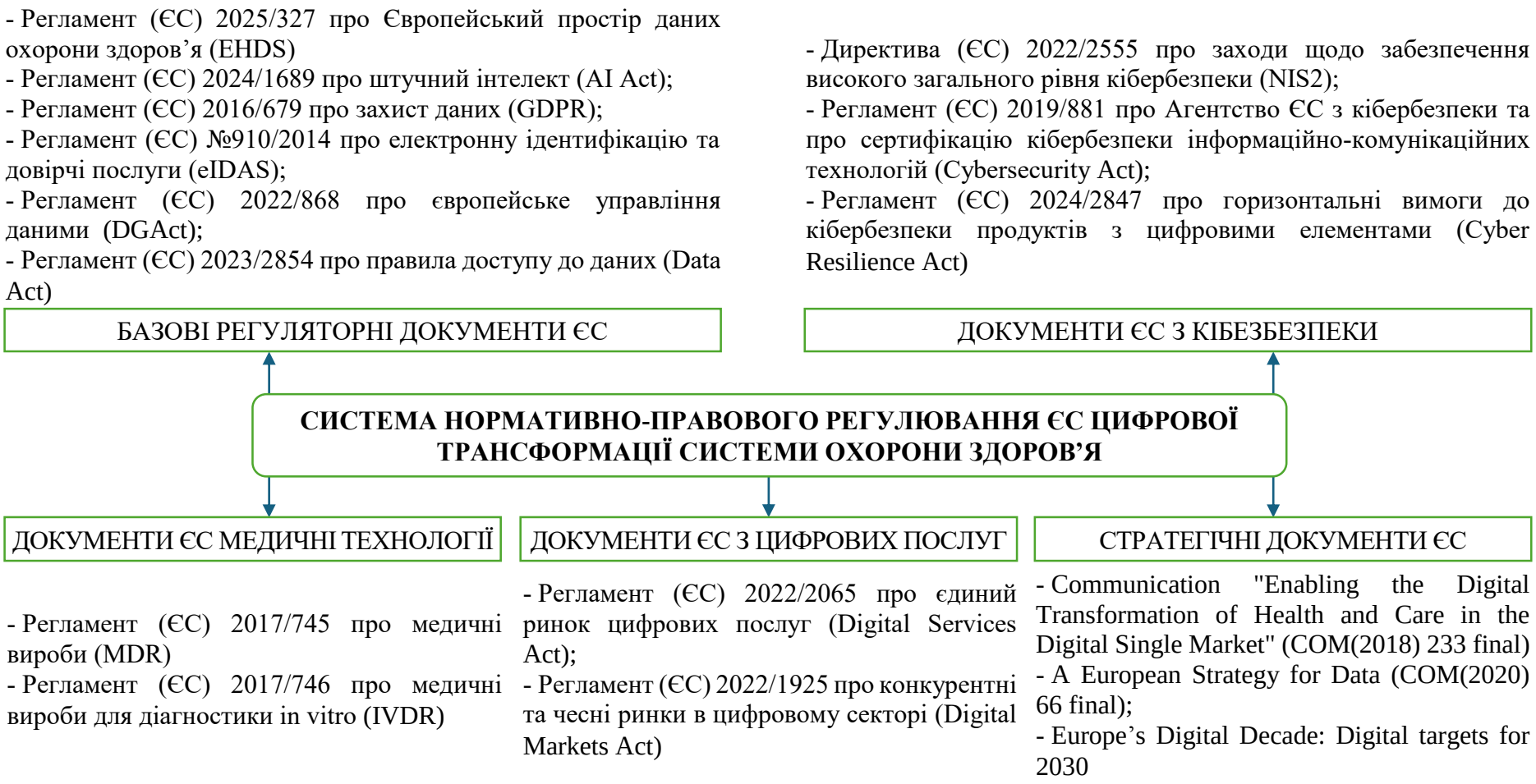


Рис. 6. Структура системи нормативно-правових актів Європейського Союзу, що регулюють цифрову трансформацію системи охорони здоров'я

Водночас практика застосування всіх проаналізованих актів засвідчила однотипну проблему, яка має ключове значення для формування українських механізмів державного управління: критичним бар'єром виявилася не якість матеріальних норм, а нестача інституційної та інфраструктурної спроможності для їх реалізації. З урахуванням наведеного, для України обґрунтованими є такі напрями формування механізмів державного управління безпекою цифрової трансформації системи охорони здоров'я: 1) адаптація національного законодавства має здійснюватися шляхом змістового зближення, а не текстуального копіювання норм, із обов'язковою оцінкою впливу нових вимог на доступність медичних виробів, діагностики та цифрових сервісів для пацієнтів; 2) пріоритетом є розбудова інституційної спроможності через визначення національного органу сертифікації кібербезпеки, розширення мережі акредитованих органів оцінки відповідності та випробувальних лабораторій, підготовка кваліфікованих кадрів (у тому числі осіб, відповідальних за регуляторну відповідність та за кібербезпеку в закладах охорони здоров'я); 3) вимоги до суб'єктів системи охорони здоров'я повинні бути пропорційними та ризик-орієнтованими, із централізованою державною підтримкою кіберзахисту закладів; 4) обов'язковими елементами моделі мають бути чіткі перехідні періоди, спрощені й цифровізовані процедури для вітчизняного MedTech-сектору; 5) в умовах збройної агресії безперебійний доступ до медичних виробів, критично важливої діагностики та захищених цифрових сервісів, а також кіберстійкість медичних реєстрів становлять складову національної безпеки, що обґрунтовує підвищений рівень пріоритетності саме безпекових механізмів у державному управлінні цифровою трансформацією системи охорони здоров'я.

У ході дослідження Бельгії, Данії та Естонії було проаналізовано нормативно-правове забезпечення цифрової трансформації системи охорони здоров'я, відповідність національного законодавства регламентам і директивам ЄС, а також інституційне забезпечення цифровізації, цифрову інфраструктуру, захист даних і кібербезпеку. Окремо досліджено повноваження основних державних органів та спеціалізованих суб'єктів, відповідальних за розвиток цифрових медичних послуг, управління медичними даними та реагування на кіберзагрози. Бельгійська модель характеризується розгалуженою нормативною та інституційною системою цифровізації охорони здоров'я, що поєднує федеральне регулювання, цифрову платформу eHealth, електронний обмін медичними даними та спеціалізовані механізми кібербезпеки. Модель Данії вирізняється високим рівнем централізованої координації цифрової охорони здоров'я, розвиненою спільною цифровою інфраструктурою та чітким розподілом відповідальності між державою, регіонами, муніципалітетами й спеціалізованими органами кібербезпеки. Естонія сформувала інтегровану цифрову модель охорони здоров'я на основі єдиної системи медичних даних, розвиненої державної цифрової інфраструктури, електронної ідентифікації та комплексного забезпечення захисту даних і кібербезпеки.

Для України корисним є використання досвіду цих країн щодо формування єдиної нормативної та інституційної системи цифрової охорони здоров'я, інтегрованої з вимогами законодавства ЄС, із чітким розподілом повноважень між органами охорони здоров'я, цифровізації, захисту даних і кібербезпеки.

У п’ятому розділі **«Удосконалення механізмів державного управління процесами цифрової трансформації системи охорони здоров’я»** розроблено механізм адаптації державного управління цифровою трансформацією до вимог ЄС, обґрунтовано напрями державного регулювання використання технологій штучного інтелекту та визначено механізми забезпечення безпеки системи охорони здоров’я в умовах цифрової трансформації.

Запропонований комплексний механізм адаптації державного управління цифровою трансформацією системи охорони здоров’я до вимог ЄС, що визначає перехід від фрагментарної адаптації окремих актів до комплексної законодавчої архітектури цифрової охорони здоров’я (табл. 2). Запропоновано розширення нормативно-правової бази шляхом прийняття нових законодавчих актів: Закон України «Про обіг медичних даних»; Рамковий Закон України «Про штучний інтелект»; Закон України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації»; Закон України «Про управління даними»; Закон України «Про цифрові послуги». Запропоновано сукупність змін до законодавчих актів, що полягають у наступному: Закон України «Основи законодавства України про охорону здоров’я» пропонується доповнити положеннями щодо використання ШІ в медицині та транскордонного обміну медичними даними; Закон України «Про захист персональних даних» передбачає комплексну адаптацію до GDPR та майбутнього закону про обіг медичних даних: спеціальні правила анонімізації та псевдонімізації медичних даних, зв’язок із режимом вторинного використання, реалізація opt-out пацієнта та правові умови транскордонного обміну; Закон України «Про захист інформації в інформаційно-комунікаційних системах» передбачає поступовий перехід від КСЗІ до європейських схем кіберсертифікації EUCC, EUCS та ISO/IEC 15408. Також, передбачено диференціацію рівнів довіри: High для критичних компонентів ЕСОЗ і NCPH, а Basic/Substantial - для менш критичних МІС та MedTech-рішень; Закон України «Про захист економічної конкуренції» передбачає зміни спрямовані на цифрові гейткіпери. АМКУ пропонується надати повноваження визначати цифрові медичні платформи, забороняти самопріоритетизацію, контролювати алгоритми ранжування, проводити аудит алгоритмів та застосовувати приписи і штрафи. Важливо зазначити на потребі заміна чинних технічних регламентів № 753 та № 754 новими технічними регламентами, побудованими на MDR та IVDR, які мають: визначити SaMD як самостійний медичний виріб; оновити класифікацію програмного забезпечення за ризиком; гармонізувати перехідні строки із законодавством ЄС; адаптувати регулювання IVD до IVDR. Реалізація запропонованого механізму формує нормативно-правові та інституційні передумови переходу від фрагментарної цифровізації до цілісної, безпечної, кіберстійкої та інтегрованої в європейський цифровий простір системи охорони здоров’я.

Технології ШІ перетворюються з технічного інструменту на повноцінного суб’єкта-партнера медичної діяльності, охоплюючи наукові дослідження, первинну та спеціалізовану діагностику (онкологія, кардіологія, офтальмологія, ортопедія), персоналізоване лікування, реабілітацію та цифровий менеджмент закладів охорони здоров’я.

Таблиця 2. Комплексний механізм адаптації державного управління цифровою трансформацією системи охорони здоров'я до вимог Європейського Союзу

<table>
<tr><th colspan="5">РЕГЛАМЕНТ (ЄС) 2025/327 ПРО ЄВРОПЕЙСЬКИЙ ПРОСТІР ДАНИХ ОХОРОНИ ЗДОРОВ'Я (EHDS)</th></tr>
<tr><td colspan="5">РОЗРОБКА ТА ПРИЙНЯТТЯ ЗАКОНУ УКРАЇНИ ПРО ОБІГ МЕДИЧНИХ ДАНИХ</td></tr>
<tr><td rowspan="2">Розділ 1. Загальні положення</td><td colspan="2">Стаття 1. Визначення термінів</td><td colspan="2">Стаття 2. Сфера дії Закону</td></tr>
<tr><td colspan="2">Стаття 3. Законодавство про обіг медичних даних</td><td colspan="2">Стаття 4. Принципи обробки медичних даних</td></tr>
<tr><td rowspan="2">Розділ 2. Права фізичних осіб стосовно власних медичних даних</td><td>Стаття 5. Право на безоплатний доступ до власних медичних даних</td><td>Стаття 6. Право на внесення змін, виправлення та доповнення даних</td><td colspan="2">Стаття 7. Право на відмову від вторинного використання даних (Механізм Opt-out)</td></tr>
<tr><td colspan="2">Стаття 8. Повноваження щодо управління доступом</td><td colspan="2">Стаття 9. Право на переносність даних (Data</td></tr>
<tr><td rowspan="2">Розділ 3. Первинне використання медичних даних</td><td>Стаття 10. Мета та підстави первинного використання даних</td><td>Стаття 11. Категорії даних первинного використання</td><td>Стаття 12. Порядок та умови доступу медичних працівників до даних</td><td>Стаття 13. Транскордонний обмін для первинного використання</td></tr>
<tr><td rowspan="2">Розділ 4. Вторинне використання медичних даних</td><td>Стаття 14. Цілі та дозволені сфери вторинного використання</td><td>Стаття 15. Заборонені цілі вторинного використання</td><td colspan="2">Стаття 16. Обов'язкова анонімі-зація та псевдонімізація даних</td></tr>
<tr><td>Стаття 17. Дозвіл на доступ до даних</td><td>Стаття 18. Безпечні середовища обробки даних</td><td colspan="2">Стаття 19. Транскордонний обмін для вторинного використання</td></tr>
<tr><td rowspan="2">Розділ 5. Інституційна система управління та нагляду</td><td colspan="2">Стаття 20. Національний орган з доступу до медичних даних</td><td colspan="2">Стаття 21. Національна точка контакту з електронного здоров'я</td></tr>
<tr><td colspan="2">Стаття 22. Політика та стандарти сумісності</td><td colspan="2">Стаття 23. Реєстр дозволів та відкрита звітність</td></tr>
<tr><td>Розділ 6. Технічна інфраструктура, сертифікація та кібербезпека</td><td>Стаття 24. Вимоги до Медичних інформаційних систем</td><td>Стаття 25. Захист медичних даних та кібербезпека</td><td colspan="2">Стаття 26. Аудит та логування</td></tr>
<tr><td>Розділ 7. Відповідальність та контроль</td><td>Стаття 27. Контроль за дотриманням законодавства</td><td>Стаття 28. Відповідальність за порушення правил обігу даних</td><td colspan="2">Стаття 29. Відшкодування шкоди, завданої суб'єкту даних</td></tr>
<tr><td>Розділ8. Прикінцеві положення</td><td>Терміни набрання чинності</td><td>Перехідний період</td><td colspan="2">Внесення змін до Законів України</td></tr>
<tr><td colspan="5">РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ВТОРИННОГО ВИКОРИСТАННЯ МЕДИЧНИХ ДАНИХ (HEALTH DATA ACCESS BODY (ОРГАН З ДОСТУПУ ДО МЕДИЧНИХ ДАНИХ))</td></tr>
<tr><td colspan="2">утворення нового суб'єкту державного управління</td><td colspan="3">наділення відповідними повноваженнями існуючого суб'єкту</td></tr>
<tr><td colspan="5">НАЛАГОДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ МІЖ ЦИФРОВОЮ СИСТЕМОЮ НАЦІОНАЛЬНОЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я З ЄВРОПЕЙСЬКИМИ ТРАНСКОРДОННИМИ МЕРЕЖАМИ</td></tr>
<tr><td colspan="2">Організаційно-інституційне забезпечення</td><td>Інформаційно-інфраструктурне забезпечення</td><td colspan="2">Нормативно-правове забезпечення</td></tr>
</table>

Продовження табл. 2

РЕГЛАМЕНТ (ЄС) 2024/1689 ПРО ШТУЧНИЙ ІНТЕЛЕКТ (AI ACT)			
УНОРМУВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ			
прийняття Рамкового Закону України «Про штучний інтелект»	- внесення змін до Закону України «Основи законодавства України про охорону здоров'я»	прийняття Постанови КМУ про затвердження порядку постійного моніторингу алгоритмів після їх впровадження у лікарнях	
- розробка стандарту підготовки деперсоналізованих/анонімізованих медичних даних (знімків КТ, МРТ, ЕКГ, лабораторних карт) для навчання та тестування ШІ-систем	- внесення змін до Технічного регламенту щодо медичних виробів з метою синхронізації вимог до ШІ-систем високого ризику	- наказ МОЗ про обов'язкове інформування пацієнта про використання ШІ під час його діагностики чи розробки плану лікування	прийняття Постанови КМУ про затвердження Порядку підключення та верифікації ШІ-модулів у рамках Електронної системи охорони здоров'я
РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ			
утворення спеціалізованого суб'єкту державного управління, що вступатиме Регулятором технологій штучного інтелекту	- розширення повноважень ДЛЗ (Держлікслужби) щодо ринкового нагляду за ШІ-медичними виробами	- внесення змін до організаційної структури МОЗ щодо регулювання використання ШІ в медицині	
СТАНДАРТИЗАЦІЯ ТА ВРЕГУЛЮВАННЯ ТЕХНІКО-ТЕХНОЛОГІЧНИХ АСПЕКТІВ ВИКОРИСТАННЯ ШІ В МЕДИЦИНІ			
- створення спеціалізованих безпечних середовищ для тестування медичних алгоритмів до їх виходу на ринок	- впровадження технічних стандартів для заборгованості пост-маркетингового моніторингу алгоритмів, що самонавчаються	- створення національного реєстру медичних ШІ-систем високого ризику	
РЕГЛАМЕНТ (ЄС) 2016/679 ПРО ЗАХИСТ ДАНИХ (GDPR)			
ПРИЙНЯТТЯ НОВОГО ЗАКОНУ УКРАЇНИ ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ			
- на сьогодні розглядається Верховною Радою новий законопроект, який пропонується розширити:			
додати окрему статтю щодо стандартів анонімізації та псевдонімізації спеціальних категорій (медичних) даних, яка має передбачати, що псевдонімізовані медичні дані продовжують підпадати під дію Закону, а повністю анонімізовані дані виходять із-під його дії лише за умови проходження перевірки на ризик реідентифікації за методологією HDAB		- додати окрему статтю щодо регулювання обробки спеціальних категорій даних, прямим посиланням до спеціального законодавства про обіг медичних даних та визначає, що видача дозволу спеціалізованим органом є самостійною законною підставою для обробки даних у розумінні цього Закону.	
- передбачити норму щодо безумовного права пацієнта на безперешкодну відмову від використання його медичних даних для наукових досліджень) через Електронну систему охорони здоров'я (ЕСОЗ) або портал «Дія» та зобов'язань контролерів (МОЗ, лікарні, ЕСОЗ) автоматично враховувати цю відмову під час формування вибірок для		- додати окрему статтю щодо спрощення та легалізації транскордонного обміну медичними даними громадян України з країнами ЄС через Національну точку контакту (NCPH) в рамках мереж MyHealth@EU та HealthData@EU та передбачати, що після вступу України до ЄС або підписання відповідних двосторонніх угод, обмін через NCPH не потребуватиме додаткових окремих дозволів контролера для кожного випадку надання екстреної чи планової медичної допомоги за кордоном.	

Продовження табл. 2

ПРИЙНЯТТЯ ЗАКОНУ УКРАЇНИ ПРО НАЦІОНАЛЬНУ КОМІСІЮ З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ		
- на сьогодні розглядається Верховною Радою новий законопроект, який пропонується розширити:		
- додати статтю про Створення Спеціалізованого підрозділу/департаменту з питань медичних та біометричних даних у складі апарату Національної комісії	передбачити норму щодо надання Нацкомісії право проводити аудит алгоритмічної прозорості та відсутності упередженості у системах автоматизованого прийняття рішень	- додати статтю про запровадження спеціального екстреного протоколу реагування на сповіщення про витік медичних даних
- додати статтю про розмежування компетенції HDAB (видає дозволи (Data Permits) на вторинне використання медичних даних) та Національна комісія (проводить нагляд за тим, чи дотримуються вимоги щодо захисту даних під час використання цих дозволів)	- передбачити норму щодо закріплення за Нацкомісією статусу представника України в Європейській раді з питань захисту даних (EDPB) з можливістю делегування експертів до спеціалізованих робочих груп ЄС з медичних даних.	- додати статтю щодо вимог до кваліфікації інспекторів, які мають знання щодо технічних стандартів (ISO/IEC 27001, вимог до КСЗІ, специфіки архітектури ЕСОЗ та протоколів безпеки)
- передбачити норму щодо закріплення за Нацкомісією повноваження затвердження Типових форм та методологій Оцінки впливу на захист даних для сфери охорони здоров'я	- передбачити норму щодо надання Нацкомісії повноважень перевіряти дотримання концепції «Приватності за замовчуванням» на етапі розробки та тестування медичного ПЗ (SaMD) та модулів ЕСОЗ	- додати статтю щодо обов'язків контролерів (ЕСОЗ, МІС, лабораторій) повідомляти Нацкомісію про витік чутливих медичних даних протягом 72 годин
РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ДЕРЖАВНОГО УПРАВЛІННЯ ЩОДО ЗАХИСТУ МЕДИЧНИХ ДАНИХ		
***- створення незалежного наглядового органу* - НАЦІОНАЛЬНА КОМІСІЯ З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ**		
РЕГЛАМЕНТ (ЄС) №910/2014 ПРО ЕЛЕКТРОННУ ІДЕНТИФІКАЦІЮ ТА ДОВІРЧІ ПОСЛУГИ (EIDAS)		
ПРИВЕДЕННЯ У ВІДПОВІДНІСТЬ ІНФРАСТРУКТУРНОГО ТА ТЕХНІКО-ТЕХНОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ		
інтеграція з eIDAS 2.0 та EUDI Wallet		***впровадження електронних атрибутів лікаря (QEAA)***
- адаптувати застосунок «Дія» та ЕСОЗ до стандартів EUDI Wallet для того, щоб пацієнт міг зберігати рецепти, медзаписи та довідки у своєму цифровому гаманці та пред'являти їх у будь-якій країні ЄС		закріпити використання електронних атрибутів (підтвердження активного статусу та спеціалізації лікаря через автоматичну звірку з Реєстром медичних працівників ЕСОЗ при накладанні КЕП)
укладення Угоди про взаємне визнання КЕП з ЄС		***транскордонна ідентифікація для мережі MyHealth@EU:***
- завершити процедуру офіційного включення українського Довіреного списку до Довіреного списку ЄС, що дозволить українським медичним документам мати беззаперечну юридичну силу в країнах ЄС		- Налаштувати Національну точку контакту з електронного здоров'я (NCPH) для підтримки протоколів ідентифікації eIDAS при обміні даними пацієнтів між Україною та клініками ЄС

Продовження табл. 2

<table>
<tr><th colspan="4">РЕГЛАМЕНТ (ЄС) 2022/868 ПРО ЄВРОПЕЙСЬКЕ УПРАВЛІННЯ ДАНИМИ (DGACT)</th></tr>
<tr><td colspan="4">РОЗРОБКА ТА ПРИЙНЯТТЯ ЗАКОНУ УКРАЇНИ ПРО УПРАВЛІННЯ ДАНИХ</td></tr>
<tr><td>Розділ 1. Загальні положення</td><td>Стаття 1. Предмет та мета</td><td>Стаття 2. Сфера застосування</td><td>Стаття 3. Визначення термінів</td></tr>
<tr><td rowspan="2">Розділ 2. Повторне використання захищених даних публічного сектору</td><td colspan="2">Стаття 4. Категорії даних, що підлягають повторному використанню</td><td>Стаття 5. Умови повторного використання</td></tr>
<tr><td colspan="2">Стаття 6. Безпечні середовища обробки</td><td>Стаття 7. Роль спеціалізованих органів</td></tr>
<tr><td>Розділ 3. Послуги з обміну даними (Посередники у сфері даних)</td><td>Стаття 8. Правовий статус посередників з обміну даними</td><td>Стаття 9. Принцип нейтральності посередників</td><td>Стаття 10. Реєстрація та нагляд</td></tr>
<tr><td>Розділ 4. Альтруїзм щодо даних</td><td>Стаття 11. Поняття та засади альтруїзму щодо даних</td><td>Стаття 12. Реєстр організацій альтруїзму щодо даних</td><td>Стаття 13. Згода на альтруїзм щодо даних</td></tr>
<tr><td>Розділ 5. Інституційний механізм та компетентні органи</td><td colspan="2">Стаття 14. Національний компетентний орган з управління даними</td><td>Стаття 15. Рада з управління даними</td></tr>
<tr><td>Розділ 6. Міжнародне співробітництво та транскордонна передача</td><td colspan="2">Стаття 16. Транскордонний обмін даними</td><td>Стаття 17. Заходи протизаконного доступу третіх країн</td></tr>
<tr><td>Розділ 7. Відповідальність та нагляд</td><td colspan="2">Стаття 18. Розгляд скарг та позасудове вирішення спорів</td><td>Стаття 19. Санкції за порушення Закону</td></tr>
<tr><td>Розділ 8. Прикінцеві та перехідні положення</td><td colspan="2">Внесення змін до Законів України</td><td>Перехідний період</td></tr>
<tr><td colspan="4">РОЗШИРИТИ ІНФРАСТРУКТУРНУ СПРОМОЖНІСТЬ УПРАВЛІННЯ ДАНИМИ</td></tr>
<tr><td colspan="2">- розробити функціонал у «Кабінеті пацієнта» (у ЕСОЗ чи через «Дію»), який дозволить громадянам надавати згоду на «пожертвування» своїх анонімізованих медичних записів для науково-дослідних та MedTech-проєктів</td><td colspan="2">- розробка та реалізація Державного реєстру організацій альтруїзму щодо даних</td></tr>
<tr><th colspan="4">РЕГЛАМЕНТ (ЄС) 2023/2854 ПРО ПРАВИЛА ДОСТУПУ ДО ДАНИХ (DATA ACT)</th></tr>
<tr><td colspan="4">ПРАВОВЕ ВРЕГУЛЮВАННЯ ТЕХНІЧНОГО ХАРАКТЕРУ ЩОДО ДОСТУПУ ДО ДАНИХ</td></tr>
<tr><td>гармонізація Технічного регламенту щодо медичних виробів</td><td colspan="2">розробка та прийняття закону України про управління даних</td><td>уніфікація стандартів міграції для Медичних інформаційних систем</td></tr>
<tr><td>- внесення змін до Постанови КМУ№ 753 Про затвердження Технічного регламенту щодо медичних виробів щодо того, що медичне обладнання та носійні пристрої, що продаються в Україні, повинні мати відкриті API або стандартні інтерфейси для експорту сирих даних пацієнта у форматі HL7 FHIR чи</td><td colspan="2">- передбачити в закону норму в Законі України Про управління даними (стаття 4), що закріплює права пацієнта володіти та розпоряджатися неперсональними / персональними даними, які згенеровані його особистими медичними гаджетами, та передавати їх до ЕСОЗ</td><td>- затвердження МОЗ обов’язкових вимог до сумісності та безперешкодного вивантаження баз даних лікарень у разі зміни оператора МІС чи хмарного дата-центру</td></tr>
</table>

Продовження табл. 2

<table>
<tr><th colspan="3">ДИРЕКТИВА (ЄС) 2022/2555 ПРО ЗАХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ВИСОКОГО ЗАГАЛЬНОГО РІВНЯ КІБЕРБЕЗПЕКИ (NIS2)</th></tr>
<tr><td colspan="2">оновлення підзаконних актів КМУ щодо критичної інфраструктури в медицині</td><td>впровадження регламенту 24/72/1М сповіщення про інциденти</td></tr>
<tr><td colspan="2">- розширення переліку об’єктів критичної інфраструктури в охороні здоров’я, включивши до нього виробників ліків, виготовлювачів критичних медичних виробів, комерційні лабораторії та МІС за критеріями NIS2</td><td>- затвердження Наказом МОЗ чіткий регламент сповіщення стандартами NIS2</td></tr>
<tr><td colspan="2">перехід від КСЗІ до міжнародних стандартів (ISO/IEC 27001 та NIST)</td><td>запровадження навчання та відповідальності для керівників ЗОЗ</td></tr>
<tr><td colspan="2">- зміна застарілої системи КСЗІ на користь гнучких систем управління інформаційною безпекою (ISMS) за стандартом ISO/IEC 27001 та сертифікації заходи з управління ризиками</td><td>- запровадження обов’язкових тренінгів з кібергігієни та кіберризиків для головних лікарів та керівників ЗОЗ із закріпленням персональної відповідальності за стан кіберзахисту</td></tr>
<tr><th colspan="3">РЕГЛАМЕНТ (ЄС) 2019/881 ПРО АГЕНТСТВО ЄС З КІБЕРБЕЗПЕКИ ТА ПРО СЕРТИФІКАЦІЮ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ (CYBERSECURITY ACT)</th></tr>
<tr><td colspan="2">заміна КСЗІ на європейські схеми сертифікації</td><td>визначення національного органу із сертифікації кібербезпеки</td></tr>
<tr><td colspan="2" rowspan="2">- прийняття законопроєкту про внесення змін до Закону України «Про захист інформації в інформаційно-комунікаційних системах», який передбачає поступову заміну КСЗІ на європейські схеми сертифікації кібербезпеки (EUCC, EUCS, ISO/IEC 15408)</td><td>Варіант 1. Офіційне надання Держспецзв’язку статусу Національного органу із сертифікації кібербезпеки (NCCA)</td></tr>
<tr><td>Варіант 2. Утворення Національного агентства із сертифікації кібербезпеки</td></tr>
<tr><td colspan="2">впровадження рівня довіри «High» для центральних компонентів ЕСОЗ</td><td>спрощення доступу на ринок для розробників МІС (Рівень «Basic» та «Substantial»)</td></tr>
<tr><td colspan="2">- закріплення вимоги про те, що Центральна база даних ЕСОЗ, Національна точка контакту (NCPH) та хмарні сервіси, що їх обслуговують, повинні проходити сертифікацію за рівнем довіри High (за схемами EUCS/Common Criteria)</td><td>запровадження процедури самодекларування кібербезпеки для допоміжних модулів МІС та розробок MedTech за схемою CSA, що прискорить впровадження нових цифрових сервісів у лікарнях</td></tr>
<tr><th colspan="3">РЕГЛАМЕНТ (ЄС) 2024/2847 ПРО ГОРИЗОНТАЛЬНІ ВИМОГИ ДО КІБЕРБЕЗПЕКИ ПРОДУКТІВ З ЦИФРОВИМИ ЕЛЕМЕНТАМИ (CYBER RESILIENCE ACT)</th></tr>
<tr><td colspan="3">ОНОВЛЕННЯ ТЕХНІЧНОГО РЕГЛАМЕНТУ ЩОДО МЕДИЧНИХ ВИРОБІВ</td></tr>
<tr><td>Впровадження обов’язкових норм CRA щодо оцінки кіберстійкості цифрових елементів медичних виробів</td><td>- зобов’язати виробників MedTech-продукції та розробників МІС формувати й верифікувати SBOM за європейськими стандартами</td><td>- нормативне закріплення зобов’язання виробників надавати патчі безпеки протягом усього строку експлуатації пристрою</td></tr>
</table>

Продовження табл. 2

РЕГЛАМЕНТ (ЄС) 2017/745 ПРО МЕДИЧНІ ВИРОБИ (MDR) ТА РЕГЛАМЕНТ (ЄС) 2017/746 ПРО МЕДИЧНІ ВИРОБИ ДЛЯ ДІАГНОСТИКИ IN VITRO (IVDR)		
РОЗРОБИТИ ТА ПРИЙНЯТИ НОВІ ТЕХНІЧНІ РЕГЛАМЕНТИ ЩОДО МЕДИЧНИХ ВИРОБІВ (НА ЗАМІНУ № 753) ТА ЩОДО МЕДИЧНИХ ВИРОБІВ ДЛЯ ДІАГНОСТИКИ IN VITRO» (НА ЗАМІНУ № 754) З ПРЯМИМ ВІДСИЛАННЯМ ДО НОРМ MDR ТА IVDR		
включити чітке визначення SaMD (Software as a Medical Device) як самостійного медичного виробу	- гармонізувати періоди переходів для існуючих виробів відповідно до строків ЄС (до 2027/2028 років залежно від класу ризику)	- внести до Додатка класифікаційних критеріїв нового Технічного регламенту Правило, яке перерозподіляє класи ризику для ПЗ
ВНЕСТИ ЗМІНИ ДО ПОСТАНОВИ КМУ ЩОДО ВЕДЕННЯ ДЕРЖАВНОГО РЕЄСТРУ МЕДИЧНОЇ ТЕХНІКИ ТА ВИРОБІВ		
- перетворити Реєстр на єдину цифрову систему з обов'язковим веденням трьох нових модулів: Реєстр суб'єктів (Actors), Реєстр UDI-кодів (UDI/Device) та Реєстр сертифікатів (Certificates)	- зобов'язати Держлікслужбу забезпечити технічну сумісність (API) національного реєстру з європейською базою EUDAMED	
ЗАТВЕРДИТИ «ПОРЯДОК ПРОВЕДЕННЯ ПІСЛЯРИНКОВОГО КЛІНІЧНОГО СПОСТЕРЕЖЕННЯ (PMCF) ТА СПОСТЕРЕЖЕННЯ ЗА ФУНКЦІОНУВАННЯМ IVD (PMPF)»		
- зобов'язати розробників SaMD та ШІ-систем щорічно надавати до Держлікслужби Звіт із безпеки	- для ШІ-систем у медицині зобов'язати виробників проводити регулярну перевірку точності роботи алгоритму на реальних українських клінічних даних	

РЕГЛАМЕНТ (ЄС) 2022/2065 ПРО ЄДИНИЙ РИНОК ЦИФРОВИХ ПОСЛУГ (DIGITAL SERVICES ACT) ТА - РЕГЛАМЕНТ (ЄС) 2022/1925 ПРО КОНКУРЕНТНІ ТА ЧЕСНІ РИНКИ В ЦИФРОВОМУ СЕКТОРІ (DIGITAL MARKETS ACT)			
РОЗРОБКА ТА ПРИЙНЯТТЯ ЗАКОНУ УКРАЇНИ «ПРО ЦИФРОВІ ПОСЛУГИ»			
Розділ 1. Загальні положення	*Стаття 1.* Предмет та мета	*Стаття 2.* Сфера застосування	*Стаття 3.* Визначення термінів
Розділ 2. Відповідальність надавачів посередницьких цифрових послуг	*Стаття 4.* Звільнення від відповідальності за передачу інформації		*Стаття 5.* Кешування
	Стаття 6. Хостинг та зберігання даних		*Стаття 7.* Заборона загального моніторингу
Розділ 3. Обов'язки щодо прозорості та протидії протиправному контенту	*Стаття 8.* Механізми сповіщень про наявність протиправного контенту		*Стаття 9.* Обґрунтування рішень у разі видалення контенту, блокування акаунту чи обмеження доступу
	Стаття 10. Інститут довірених сповіщувачів		*Стаття 11.* Позасудове вирішення спорів та внутрішні системи розгляду скарг
Розділ 4. Додаткові вимоги до онлайн-платформ та маркетплейсів	*Стаття 12.* Належна перевірка продавців		Стаття 13. Заборона маніпулятивних інтерфейсів
	Стаття 14. Прозорість рекомендаційних систем та реклами		*Стаття 15.* Захист чутливих даних у таргетованій рекламі

Продовження табл. 2

Розділ 5. Системні ризики та обов'язки дуже великих онлайн-платформ	*Стаття 16.* Критерії визначення великих платформ	*Стаття 17.* Оцінка та мінімізація системних ризиків	*Стаття 18.* Незалежний аудит та доступ до даних для дослідників
Розділ 6. Координація, нагляд та співробітництво	*Стаття 19.* Координатор цифрових послуг	*Стаття 20.* Взаємодія з галузевими регуляторами	
Розділ 7. Відповідальність та санкції	*Стаття 21.* Розгляд скарг та захист прав користувачів	*Стаття 22.* Штрафні санкції	
Розділ 8. Прикінцеві та перехідні положення	*Стаття 23.* Набрання чинності	*Стаття 24.* Внесення змін до інших законів	
ВНЕСТИ ЗМІНИ ДО ЗАКОНУ УКРАЇНИ «ПРО ЗАХИСТ ЕКОНОМІЧНОЇ КОНКУРЕНЦІЇ» шляхом надання повноважень АМКУ щодо:			
Внести зміни до Постанови КМУ			
- зобов'язати операторів МІС та розробників пацієнтських сервісів надавати користувачу можливість у будь-який момент завантажити повний масив його медичних даних у структурованому, загальновживаному та машинозчитуваному форматі	встановити вимогу до МІС забезпечити наявність відкритих та стандартизованих API (Application Programming Interfaces) для підключення сторонніх авторизованих застосунків (телемедичних платформ, діагностичних гаджетів, мобільних додатків)		
- заборонити фінансові та технічні бар'єри при зміні МІС закладом, зокрема стягнення плати за «деімплементацію» чи «експорт архіву» при переході лікарні на інше програмне забезпечення	- доповнити критерії відповідності МІС вимогами щодо відсутності обмежень на експорт даних та дотримання правил відкритих API		

Використання технологій штучного інтелекту у функціонуванні системи охорони здоров'я поступово трансформується з окремого напряму технологічних інновацій у самостійний об'єкт державного регулювання. Це обумовлено виникненням принципово нових правових, безпекових, економічних, організаційних та етичних ризиків.

Встановлено, що існуюча система державного регулювання в Україні не повною мірою відповідає особливостям розроблення, впровадження та використання технологій ШІ у сфері охорони здоров'я. Серед ключових проблем визначено невизначеність відповідальності за шкоду, заподіяну внаслідок використання ШІ, невідповідність традиційних процедур оцінки та сертифікації особливостям систем, здатних до самонавчання, недостатність механізмів протидії алгоритмічній дискримінації, проблеми якості та репрезентативності даних, а також організаційні й економічні бар'єри впровадження таких технологій. Відтак державне регулювання має формувати комплекс взаємопов'язаних правових, організаційних та інституційних інструментів, які одночасно забезпечуватимуть безпеку людини, захист медичних даних, дотримання етичних вимог та створення умов для технологічних інновацій.

Доведено, що формування державної політики у сфері медичного ШІ в Україні має здійснюватися з урахуванням трьох груп факторів: політико-правових (гармонізація з EU AI Act та Product Liability Directive), соціально-економічних (обмеженість бюджетного фінансування через наслідки війни) та ментально-культурних (подолання застережень суспільства та медичної спільноти щодо етичності ШІ). Особливого значення набуває євроінтеграційний вектор, який визначає необхідність адаптації національної моделі регулювання до нормативних підходів Європейського Союзу із одночасним урахуванням національних інтересів, ресурсних обмежень системи охорони здоров'я та готовності суспільства і медичних працівників до використання нових технологій.

Запропоновано комплексний механізм державного регулювання використання технологій штучного інтелекту у функціонуванні системи охорони здоров'я, центральним елементом якого визначено формування цілісної нормативно-правової та інституційної моделі регулювання ШІ (табл. 3). Її основу запропоновано сформувати шляхом прийняття рамкового Закону України «Про штучний інтелект», що має закріпити ризик-орієнтований підхід, вимоги до безпеки, прозорості та людського контролю, розподіл відповідальності між суб'єктами, механізми державного нагляду, економічного стимулювання, міжвідомчої взаємодії та міжнародного співробітництва, а також спеціальний правовий режим використання ШІ в охороні здоров'я. Водночас законодавче врегулювання має бути доповнене системою підзаконного нормативно-правового та технічного регулювання, що забезпечуватиме практичну реалізацію встановлених законом вимог. Запропоновано врегулювати постійний моніторинг алгоритмів після їх впровадження у закладах охорони здоров'я, постринковий контроль систем, що самонавчаються, синхронізацію вимог до високоризикових систем ШІ з технічним регулюванням медичних виробів, обов'язкове інформування пацієнта про застосування ШІ, а також порядок підключення і верифікації ШІ-модулів в електронній системі охорони здоров'я.

Таблиця 3. Комплексний механізм державного регулювання використання технологій штучного інтелекту у функціонуванні системи охорони здоров'я

РОЗРОБКА ТА ПРИЙНЯТТЯ РАМКОВОГО ЗАКОНУ УКРАЇНИ ПРО ШТУЧНИЙ ІНТЕЛЕКТ			
Розділ 1. Загальні положення	*Стаття 1.* Сфера застосування Закону	*Стаття 2.* Визначення термінів	*Стаття 3.* Принципи регулювання сфери ШІ
	Стаття 4. Суб'єкти відносин у сфері ШІ	*Стаття 5.* Забезпечення цифрової грамотності	
Розділ 2. Класифікація систем ШІ за рівнем ризику	*Стаття 6.* Категоризація ризиків	*Стаття 7.* Системи ШІ високого ризику	
	Стаття 8. Заборонені системи ШІ (Неприйнятний ризик)	*Стаття 9.* Системи ШІ з обмеженим та мінімальним ризиком	
	Стаття 10. Інші системи ШІ та спеціальні вимоги щодо прозорості	*Стаття 11.* Система управління ризиками	
Розділ 3. Вимоги до систем ШІ високого ризику	*Стаття 12.* Управління та забезпечення якості даних	*Стаття 13.* Технічна документація та ведення записів	*Стаття 14.* Прозорість та інформація для користувача
	Стаття 15. Автоматичне журналювання діяльності системи ШІ	Стаття 16. Людський нагляд	
	Стаття 17. Особливості адаптивних систем та істотних модифікацій ШІ	*Стаття 18.* Точність, надійність та кібербезпека	
Розділ 4. Суб'єкти у сфері ШІ та їхні обов'язки	*Стаття 19.* Обов'язки провайдера системи ШІ	*Стаття 20.* Обов'язки суб'єкта, який використовує систему ШІ	
	Стаття 21. Обов'язки імпортера та дистриб'ютора	*Стаття 22.* Обов'язки уповноваженого представника	*Стаття 23.* Зміна статусу суб'єкта у разі істотної модифікації системи
Розділ 5. Оцінка відповідності, реєстрація та допуск до використання	*Стаття 24.* Оцінка відповідності систем ШІ високого ризику	*Стаття 25.* Органи з оцінки відповідності	
	Стаття 26. Декларація відповідності	*Стаття 27.* Державна реєстрація високоризикових систем ШІ	*Стаття 28.* Істотні зміни системи та повторна оцінка відповідності
Розділ 6. Права фізичних осіб та захист від ризиків ШІ	*Стаття 28.* Право на інформацію про застосування ШІ	*Стаття 29.* Оцінка впливу систем ШІ на основоположні права	*Стаття 30.* Право на звернення та оскарження
	Стаття 31. Право на отримання інформації щодо рішення, прийнятого із застосуванням високоризикової системи ШІ	*Стаття 32.* Захист від дискримінаційних та упереджених рішень	

Продовження табл. 3

Розділ 7. Особливості використання ШІ в окремих сферах	*Стаття 33.* Загальні засади галузевого регулювання	*Стаття 34.* Штучний інтелект у сфері охорони здоров'я	*Стаття 35.* Використання ШІ як медичного виробу або складової медичного виробу
	Стаття 36. Використання ШІ для підтримки клінічних рішень	*Стаття 37.* Використання ШІ для наукових досліджень та вторинного використання медичних даних	*Стаття 38.* Особливості людського контролю за медичними системами ШІ
Розділ 8. Економічні механізми розвитку та впровадження ШІ	*Стаття 39.* Державна підтримка розроблення та впровадження ШІ	*Стаття 40.* Фінансування досліджень та інновацій у сфері ШІ	*Стаття 41.* Економічні стимули для впровадження безпечних систем ШІ
	Стаття 42. Особливості фінансування та відшкодування вартості технологій ШІ в охороні здоров'я	*Стаття 43.* Державна підтримка доступу закладів охорони здоров'я до технологій ШІ.	
Розділ 9. Державне управління та державний нагляд у сфері ШІ	*Стаття 44.* Кабінет Міністрів України	*Стаття 45.* Центральний орган державної влади, відповідальний за формування державної політики у сфері ШІ	*Стаття 46.* Компетентний орган державного нагляду у сфері ШІ
	Стаття 47. Галузеві компетентні органи	*Стаття 48.* Повноваження МОЗ України щодо медичних систем ШІ	*Стаття 49.* Державний реєстр систем ШІ високого ризику
Розділ 10. Міжвідомча та міжнародна взаємодія у сфері штучного інтелекту	*Стаття 50.* Засади міжвідомчої взаємодії у сфері штучного інтелекту	*Стаття 51.* Координація діяльності органів державної влади у сфері штучного інтелекту	*Стаття 52.* Інформаційна взаємодія та обмін даними між органами державної влади
	Стаття 53. Міжвідомча взаємодія у сфері застосування ШІ в охороні здоров'я	*Стаття 54.* Міжнародне співробітництво України у сфері штучного інтелекту	*Стаття 55.* Взаємодія з інституціями та компетентними органами ЄС
	Стаття 56. Міжнародний обмін інформацією про ризики та інциденти у сфері штучного інтелекту	Стаття 57. Міжнародне науково-технологічне співробітництво та трансфер технологій штучного інтелекту	
Розділ 10. Постринковий моніторинг та реагування на інциденти	*Стаття 51.* Постринковий моніторинг	*Стаття 52.* Коригувальні заходи	
	Стаття 52. Повідомлення про серйозні інциденти	*Стаття 54.* Тимчасове обмеження, призупинення та заборона використання системи ШІ	

Продовження табл. 3

Розділ 11. Підтримка інновацій	*Стаття 55.* Регуляторні пісочниці у сфері ШІ	*Стаття 56.* Тестування систем ШІ в реальних умовах	*Стаття 57.* Підтримка стартапів, малих і середніх підприємств та наукових установ
Розділ 12. Відповідальність та заходи державного примусу	*Стаття 58.* Відповідальність за порушення законодавства у сфері ШІ	*Стаття 59.* Фінансові санкції	
	Стаття 60. Відшкодування шкоди, завданої системою ШІ	*Стаття 61.* Особливості доказування та доступу до інформації	
Розділ 13. Прикінцеві та перехідні положення	Перехідний період	Внесення змін до законів	
ВНЕСЕННЯ ЗМІН ДО ЗАКОНУ УКРАЇНИ «ОСНОВИ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ОХОРОНУ ЗДОРОВ'Я»			
внести зміни до статей			
Доповнити Статтю 3 новими термінами: - медична система штучного інтелекту; - система підтримки прийняття клінічних рішень на основі штучного інтелекту	*Доповнити статтею 35-7:* - Стаття 35-7. Застосування технологій штучного інтелекту в медичній практиці	*Доповнити статтю 39 новою частиною:* - щодо інформування	
Доповнити Статтю 77 новою частиною: - щодо цивільно-правової відповідальності медичних працівників	*Доповнити статтю 78 новою частиною:* - щодо цифрових компетенцій	*Доповнити статтю 39-1 новою частиною:* - щодо перегляду	
ВНЕСЕННЯ ЗМІН ДО ДІЮЧИХ ТА ПРИЙНЯТТЯ НОВИХ ПІДЗАКОННИХ НОРМАТИВНО-ПРАВОВИХ АКТІ			
- прийняття Постанови КМУ про затверд-ження порядку постій-ного моніторингу алгоритмів після їх впровадження у лікарнях	- впровадження технічних стандартів для забезпечення пост-маркетингового моніторингу алгоритмів, що самонавчаються	- внесення змін до Технічного регламенту щодо медичних виро-бів з метою синхронізації вимог до ШІ-систем високого ризику	
- наказ МОЗ про обов'язкове інформування пацієнта про використання ШІ під час його діагностики чи розробки плану лікування	- прийняття Постанови КМУ про затвердження Порядку підключе-ння та верифікації ШІ-модулів у рамках Електронної системи охорони здоров’я	- розробка стандарту підготовки деперсоналізованих/анонімізованих медичних даних (знімків КТ, МРТ, ЕКГ, лабораторних карт) для навчання та тестування ШІ-систем	

Це дозволить забезпечити перехід від фрагментарного регулювання окремих технологій та пов'язаних із ними правовідносин до комплексної моделі державного регулювання всього життєвого циклу систем ШІ в охороні здоров'я (розроблення, навчання, тестування та допуску до використання до постринкового моніторингу, реагування на інциденти та припинення використання). Такий підхід дозволяє поєднати регуляторну, інституційну, організаційну, інформаційну, економічну та безпекову складові державного впливу та забезпечити їх спрямування не на обмеження технологічного розвитку, а на формування контрольованого середовища його реалізації.

Реалізація запропонованого комплексного механізму створить передумови для керованого, безпечного та людиноцентричного впровадження ШІ в цифрову СОЗ України, забезпечить баланс між стимулюванням інновацій і захистом прав пацієнта, підвищить прозорість та підзвітність використання алгоритмічних систем і сприятиме наближенню національної системи державного регулювання до регуляторної моделі ЄС. У ширшому контексті це дозволяє розглядати державне регулювання ШІ не як окремий напрям цифрової політики, а як складову державного управління цифровою трансформацією СОЗ, від ефективності якої залежатимуть якість, доступність, безпека та інноваційність медичної допомоги.

Розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров'я є критичною передумовою для її євроінтеграції та відповідності сучасним регламентам ЄС. Для вирішення визначеної проблеми розроблено комплексний механізм розширення інституційної спроможності державного управління цифровою трансформацією СОЗ, який передбачає поєднання утворення нових спеціалізованих суб'єктів, розширення компетенцій існуючих суб'єктів та формування міжінституційної взаємодії (табл. 4). Обґрунтовано альтернативні моделі формування суб'єкту державного управління щодо вторинного використання медичних даних та визначено організаційно-інституційне забезпечення транскордонної взаємодії з європейськими мережами. Запропоновано інституційну модель регулювання ШІ в медицині через поєднання загального регулятора ШІ, галузевої компетенції МОЗ України та ринкового нагляду Держлікслужби; визначено напрями розвитку інституційної спроможності у сферах кібербезпеки, захисту персональних даних та конкуренції.

Запропонований підхід, ґрунтується на функціональному розподілі регуляторних, дозвільних, наглядових, контрольних, інформаційно-комунікаційних та координаційних повноважень відповідно до ключових об'єктів цифрової трансформації. Механізм дозволяє сформувати інституційно цілісну систему державного управління цифровою трансформацією СОЗ, у якій усуваються прогалини та невизначеність компетенцій, розмежовуються функції між суб'єктами та одночасно забезпечується їх координація. Системна реалізація окреслених організаційно-правових, інфраструктурних та контрольно-наглядових заходів дозволить подолати наявні інституційні розриви, збалансувати процеси впровадження високотехнологічних цифрових рішень із вимогами безпеки даних, а також створити стійку, прозору й високоадаптивну модель державного управління, спроможну ефективно захищати права громадян.

Таблиця 4. Комплексний механізм розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров'я

<table>
<tr><td colspan="4">РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ВТОРИННОГО ВИКОРИСТАННЯ МЕДИЧНИХ ДАНИХ (HEALTH DATA ACCESS BODY (ОРГАН З ДОСТУПУ ДО МЕДИЧНИХ ДАНИХ))</td></tr>
<tr><td colspan="2">утворення нового суб'єкту державного управління</td><td colspan="2">наділення відповідними повноваженнями існуючого суб'єкту</td></tr>
<tr><td colspan="2">Утворення Національного агентства з доступу до медичних даних (HDAB Ukraine)</td><td colspan="2">- наділення повноважень та формування структурного підрозділу на базі ДУ «Центр громадського здоров'я МОЗ України»</td></tr>
<tr><td colspan="2" rowspan="2">- орган центральної виконавчої влади, що наділений відповідними повноваженнями та має повну функціональну незалежність та автономність прийняття рішень щодо для забезпечення безпечного вторинного використання медичних даних</td><td colspan="2">- наділення повноважень та формування структурного підрозділу в структурі Міністерства охорони здоров'я України</td></tr>
<tr><td colspan="2">- наділення повноважень та формування структурного підрозділу на базі ДП «Електронне здоров'я»</td></tr>
<tr><td colspan="4">основні завдання</td></tr>
<tr><td>- видача дозволів на доступ до даних</td><td>- забезпечення анонімізації та псевдонімізації</td><td>- управління безпечними середовищами обробки</td><td>контроль вивантаження результатів</td></tr>
<tr><td>- адміністрування реєстру відмов пацієнтів</td><td>- забезпечення інтеграції в єдину мережу HealthData@EU</td><td>- прийняття участі в наукових дослідженнях</td><td>- регуляторна діяльність щодо суб'єктів медичних даних</td></tr>
<tr><td colspan="4">НАЛАГОДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ МІЖ ЦИФРОВОЮ СИСТЕМОЮ НАЦІОНАЛЬНОЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я З ЄВРОПЕЙСЬКИМИ ТРАНСКОРДОННИМИ МЕРЕЖАМИ</td></tr>
<tr><td>Організаційно-інституційне забезпечення</td><td>Інформаційно-інфраструктурне забезпечення</td><td colspan="2">Нормативно-правове забезпечення</td></tr>
<tr><td>надати функції та статус NCPH ДП «Електронне здоров'я», яке є адміністратором Центральної бази даних ЕСОЗ)</td><td>побудова вузла взаємодії (NCPH Node);
- впровадження єдиного формату EEHRxF;
- гармонізація медичних кодифікаторів</td><td colspan="2">- внесення змін до Постанови КМУ Про затвердження Порядку функціонування ЕСОЗ
- розробка Порядку транскордонного обміну медичними даними;
- угода про приєднання до мережі</td></tr>
<tr><td colspan="4">РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ</td></tr>
<tr><td>утворення спеціалізованого суб'єкту державного управління, що вступатиме Регулятором технологій штучного інтелекту</td><td colspan="2">- розширення повноважень ДЛЗ (Держлікслужби) щодо ринкового нагляду за ШІ-медичними виробами</td><td>- внесення змін до організаційної структури МОЗ щодо регулювання використання ШІ в медицині</td></tr>
</table>

Продовження табл. 4

<table>
<tr><td colspan="4">РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ЩОДО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ</td></tr>
<tr><td colspan="2">Варіант 1. Офіційне надання Держспецзв'язку статусу Національного органу із сертифікації кібербезпеки (NCCA)</td><td colspan="2">Варіант 2. Утворення Національного агенства із сертифікації кібербезпеки</td></tr>
<tr><td colspan="4">РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ДЕРЖАВНОГО УПРАВЛІННЯ ЩОДО ЗАХИСТУ МЕДИЧНИХ ДАНИХ</td></tr>
<tr><td colspan="4">- створення незалежного наглядового органу - НАЦІОНАЛЬНА КОМІСІЯ З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ</td></tr>
<tr><td colspan="4">ключові повноваження в реалізації механізмів державного управління цифровою. трансформацією системи охорони здоров’я</td></tr>
<tr><td>регуляторний нагляд</td><td>затвердження стандартів та методологій</td><td>аудит та контроль медичних ШІ-алгоритмів</td><td>реагування на інциденти та розслідування витоків</td></tr>
<tr><td>- здійснення перевірок Електронної системи охорони здоров’я, Медичних інформаційних систем, лабораторних баз даних та реєстрів на предмет дотримання правил обробки чутливих даних про здоров'я та принципів «приватності за замовчуванням»</td><td>- розробка та затвердження інструкцій, правил анонімізації / псевдонімізації медичних даних, а також типових методологій оцінки впливу на захист даних для розробників MedTech-рішень, телемедичних платформ і закладів охорони здоров’я</td><td>- перевірка прозорості та безпеки автоматизованих систем прийняття клінічних рішень і діагностичних нейромереж, щоб унеможливити алгоритмічні помилки, упередженість або несанкціоноване профілювання пацієнтів</td><td>- прийом 72-годинних сповіщень про кіберінциденти й витоки медичних даних (Data Breaches), проведення оперативних розслідувань, видача обов'язкових до виконання приписів та накладення санкцій на порушників</td></tr>
<tr><td colspan="4">ВНЕСТИ ЗМІНИ ДО ЗАКОНУ УКРАЇНИ «ПРО ЗАХИСТ ЕКОНОМІЧНОЇ КОНКУРЕНЦІЇ»
шляхом надання повноважень АМКУ щодо:</td></tr>
<tr><td colspan="2">- право визначати «Цифрових гейткіперів»: встановити критерії для цифрових медичних платформ (за кількістю активних пацієнтів/лікарів на місяць та оборотом)</td><td>заборона прямої та опосередкованої пріоритетизації: заборона гейткіперам застосовувати алгоритми, що надають вищий рейтинг власним послугам</td><td>забезпечення рівних умов: вимога застосовувати прозорі, об'єктивні та недискримінаційні параметри ранжування для всіх учасників ринку</td></tr>
<tr><td colspan="2">- право аудіювати алгоритми та аналізувати вихідний код: АМКУ має отримати доступ до технічної документації та алгоритмів видачі цифрових сервісів для перевірки на наявність прихованої пріоритетизації власних продуктів</td><td colspan="2">- застосування оборотних штрафів та строкових приписів: повноваження видавати приписи про негайну зміну алгоритму та накладати штрафи за порушення цієї заборони</td></tr>
</table>

Його реалізація створює інституційні передумови для інтеграції цифрової СОЗ України до європейського цифрового простору, безпечного використання медичних даних і технологій ШІ, захисту прав громадян та забезпечення належного державного нагляду за цифровими процесами у сфері охорони здоров'я.

ВИСНОВКИ

1. Визначено сукупність факторів, що впливають на формування та реалізацію державно-управлінських рішень у сфері цифрової трансформації системи охорони здоров'я. Так, політико-правові фактори (правові, політичні, євроінтеграційні) визначають особливості легітимізації цифрових практик та гармонізації їх із європейськими стандартами. Ресурсні (фінансові, кадрові, інфраструктурні, техніко-технологічні) фактори створюють матеріальний і технологічний фундамент реформи та забезпечують комплексність досягнення цілей цифрової трансформації. Державно-управлінські (інституційні, організаційні, інформаційні) фактори визначають керованість, узгодженість дій суб'єктів державного управління та якість прийняття рішень на основі даних. Управління безпековими (інформаційно-безпекові, кібербезпекові, медико-безпекові) факторами має забезпечити життєздатність, захищеність та безперервність функціонування медичної системи в умовах криз і загроз. Ефективність державного управління цифровою трансформацією галузі залежить від здатності органів публічної влади забезпечити синергію між цими чинниками. Цифрова трансформація СОЗ є не лише технічним оновленням інфраструктури, а виступає стратегічним інструментом оптимізації обмежених ресурсів держави, зниження соціальної напруги та гарантування національної безпеки.

2. Проведений бібліометричний аналіз публікацій, відібраних у наукометричній базі Scopus за пошуковим запитом «digital healthcare systems», засвідчив стрімке зростання наукового інтересу до цифрових систем охорони здоров'я, особливо після 2020 р. Основними напрямами досліджень є застосування штучного інтелекту, машинного навчання та великих даних у медицині, розвиток електронних медичних записів і телемедицини, а також забезпечення конфіденційності та кібербезпеки. Найбільш поширеними термінами є health care, healthcare systems, medical computing, electronic health record та artificial intelligence. Розподіл публікацій за галузями знань підтвердив міждисциплінарний характер проблематики з переважанням комп'ютерних наук, інженерії та медицини. Провідні позиції за кількістю публікацій і цитувань займає Індія, яка також є центральним вузлом міжнародного наукового співробітництва. Значну активність демонструють США, Південна Корея, Велика Британія, Австралія та Китай, а серед основних джерел фінансування переважають державні фонди й профільні установи Китаю та Південної Кореї. Отже, цифрові системи охорони здоров'я сформувалися як динамічний міжнародний напрям, що поєднує технологічні, медичні, управлінські та безпекові аспекти. Подальші дослідження доцільно спрямувати на безпечне використання штучного інтелекту, сумісність цифрових платформ, захист медичних даних та оцінювання ефективності впроваджених цифрових рішень.

3. Розширено теоретичне наукове значення державного управління через уточнення змісту понять та категорій, а саме: система охорони здоров'я (багаторівнева соціально-економічної система, що об'єднує взаємопов'язані

суб’єкти (суб’єкти державного регіонального, місцевого управління, заклади охорони здоров’я, виробників та пастильників ліків, наукові установи, заклади вищої освіти, інститути громадського суспільства та інші), ресурси, інфраструктуру та процеси (управлінські, медичні (профілактики, діагностування, лікування, реабілітація), організаційні, інформаційні, регламентаційні), функціонування якої регулюється державою та спрямована на формування, збереження, зміцнення та відновлення здоров’я населення та забезпечення високого рівня громадського здоров’я як складової соціальної функції), цифрова трансформація (цілеспрямований, керований і комплексний процес якісної зміни властивостей, структури, функцій, процесів, моделей взаємодії та способів функціонування певного об’єкта шляхом системного впровадження й використання цифрових технологій, даних та цифрових рішень, що приводить до формування його нового стану і потребує відповідних організаційних, інституційних, правових, кадрових та ресурсних змін) та цифрова трансформація системи охорони здоров’я (цілеспрямований, комплексний і керований процес якісної зміни структури, властивостей, функцій, процесів, механізмів державного управління, моделей взаємодії суб’єктів та способів реалізації медичних послуг шляхом системного впровадження цифрових технологій, цифрових даних і цифрових сервісів, результатом якого є формування цифрової системи охорони здоров’я, здатної забезпечити більш ефективне, доступне, безпечне, інтегроване та людиноцентричне функціонування сфери охорони здоров’я).

4. У результаті дослідження розроблено цілісну систему властивостей СОЗ, яка об'єднує її базові соціально-економічні характеристики та параметри розвитку. Встановлено, що цифрова трансформація якісно змінює ці властивості, наділяючи систему новими перевагами (інтероперабельність, прогностичність, масштабованість) та викликами (кібер-, технологічна та інфраструктурна залежності). Обґрунтована система властивостей доводить, що цифровізація вимагає від держави не лише технічних рішень, а й комплексної трансформації управління (фінансового, правового та організаційного забезпечення). Виявлена специфіка цифрових переваг і загроз формує підґрунтя для розробки адекватних механізмів державного захисту та розвитку сфери. Запропонована система властивостей розширює теоретичне знання й слугує методологічною основою для прийняття ефективних управлінських рішень.

5. Зважаючи на нові властивості системи охорони здоров’я, розроблено багаторівневу структуру принципів державного управління цифровою трансформацією СОЗ та власне функціонуванням цифрової системи охорони здоров’я. Вона охоплює: 1) стратегічні принципи (людиноцентричність, випереджувальний розвиток, євроінтеграція), які задають довгострокові орієнтири державної політики; 2) організаційні принципи (інституційна взаємодія, координованість, субсидіарність) регламентують розподіл повноважень та порядок прийняття управлінських рішень; 3) принципи цифрового функціонування (даноцентричність, цифровий доступ, масштабованість) визначають безпосередні вимоги до використання інформаційних ресурсів та інфраструктури; 4) принципи забезпечення регулюють нормативно-правові, фінансові, кадрові й безпекові умови для стабільного та етичного розвитку цифрового середовища.

6. Методологію державного управління розвинено шляхом обґрунтування триєдиної структури його об’єкта, що охоплює процеси трансформації, перехідний період та функціонування зрілої цифрової СОЗ. Доведено, що державне управління в цій сфері є не статичним станом, а керованим переходом через синергію правового, організаційного, інформаційного, кадрового та фінансового механізмів. Уточнено зміст мети та завдань управління з урахуванням полісуб’єктності, динамічності й багаторівневості СОЗ. Визначено ключові вектори розвитку методів реалізації зазначених механізмів для досягнення цілісності та практичної спрямованості управлінського впливу.

7. Встановлено, що сучасна модель цифрової трансформації СОЗ ґрунтується на людиноцентричному підході, відповідно до якого цифрові технології використовуються не лише для автоматизації окремих процесів, а й для забезпечення доступності, безперервності, якості та персоналізації медичної допомоги. Світовий досвід підтверджує, що успішність цифрових перетворень безпосередньо залежить від рівня розвитку цифрового врядування, наявності інтегрованих інформаційних систем, ефективного управління медичними даними, нормативно-правового забезпечення та розвитку цифрових компетентностей населення і медичних працівників.

8. Дослідження європейського досвіду засвідчило формування єдиного цифрового простору СОЗ, у межах якого пріоритетного значення набувають інтероперабельність медичних інформаційних систем, розвиток електронних медичних записів, транскордонний обмін медичними даними та використання цифрових сервісів для забезпечення мобільності пацієнтів. Визначено, що створення Європейського простору даних СОЗ формує новий етап розвитку цифрового здоров’я, заснований на безпечному використанні медичних даних для лікування, наукових досліджень, управлінської діяльності та інноваційного розвитку галузі.

9. У результаті аналізу сучасного стану цифровізації охорони здоров’я України встановлено, що національна система охорони здоров’я демонструє високі темпи цифрової трансформації та поступово інтегрується до європейського цифрового середовища. Запровадження електронної СОЗ, розвиток цифрових медичних сервісів, удосконалення механізмів управління медичними даними та розширення електронної взаємодії між усіма учасниками медичної системи створили передумови для формування цілісної цифрової екосистеми СОЗ навіть в умовах воєнного стану. Узагальнення результатів дослідження дає підстави стверджувати, що подальший розвиток СОЗ у світі, країнах ЄС та Україні буде пов’язаний із поглибленням використання великих масивів медичних даних, технологій штучного інтелекту, телемедицини, персоналізованої медицини та цифрових платформ управління СОЗ. Це обумовлює необхідність удосконалення механізмів публічного управління цифровою трансформацією галузі, посилення захисту медичних даних, забезпечення інтероперабельності цифрових систем та розвитку цифрової компетентності учасників медичних відносин.

10. ЄС пройшов шлях від фрагментарних ініціатив 1990-х років до цілісного єдиного технологічного простору, побудованого на принципах пацієнтоцентричності. Нормативне ядро цього простору становлять Регламент (ЄС) 2025/327 (EHDS), Регламент (ЄС) 2024/1689 (AI Act), Регламент (ЄС) 2016/679

(GDPR), Регламент (ЄС) 910/2014 (eIDAS), Регламент (ЄС) 2022/868 (Data Governance Act), Регламент (ЄС) 2023/2854 (Data Act), галузеві Регламент (ЄС) 2017/745 (MDR) і Регламент (ЄС) 2017/746 (IVDR), а також Регламент (ЄС) 2022/2065 (DSA) та Регламент (ЄС) 2022/1925 (DMA). Водночас європейська модель має ризики регуляторного перевантаження, алгоритмічної дискримінації та правової невизначеності щодо контролю особи над власними даними. Для України, яка вже створила базові цифрові сервіси (е-рецепти, медичні записи), пріоритетом є врегулювання вторинного використання даних та досягнення повної технічної інтероперабельності з ЄС. Гармонізація законодавства повинна відбуватися шляхом гнучкої адаптації, а не механічного копіювання, із визначенням компетентних органів цифрової охорони здоров'я. Реалізація цих стратегічних кроків вимагає від держави належного кадрового, інфраструктурного та фінансового забезпечення.

11. Аналіз регуляторної бази ЄС свідчить, що безпека цифрової охорони здоров’я забезпечується комплексною системою, яка охоплює вироби, інфраструктуру та процеси. Регламент (ЄС) 2017/745 (MDR), Регламент (ЄС) 2017/746 (IVDR), Директива (ЄС) 2022/2555 (NIS2), Регламент (ЄС) 2019/881 (Cybersecurity Act) та Регламент (ЄС) 2024/2847 (Cyber Resilience Act) доповнюють один одного й охоплюють усі рівні від медичних пристроїв до кіберстійкості самих закладів. Головним бар’єром реалізації цих норм у ЄС виявилася не якість законів, а нестача інституційної та інфраструктурної спроможності. Для України адаптація цього законодавства має полягати у змістовному зближенні норм із ризик-орієнтованим підходом і пріоритетом розбудови власної інституційної бази. Насамперед необхідно розширити мережу органів оцінки відповідності, підготувати кадри та надати закладам централізовану підтримку з кіберзахисту. В умовах збройної агресії безпека медичних реєстрів і безперебійний доступ до цифрових сервісів є прямою складовою національної безпеки.

12. Дослідження засвідчило, що Бельгія сформувала розгалужену федеральну систему із цифровою платформою eHealth та спеціалізованими механізмами кібербезпеки. Модель Данії вирізняється високим рівнем централізованої координації, розвиненою спільною інфраструктурою та чітким розподілом відповідальності між державою, регіонами й муніципалітетами. Естонія побудувала повністю інтегровану цифрову систему охорони здоров’я на основі єдиного простору медичних даних, державної електронної ідентифікації та комплексного кіберзахисту. Усі три країни успішно адаптували національне законодавство до вимог регуляторних актів ЄС, забезпечивши сумісність даних і надійний захист персональної інформації пацієнтів. Для України цей досвід є цінним орієнтиром для розбудови єдиної нормативно-інституційної системи, посилення секторної кібербезпеки та безпечного впровадження технологій штучного інтелекту.

13. Здійснено комплексний аналіз стану відповідності вітчизняної системи державного управління цифровою трансформацією СОЗ регуляторним актам ЄС та розроблено механізм її адаптації. Сформований підхід спрямований на подолання суттєвого розриву між наявною інфраструктурою електронної СОЗ і європейськими директивами та регламентами. Для вирішення зазначеної проблеми запропоновано структуру та змістовне наповнення сукупності нових нормативно-правових актів, зокрема: Закону України «Про захист персональних даних»; Закон України «Про обіг

медичних даних», Рамковий Закон України «Про штучний інтелект»; Закон України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації»; Закон України «Про управління даними»; Закон України «Про цифрові послуги». Запропоновано сукупність змін до законодавчих актів, що полягають у наступному: Закон України «Основи законодавства України про охорону здоров'я»; Закон України «Про захист інформації в інформаційно-комунікаційних системах»; Закон України «Про захист економічної конкуренції». На рівні підзаконного регулювання обґрунтовано необхідність оновлення Постанови КМУ № 411, Технічних регламентів щодо медичних виробів (№ 753, № 754) під стандарти MDR/IVDR та розробки нових порядків класифікації ШІ-систем і проведення DPIA. У контексті інституційної спроможності запропоновано створення Національного органу з доступу до медичних даних (HDAB Ukraine), Національної точки контакту (NCPH). Таке комплексне рішення забезпечує перехід від базової функціональної цифровізації до побудови повноцінної, кіберстійкої та інтегрованої в європейський цифровий простір екосистеми eHealth.

14. Технології ШІ у СОЗ перетворюються з технічного інструменту на самостійний об'єкт державного регулювання через виникнення специфічних правових, етичних та безпекових ризиків, що вимагає переходу від фрагментарного контролю до комплексної моделі управління всім життєвим циклом систем ШІ. Обґрунтовано, що формування державної політики в Україні має базуватися на гармонізації з нормами ЄС (зокрема EU AI Act та Product Liability Directive), урахуванні соціально-економічних обмежень та подоланні ментально-культурних бар'єрів. Центральним елементом запропонованого комплексного механізму є прийняття рамкового Закону України «Про штучний інтелект» із запровадженням ризик-орієнтованого підходу, чітким розподілом відповідальності, людським контролем та створенням спеціального правового режиму для медицини, що доповнюється системою підзаконного й технічного регулювання (постринковий моніторинг, синхронізація із вимогами до медичних виробів та інформування пацієнтів). Реалізація цього підходу дозволить сформувати безпечне, прозоре й людиноцентричне середовище впровадження інновацій, збалансувати захист прав пацієнтів зі стимулюванням MedTech-сектору та забезпечити повноцінну інтеграцію цифрової СОЗ України до європейського простору.

15. Проведене дослідження засвідчило необхідність розширення інституційної спроможності державного управління цифровою трансформацією СОЗ, зумовлену появою нових об'єктів регулювання та необхідністю адаптації до вимог ЄС. Запропоновано комплексний механізм такого розширення, що передбачає утворення Національного агентства з доступу до медичних даних (HDAB Ukraine), Національного регулятора у сфері штучного інтелекту, Національного центру кібербезпеки цифрової СОЗ, а також відповідних спеціалізованих структурних підрозділів у системі органів державного управління та розширення повноважень існуючих суб'єктів у сферах захисту персональних даних, ринкового нагляду за ШІ-медичними виробами та регулювання цифрових ринків. Реалізація запропонованих положень дозволить сформувати цілісну інституційну систему державного управління цифровою трансформацією охорони здоров'я та забезпечити її функціональну сумісність з інституційною моделлю цифрового простору ЄС.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації:

1. Криза системи охорони здоров'я: монографія / За загальною редакцією Д.О. Грицишена. Житомир: Видавничий дім «Бук-друк», 2024. 696 с. *Особистий внесок: визначено цифрову трансформацію як стратегічний напрям підвищення адаптивності, стійкості та результативності державного управління системою охорони здоров'я.*

2. Дмитренко І.А. Державне управління цифровою трансформацією системи охорони здоров'я: монографія. – К. : ТОВ «Наукове видавництво "Нова думка"», 2026. 300 с.

3. Herasymenko O., Smolych D., Bavyko O., Dmytrenko I., Martyniuk O. Updating Mechanisms for Cooperation between the State and Business to Stimulate Economic Development. *OIDA International Journal of Sustainable Development*. 2026. Vol. 19, Iss. 06, Pg. 25-38. DOI: https://doi.org/10.64211/oidaijsd190602 (Scopus). *Особистий внесок: досліджено та обґрунтовано напрями оновлення механізмів взаємодії держави та бізнесу як важливої передумови стимулювання економічного розвитку.*

4. Somak O., Dmytrenko I., Suray I., Nakonechnyi O. Innovative practices of public administration: approaches to public sector management in the era of digitalization and open government. *Journal of Theoretical and Applied Information Technology*. 2026. Vol.104. No.2. Pp. 270-285. (Scopus). *Особистий внесок: досліджено сучасні інноваційні практики публічного управління та обґрунтовано нові підходи до управління державним сектором в умовах цифровізації та розвитку концепції відкритого уряду.*

5. Grytsyshen D., Rachynskyi A., Sergiienko L., Grynchuk N., Dmytrenko I. The potential of public-private collaborations in the european union: practices for ukraine's post-war reconstruction. *Notas Economicas*. 2025. Iss. 60, Pp. 75-91. DOI: https://doi.org/10.14195/2183-203X_60_5 (Scopus). *Особистий внесок: проаналізовано основні механізми державно-приватного партнерства, що застосовуються в державах ЄС, а також визначено їх роль у системі охорони здоров'я.*

6. Bobak A., Vivsyannyk O, Khanina O., Kazarian A., Dmytrenko I. Public Administration in the Healthcare System: Prospects for Modernization. *Espacio Abierto.* 2026. Vol. 35.Iss. 4. Pp. 50-70. DOI: https://doi.org/10.5281/zenodo.21315285 (WoS). *Особистий внесок: досліджено сучасний стан та перспектив модернізації державного управління у системі охорони здоров'я.*

7. Grytsyshen D., Sergiienko L., Dmytrenko I., Abdallah I., Shpak D. State policy of ensuring the financial security of the healthcare system in crisis conditions. *Financial And Credit Activity-Problems Of Theory And Practice*. 2026. Vol. 1. Iss. 66. Pp. 533-543. DOI: https://doi.org/10.55643/fcaptp.1.66.2026.5145 (WoS). *Особистий внесок: проаналізовано сучасні загрози фінансовій стійкості системи охорони здоров'я, визначено основні ризики та чинники, що впливають на стабільність її фінансового забезпечення.*

8. Parubchak I., Krynychko L., Motailo O., Dmytrenko I., Zakharov S. Formation and implementation of state policy to ensure the financial sustainability of the health care system in indeterminate conditions. *Financial And Credit Activity-Problems Of Theory And Practice*. 2026. Vol. 2. Iss. 67. Pp. 598-611. DOI:

https://doi.org/10.55643/fcaptp.2.67.2026.5218 (WoS). *Особистий внесок: визначено ключові проблеми формування та реалізації державної політики у сфері фінансового забезпечення охорони здоров'я.*

9. Zakharchuk M., Petrukha S., Dmytrenko I., Petrukha N., Andrieiev A. Tools for Assessing the Effectiveness of Management Decisions in the Public Sector: An Analytical Approach. *Cultura Cientifica*. 2026. Iss. 24. Pp. 220-228 (WoS). *Особистий внесок: досліджено можливості використання цифрових технологій, управління даними та аналітичних інструментів для підвищення обґрунтованості управлінських рішень.*

10. Дмитренко І.А. Джерельна база наукового дослідження державного управління цифровою трансформацією системи охорони здоров'я. *Економіка, управління та адміністрування*. 2026. №1(115), С. 282–294. DOI: https://doi.org/10.26642/ema-2026-1(115)-282-294

11. Dmytrenko I. Current State and Trends in the Digitalization of Healthcare Systems in European Countries. *Public Policy and Accounting*. 2026. №1(13), С. 75–84. DOI: https://doi.org/10.26642/ppa-2026-1(13)-75-84

12. Дмитренко І. Сучасний стан та основні напрями цифрової трансформації системи охорони здоров'я України. *Society and Security*. 2026. №1(13), С. 79–89. DOI: https://doi.org/10.26642/sas-2026-1(13)-79-89

13. Дмитренко І.А. Понятійно-категоріальний апарат державного управління цифровою трансформацією системи охорони здоров'я. *Економіка, управління та адміністрування*. 2025. №4(114), С. 315–322. DOI: https://doi.org/10.26642/ema-2025-4(114)-315-322

14. Dmytrenko I. Methodological Foundations of Public Administration of the Digital Transformation of the Healthcare System. *Public Policy and Accounting*. 2025. №2(12), С. 74–80. DOI: https://doi.org/10.26642/ppa-2025-2(12)-74-80

15. Дмитренко І. Принципи державного управління цифровою трансформацією системи охорони здоров'я. *Society and Security*. 2025. №6(12), С. 121–130. DOI: https://doi.org/10.26642/sas-2025-6(12)-121-130

16. Дмитренко І.А. Світові тенденції цифровізації системи охорони здоров'я. *Економіка, управління та адміністрування*. 2025. №3(113), С.242–252. DOI: https://doi.org/10.26642/ema-2025-3(113)-242-252

17. Дмитренко І. Вплив цифровізації на властивості системи охорони здоров'я та процес прийняття державно-управлінських рішень. *Society and Security*. 2025. №5(11), С. 118–126. DOI: https://doi.org/10.26642/sas-2025-5(11)-118-126

18. Dmytrenko I. Prerequisites and Factors for the Development of Digital Transformation of the Healthcare System as an Object of Public Administration. *Public Policy and Accounting*. 2025. №1(11), С. 82–88. DOI: https://doi.org/10.26642/ppa-2025-1(11)-82-88

19. Dmytrenko I. Security Regulation of the Digital Transformation of the Healthcare System in the European Union. *Public Policy and Accounting*. 2024. № 2(10), С. 113–120. DOI: https://doi.org/10.26642/ppa-2024-2(10)-113-120

20. Дмитренко І.А. Опанасюк М.О., Петрик С.М. Бібліометричний аналіз понятійно-категоріального апарату дослідження фінансових механізмів публічного управління цифровою трансформацією системи охорони здоров'я. *Актуальні проблеми економіки*. 2026. № 1 (295). С.818-825. *Особистий внесок:*

систематизовано наукові підходи до формування понятійно-категоріального апарату дослідження фінансових механізмів публічного управління цифровою трансформацією системи охорони здоров'я.

21. Дмитренко І.А., Опанасюк М.О., Петрик С.М. Стратегічні положення управління цифровою трансформацією систем охорони здоров'я. *Актуальні проблеми економіки*. 2026. № 4 (298). С. 748-755. *Особистий внесок: визначено ключові стратегічні пріоритети та напрями цифрового розвитку галузі.*

22. Дмитренко І.А., Опанасюк М.О., Петрик С.М. Розвиток фінансових механізмів публічного управління цифровою трансформацією системи охорони здоров'я в Україні. *Актуальні проблеми економіки*. 2025. № 11 (293). С.348-355. *Особистий внесок: обґрунтовано напрями розвитку фінансових механізмів публічного управління цифровою трансформацією системи охорони здоров'я.*

23. Дмитренко І.А. Опанасюк М.О., Петрик С.М. Світові тенденції цифрової трансформації системи охорони здоров'я як об'єкта публічного управління. *Академічні візії*. 2026. №53. С. 1-21. DOI: https://doi.org/10.66556/2786-586X.53.dmytrenko-i. *Особистий внесок: визначено основні глобальні напрями цифровізації охорони здоров'я*

24. Дмитренко І.А., Опанасюк М.О., Петрик С.М. Методологічні положення дослідження фінансових механізмів публічного управління цифровою трансформацією системи охорони здоров'я. *Академічні візії*. 2025. №50. С. 1-23. *Особистий внесок: визначено основні принципи та інструменти фінансового забезпечення цифрової трансформації системи охорони здоров'я.*

Праці, які засвідчують апробацію матеріалів дисертації

25. Дмитренко І. Суспільні фактори цифрової трансформації системою охорони здоров'я. *Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття: збірник тез доповідей Міжнародної науково-практичної конференції*, 11-12 грудня 2025 року. – Житомир: Житомирська політехніка, 2025. С. 668-671

26. Дмитренко І. Нормативно-правове забезпечення цифрової трансформації системи охорони здоров'я в Європейському Союзі. *Правова політика України: історія та сучасність: матеріали VI Всеукраїнського науково-практичного семінару,* 9–10 жовтня 2025 року. Житомир: Житомирська політехніка, 2025. С. 255-257.

27. Дмитренко І. Політико-правові фактори цифрової трансформації системою охорони здоров'я. *Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття: збірник тез доповідей Всеукраїнської науково-практичної конференції з міжнародною участю*, 12-13 грудня 2024 року. – Житомир: Житомирська політехніка, 2024. С.792-796.

28. Дмитренко І. Ресурсні фактори цифрової трансформації системою охорони здоров'я. *Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття: збірник тез доповідей Всеукраїнської науково-практичної конференції*, 7-8 грудня 2023 року. – Житомир: Житомирська політехніка, 2023. С. 609-612.

29. Дмитренко І. Принципи державного управління цифровою трансформацією системи охорони здоров'я. Тези Всеукраїнської науково-практичної онлайн-

конференції аспірантів, молодих учених та студентів, присвяченої Дню науки. – Житомир : «Житомирська політехніка», 2023. С. 682-684.

30. Дмитренко І. Структуризація об'єкта державного управління цифровою трансформацією системи охорони здоров'я. Тези Всеукраїнської науково-практичної онлайн-конференції аспірантів, молодих учених та студентів, присвяченої Дню науки. – Житомир : «Житомирська політехніка», 2024. С. 723-724.

31. Дмитренко І. Система механізмів державного управління цифровою трансформацією системи охорони здоров'я. Тези Всеукраїнської науково-практичної онлайн-конференції аспірантів, молодих учених та студентів, присвяченої Дню науки. – Житомир : «Житомирська політехніка», 2025. С. 832-833.

32. Дмитренко І. Еволюція системи регулювання процесів цифрової трансформації системи охорони здоров'я Європейським Союзом. Правова політика України: історія та сучасність: матеріали IV Всеукраїнського науково-практичного семінару (м. Житомир, 6 жовтня 2023 року). – Ж.: Житомирська політехніка, 2023. С. 255-256.

33. Дмитренко І. Цифрова трансформація системи охорони здоров'я Європейським Союзом. Правова політика України: історія та сучасність: матеріали V Всеукраїнського науково-практичного семінару (м. Житомир, 10 жовтня 2024 року). Житомир: Житомирська політехніка, 2024. С. 232-234.

АНОТАЦІЯ

Дмитренко І.А. Державне управління цифровою трансформацією системи охорони здоров'я. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора наук за спеціальністю 25.00.02 – механізми державного управління (галузь знань «Публічне управління та адміністрування»). Державний університет «Житомирська політехніка», Житомир, 2026.

Визначена сукупність факторів впливають на формування та реалізацію державно-управлінських рішень в сфері цифрової трансформації системи охорони здоров'я. Так, політико-правові фактори (правові, політичні, євроінтеграційні) визначають особливості легітимізації цифрових практик та гармонізації їх із європейськими стандартами. Ресурсні (фінансові, кадрові, інфраструктурні, техніко-технологічні) фактори створюють матеріальний і технологічний фундамент реформи та забезпечують комплексність досягнення цілей цифрової трансформації. Державно-управлінські (інституційні, організаційні, інформаційні) фактори визначають керованість, узгодженість дій суб'єктів державного управління та якість прийняття рішень на основі даних. Управління безпековими (інформаційно-безпекові, кібербезпекові, медико-безпекові) факторами має забезпечити життєздатність, захищеність та безперервність функціонування медичної системи в умовах криз і загроз. Ефективність державного управління цифровою трансформацією галузі залежить від здатності органів публічної влади забезпечити синергію між цими чинниками.

Проведений бібліометричний аналіз публікацій, відібраних у наукометричній базі Scopus за пошуковим запитом «digital healthcare systems», засвідчив стрімке зростання наукового інтересу до цифрових систем охорони

здоров’я, особливо після 2020 р. Основними напрямами досліджень є застосування штучного інтелекту, машинного навчання та великих даних у медицині, розвиток електронних медичних записів і телемедицини, а також забезпечення конфіденційності та кібербезпеки. Розподіл публікацій за галузями знань підтвердив міждисциплінарний характер проблематики з переважанням комп’ютерних наук, інженерії та медицини. Провідні позиції за кількістю публікацій і цитувань займає Індія, яка також є центральним вузлом міжнародного наукового співробітництва.

Розширено теоретичне наукове значення державного управління через уточнення змісту понять та категорій, а саме: система охорони здоров’я, цифрова трансформація та цифрова трансформація системи охорони здоров’я.

Розроблено цілісну систему властивостей системи охорони здоров’я, яка об'єднує її базові соціально-економічні характеристики та параметри розвитку. Встановлено, що цифрова трансформація якісно змінює ці властивості, наділяючи систему новими перевагами (інтероперабельність, прогностичність, масштабованість) та викликами (кібер-, технологічна та інфраструктурна залежності). Обґрунтована система властивостей доводить, що цифровізація вимагає від держави не лише технічних рішень, а й комплексної трансформації управління (фінансового, правового та організаційного забезпечення).

Зважаючи на нові властивості системи охорони здоров’я, розроблено багаторівневу структуру принципів державного управління цифровою трансформацією системи охорони здоров’я та власне функціонуванням цифрової системи охорони здоров’я. Вона охоплює: 1) стратегічні принципи; 2) організаційні принципи; 3) принципи цифрового функціонування; 4) принципи забезпечення.

Методологію державного управління розвинено шляхом обґрунтування триєдиної структури його об’єкта, що охоплює процеси трансформації, перехідний період та функціонування зрілої цифрової системи. Доведено, що державне управління в цій сфері є не статичним станом, а керованим переходом через синергію правового, організаційного, інформаційного, кадрового та фінансового механізмів. Уточнено зміст мети та завдань управління з урахуванням полісуб’єктності, динамічності й багаторівневості досліджуваного середовища. Визначено ключові вектори розвитку методів реалізації зазначених механізмів для досягнення цілісності та практичної спрямованості управлінського впливу. Запропонований підхід створює методологічну основу для формування та практичного втілення результативних рішень на всіх етапах цифровізації медицини.

Встановлено, що сучасна модель цифрової трансформації охорони здоров’я ґрунтується на людиноцентричному підході, відповідно до якого цифрові технології використовуються не лише для автоматизації окремих процесів, а й для забезпечення доступності, безперервності, якості та персоналізації медичної допомоги. Світовий досвід підтверджує, що успішність цифрових перетворень безпосередньо залежить від рівня розвитку цифрового врядування, наявності інтегрованих інформаційних систем, ефективного управління медичними даними, нормативно-правового забезпечення та розвитку цифрових компетентностей населення і медичних

працівників. Дослідження європейського досвіду засвідчило формування єдиного цифрового простору охорони здоров'я, у межах якого пріоритетного значення набувають інтероперабельність медичних інформаційних систем, розвиток електронних медичних записів, транскордонний обмін медичними даними та використання цифрових сервісів для забезпечення мобільності пацієнтів. Встановлено, що національна система охорони здоров'я демонструє високі темпи цифрової трансформації та поступово інтегрується до європейського цифрового середовища. Узагальнення результатів дослідження дає підстави стверджувати, що подальший розвиток систем охорони здоров'я у світі, країнах Європейського Союзу та Україні буде пов'язаний із поглибленням використання великих масивів медичних даних, технологій штучного інтелекту, телемедицини, персоналізованої медицини та цифрових платформ управління охороною здоров'я. Це обумовлює необхідність удосконалення механізмів публічного управління цифровою трансформацією галузі, посилення захисту медичних даних, забезпечення інтероперабельності цифрових систем та розвитку цифрової компетентності учасників медичних відносин.

Європейський Союз пройшов шлях від фрагментарних ініціатив 1990-х років до цілісного єдиного технологічного простору, побудованого на принципах пацієнтоцентричності. Нормативне ядро цього простору становлять Регламент (ЄС) 2025/327 (EHDS), Регламент (ЄС) 2024/1689 (AI Act), Регламент (ЄС) 2016/679 (GDPR), Регламент (ЄС) 910/2014 (eIDAS), Регламент (ЄС) 2022/868 (Data Governance Act), Регламент (ЄС) 2023/2854 (Data Act), галузеві Регламент (ЄС) 2017/745 (MDR) і Регламент (ЄС) 2017/746 (IVDR), а також Регламент (ЄС) 2022/2065 (DSA) та Регламент (ЄС) 2022/1925 (DMA). Водночас європейська модель має ризики регуляторного перевантаження, алгоритмічної дискримінації та правової невизначеності щодо контролю особи над власними даними.

Аналіз регуляторної бази ЄС свідчить, що безпека цифрової охорони здоров'я забезпечується комплексною системою, яка охоплює вироби, інфраструктуру та процеси. Регламент (ЄС) 2017/745 (MDR), Регламент (ЄС) 2017/746 (IVDR), Директива (ЄС) 2022/2555 (NIS2), Регламент (ЄС) 2019/881 (Cybersecurity Act) та Регламент (ЄС) 2024/2847 (Cyber Resilience Act) доповнюють один одного й охоплюють усі рівні від медичних пристроїв до кіберстійкості самих закладів. Головним бар'єром реалізації цих норм у ЄС виявилася не якість законів, а нестача інституційної та інфраструктурної спроможності.

Дослідження засвідчило, що Бельгія сформувала розгалужену федеральну систему із цифровою платформою eHealth та спеціалізованими механізмами кібербезпеки. Модель Данії вирізняється високим рівнем централізованої координації, розвиненою спільною інфраструктурою та чітким розподілом відповідальності між державою, регіонами й муніципалітетами. Естонія побудувала повністю інтегровану цифрову систему охорони здоров'я на основі єдиного простору медичних даних, державної електронної ідентифікації та комплексного кіберзахисту.

Розроблено механізм адаптації державного управління цифровою трансформацією системи охорони здоров'я до положень регламентів та директив Європейського Союзу, що спрямований на подолання суттєвого розриву між наявною інфраструктурою цифрової системи охорони здоров'я і європейськими нормами та передбачає: 1) впровадження нових нормативно-правових актів (Закону

України «Про захист персональних даних»; Закон України «Про обіг медичних даних», Рамковий Закон України «Про штучний інтелект»; Закон України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації»; Закон України «Про управління даними»; Закон України «Про цифрові послуги»); 2) зміни до законодавчих актів (Закон України «Основи законодавства України про охорону здоров'я»; Закон України «Про захист інформації в інформаційно-комунікаційних системах»; Закон України «Про захист економічної конкуренції»); 3) оновлення підзаконних нормативно-правових актів (Технічних регламентів щодо медичних виробів; Порядків класифікації ШІ-систем і проведення DPIA); 4) вектори трансформації інституційної структури державного управління.

Розроблено структуру державно-регуляторної діяльності щодо використання технологій штучного інтелекту в медицині, що полягають в сукупності змін до нормативно-правових актів, адаптованих до Регламентів Європейського Союзу, та передбачають: правове забезпечення (класифікацію ризиків, сертифікацію, безпеку та якість даних, етичні положення, порядок забезпечення прозорості, постійного моніторингу та людського контролю; встановлення відповідальності користувачів) та інституційне забезпечення (утворення спеціалізованого суб'єкту виконавчої влади, що реалізує державну політику в сфері технологій штучного інтелекту).

Запропоновано комплексний механізм розширення інституційної спроможності державного управління забезпечення безпеки процесів цифрової трансформації, що полягає утворенні спеціалізованих суб'єктів виконавчої влади, що реалізують державну політику в сфері інформаційної безпеки (Національного агентства з доступу до медичних даних (HDAB Ukraine), Національного регулятора у сфері штучного інтелекту, Національного центру кібербезпеки цифрової системи охорони здоров'я), також відповідних спеціалізованих структурних підрозділів у системі органів державного управління та розширення повноважень існуючих суб'єктів у сферах захисту персональних даних, ринкового нагляду за ШІ-медичними виробами та регулювання цифрових ринків;

Одержані результати дослідження розширюють теоретико-методологічне підґрунтя державного управління цифровою трансформацією системи охорони здоров'я та можуть бути використані органами державної влади, закладами охорони здоров'я, а також у подальших наукових дослідженнях проблематики цифровізації медичної галузі.

Ключові слова: державне управління, цифрова трансформація, система охорони здоров'я, цифрове здоров'я, євроінтеграція, кібербезпека, штучний інтелект, електронна система охорони здоров'я, цифрова зрілість, медичні дані.

ABSTRACT

Dmytrenko I.A. Public administration of the digital transformation of the healthcare system. – Qualifying scientific paper. Manuscript.

Dissertation for the degree of Doctor of Science in the specialty 25.00.02 – mechanisms of public administration (field of knowledge "Public Management and Administration"). Zhytomyr Polytechnic State University, Zhytomyr, 2026.

A set of identified factors influences the formation and implementation of public administration decisions in the digital transformation of the healthcare system. Political and

legal factors (legal, political, and European integration) define the characteristics of legitimizing digital practices and harmonizing them with European standards. Resource factors (financial, staffing, infrastructural, and techno-technological) create the material and technological foundation of the reform, ensuring comprehensive achievement of digital transformation goals. Public administration factors (institutional, organizational, and informational) determine controllability, coordination among public administration entities, and the quality of data-driven decision-making. Managing safety and security factors (information security, cybersecurity, and medical security) aims to ensure the viability, protection, and operational continuity of the medical system during crises and threats. The effectiveness of public administration in sector-wide digital transformation depends on the ability of public authorities to foster synergy among these factors.

A bibliometric analysis of publications indexed in the Scopus database for the search query "digital healthcare systems" revealed a rapid increase in scientific interest in digital healthcare systems, particularly after 2020. The main research streams focus on the application of artificial intelligence, machine learning, and big data in medicine; the development of electronic health records and telemedicine; and the provision of data privacy and cybersecurity. The distribution of publications by field of study confirmed the interdisciplinary nature of the field, dominated by computer science, engineering, and medicine. India holds a leading position in publication volume and citations, serving as a central hub for international research collaboration.

The theoretical scientific foundation of public administration has been expanded by refining the content of key concepts and categories, specifically: healthcare system, digital transformation, and digital transformation of the healthcare system.

A comprehensive framework of healthcare system properties has been developed, integrating its basic socio-economic characteristics and development parameters. Digital transformation qualitatively alters these properties, endowing the system with new advantages (interoperability, predictability, and scalability) and introducing challenges (cyber, technological, and infrastructure dependencies). The substantiated system of properties proves that digitalization requires not only technical solutions from the state, but also a comprehensive governance transformation involving financial, legal, and organizational support.

Accounting for the new properties of the healthcare system, a multi-level structure of public administration principles has been developed for both the digital transformation process and the actual operation of the digital healthcare system. It encompasses: Strategic principles; Organizational principles; Digital operational principles; Supporting/enabling principles.

The methodology of public administration has been advanced by substantiating a threefold structure of its object, which covers transformation processes, the transition period, and the functioning of a mature digital system. Public administration in this domain is shown to be a managed transition driven by the synergy of legal, organizational, informational, human resource, and financial mechanisms rather than a static state. The scope of governance goals and objectives has been clarified to reflect the multi-actor, dynamic, and multi-layered nature of the environment. Key vectors for developing methods to implement these mechanisms were identified to achieve cohesive and practical governance impact. This approach establishes a methodological basis for formulating and

executing effective decisions across all stages of healthcare digitalization.

The modern model of digital health transformation relies on a human-centric approach, where digital technologies are used to automate individual processes while delivering accessible, continuous, high-quality, and personalized medical care. Global experience demonstrates that successful digital transformations depend directly on advanced digital governance, integrated information systems, effective health data management, robust legal frameworks, and digital competency among both the public and healthcare professionals. Research into European practices highlights the emergence of a unified digital health area prioritized around health information system interoperability, electronic health record development, cross-border health data exchange, and digital services that support patient mobility. The national healthcare system demonstrates rapid digital transformation progress and is gradually integrating into the European digital space. Generalizing these findings indicates that future healthcare developments globally—including in the EU and Ukraine—will depend heavily on expanding the use of health big data, AI technologies, telemedicine, personalized medicine, and digital management platforms. This underscores the need to refine public management mechanisms, strengthen health data protection, ensure digital system interoperability, and build digital competencies among all healthcare stakeholders.

The European Union has progressed from fragmented initiatives in the 1990s to a unified technological ecosystem built on patient-centric principles. The regulatory core of this ecosystem comprises Regulation (EU) 2025/327 (EHDS), Regulation (EU) 2024/1689 (AI Act), Regulation (EU) 2016/679 (GDPR), Regulation (EU) 910/2014 (eIDAS), Regulation (EU) 2022/868 (Data Governance Act), Regulation (EU) 2023/2854 (Data Act), sector-specific Regulation (EU) 2017/745 (MDR) and Regulation (EU) 2017/46 (IVDR), as well as Regulation (EU) 2022/2065 (DSA) and Regulation (EU) 2022/1925 (DMA). However, the European model faces challenges such as regulatory overload, algorithmic discrimination, and legal uncertainty regarding individual control over personal data.

An analysis of the EU regulatory framework shows that digital health safety is secured through a comprehensive system covering devices, infrastructure, and operational processes. Regulation (EU) 2017/745 (MDR), Regulation (EU) 2017/746 (IVDR), Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2019/881 (Cybersecurity Act), and Regulation (EU) 2024/2847 (Cyber Resilience Act) complement one another to cover levels ranging from medical devices to institutional cyber resilience. The primary bottleneck in implementing these norms across the EU has been a deficit in institutional and infrastructural capacity rather than legislative quality.

The research highlights Belgium's extensive federal system featuring the eHealth digital platform and specialized cybersecurity mechanisms. Denmark's model stands out for its high degree of centralized coordination, mature shared infrastructure, and clear division of responsibilities among national, regional, and municipal levels. Estonia has built a fully integrated digital health system grounded in a unified health data space, national electronic identification (eID), and end-to-end cybersecurity protection.

A mechanism has been designed to align public administration of healthcare digital transformation with EU regulations and directives. Aimed at bridging the gap between current digital health infrastructure and European standards, it includes: 1) Enacting new legislative acts (Draft Laws of Ukraine «On Personal Data Protection», «On Circulation of

Medical Data», Framework Law «On Artificial Intelligence», «On the National Commission for Personal Data Protection and Access to Public Information», «On Data Governance», and «On Digital Services»); 2) Amending existing legislation (Law of Ukraine «Fundamentals of Ukrainian Legislation on Healthcare», «On Information Protection in Information and Communication Systems», and «On Protection of Economic Competition»); 3) Updating secondary regulations (Technical Regulations on Medical Devices; procedures for AI system classification and conducting Data Protection Impact Assessments [DPIA]); 4) Vectors for transforming the institutional structure of public administration. A state-regulatory framework for using AI technologies in medicine has been structured. It comprises a set of legislative amendments harmonized with EU Regulations, encompassing: 1) Legal provision: Risk classification, certification, data safety and quality, ethical standards, transparency enforcement, continuous monitoring, human oversight, and user liability establishment; 2) Institutional provision: Establishing a specialized executive body to implement state policy in artificial intelligence technologies. A comprehensive mechanism to expand the institutional capacity of public administration in securing digital transformation processes has been proposed. It involves creating specialized executive entities responsible for information security policies (such as the Health Data Access Body [HDAB Ukraine], National AI Regulator, and National Center for Digital Healthcare System Cybersecurity), establishing dedicated structural units within public administration bodies, and expanding the mandates of existing authorities regarding personal data protection, market surveillance of AI medical devices, and digital market regulation.

The research findings expand the theoretical and methodological foundations of public administration in healthcare digital transformation and can be applied by government agencies, healthcare facilities, and future academic research into medical sector digitalization.

Keywords: public administration, digital transformation, healthcare system, digital health, European integration, cybersecurity, artificial intelligence, electronic healthcare system, digital maturity, health data.

Формат 60х90/16. Обл.-вид. арк. 1,9
Гарнітура Times.
Видавець і виготовлювач Державний університет «Житомирська політехніка